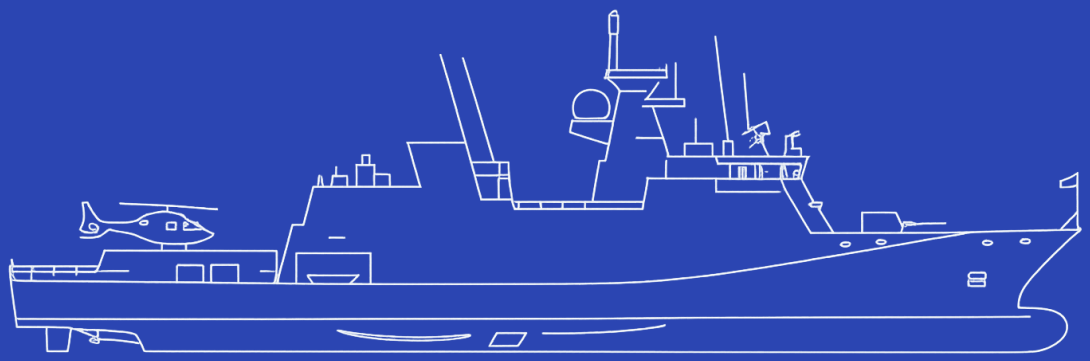
Accelerating Innovation through the Integration of Risk-Based Design and Model-Based Systems Engineering

A Structured and Traceable Approach to Integrating RBD Artefacts within MBSE

C. (Niek) Verhoeven



TU Delft

DAMEN NAVAL

Accelerating Innovation through the Integration of Risk-Based Design and Model-Based Systems Engineering

A Structured and Traceable Approach to Integrating RBD Artefacts within MBSE

Thesis Report

by

C. (Niek) Verhoeven

Performed at

DAMEN Naval

to obtain the degree of Master of Science in Marine Technology in the specialization of Ship Design
at the Delft University of Technology
to be defended publicly on March 20, 2026 at 13:45

This thesis (MT.25/26.020.M) is classified as confidential in accordance with the general conditions for projects performed by the TUDelft.

Thesis exam committee:

Chair/Responsible Professor:	Dr. A.A. Kana
Staff Member:	ir. J.L. Gelling
Company Member:	ir. K. Droste

Company Supervisors:

Responsible Supervisor:	ir. K. Droste
E-mail:	K.Droste@damennaval.com

Author Details

Project Duration:	September, 2025 - March, 2026
Student number:	5479908
Author contact e-mail:	niekverhoeven@live.nl

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

Faculty of Mechanical Engineering · Delft University of Technology

AI Statement:

For this thesis (MT54035) I have used Generative AI to: Obtain inspiration for the overall structure of the report and improve the grammar, style, layout, and spelling for some parts of the text. In all cases I have reviewed and corrected the work and remain fully responsible for the content of the report.

TU Delft Delft University of Technology

Preface

This thesis is the result of the final phase of the MSc programme in Marine Technology at Delft University of Technology. The research was conducted in close collaboration with Damen Naval and focuses on the integration of Risk-Based Design (RBD) into a model-based systems engineering (MBSE) environment for naval ship design.

The motivation for this work originates from the increasing complexity of modern naval systems and the growing reliance on risk-based justification when prescriptive regulations no longer fully cover novel technologies, operational concepts, or system configurations. While MBSE has become an established approach for managing system complexity, risk-related information is still commonly captured in document-based artefacts that are only loosely or not connected at all to a system model. This separation often leads to fragmented traceability, duplication of effort, and challenges in maintaining consistency as designs evolve. The aim of this thesis is to explore how these issues can be addressed by embedding qualitative RBD artefacts directly within an MBSE framework.

The research adopts an exploratory and design-oriented approach. Rather than proposing a fully formalised or quantitative risk analysis method, the focus is on developing and demonstrating a structured model-based representation that supports risk reasoning, traceability, and design decision-making. A representative functional chain is used as a pilot case to investigate how hazards, acceptance criteria, and ALARP considerations can be integrated into system models in a practical and coherent manner.

This thesis is structured in three main phases. The first phase analyses current RBD practices and identifies challenges and limitations related to document-centric workflows. The second phase translates these findings into conceptual and process requirements and implements a model-based prototype using Capella and the Arcadia method. The third phase evaluates the implemented approach against the identified requirements and reflects on its relevance, limitations, and potential for further development.

The work presented in this thesis would not have been possible without the support and guidance of my supervisors and colleagues. I would like to thank my academic supervisors at Delft University of Technology for their constructive feedback and critical questions throughout the research process. I am also grateful to the engineers and specialists at Damen Naval for sharing their experience, insights, and practical perspectives, which were essential in grounding this research in real-world design practice.

Finally, I would like to thank those close to me for their support during this project. Their encouragement and understanding made it possible to complete this work alongside the demands of a technically and intellectually challenging programme.

Niek Verhoeven
Krabbendijke, Monday 9th March, 2026

Abstract

Risk-based design (RBD) has become increasingly important in naval ship design as traditional, prescriptive regulations struggle to keep pace with technological innovation and system complexity. Innovative concepts often fall outside the assumptions embedded in existing rules, requiring designers to justify safety and performance on risk grounds rather than on compliance alone. At the same time, model-based systems engineering (MBSE) is widely used to manage system complexity, yet risk information is still predominantly captured in document-based artefacts that remain weakly connected to system models.

This separation between design models and risk documentation results in fragmented traceability, excessive documentation overhead, and limited reuse of risk knowledge as designs evolve. While previous work has addressed process-level integration between RBD and MBSE, the question of how qualitative RBD artefacts can be meaningfully represented within system models remains largely unresolved.

This thesis proposes a new method that aims to address this challenge. The results show that qualitative RBD artefacts can be embedded as explicit, traceable elements within an MBSE environment by integrating hazards and acceptance criteria directly into functional system models. Using a representative naval bunkering scenario as a pilot case, hazards are linked to functional chains and supported by model-based criteria that underpin ALARP (as low as reasonably possible) decision-making. This enables risks to be evaluated in the context of system behaviour and architectural allocation, rather than as isolated compliance documents.

Compared to traditional document-based RBD workflows, the proposed approach reduces reliance on manual traceability and supports more context-aware risk reasoning in all design phases. These results indicate that combining MBSE and RBD not only mitigates the limitations of prescriptive regulation, but also provides a more robust foundation for informed decision-making in innovation-driven naval ship design.

Contents

Glossary

Model-Based Systems Engineering (MBSE): Extension of the traditional systems engineering by implementing the use of a central model, composed by individual department-specific models, throughout the process, hereby increasing requirements traceability and early validation during the design phase. The constituents of a functioning MBSE include a universal language between models, synchronous access by all stakeholders and a continuously up-to-date source of information [1].

Risk-Based Design (RBD): A design philosophy that integrates risk assessment and management into the engineering process, ensuring that safety and reliability considerations are embedded alongside performance and cost trade-offs a formalized methodology that integrates systematically risk assessment in the design process with prevention/reduction of risk embedded as a design objective, alongside “conventional” design objectives [2].

System: A combination of interacting elements organized to achieve one or more stated purposes [3].

System of Systems (SoS): The system hierarchy used to define higher level systems by combining independent systems into groups. The interaction between the systems often adds a further complexity; specifically, by constraining how the resulting system can be changed or controlled and, therefore, affects the management and control aspects of the systems approach [4].

Systems Architecture (SA): Abstract representation of a system, encompassing its components, relationships, and organizational principles. It serves as a framework to understand, analyze, and communicate the system’s structure, behavior, and evolution across operational, functional, logical, and physical dimensions [5].

Formal Safety Assessment (FSA): A structured five-step methodology established by the IMO for identifying hazards, assessing risk, and evaluating control options to support regulatory decisions [6].

Arcadia Method: A model-based systems engineering methodology developed by Thales, structured into operational, functional, logical, and physical layers to improve traceability and collaboration [7].

Capella: An open-source modeling tool implementing the Arcadia method, used for creating, analyzing, and maintaining consistent system architectures [8].

SysML (Systems Modeling Language): A standardized graphical language used in MBSE to specify and analyze system requirements, structure, and behavior [9].

Probabilistic Risk Assessment (PRA): A quantitative framework for assessing the likelihood and consequences of hazardous events using probabilistic models and data [10].

Fault Tree Analysis (FTA): A deductive, top-down technique that models how combinations of component failures can lead to a predefined system-level hazard [11].

Event Tree Analysis (ETA): An inductive, bottom-up method that maps possible outcomes of an initiating event, accounting for both successful and failed safety responses [12].

ALARP (As Low As Reasonably Practicable): Risk acceptance principle stating that risks must be reduced as far as reasonably possible unless the cost of further reduction is grossly disproportionate to the safety benefits achieved [13].

Goal-Based Standards (GBS): IMO framework defining high-level safety goals rather than prescriptive requirements, enabling justification of innovative designs through risk-based reasoning [14].

Naval Ship Code (ANEP-77): NATO's goal-based safety framework for warships, applying risk-based principles to ensure an equivalent level of safety compared to conventional vessels [15].

1 Introduction

1.1. Problem Context

The increasing complexity of naval ship systems, driven by integrated capabilities, rapid technological advancements, and evolving mission profiles, presents significant challenges for both designers and integrators. Naval vessels are no longer standalone entities but complex systems-of-systems (SoS) requiring holistic coordination across multiple disciplines and stakeholders [16]. At the same time, the introduction of novel technologies increasingly requires explicit safety justification and risk argumentation, which traditionally remain documented in separate risk studies rather than being integrated into the system design itself.

In response to these challenges, the naval industry is transitioning from traditional document-centric approaches toward Model-Based Systems Engineering (MBSE), which enables system modelling across the operational, functional, logical, and physical domains. MBSE is a philosophy that advocates to work with connected models as primary source of information over documents. However, current MBSE practices rarely include explicit representations of risk artefacts such as hazards, event scenarios, or acceptance criteria within the system model itself. It can provides a digital environment for structured design development and supports traceability, early validation, and change impact analysis throughout the design lifecycle [15, 17, 18, 19].

While MBSE supports the consistency and manageability of design data, it often lacks a structured mechanism for integrating risk justifications. This is also the case in innovative or non-standard configurations where regulation is lacking, such as alternative fuel systems or uncrewed platforms. In these cases, Risk-Based Design (RBD) is a proven approach to achieving class approval by providing a structured method to identify, quantify, and manage risks during the design phase. However, applying RBD in practice can be burdensome due to the extensive administrative effort it requires. This is where integration with MBSE could offer a solution: embedding risk reasoning into the system model may reduce documentation workload, improve traceability, and accelerate approval processes. This research therefore explores whether risk artefacts traditionally produced in document-based RBD processes can instead be represented as structured elements within a system model. Rather than adopting a fixed version of RBD from existing literature [12, 14], this project will explore how risk-handling principles can be systematically incorporated into MBSE workflows in a way that suits naval innovation contexts.

Integrating MBSE and RBD into a unified design process offers the potential to accelerate the implementation of innovations by embedding risk logic directly within system models. This approach can shorten approval timelines, improve system transparency, and enhance stakeholder confidence. However, such integration is not yet common practice [9, 20, 21]. Several studies point to the lack of practical frameworks and tooling to support this synergy as will be further elaborated in chapter 3 [1, 22, 23]. The novelty of this research lies in developing a concrete modelling approach that embeds qualitative RBD artefacts—such as hazards, event–consequence reasoning, and performance criteria—directly into the functional architecture of an MBSE environment .

Damen Naval, acting as an original equipment manufacturer (OEM), is positioned to oversee the implementation of such a method. With prior experience in MBSE and experience in applying RBD in programmes like RAMSSES and ASWF superstructure models, Damen Naval is interested in research, development, and validation of a combined MBSE-RBD methodology [24].

This graduation research seeks to address this gap by exploring how MBSE and RBD can be integrated into a coherent design process that supports faster innovation implementation while ensuring system-level safety, traceability, and compliance. Rather than treating risk assessments as external documentation, the proposed approach investigates how hazards, mitigation logic, and acceptance criteria can become first-class elements within the system model itself.

1.2. DAMEN Naval

Damen Naval is part of the Damen Shipyards Group and represents the defense division of the company. Located in Vlissingen, the Netherlands. Damen Naval focuses on the design, construction, and maintenance of naval vessels for both national and international clients [25]. With decades of experience in naval shipbuilding, the company has been responsible for delivering a wide range of vessels, including frigates, patrol vessels, and logistic support ships [26].

The organization works in close collaboration with the Dutch government, NATO partners, and various international stakeholders. Innovation plays a key role in this process: Damen Naval combines traditional shipbuilding expertise with modern technologies such as MBSE and RBD [27].

For the purpose of this research, Damen Naval provides a relevant and challenging research environment. The question of how to accelerate the implementation of innovations is particularly significant in the context of large-scale, complex projects such as naval shipbuilding, where efficiency, reliability, and risk management must be balanced with flexibility and adaptability. This study contributes to improving the transparency and traceability of innovation in naval ship design, thereby supporting safer and more sustainable naval innovation.

1.3. Research Gap

Despite increasing adoption of both MBSE and RBD in the naval sector, these approaches are typically applied separately. MBSE improves traceability, consistency, and early validation in system design, while RBD offers structured reasoning for risk management and certification of innovations. However, there is currently no standardised method that combines these two approaches into a single, integrated design process.

This lack of integration creates a practical barrier. Innovations, particularly those that deviate from existing regulations or involve novel technologies, require both technical validation and risk justification. Without a unified process, risk-related insights remain disconnected from the system model, reducing transparency and slowing down implementation. Furthermore, tooling and process support for integrating RBD into existing MBSE workflows (such as Capella or SysML-based tools) is still limited. As a result, risk reasoning remains largely disconnected from system architecture models, limiting the ability to analyse risk in the context of functional interactions and design dependencies.

At the same time, stakeholders such as classification societies, clients, and suppliers increasingly expect system-level justification for innovation, especially in complex systems-of-systems. For OEMs like Damen Naval, this creates a strategic need for a design process that supports early, model-based integration of risk and safety information.

The introduction of innovative technologies in naval ship design depends on the ability to manage complexity, uncertainty, and regulatory compliance in an integrated manner. Two methodological frameworks play a role in this process: MBSE and RBD. Both aim to improve the quality, traceability, and justification of engineering decisions, yet they approach this goal from distinct perspectives. MBSE provides the structural and organizational backbone for managing system complexity through model-centric information management, while RBD establishes the analytical and regulatory mechanisms that enable safe innovation beyond prescriptive rules.

1.4. Research Objective

The objective of this research is to develop and evaluate a combined MBSE-RBD methodology that enables faster implementation of innovations in naval ship design. This method should support system-level risk reasoning inside the MBSE framework and allow for early-stage verification of both performance and risk. The method will be evaluated using a representative test-case on Methanol bunkering within an naval vessel

design. This case focuses on the integration of hazards and performance criteria into the system model, allowing the proposed approach to be assessed in a realistic shipbuilding context. By modelling these risk artefacts alongside functional behaviour and architectural allocation, the study evaluates whether risk reasoning can be performed directly within the design model rather than through separate documentation.

1.4.1. Main Question

The Objective leads to the following research question:

Research Question

To what extent can the RBD process be combined with MBSE practices to reduce the effort of getting class approval for novel innovations?

1.4.2. Subquestions

For answering the research question, the following subquestions are asked:

Research Question 1

What are the key principles and methods of MBSE and RBD relevant for innovation? *(Chapter 2)*

Research Question 2

What are the current challenges in applying MBSE and RBD for innovative naval systems? *(Chapter 3)*

Research Question 3

How can the artefacts and reasoning of RBD be represented within a MBSE framework to improve traceability and reduce administrative workload in naval ship design? *(Chapter 4)*

Research Question 4

How can this combined MBSE-RBD approach be implemented and tested using a representative design case? *(Chapter 5 & 6)*

Research Question 5

How does the integrated method perform in terms of approval efficiency, traceability, and design clarity compared to traditional approaches? *(Chapter 7)*

2

Background and key concepts of MBSE and RBD

This chapter addresses Research Question 1: What are the key principles and methods of MBSE and RBD relevant for innovation?

Therefore, it outlines the theoretical foundation for both MBSE and RBD and examines how they contribute to innovation in the maritime domain. Section 2.1 introduces the principles and methods of MBSE, focusing on its role in improving design consistency, stakeholder communication, and lifecycle traceability through methods such as Arcadia and its supporting tool Capella. Section 2.2 then discusses the principles and methods of RBD, including Formal Safety Assessment, Probabilistic Risk Assessment, and the regulatory frameworks that allow risk-based justification of novel designs, such as the IMO guidelines and the Naval Ship Code (NSC). Together, these sections provide the background needed to understand how both approaches can be combined to create a model-based, risk-informed design environment. The chapter concludes by identifying key complementarities between MBSE and RBD that form the basis for the integration challenges discussed in Chapter 3.

2.1. Principles and methods of Model Based Systems Engineering

The increasing complexity of modern engineering projects has exposed the limitations of traditional document-based systems engineering. As projects grow larger and more interdisciplinary, maintaining consistency between requirements, design documents, and analyses becomes increasingly difficult. To address these challenges, MBSE was introduced as a way to centralize and structure system information through a shared model-based environment. MBSE is an evolution of traditional systems engineering that shifts the focus from document-centric approaches to model-centric practices. Instead of managing large sets of static documents, MBSE organizes and integrates system information into a central, digital model. This approach provides a single source of truth that can be accessed and updated by stakeholders throughout the system lifecycle [17, 19].

2.1.1. Principles of MBSE

The core ideas of MBSE come from the need to improve traditional, document-based systems engineering. These principles describe how information is structured, shared, and kept up to date during the system lifecycle. They help engineers work in a consistent way and make collaboration between disciplines easier. Understanding these principles is important because they form the basis for the methods and tools used in MBSE.

Centralized System Model

A central principle of MBSE is the use of an integrated system model in which all system-related information is consolidated. This includes requirements, functions, logical structures, and physical components (see figure 2.1). By unifying these elements in a single, consistent representation, MBSE provides a central source of truth that can be accessed and updated by all stakeholders. This approach reduces redundancy in documentation, makes relationships between design decisions explicit, and enhances the traceability of requirements across the entire design chain. Furthermore, the model can be used to validate concepts at an early stage and to detect inconsistencies in the system architecture [18, 19].

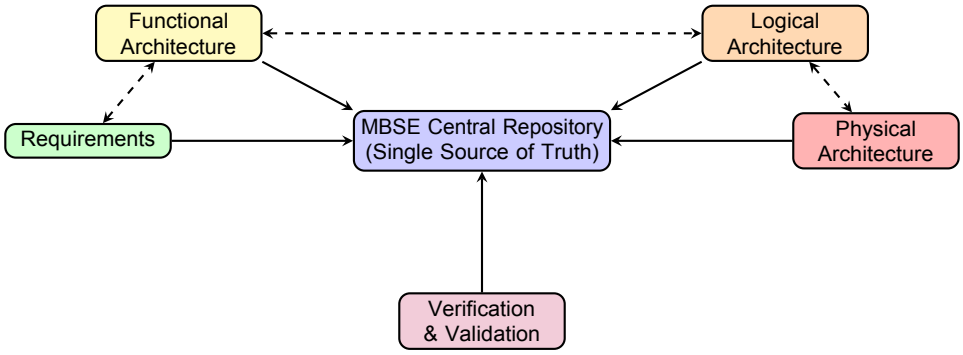


Figure 2.1: Schematic representation of MBSE: domains connected through a central model repository.

Multi-domain Integration
A second principle is the integration of multiple engineering domains within one modeling environment. Complex systems, such as naval vessels, combine contributions from among others mechanical, electrical, software, and operational disciplines. MBSE enables these disciplines to be connected in a shared system model, thereby supporting trade-offs at the system level. This integration improves cross-domain consistency and allows for holistic analyses and verification. As a result, MBSE supports not only technical coherence but also the coordination between diverse stakeholders involved in the development process [15, 28].

Lifecycle Support
Another principle of MBSE is its ability to support the entire system lifecycle. The system model evolves from the earliest conceptual design phase, through detailed design and implementation, to operational use and eventual decommissioning. By maintaining continuity across these stages, MBSE ensures that design decisions, risks, and changes are consistently documented and traceable. This lifecycle perspective prevents the loss of critical information during transitions between phases or between organizations involved in the system's life [1]. Such continuity is particularly important in naval shipbuilding, where vessels remain in service for decades .

Stakeholder Communication
Finally, MBSE explicitly enhances communication between stakeholders. The use of model-based representations and architecture diagrams makes complex systems more transparent to diverse audiences, ranging from engineers and project managers to clients and regulatory authorities. These visualizations bridge the gap between technical experts and non-technical decision-makers, fostering shared understanding and broader acceptance of design choices. In this way, MBSE functions not only as a technical tool but also as a communication medium within multidisciplinary and international project teams [7, 28].

2.1.2. Methods of MBSE
While the principles of MBSE describe the underlying philosophy of model-centric engineering, its practical implementation relies on specific methods, tools, and modeling languages. These methods provide the structure through which system requirements, architectures, and analyses are captured and maintained in a consistent and traceable manner. Over the past two decades, several MBSE methodologies and modeling approaches have emerged as the most influential in both research and industry practice. In the maritime domain, these approaches such as SysML, Arcadia/Capella, COMET, Dassault 3D experience, digital twin integration, and information traceability provide a structured way to manage complex ship design processes [7, 29, 30, 31].

SysML (Systems Modeling Language)
One of the most widely adopted modeling languages used in MBSE is the Systems Modeling Language (SysML). SysML provides a standardized way to represent different aspects of a system, including requirements, behaviors, structures, and parametric relations. Its broad adoption across industry and academia makes it a de facto modeling language for systems engineering, facilitating interoperability between organizations and toolchains. By capturing system requirements alongside structural and behavioral models,

SysML helps to maintain consistency and provides engineers with the ability to analyze design alternatives within a unified modeling environment [9]. The next version, SysML v2, officially approved by the OMG in 2025, addresses limitations of the original language such as interoperability and formal semantics [32].

Arcadia method

The Arcadia method is a MBSE method developed by a Thales led consortium to address the challenges of designing and managing large-scale, complex systems [7]. Arcadia is structured around a layered framework that refines system concepts from abstract needs to concrete solutions while maintaining traceability across abstraction levels (see figure 2.2.) It distinguishes four principal layers:

1. *Operational Analysis*: Captures stakeholder needs and the system's operational context;
2. *Functional & Non functional Need*: Defines the system's functional expectations and boundaries;
3. *Logical Architecture*: Here the system is decomposed into logical components and their interactions;
4. *Physical Architecture*: Maps the design onto technical subsystems and components.

This layered method ensures separation of concerns, supports validation at each level, and enables communication between disciplines. Arcadia has been applied in large engineering projects, including naval shipbuilding, where such structuring is essential to manage multidisciplinary complexity [7, 16, 17, 33]. Although Arcadia has proven effective in improving communication and traceability across disciplines, its application in early design stages can be limited by the effort required to build and maintain consistent models. Moreover, the integration between Arcadia and quantitative analysis tools such as reliability or cost models remains an ongoing challenge, particularly in domains like naval shipbuilding where risk-based decision-making is central [16].

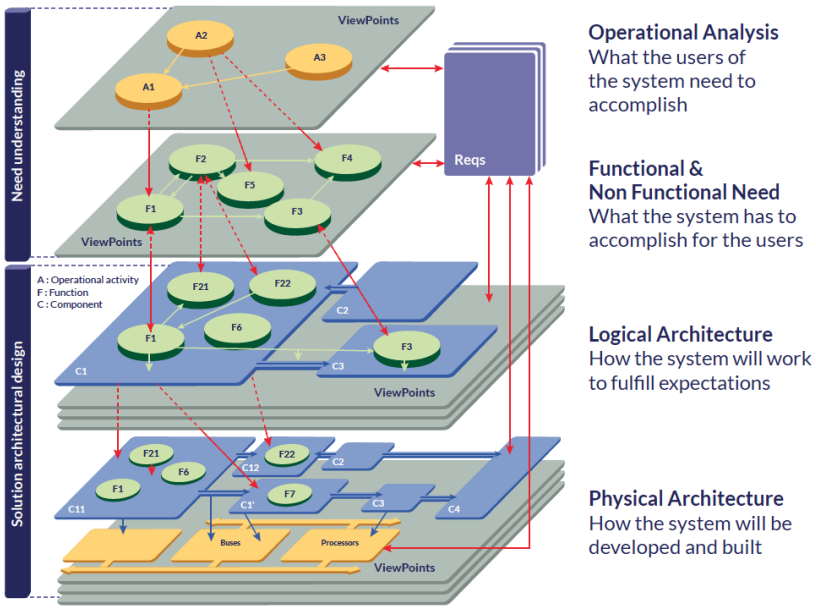


Figure 2.2: Arcadia method layers overview [34].

Capella tool

Capella is the open-source modeling tool designed to implement the Arcadia method. Originally developed by Thales and later released as an Eclipse project. Capella provides engineers with a practical environment to build and maintain Arcadia-compliant models. Unlike general-purpose SysML tools, Capella is closely aligned with Arcadia's methodological principles, which makes it effective in large-scale, safety-critical domains such as aerospace and naval shipbuilding [34, 35].

Capella supports the three pillars of MBSE: *language*, *method*, and *tool*. Figure 2.3 illustrates the relationship between the Arcadia method, the Capella tool, and NAFv4 language. Arcadia defines the

methodological framework that structures the MBSE process, while Capella implements this method as a modeling environment. NAFv4 language can be integrated to align architectural views with defence and naval standards. This combination enables the application of Arcadia within the maritime domain, ensuring both methodological rigor and domain relevance.

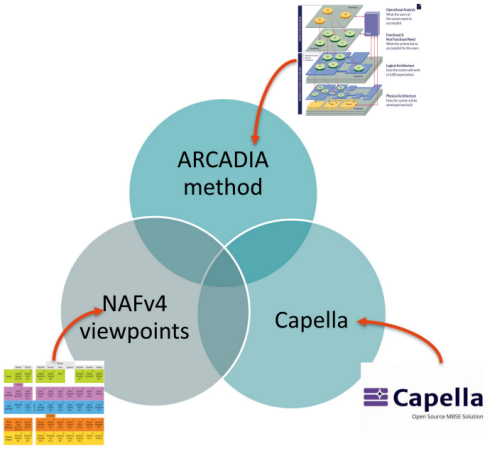


Figure 2.3: Relationship between the Arcadia method, the Capella tool, and NAFv4 Language.

A key feature of Capella is its layered modeling environment, which mirrors Arcadia's four abstraction levels. Figure 2.4 illustrates how system models are refined from 'Operational Analysis' to 'System Analysis', 'Logical Architecture', and 'Physical Architecture'. At each layer, Capella provides viewpoints for capturing requirements, defining capabilities, allocating functions, modeling structures, and specifying data and interfaces. Automatic traceability between these viewpoints ensures that design changes propagate across all layers, enabling systematic impact analysis and validation against stakeholder expectations.

Arcadia layer	Requirements	Capability	Capability description	Functional	Structure	Modes and States	Data	Interfaces
	R-OA	OA1	OA2	OA3	OA4	M&S-OA5	D-OA6	I-OA7
Operational Analysis	Capture stakeholder requirements	Define Operational Capabilities	Define processes and scenarios	Define Operational Activities and interactions	Capture Operational Entities and Actors. Allocate Operational Activities to Operational Actors, Entities	Define operational modes and states	Define operational data model	Define interfaces and describe interfaces scenarios
	R-SA	SA1	SA2	SA3	SA4	M&S-SA5	D-SA6	I-SA7
System Analysis	Derive Stakeholder requirements and capture System requirements	Define System Missions and System Capabilities	Define Functional Chains and Scenarios.	Define System Functions. Define Functional Exchanges and components	Allocate System Functions to System and Actors	Define system modes and states	Define system data model	Define interfaces and describe interfaces scenarios Enrich Logical Scenarios.
	R-LA	LA1	LA2	LA3	LA4	M&S-LA5	D-LA6	I-LA7
Logical Architecture	Derive system requirements and Capture components requirements	Transition Capabilities Realization from system layer	Define Functional Chains and scenarios	Derive System Functions and define Logical Functions. Define Functional Exchanges and components.	Allocate Logical Functions to Logical Components	Define logical components modes and states	Define logical data model	Delegate System Interfaces and create Logical Interfaces. Enrich Logical Scenarios.
	R-PA	PA1	PA2	PA3	PA4	M&S-PA5	D-PA6	I-PA7
Physical Architecture	Derive logical requirements and capture physical requirements	Transition Capabilities Realization from logical layer	Define Functional Chains, Scenarios, and Physical Path	Derive Logical Functions and define Physical Functions. Define Functional Exchanges and components.	Define Physical Nodes and refine Behavioural Physical Components. Allocate Behavioural Components.	Define physical nodes modes and states	Define physical data model	Delegate Logical Interfaces and create Physical Interface. Enrich Physical Scenarios.

Figure 2.4: MBSE with Arcadia method step-by-step [34].

Add-ins

In addition to its core capabilities, Capella supports extensions and plug-ins that integrate safety and dependability analyses directly into MBSE workflows. Examples include ATICA4Capella, which enables

functional hazard analysis, fault tree analysis, and Failure Mode, Effects, and Criticality Analysis (FMECA), and Reliability, Availability, Maintainability, Safety (RAMS) extensions for reliability and availability modeling [8, 36]. However, these add-ins are often loosely coupled and not fully embedded within the system architecture model. This limited integration highlights an opportunity to further align dependability analysis with model-based design.

Current Extensions of Capella for Safety and Risk Analysis

To understand the current state of integrating risk and dependability analyses within MBSE, several studies have explored extensions of the Capella tool. These examples illustrate both the potential and current limitations of linking model-based design with risk-based reasoning. Several studies have demonstrated how Capella can be extended beyond architecture modeling to support safety and dependability analyses. An example is the proof-of-concept by Bitetti et al. [8], who applied Capella to perform RAMS analyses in the satellite domain. In their approach, dependability attributes such as failure rates, duty cycles, and redundancy schemes were embedded directly into Arcadia system models. These data were then exported to an external reliability tool (Excel), which automatically generated artefacts such as Failure Mode and Effects Analysis (FMEA), fault trees, and reliability block diagrams. The case study on a Telemetry, Tracking, and Command (TT&C) subsystem illustrated how architectural choices on redundancy directly influenced reliability indicators, enabling early trade-offs between mass, cost, and system reliability.

This model-based coupling reduces the separation between system engineers and RAMS specialists, illustrating how MBSE can function as a shared reference for design and assurance activities. At the same time, the study also revealed limitations: the integration remained partial, since reliability calculations were still performed externally; exported artefacts often required post-processing for readability; and the quality of the analyses continued to depend on manual input of reliability data. Moreover, RAMS viewpoints frequently require a different level of detail than architecture models, which may create tensions in model scope and complexity.

Comparable initiatives have been reported in other domains. Héroux Devtek Spain (CESA) and ANZEN Engineering applied Capella to an electromechanical actuation system in the aviation sector, comparing it with Cameo System Modeler and Matlab System Composer. Their evaluation concluded that Capella's layered Arcadia method, combined with the ATICA4Capella safety extension, provided strong support for functional hazard analysis, fault tree analysis, and FMECA directly within the system model [36]. Requirements management was integrated through IBM DOORS, and interoperability with Simulink enabled early-stage design validation. Nevertheless, the authors note that embedding safety models into MBSE workflows requires considerable integration effort and user expertise.

Similar observations have been made in robotics, where Yakymets et al. demonstrated the coupling of Papyrus/RobotML models with dedicated safety tools such as Sophia and Safety Architect to automatically generate hazard analyses, FMEAs, and fault trees for humanoid personal care robots [37]. Their platform demonstrates the feasibility of Model-Based Safety Assessment (MBSA) when aligned with MBSE, but also exposes challenges in data propagation, semantic consistency between tools, and the need for specialized safety extensions to capture risk information within system models.

Taken together, these studies confirm that Arcadia and Capella can be effectively extended to support safety and risk analyses and even enable early-stage trade-offs between dependability, performance, and cost. However, they also demonstrate that such integration remains partial and tool-dependent. While safety artefacts can be generated from MBSE models, full methodological integration where risk reasoning is treated as an integral part of the system model remains an open challenge.

Reliability viewpoint in Capella

To strengthen the integration of dependability analyses into MBSE, Bitetti et al. introduced a dedicated reliability viewpoint within Capella [38]. This viewpoint enriches Arcadia models with attributes that capture reliability-relevant information, including component duty cycles, failure rates (FIT values), redundancy schemes (hot, warm, or cold standby), and the number of parallel units available. By embedding these attributes directly in the system architecture, the viewpoint enables reliability assessments to be generated alongside traditional functional and physical descriptions.

The reliability viewpoint allows system engineers to export structured reliability data from Capella into external tools for further analysis. For example, FMEA's, Fault Tree Analyses (FTA), and Reliability

Block Diagrams (RBDs) can be generated automatically based on the enriched architecture model. This approach reduces duplication between engineering and RAMS workflows and ensures that dependability considerations evolve consistently with system design.

The proof-of-concept developed by Bitetti et al.[8] was applied to satellite subsystems such as the Electrical Power Subsystem (EPS) and TT&C subsystem. In these cases, engineers were able to compare alternative configurations by quantifying how redundancy strategies affected reliability outcomes. This demonstrates how a model-based reliability viewpoint can shift RAMS from a downstream verification activity to an integral part of early-stage architectural trade-offs.

Capella Challenges
Despite these advantages, Capella is not without challenges. Studies have reported a steep learning curve for new users, as well as significant effort required to integrate Capella with other engineering environments such as Simulink or DOORS [36]. Moreover, while safety extensions exist, their integration remains partial and often tool-dependent, meaning that risk reasoning is still not embedded as a native element within the system model.

Digital Twins and Simulation Integration
MBSE methods are increasingly combined with digital twin concepts and simulation environments. By linking system models with simulations and operational data, engineers can validate designs at an earlier stage and predict performance under varying conditions. This integration not only accelerates the identification of potential design flaws but also supports iterative design refinement. In naval applications, digital twins derived from MBSE models are particularly useful for testing innovative technologies that lack prescriptive regulatory frameworks, enabling early experimentation and risk evaluation in a controlled environment [15].

Information Traceability
Finally, MBSE methods place a strong emphasis on information traceability. Within model repositories, explicit links are created between requirements, functions, design elements, and verification activities. This web of traceability allows engineers to perform change impact analysis, ensuring that the consequences of design modifications are fully understood across the system. Moreover, traceability supports compliance verification by demonstrating how high-level requirements are satisfied at lower levels of the system hierarchy. Without such links, complex projects risk inconsistencies and gaps in the design rationale. In practice, however, many organizations still struggle to implement traceability effectively, which highlights the ongoing need for methodological improvement [20].

Summary
MBSE has emerged as a structured approach to manage the growing complexity of modern engineering systems. By replacing document-based practices with model-centric ones, MBSE provides a single source of truth that integrates requirements, functions, architectures, and verification throughout the system lifecycle. Its principles (centralized modeling, multi-domain integration, and lifecycle traceability) enable collaborative and transparent system development.

The Arcadia method operationalizes these principles through a layered framework that refines operational needs into physical solutions. Its supporting tool, Capella, is widely used in industry to manage architectures across abstraction levels. Extensions such as ATICA4Capella show how safety and reliability analyses can be embedded in model-based workflows, although integration with the architecture model remains partial.

In maritime design, these capabilities are increasingly valuable for managing interdisciplinarity and regulatory complexity. Coupling MBSE with digital twins and traceability mechanisms allows earlier validation and systematic change management yet the full integration of risk and safety reasoning remains a challenge.

2.2. Principles and methods of Risk-Based Design

RBD is an approach to ship design that explicitly incorporates risk assessment and management into the design process. Rather than solely relying on prescriptive regulations, RBD allows designers to justify novel or unconventional solutions by systematically identifying, evaluating, and mitigating risks. This is particularly relevant in innovative contexts, where existing rules may not yet provide adequate guidance [2, 14].

2.2.1. Principles of RBD

RBD is founded on a set of principles that distinguish it from prescriptive, rule-based design approaches. Instead of relying solely on fixed standards, RBD emphasizes explicit risk reasoning throughout the design process. These principles ensure that safety and reliability considerations are systematically embedded into engineering practice and remain connected to performance and cost trade-offs.

Figure 2.15 summarizes the main logic of the RBD process as implemented in Damen Naval. Rather than prescribing fixed rules, RBD iteratively evaluates design alternatives through probabilistic risk assessments and performance trade-offs, ensuring that safety considerations are embedded throughout the design lifecycle.

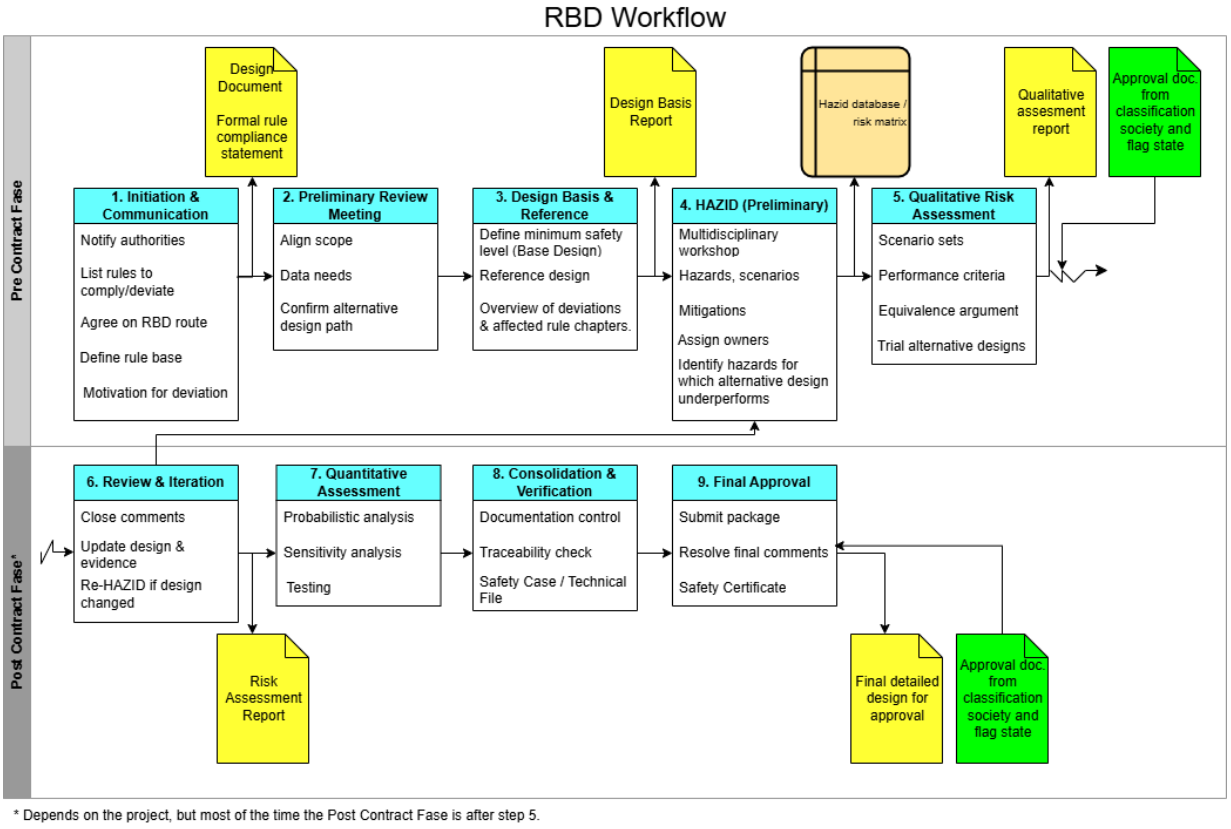


Figure 2.5: Flowchart of the RBD process.

Risk Identification and Assessment

A principle of RBD is the early identification and assessment of risks. Hazards and failure modes must be recognized as soon as possible in the design process to avoid costly redesign later. Risks are quantified using probabilistic models, simulations, or expert judgement, and their potential consequences for safety, operability, and the environment are systematically assessed [2]. This early focus on hazards ensures that risk awareness becomes a driver of design choices rather than an afterthought.

Integration with Design Decisions

RBD differs from traditional safety processes by embedding risk directly into design decision-making. Instead of treating safety and reliability as external verifications, RBD integrates them into trade-off analyses where performance, cost, and safety are considered simultaneously. In this way, design solutions are justified not only on technical and economic grounds but also on their ability to mitigate risks to acceptable levels [39].

Compliance through Justification

A central feature of RBD is that compliance is demonstrated through risk justification rather than strict adherence to prescriptive rules. While conventional designs secure approval by meeting existing regulations,

RBD provides flexibility by showing that risks have been systematically identified, managed, and reduced to a tolerable level. This approach is particularly important for the introduction of novel technologies where prescriptive standards may not yet exist [13, 14].

Iterative Lifecycle Process
Finally, RBD is inherently iterative. Risk assessment is not a one-off activity at the start of a project but continues throughout the design lifecycle. As the design matures, new data and operational insights are incorporated into updated risk assessments, ensuring that safety justifications remain valid. This iterative character supports adaptive learning and continuous refinement of both technical solutions and their associated risk management strategies [39].

2.2.2. Methods of RBD

To operationalize its principles, RBD relies on a number of established methods and frameworks that embed risk reasoning into maritime engineering practice. These methods provide the structured processes, quantitative tools, and acceptance criteria needed to justify innovative designs in the absence of fully prescriptive rules. RBD asks four fundamental questions:

1. What can go wrong? (hazard identification)
2. How likely is it to happen, and with what consequences? (risk assessment)
3. What options exist to reduce or control these risks? (risk control options)
4. Are these options justified in terms of cost and benefit, and do they lead to an acceptable level of safety? (cost/benefit assessment and decision-making)

These steps are structured in the Formal Safety Assessment (FSA) framework developed by the International Maritime Organization (IMO), which is widely applied as the methodological backbone of RBD. The FSA process is shown in Figure 2.6, illustrating how hazards are systematically identified, analyzed, mitigated, and justified before recommendations are presented to decision-makers [40].

Formal Safety Assessment
A cornerstone of RBD in the maritime domain is the FSA, a structured framework developed by the IMO to support safety-related decision-making [6]. FSA was introduced in the 1990s as a systematic alternative to prescriptive regulations, enabling designers and regulators to evaluate novel solutions in terms of their actual risk contribution. It provides a transparent process for identifying hazards, quantifying risks, evaluating control measures, and justifying decisions based on both safety and cost-effectiveness.

The FSA methodology is structured into five sequential steps, as illustrated in Figure 2.6 [6]:

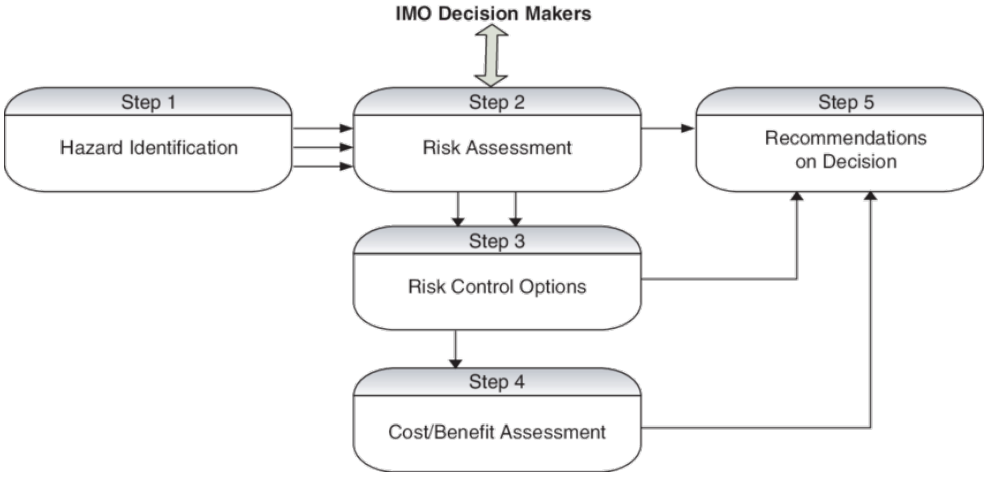


Figure 2.6: FSA process as defined by the IMO [6].

1. **Hazard Identification (Step 1):** The process begins with a comprehensive survey of potential hazards relevant to the vessel or system under design. Techniques such as Hazard and Operability

Studies (HAZOP), FMEA's, and brainstorming workshops are commonly used at this stage. The goal is to ensure that no credible accident scenarios are overlooked.

2. **Risk Assessment (Step 2):** For each identified hazard, the associated risk is assessed by combining the probability of occurrence with the severity of its consequences. Probabilistic Risk Assessment (PRA) methods, such as FTA and Event Tree Analysis (ETA), are typically applied. This step provides a quantitative or semi-quantitative estimate of risk levels, which forms the evidence base for subsequent decision-making.
3. **Risk Control Options (Step 3):** Once risks are evaluated, potential control measures are developed and compared. These may include design modifications, operational procedures, or additional safety systems. The emphasis is on exploring alternatives that either reduce the probability of failure or mitigate its consequences, ensuring a systematic search for effective solutions.
4. **Cost–Benefit Assessment (Step 4):** Control options are subjected to an economic evaluation to determine whether the expected safety benefits outweigh the costs. This step embodies the ALARP principle ("As Low As Reasonably Practicable"), ensuring that risks are reduced as far as possible unless the required mitigation is grossly disproportionate to the benefit gained [13].
5. **Recommendations for Decision (Step 5):** Finally, the results of the analysis are consolidated into recommendations for decision-makers, typically IMO committees or flag state authorities. At this stage, the trade-offs between safety, operability, innovation, and cost are made explicit, providing a transparent justification for regulatory approval.

Since its adoption, FSA has become the methodological backbone of risk-based regulatory frameworks, particularly for alternative design and arrangements in SOLAS (see Section 2.2.2). Its systematic nature ensures that safety justifications are evidence-based and transparent, rather than relying solely on prescriptive rule compliance [41].

Recent research has extended the FSA framework to address its limitations. One challenge is that early design phases often suffer from incomplete data and heavy reliance on expert judgement. To address this, fuzzy logic has been integrated with FSA, creating the so-called Fuzzy Formal Safety Assessment (FFSA). This approach uses fuzzy set theory and linguistic variables to capture uncertainty and subjectivity in expert evaluations, translating qualitative assessments (e.g., "high risk", "moderate likelihood") into quantifiable risk measures. Huang et al. [40] demonstrate the application of FFSA to China's maritime passages, showing that the approach can improve decision-making in contexts where quantitative data are scarce or uncertain. Such extensions illustrate how FSA continues to evolve as a practical decision-support framework within RBD.

Probabilistic Risk Assessment

PRA provides the quantitative foundation for evaluating risks within RBD, particularly during Step 2 of the FSA process (see Figure 2.6). Whereas hazard identification generates a comprehensive list of potential failure scenarios, PRA evaluates their likelihood of occurrence and quantifies the associated consequences. By doing so, PRA moves beyond qualitative judgement and establishes a numerical risk profile that can be compared across design options.

At its core, PRA is based on the definition of risk as:

$$\text{Risk} = \text{Probability of Failure} \times \text{Consequence}.$$

This expression highlights the dual nature of risk: even a low-probability event may warrant design modifications if the associated consequences are catastrophic. PRA methods therefore provide a structured way of combining probability theory with engineering judgement to support decision-making [2].

A range of analytical tools are commonly employed in PRA:

- **FTA:** A top-down method that models the logical relationships leading to a system failure. See figure 2.7 for an example. FTA is widely used for identifying combinations of component failures that may cause hazardous events.

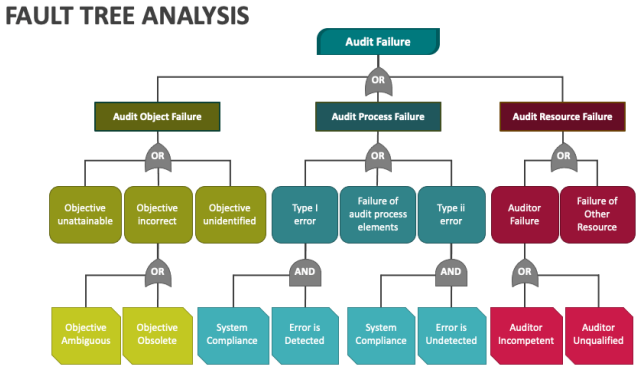


Figure 2.7: FTA analysis [11].

- **ETA:** A complementary, bottom-up technique that maps out the possible outcomes of an initiating event, such as a fire or flooding incident, capturing both success and failure paths of safety systems.
- **Monte Carlo Simulation:** A computational technique that repeatedly samples probabilistic input distributions to evaluate the range and likelihood of system performance outcomes. This is particularly useful when uncertainties are high or when input data are incomplete.

As illustrated in Figure 2.7, these analytical tools together provide a systematic way to identify and quantify failure scenarios within the probabilistic risk assessment process.

In addition to these techniques, PRA is often supported by structural reliability theory, as emphasized in recent research [42]. In this context, the probability of failure is defined using a *limit state function* $g(X)$, where X represents a vector of uncertain input parameters (such as loads, material properties, or environmental conditions). Failure is said to occur when $g(X) \leq 0$. Methods such as the First-Order Reliability Method (FORM) and Second-Order Reliability Method (SORM) provide ways of estimating these failure probabilities without resorting to exhaustive simulation.

PRA thus provides RBD with a quantitative backbone that complements the structured process of FSA. It ensures that design alternatives can be compared not only on qualitative grounds but also on the basis of numerical risk indicators. In naval ship design, PRA has been applied to scenarios such as progressive flooding, fire safety, and structural reliability of lightweight materials [2]. These applications demonstrate its ability to guide innovative design choices by quantifying both the likelihood and the impact of hazardous events.

Qualitative and quantitative techniques in RBD

FSA and PRA rely on a wide spectrum of supporting techniques that vary in scope, level of detail, and degree of quantification. These techniques provide the building blocks for systematic hazard identification and risk evaluation in maritime design [13, 43].

At the qualitative end of the spectrum, methods such as Hazard Identification (HAZID), HAZOP, and FMEA's are used to identify potential hazards, failure modes, and operability issues at an early stage. These approaches are effective in capturing expert knowledge and generating comprehensive lists of possible accident scenarios, but they do not provide numerical estimates of probability or consequence. Their value lies in ensuring completeness during Step 1 of the FSA process [12, 44].

Semi-quantitative techniques bridge the gap between qualitative brainstorming and fully probabilistic models. FTA and ETA model logical relationships between failures and outcomes [10]. FTA follows a top-down approach, decomposing an undesired top event into combinations of lower-level failures, while ETA starts from an initiating event and maps possible success and failure paths of safety systems. These methods provide structured, scenario-based models that can be populated with probabilities when data are available, but also remain useful in qualitative form when data are scarce.

At the quantitative end, full PRA combines these techniques with probabilistic input data and computational tools, such as Monte Carlo simulation or structural reliability methods, to calculate failure probabilities and

associated consequences. PRA thus represents the most rigorous form of risk evaluation, but it depends heavily on the availability of reliable statistical data [15, 45]. This forms a recurring challenge in maritime innovation.

In practice, effective risk-based design relies on the combined application of these methods: qualitative techniques to ensure scenario completeness, semi-quantitative techniques to structure causal logic, and quantitative techniques to provide numerical estimates for decision-making. The integration of these approaches ensures that RBD captures both expert judgement and probabilistic evidence, thereby strengthening the justification of innovative designs.

Risk Acceptance Criteria

Defining clear criteria for what constitutes an acceptable level of risk lies at the heart of RBD. Without such criteria, the results of hazard identification and PRA remain descriptive rather than actionable. Risk acceptance criteria provide the benchmark against which design alternatives are judged, and thus form the basis for regulatory approval in a risk-based framework. This stage corresponds to Step 4 of the FSA process (see Figure 2.6).

The most widely applied concept in maritime RBD is the ALARP principle. According to ALARP, risks must be reduced as far as reasonably possible, unless further reduction would require costs or sacrifices that are grossly disproportionate to the safety benefits achieved [13]. This principle ensures that designers actively search for improvements rather than settling for the minimum acceptable standard, while at the same time recognizing the economic constraints of shipbuilding. Figure 2.8 shows the ALARP-region: as far as possible to the bottom-left corner.

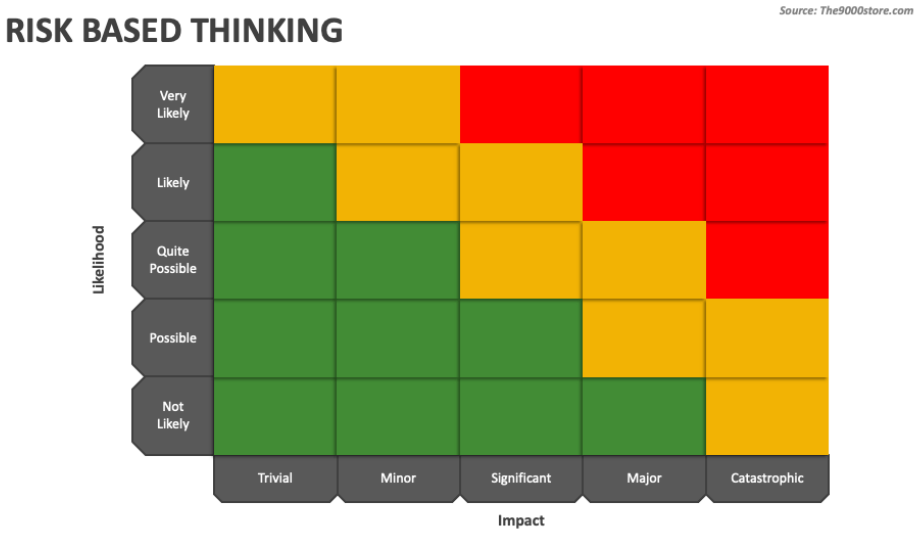


Figure 2.8: Risk definition matrix [11].

Beyond ALARP, additional frameworks have been developed to structure acceptance criteria. Goal-Based Standards (GBS), introduced by the IMO, define high-level safety objectives rather than detailed prescriptive requirements. Under GBS, it is up to the designer to demonstrate through risk analysis that these goals are achieved [14]. A related concept is the Safety Level Approach (SLA), which seeks to establish target failure probabilities or risk levels for specific functions, such as watertight integrity or fire protection [2]. These quantitative thresholds provide greater transparency and comparability across different designs.

In practice, risk acceptance criteria often involve a combination of qualitative categories and quantitative thresholds. For example, risks may be classified into three regions:

1. *Unacceptable risks*: Must be mitigated regardless of cost.
2. *Tolerable risks within the ALARP region*: Further reduction should be pursued unless costs are disproportionate

3. *Broadly acceptable risks:* No further action is required.

This approach provides a balanced framework for decision-making, ensuring that innovative designs can be justified while maintaining a demonstrably safe standard of operation.

By defining explicit acceptance benchmarks, RBD ensures that the risk analysis process does not remain an academic exercise but instead directly informs design decisions. For naval ship design, where innovative technologies often lack prescriptive rules, such criteria provide the foundation for regulatory approval and stakeholder confidence.

IMO Guidelines for Alternative Design and Arrangements

The IMO has formalized the application of RBD through a series of guidelines on alternative design and arrangements. These guidelines allow ship designers to deviate from prescriptive requirements in conventions such as SOLAS, provided that they can demonstrate (using structured risk analysis) that the alternative achieves an equivalent or superior level of safety. This regulatory framework enables innovative solutions to be introduced while maintaining required safety levels, forming an important foundation for risk-based approaches in naval architecture.

The foundational document is MSC/Circ.1002 (2001), which established guidelines for alternative designs in fire safety systems [46]. This circular defined the principle that equivalence can be demonstrated through engineering analysis, supported by quantitative risk assessment and cost–benefit studies. It emphasized that alternative arrangements must follow a transparent process, including documentation of hazard identification, risk analysis, and justification of design choices.

A distinctive feature of MSC/Circ.1002 is its stepwise process for demonstrating equivalence under SOLAS II-2/17. Designers must first develop a set of design fire scenarios, systematically identifying and selecting hazards relevant to the ship type and operation. For each scenario, measurable performance criteria must be defined. These benchmarks allow both qualitative and quantitative analyses from expert workshops to CFD fire simulations to be performed. The guideline also stresses the role of multidisciplinary design teams and requires a comprehensive documentation package, ranging from a preliminary design report to a final approval dossier submitted to the Administration. While this framework offers significant flexibility, it also illustrates two key challenges of RBD: strong dependence on scenario selection and the document-heavy nature of current practice.

Subsequent circulars have refined and expanded this framework. MSC.1/Circ.1212 (2007) introduced the Netherlands Regulatory Framework (NeRF), providing practical guidance on how alternative design can be applied in SOLAS Chapters II-1 and III, covering subdivision, stability, and life-saving appliances [47]. The NeRF highlighted the importance of multidisciplinary design teams and early engagement with flag states to ensure that risk analyses are accepted as valid substitutes for prescriptive compliance.

MSC.1/Circ.1455 (2013) further consolidated the approval process for alternatives and equivalents under IMO instruments [48]. It builds on the principles of MSC/Circ.1002 and MSC.1/Circ.1212, but extends their scope and introduces more explicit requirements. It established clear procedural steps for submitting, reviewing, and approving alternative designs. These steps include:

1. Preliminary design proposals,
2. Agreement on the scope of the risk assessment,
3. Execution of a structured safety analysis (often based on FSA) and
4. Documentation of results demonstrating equivalent safety.

By formalizing these procedures, MSC.1/Circ.1455 provides a structured pathway for innovative naval and commercial ship designs to achieve approval under international regulation.

In practice, the IMO guidelines anchor RBD within the global regulatory framework. They ensure that the methods described earlier (FSA, PRA, and risk acceptance criteria) are not only theoretical tools but also recognized instruments for achieving compliance. For naval design, where innovations such as lightweight superstructures, new propulsion systems, or novel combatant configurations often lie outside existing rules, the alternative design guidelines provide the legal and procedural foundation for risk-based approval. Through these developments, IMO has established RBD as a recognized framework for balancing innovation with safety in maritime engineering.

Approval of alternatives and equivalents under MSC.1/Circ.1455

Before the approval matrix can be applied, MSC.1/Circ.1455 requires that the novelty of the technology is first categorized. Table 2.1 illustrates the categorization framework, which combines the application area (known or new) with the technology status (proven, limited field history, or novel/unproven). This results in four categories, ranging from Category 1 (known application of proven technology) to Category 4 (new application of novel or unproven technology). The assigned category then determines the level of analysis required in the subsequent approval matrix.

While this framework provides a structured way to classify innovations, in practice the categorization remains partly subjective. Determining whether a concept is “new” or “proven” depends on available data, operational experience, and the interpretation of the Administration, which introduces variability in how different authorities apply the guidelines.

Table 2.1: Categorization of new technology according to MSC.1/Circ.1455 [48]. Categories (1–4) define the novelty level, which determines the required depth of risk assessment in the approval matrix.

Application Area	**Technology status**		
	Proven	Limited field history	New or unproven
Known	1	2	3
New	1	2	4

The circular also highlights the range of stakeholders and qualifications needed in the process, including shipyards, consultants, classification societies, flag administrations, surveyors, and crew representatives. Their involvement ensures that risk assessments are not only technically rigorous but also operationally feasible and enforceable.

A key element of MSC.1/Circ.1455 is the introduction of an approval matrix, shown in Table 2.2. This matrix links the required depth of risk assessment to the novelty of the technology being assessed. For proven technologies, prescriptive rules such as SOLAS and MARPOL remain sufficient, and no formal risk analysis is required. As the degree of novelty increases, however, additional steps are mandated: from semi-quantified assessments for limited field history applications, to fully quantified probabilistic analyses and continuous monitoring for novel or unproven concepts. The framework also specifies requirements for the qualifications of analysts, the type of guidance and rules that apply, and the level of third-party review expected.

This matrix provides administrations with a structured decision tool that helps scale the regulatory effort to the maturity of the technology. At the same time, it illustrates one of the challenges of RBD in practice: determining whether a concept is “proven” or “novel” remains partly subjective, and the corresponding analytical requirements can vary depending on the interpretation of the administration and the availability of data. Such ambiguity reinforces the need for systematic approaches (potentially supported by MBSE) that can make novelty classification and evidence traceability more transparent.

Table 2.2: Approval matrix from MSC.1/Circ.1455, linking required risk-assessment depth to technology novelty [48].

Requirements	Known application of proven technology (conventional process)	Known application of a technology with a limited field history / New application of proven technology	New application of a technology with a limited field history / Known application of a new or unproven technology	New application of novel or unproven technology
A) Basic risk assessment	Not required	Required (if rule challenge deemed significant)	Required	Required
B) Further analysis requirements	Not required	Depending on outcome of basic risk assessment; hazards medium/high may be semi-quantified	Semi-quantified; all hazards medium/high examined quantitatively if possible	Quantified assessment of all hazards; novelty may limit credibility, but full analysis expected
C) Qualifications of analysts	N/A	Operational experience; general knowledge of risk assessment techniques	Operational experience; in-depth experience with risk assessment	Operational experience; risk assessment experts
D) Applied rules and guidance	Prescriptive rules (SOLAS, MARPOL, codes, national regulations, class rules)	Same prescriptive rules; class/industry guidance if available	IMO circulars on alternative arrangements; class guidance on risk-based approval; relevant standards	IMO circulars on alternative arrangements; class guidance on risk-based approval
E) Additional tests, surveys, compliance control	As per SMS and existing regulation	Internal surveying. Additional review at safety related events subject to recording and corrective action	Internal/external surveys; recording and additional reviews as required	Continuous monitoring and review until sufficient experience is gained
F) Review by third party	Considered	Considered	Considered	Recommended

2.2.3. The Naval Ship Code (ANEP-77)

While the IMO guidelines define regulatory frameworks also for commercial vessels, the naval domain applies a parallel risk-based framework: the NSC, formally issued as ANEP-77. Developed under the NATO Naval Armaments Group (NNAG) and maintained by the International Naval Safety Association (INSA), the NSC provides a functional, goal-based approach for demonstrating safety equivalence in warship design [49, 50]. It translates the principles of RBD into a comprehensive framework that allows navies to balance mission requirements, operational flexibility, and safety assurance within a structured risk management system.

The Code is structured around a Safety Management System (SMS) framework that mandates a risk-based approach to design, construction, and operation. Rather than prescribing detailed technical rules, it defines high-level safety goals and functional objectives for key ship systems, including fire protection, stability, evacuation, and propulsion. Compliance is demonstrated through structured risk analyses typically using FSA or equivalent methods that show the design achieves an equivalent or superior level of safety. This approach aligns closely with the RBD philosophy established under IMO guidelines, but is specifically adapted to the operational freedom and mission-driven trade-offs required for naval platforms.

A key feature of ANEP-77 is its emphasis on documentation and traceability. Each safety goal must be supported by a Safety Case, which provides evidence that risks have been identified, assessed, and mitigated to a level that is ALARP. The Safety Case integrates risk assessments, design justification, and verification results into a single auditable record, functioning as the foundation for naval class approval.

Through this structure, ANEP-77 institutionalizes risk-based reasoning within the naval design process, embedding safety assurance as a continuous activity throughout the ship's lifecycle.

The NSC relies heavily on risk analyses and documentation to support design justification. These activities are currently document-centric and time-consuming.

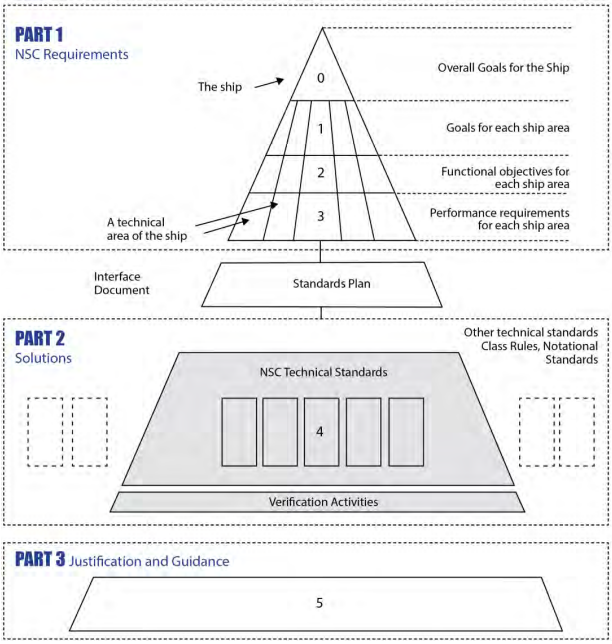


Figure 2.9: Arrangement of the NSC

The structure of the NSC, shown in Figure 2.9, illustrates how safety objectives are organised across multiple hierarchical levels that together define the functional safety framework for naval design. The upper part of the figure (Part 1) represents the NSC Requirements, arranged as a goal-based hierarchy. At the top, Level 0 defines the overall safety goals for the entire ship-broad principles such as protection of life, mission continuity, and environmental integrity. Level 1 refines these into goals for specific ship areas (For example: fire safety, stability, evacuation, and propulsion). Levels 2 and 3 translate these goals into increasingly concrete functional objectives and measurable performance requirements for each technical subsystem. At the base of the pyramid, the Standards Plan links these requirements to applicable technical standards, class rules, or verification criteria, ensuring that each design decision can be traced back to the overarching safety goals.

Part 2 of the figure depicts the Solutions phase, in which the design is verified against the established safety goals using technical standards, simulations, and verification activities. The NSC does not prescribe a single technical solution; instead, it provides the framework within which different engineering standards such as class society rules or national defence standards can be used to demonstrate equivalence. This flexibility enables innovation while maintaining an auditable safety justification process. Verification activities within Part 2 close the loop between the functional objectives defined in Part 1 and the technical evidence required to demonstrate compliance.

Finally, Part 3 represents the Justification and Guidance layer, which consolidates all supporting evidence in the form of the Safety Case. The Safety Case documents how each safety goal and objective has been satisfied, integrating hazard identification, risk analyses, design justification, and verification results into a single traceable record. This part of the framework embodies the document-intensive nature of current risk-based naval design practices: while it ensures accountability and transparency, it also results in a large volume of static evidence artefacts that must be maintained and updated as the design evolves [49, 50].

From the perspective of MBSE, the hierarchical and traceable structure of ANEP-77 aligns naturally with the architecture of model-based frameworks such as Arcadia and Capella. Each level of the NSC hierarchy

goals, objectives, and performance requirements can be directly mapped to corresponding model layers and elements. In a model-based environment, the Standards Plan and Safety Case could be represented as linked model artefacts rather than as static documents, allowing risk evidence and verification results to be updated automatically when the design changes.

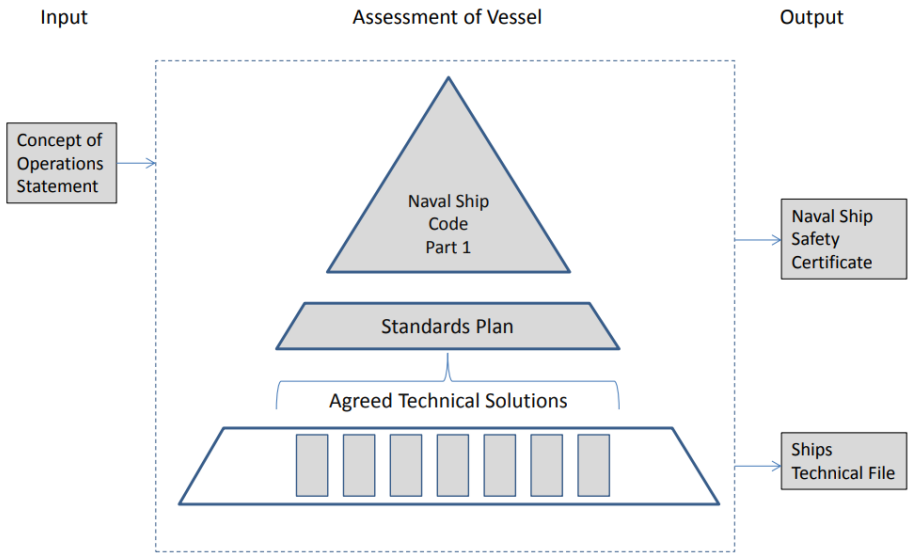


Figure 2.10: Main regulatory elements in the certification process of ships

The process shown in Figure 2.10 illustrates how the NSC is applied in practice. The Concept of Operations provides the operational baseline for defining applicable safety goals, which are then addressed through the Standards Plan and verified by agreed technical solutions. The resulting evidence forms the Ship's Technical File and leads to the issue of a Naval Ship Safety Certificate by the competent authority. In current practice, this process remains largely document-driven, with risk analyses, verifications, and approvals maintained as static reports. Within a model-based environment, however, each of these artefacts could be represented as interconnected model elements linking operational concepts, safety requirements, verification activities, and approval evidence in a single traceable framework.

Applications in commercial and naval design

The methods of RBD have been applied in naval and commercial ship projects, demonstrating their value in enabling innovation where prescriptive rules are absent or insufficient. For instance, Valcalda et al. [51] developed a risk-based assessment method to support compliance with the IMO's Safe Return to Port framework in passenger-ship concept design. His work illustrates how structured risk analysis and tool-supported verification can mitigate non-compliance risks during early design stages. It is an approach that parallels the objectives of RBD in other maritime sectors.

A second important area of application has been in the design of novel naval combatants. These ships often integrate advanced combat systems, lightweight structures, and unconventional arrangements that fall outside the scope of existing prescriptive regulations. By applying RBD, designers can demonstrate that despite deviations from established rules, the overall level of safety remains equivalent or superior. For example, probabilistic risk assessments of flooding, fire, and combat damage scenarios have been used to compare alternative structural configurations and justify design trade-offs in next-generation warships [2].

Another domain is the use of lightweight materials and superstructures. Naval and passenger ships increasingly incorporate aluminum or composite structures to reduce weight and improve fuel efficiency. However, prescriptive rules for fire protection and structural reliability were developed for conventional steel designs. RBD has allowed these innovations to proceed by demonstrating, through fire safety assessments, evacuation analyses, and structural reliability models, that equivalent safety levels can be maintained [14]. These applications have not only enabled novel material choices but have also influenced the development of new classification society guidelines.

A further example concerns alternative fire safety concepts. In some naval projects, traditional prescriptive requirements for fire insulation or separation have been replaced by performance-based arrangements. By using the IMO's alternative design guidelines (see Section 2.2.2), risk assessments were carried out to show that active fire suppression systems, enhanced detection, and improved evacuation procedures could achieve an equivalent level of safety to prescriptive fire boundaries [46]. Such cases illustrate the flexibility of RBD in balancing design freedom with robust safety justification.

Despite these successful applications, the implementation of RBD in ship design still faces several challenges. First, the effectiveness of RBD depends heavily on the availability and quality of quantitative risk data, which are often limited or proprietary in the maritime domain. As a result, many analyses rely on expert judgement, introducing uncertainty and potential bias. Second, the translation of probabilistic findings into design decisions can be difficult, particularly when different stakeholders—such as shipyards, classification societies, and regulatory bodies—apply diverging interpretations of acceptable risk. Finally, RBD requires multidisciplinary collaboration between safety engineers, designers, and regulators, yet in practice these groups often operate within separate workflows. These limitations highlight that while RBD offers significant flexibility and innovation potential, its consistent and practical implementation across the industry remains an ongoing challenge [15, 45].

Fundamentals and applications of RBD

Beyond its regulatory embedding in FSA and IMO circulars, RBD can also be understood from the perspective of reliability theory and optimization. In this view, RBD is formulated as a probabilistic design optimization problem, where uncertainties in loads, material properties, and operational conditions are explicitly represented. The design task is then to minimize expected cost or maximize performance while keeping the probability of failure below an acceptable threshold [52]. This formulation highlights that RBD is not only a procedural framework for hazard assessment, but also a mathematical approach for balancing safety and efficiency under uncertainty.

A key regulatory development in this direction is the IMO Goal-Based Standards – Safety Level Approach (GBS–SLA). The SLA concept defines target safety levels in quantitative terms and links them directly to the development of design rules. By connecting risk metrics with prescriptive standards, GBS–SLA provides a structured mechanism for embedding risk-based reasoning into rulemaking itself, rather than applying it only at the project level. This elevates RBD from a tool for exceptional cases to a systematic foundation for maritime regulation [52].

The ClassNK review emphasizes that conventional RBD methods face limitations when applied to Maritime Autonomous Surface Ships (MASS). The absence of onboard crew, reliance on digital control systems, and exposure to cyber risks introduce fundamentally new hazard categories. Addressing these requires a system-of-systems approach that integrates functional safety, vulnerability analysis, and real-time risk monitoring. These insights align closely with the need for integration between MBSE and RBD, as only model-based approaches can capture the complex interactions between autonomy, safety, and regulatory acceptance in MASS [52].

2.2.4. Continues process

As illustrated in Figure 2.11, risk assessment is not a separate process but directly feeds into the design decision-making cycle. Performance expectations, functional requirements, and technical feasibility are considered alongside safety goals, hazard identification, and risk analysis. This integrated perspective illustrates the intended role of RBD as a decision-support mechanism within naval architecture. It also emphasizes the importance of embedding risk reasoning directly into model-based design environments.

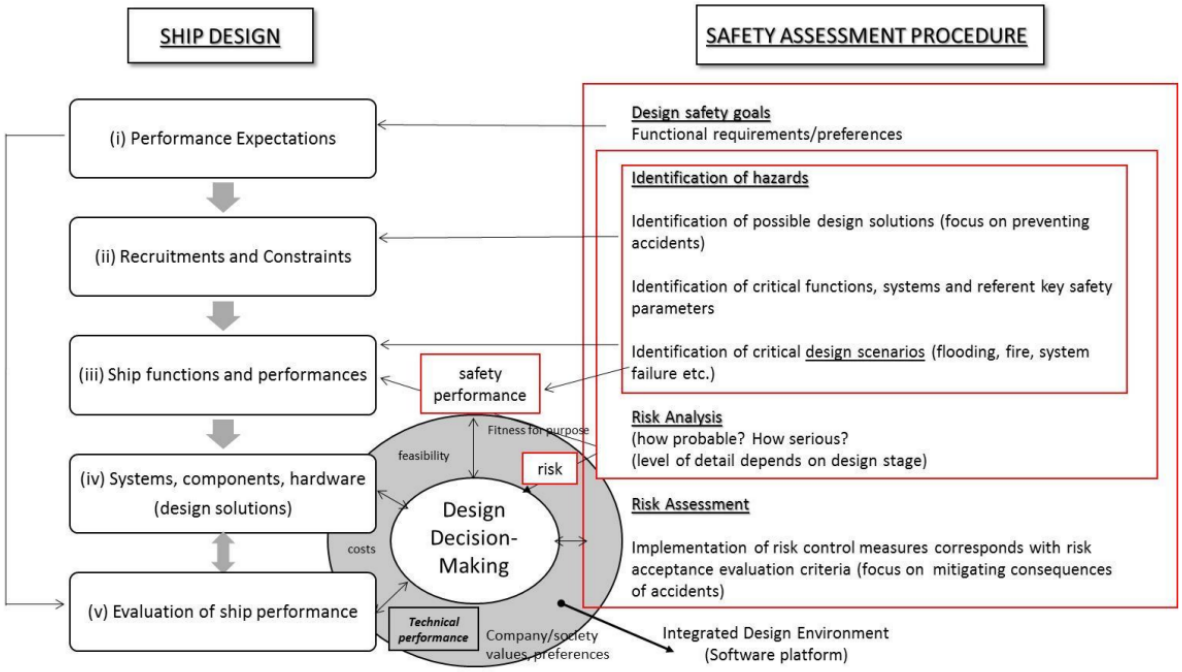


Figure 2.11: Interaction between ship design stages and safety assessment procedure, highlighting how risk reasoning informs design decision-making [53].

2.2.5. Document-driven approval processes

The approval of alternative designs under IMO guidelines remains dominated by a document-centric workflow. Figure 2.14 illustrates this by contrasting the formal design and approval process (Fig. 2.12) with its associated documentation stream (Fig 2.13), as defined in MSC.1/Circ.1455. The left-hand side shows the sequence of design steps, from preliminary concept to final approval and operation, with continuous interaction between the submitter and the Administration. Each stage requires review and acceptance before the process can progress, which ensures regulatory oversight but also enforces a sequential and time-consuming structure.

The right-hand side expands this view by including the documentation produced at each step: design reports, analysis records, approval statements, testing reports, and final certificates. These artefacts are generated and reviewed in parallel to the design process, resulting in a fragmented evidence chain spread across numerous static documents. Updates to the design propagate through new versions of reports rather than through a central source of truth, which makes consistency and traceability difficult to maintain. The process therefore illustrates two persistent challenges of RBD: its document-heavy implementation and the lack of integration between technical analyses and regulatory approval artefacts.

From the perspective of MBSE, these figures highlight a research opportunity. While current RBD practice anchors safety justifications in documents, MBSE could provide a model-centric environment where requirements, hazards, analyses, and approval conditions are represented consistently and updated dynamically. Embedding risk reasoning in such a model repository would reduce duplication, strengthen traceability, and improve the alignment between design evolution and regulatory oversight.

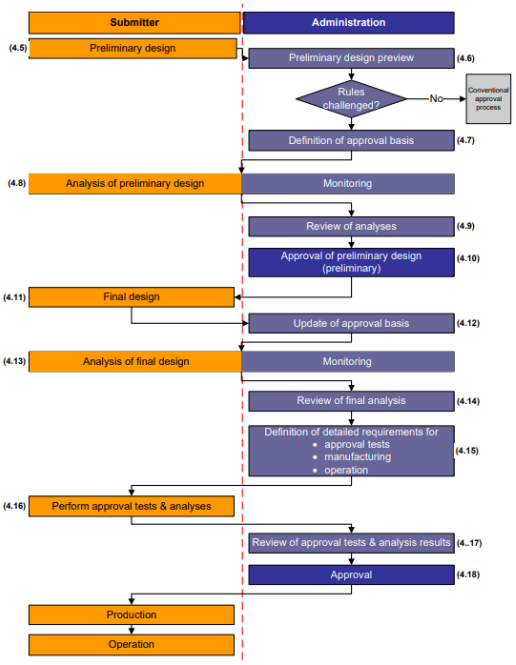


Figure 2.12: Design and approval process [48].

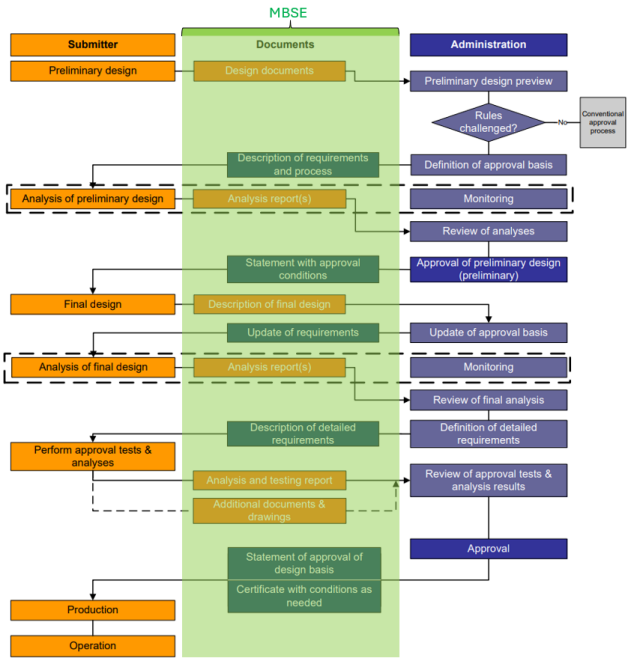


Figure 2.13: Documentation flowchart for the approval procedure [48].

Figure 2.14: Approval process (Fig. 2.12) and its associated documentation stream (Fig. 2.13) as described in MSC.1/Circ.1455. The comparison illustrates the document-heavy nature of current RBD practice and the potential role of MBSE.

2.2.6. Practical implementation of RBD at Damen Naval

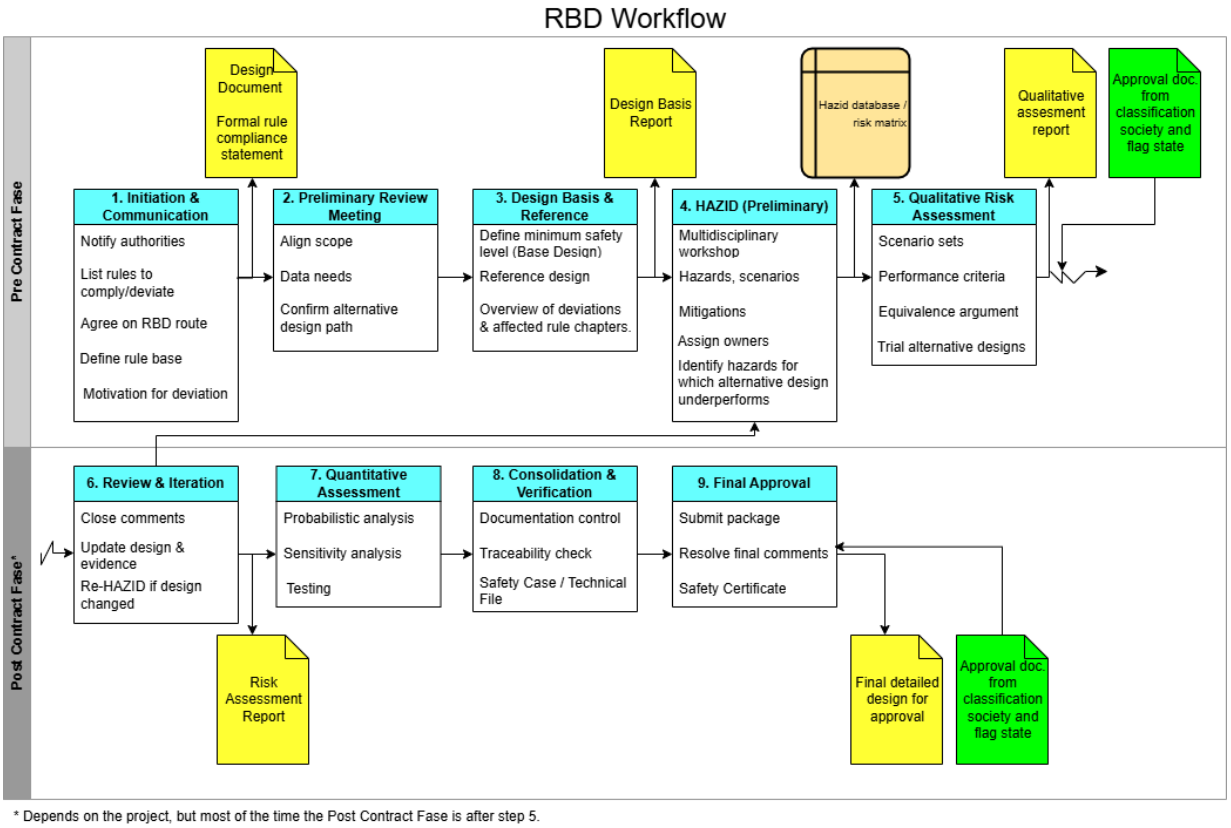


Figure 2.15: Flowchart of the RBD process.

In practice, the RBD process within Damen Naval follows a structured sequence that closely mirrors the IMO guidelines on Alternative Design and Arrangements (see Figure 2.15) [46]. The process begins with a formal communication to all approval authorities, such as DNV and COMMIT, specifying which rules will be followed and where deviations are expected. This early alignment ensures that all stakeholders agree on the use of a risk-based route from the outset of the project and that the approval process proceeds transparently.

Subsequently, a *Design Basis* and a *Reference Design* document are prepared. The Design Basis defines the minimum safety level to be demonstrated and forms the foundation for all validation activities. The Reference Design represents an existing certified vessel and provides a benchmark against which innovations are evaluated. Both documents identify the affected rule chapters, expected deviations, and the new technologies or design features to be assessed.

For each deviation, Damen must demonstrate how equivalent safety is achieved. This involves a combination of qualitative and quantitative risk assessments, analytical evidence, and, where necessary, physical testing. The process is supported by multidisciplinary *HAZID* workshops, which are considered the most critical step of the assessment. The quality of the HAZID depends on the completeness and expertise of the participating specialists, and its findings form the basis for the subsequent qualitative and quantitative analyses.

All results are consolidated in a comprehensive *Design Basis Risk Assessment Report*, containing both qualitative and, where applicable, quantitative assessments. The report is updated iteratively as the design evolves. Each major modification needs a new HAZID and reassessment cycle. Completing these steps typically requires about one year, depending on the novelty and complexity of the subject.

The *Post-Contract Phase* begins once the Approval document from classification societies and flag states is received. This phase includes probabilistic analysis, sensitivity studies, and verification activities. All

evidence is compiled in a traceable *Safety Case* or *Technical File*, which serves as the formal submission package to the classification society and flag administration. The process concludes with the issue of a *Statement of Approval of Design Basis (SoADB)* and a corresponding *Safety Certificate*, confirming that the design achieves an acceptable level of safety under IMO or DNV principles.

Damen's RBD workflow is structured and aligned with international procedures. The sequential exchange of reports and the manual updating of HAZID findings and design evidence introduce delays and increase the risk of outdated information when design changes occur.

Summary
RBD embeds explicit risk reasoning into ship design, allowing innovative or unconventional solutions to be justified against demonstrable safety levels rather than strict rule compliance. Its principles are early hazard identification, quantitative assessment, integration with design trade-offs, compliance by justification, and iterative validation. This ensure that safety, performance, and cost are assessed throughout development. The IMO's FSA structures RBD into five steps, supported by probabilistic tools such as FTA, ETA, Monte Carlo simulation, and structural reliability methods.

Risk acceptance follows explicit criteria, most notably the ALARP principle and the IMO's GBS-SLA, which link safety targets to design and rule formulation. The procedural pathway for implementation is defined in IMO circulars MSC/Circ.1002, MSC.1/Circ.1212, and MSC.1/Circ.1455, outlining how to demonstrate equivalent safety. In naval projects, these principles are mirrored in NATO's ANEP-77 framework, which defines hierarchical safety objectives, functional requirements, and verification processes for warships.

Together, the IMO and ANEP-77 frameworks position RBD as a unified approach for balancing innovation and safety in both civilian and naval ship design. Yet both remain largely document-centric, relying on static reports for traceability and approval evidence.

2.3. Conclusion

This chapter answers the question: What are the key principles and methods of MBSE and RBD relevant for innovation? Both MBSE and RBD provide structured approaches to enable innovation in naval ship design. Their shared purpose is to manage system complexity while ensuring that novel or unconventional technologies can be introduced safely.

The key principles of MBSE are centralized system modeling, multi-domain integration, lifecycle continuity, and stakeholder communication. This creates a single, traceable source of truth that supports early validation and collaborative innovation. Methods such as Arcadia, implemented in Capella, operationalize these principles through layered architectures and standardized viewpoints. Extensions such as ATICA4Capella demonstrate how MBSE can begin to incorporate dependability and safety reasoning.

RBD, on the other hand, embeds explicit risk reasoning into the design process. Its core principles are early hazard identification, quantitative assessment, integration with design trade-offs, and justification-based compliance. This allows designers to pursue innovation within an acceptable level of safety. The IMO's FSA framework and instruments such as ALARP, GBS, and ANEP-77 formalize these methods and define the regulatory pathway for innovative solutions to gain approval.

Together, MBSE and RBD form complementary foundations for innovation: MBSE enhances internal design traceability and coherence, while RBD ensures regulatory acceptance through demonstrable safety justification. Integrating both approaches (embedding risk reasoning directly within system models) offers a pathway toward innovation processes that are simultaneously traceable, risk-informed, and compliant.

3

Current challenges of MBSE & RBD

This chapter addresses Research Question 2: What are the current challenges in applying MBSE and RBD for innovative naval systems?

While both MBSE and RBD have been widely promoted as enablers of innovation in safety-critical ship design, their practical application reveals limitations. These challenges appear both within each approach individually and in their attempted integration. Understanding these obstacles is important, as they delineate the research gap that this research addresses. This chapter first discusses current challenges in MBSE, followed by challenges in RBD, and finally explores the difficulties of combining the two into a coherent framework.

3.1. Challenges of MBSE in practice

Although MBSE has been widely recognized for improving traceability, consistency, and collaboration in complex system design, its practical application reveals a number of limitations. These limitations become particularly evident in large-scale projects, such as naval shipbuilding, where multiple stakeholders, disciplines, and tools must be coordinated over long timescales. Understanding these challenges is important, as they not only highlight the boundaries of current MBSE practice but also point to areas where integration with complementary approaches, such as RBD, may provide significant added value.

Limitation M1: Model complexity and governance

In theory, MBSE promises a single, shared model that improves traceability and early validation throughout the system lifecycle [1, 18, 19]. In practice, however, engineering teams often struggle to keep these models consistent and manageable. As projects grow, model repositories can become fragmented, with overlapping views and duplicated information. This makes version control and configuration management important, but especially in long naval projects also challenging as multiple suppliers contribute asynchronously to the same model.

Studies acknowledge that MBSE can improve collaboration and design insight, but they also warn that without careful model governance, its advantages may erode [1, 18, 19]. Poorly coordinated updates, unclear ownership of model elements, and weak tool integration can all undermine the “single source of truth” that MBSE aims to create [9]. Effective model governance through disciplined processes for change management, versioning, and validation is therefore essential to keep models reliable and useful as decision-support tools.

Limitation M2: Tool and method heterogeneity

Tool and method heterogeneity is a second friction point. Arcadia/Capella provides a rigorous separation of operational, functional, logical, and physical views that helps structure architecture work [7]. Yet, when these architecture views must interoperate with requirement databases, simulation models, safety analyses, and PLM/ALM environments, data exchange is often lossy or brittle. SysML-based toolchains alleviate some of this through standard notations, but differ in metamodel extensions and repository implementations, which complicates interoperability. Industrial case material in complex warship design confirms that “virtual integration” across domains requires significant bespoke glue-scripts, custom profiles, and governance

conventions before model artefacts can support robust design integration or design-space exploration [15]. Earlier naval work already observed that the value of MBSE is tightly coupled to organizational adoption and process integration, not just notation choice [17].

Limitation M3: Limitations of traditional Reliability, Availability, Maintainability, and Safety (RAMS) approaches

RAMS analyses have traditionally been conducted as parallel activities to systems engineering. In the space and maritime domains, methods such as FMEA, FTA and Reliability Block Diagrams have long been applied to demonstrate compliance with reliability and safety requirements. While these techniques are effective in identifying hazards and failure paths, the traditional document-driven workflow presents several shortcomings.

First, RAMS requirements are often allocated by extrapolating from previous designs rather than by systematically linking reliability needs to system-level functions. This approach tends to reinforce conservative redundancies without exploring optimized design solutions or graceful degradation concepts [8].

Second, RAMS analyses are frequently performed late in the design process, after architectural choices have already been made. As a result, their influence on design trade-offs is limited, and findings are often fed back as corrective actions rather than proactive design guidance [54, 55].

Third, the lack of integration between RAMS tools and systems engineering environments creates inefficiencies and inconsistencies: hazard logs, fault trees, and reliability allocations are generated as static documents, disconnected from evolving architecture models [31, 56, 57].

Limitation M4: Non-functional evidence and risk integration

Another limitation concerns the representation of non-functional evidence. Especially uncertainty, risk, and safety justification inside the system model. MBSE models excels at structural and behavioral consistency, but the model elements used to argue about safety (hazard logs, risk registers, acceptance criteria) often live outside the MBSE model repository in documents or specialist tools. The result is a broken evidence chain: requirements trace to functions and components within the model, while risk rationales and acceptance arguments sit elsewhere, weakening change impact analysis and auditability. INCOSE's strategic vision highlights lifecycle integration, yet leaves open how probabilistic risk reasoning and assurance cases should be embedded as first-class model citizens [1]. Industry commentary underscores that many organizations remain "document-heavy with a model veneer," where models reference PDFs rather than subsume their logic, limiting the automation potential of verification and reviews [20].

Limitation M5: Adoption and return on investment

MBSE adoption can stall without a clear, program-level business case. Multiple studies note that the effort to build a high-quality architecture model is front-loaded, whereas the payoffs (fewer defects, faster integration, improved change impact analysis) accrue later and across stakeholders [9, 58, 59, 60, 61]. This timing often incentivizes "minimal modeling": just enough artefacts to pass process gates, but with insufficient semantic depth for quantitative trade-offs or automated checks [61, 62]. Under such conditions, MBSE may not eliminate rework but rather shift it to later project phases, where inconsistencies can become more costly to correct. [60, 63]. Naval programs with long lead times, distributed supply chains, and tight regulatory interfaces tend to amplify these adoption dynamics [59, 64].

Implications for research

Together, these observations delineate a clear research gap: current MBSE practice provides structural traceability and architectural coherence but lacks native, rigorous integration of risk reasoning including uncertainty modeling, acceptance criteria, and safety case argumentation into the same model that governs design decisions. Bridging this gap requires methods that embed risk concepts (hazards, likelihoods, mitigations, and acceptance arguments) as typed, queryable model artefacts linked to requirements and architecture, so that changes propagate through both design and assurance logic. This need motivates the present research to investigate a principled integration of MBSE with RBD.

3.2. Challenges of RBD in practice

Although RBD has been recognized as a promising framework for justifying innovative ship designs, its practical application reveals a number of persistent challenges. These challenges concern the availability of data, the definition of scenarios, the implementation of acceptance criteria, and the way results are documented and communicated. In naval architecture, where designs are safety-critical and subject to regulatory approval, these difficulties often determine whether RBD can be applied effectively.

Limitation R1: Data availability and probabilistic uncertainty

A central challenge in RBD lies in the availability of reliable data for probabilistic risk assessments. Methods such as FTA, ETA, and Monte Carlo simulation require statistical information on failure rates, environmental loads, and human reliability. In practice, such data are often scarce, outdated, or context-specific, especially for novel technologies where no historical record exists [2]. As a result, designers must rely heavily on expert judgement, which introduces subjectivity and variability. This undermines the quantitative rigor of RBD and complicates regulatory acceptance, since authorities may question the assumptions on which risk estimates are based.

Limitation R2: Scenario dependence

Another limitation is the strong dependence of RBD on scenario definition. Hazard identification (Step 1 of the FSA framework) requires the enumeration of credible accident scenarios, but there is no universal agreement on which scenarios must be included. Different stakeholders may emphasize different hazards, leading to inconsistencies between analyses. Furthermore, scenario modeling can become prohibitively complex when cascading failures or human factors are considered. This creates a tension between model completeness and practical feasibility, and increases the risk that critical hazards remain unaddressed [46, 48].

Limitation R3: Ambiguity in acceptance criteria

While frameworks such as ALARP, GBS, and the SLA provide structured ways to evaluate risks, their practical application is not straightforward. The definition of what constitutes a “tolerable risk” remains context-dependent and sometimes politically influenced. For example, ALARP requires judgements about whether further risk reduction would be “grossly disproportionate” to its benefits, but this balance is inherently subjective [13]. Similarly, quantitative thresholds in SLA approaches differ across classification societies and flag states, which reduces comparability between projects and undermines the predictability of regulatory outcomes.

Limitation R4: Document-heavy implementation

Despite its systematic framework, RBD is still predominantly implemented in document-centric form. Risk assessments are often conducted in spreadsheets, reports, and PDF files, which are submitted to regulators as part of the approval process. This creates challenges for traceability: when design changes occur, the link between updated system architectures and previously conducted risk assessments is easily broken. The result is a fragmented evidence chain, where requirements and design solutions may be modeled in digital tools, but risk justifications remain locked in static documents [20]. This limits the potential for automation and integration of RBD with other engineering practices.

Limitation R5: Life-Cycle Limitations of Current RBD Practice

A further challenge of RBD is its limited consideration of the entire ship life cycle. Traditional applications focus strongly on the design stage, where hazards are identified and risks are quantified to justify deviations from prescriptive rules. However, once the vessel enters operation, the systematic risk reasoning that underpins the design process is often no longer applied with the same rigor.

The State-of-the-Art review presented at IMDC 2015 highlights this gap by introducing the concept of Life-Cycle Risk Management (LCRM) [53]. According to this framework, safety should not be treated merely as a constraint during design, but as a continuous objective across all phases of the vessel’s life. This includes not only design and construction, but also operation, maintenance, and emergency response. The review emphasizes that measures such as the ISM Code or onboard decision support systems are rarely validated with the same methodological discipline as design measures, creating an asymmetry in

how risk is managed across different stages.

This life-cycle gap undermines one of the central promises of RBD: that risks can be transparently managed and justified throughout the vessel's lifetime. In practice, risk-based justifications remain document-heavy and static, making it difficult to adapt them as operational knowledge evolves. Bridging this gap requires methods that maintain risk traceability beyond the design office, ensuring that operational and emergency risks are addressed with equal rigor.

Limitation R6: Emerging challenges in novel technologies such as Autonomous Ships

Another domain where the limitations of current RBD practice become apparent is in the design of MASS. These vessels introduce fundamentally new risk profiles, including failures in autonomy software, cyber-security vulnerabilities, and the absence of onboard crew for emergency response. Conventional RBD methods, developed primarily for manned vessels, struggle to capture these aspects.

Recent research proposes combined methods such as the COFA-HAZID framework, which integrates functional analysis with hazard identification to better address the risks of MASS [65]. By mapping functions and subsystems using model-based representations, COFA-HAZID enables hazards to be identified directly from the system architecture, thereby aligning risk analysis with the system design. Furthermore, the study highlights the importance of *real-time risk assessment*: because MASS operate in dynamic and uncertain environments, risk evaluations cannot be limited to the design stage but must be updated continuously during operation as illustrated in Figure 3.1 .

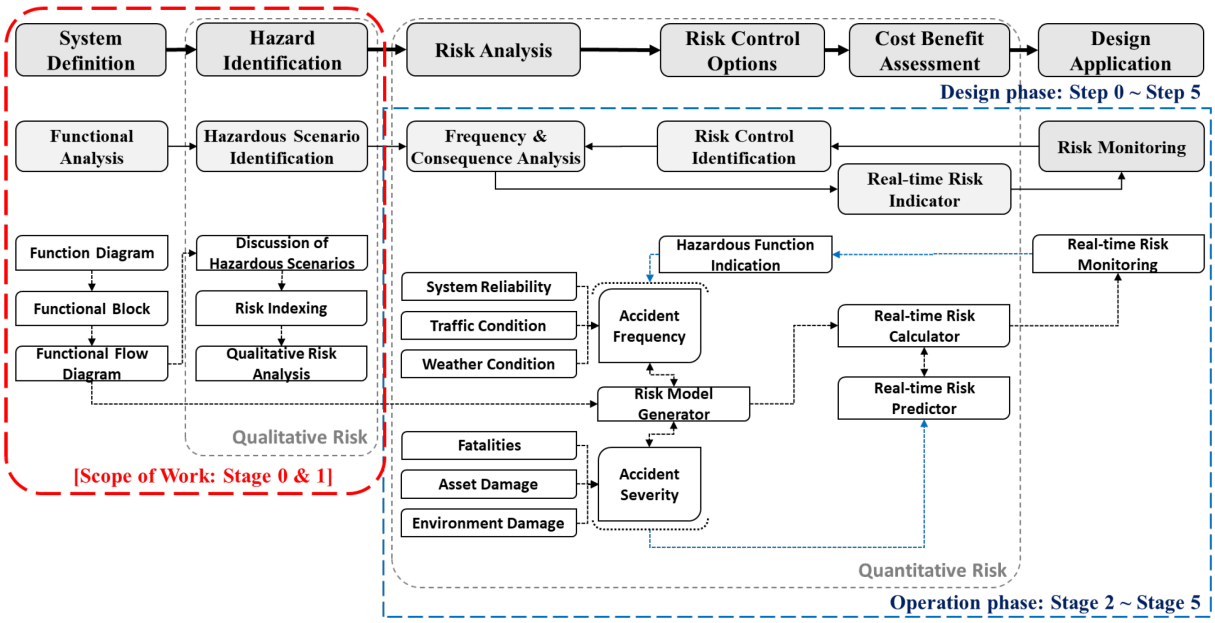


Figure 3.1: Risk assessment procedure [65].

Limitation R7: Completeness and subjectivity of risk techniques

A recurring limitation of RBD is the dependence on the techniques used for hazard identification and risk evaluation. Qualitative methods such as HAZID, HAZOP, and FMEA are effective for generating comprehensive hazard lists, but their outputs depend heavily on the expertise and perspectives of the participants. As a result, analyses may vary significantly between design teams, creating uncertainty about whether all relevant hazards have been identified [12].

Semi-quantitative methods such as FTA and ETA provide structure, but their completeness still depends on the initiating events and causal paths defined by analysts. If critical initiating events are overlooked, the resulting fault or event trees can give a misleading sense of coverage. Quantitative PRA techniques add rigor by attaching probabilities to failure modes and consequences, yet these results remain only as reliable as the data used to populate the models [10, 12, 43].

This reliance on expert judgement, scenario selection, and limited data makes risk assessments vulnerable to subjectivity and inconsistency. For naval innovation, where empirical data can be scarce, this challenge is particularly there [15, 45].

Implications for research

Taken together, these challenges demonstrate that while RBD provides a valuable framework for balancing innovation and safety, its practical implementation suffers from uncertainty, subjectivity, and fragmentation. For naval architecture, where innovative technologies often precede prescriptive rules, these issues are particularly critical. They highlight the need for complementary frameworks that can improve traceability, ensure consistency, and reduce reliance on subjective judgement, motivating the integration of RBD with MBSE, which will be further explored in the next section.

3.3. Challenges of integrating MBSE and RBD

While both MBSE and RBD have individually demonstrated value in managing complexity and enabling innovation, their integration remains underdeveloped. Bridging these two approaches would allow risk reasoning to be embedded directly within system models, creating a unified framework for design and safety justification. However, several challenges prevent such integration from being fully realized in practice.

Challenge 1: Lack of native representation of risk in MBSE models

Most MBSE tools and frameworks, such as Arcadia/Capella or SysML-based environments, are designed to capture system structure, functions, and behavior, but not the reasoning behind their safety justifications (Limitation M1, M4 and M5). These environments provide dedicated constructs for elements such as components, interfaces, and requirements, yet they lack native objects for hazards, failure probabilities, or risk acceptance criteria. As a result, risk analyses are often conducted in parallel using external tools or spreadsheets, and their outcomes are only referenced in the model as static annotations or hyperlinks [7, 20, 66, 67].

This fragmentation undermines the intended role of MBSE as a “single source of truth.” Risk evidence becomes detached from the architecture that it is meant to justify, making it difficult to demonstrate how identified hazards propagate through system functions or how design changes affect the overall risk posture. When the system evolves, the associated risk information often remains outdated or inconsistent. This erodes the traceability between the technical and assurance aspects of the design.

The lack of native risk constructs is not a limitation of the tools alone (Limitation M4 and R1) but reflects a deeper methodological gap. MBSE languages were historically designed for descriptive architecture modeling, not for quantitative reasoning under uncertainty. Risk, however, is inherently probabilistic and contextual: it depends on operational conditions, human factors, and environmental interactions that are difficult to formalize within static architecture models. Addressing this gap therefore requires extending MBSE metamodels to include typed artefacts for hazards, likelihoods, mitigations, and acceptance arguments. In other words: elements that can be queried, updated, and verified within the same model repository.

Moving forward, research and industry initiatives could focus on embedding risk reasoning as a first-class model citizen. This would allow each system element to be associated not only with functional or physical attributes, but also with explicit risk parameters and mitigations. Such extensions would enable continuous validation (Limitation R5) of risk throughout the lifecycle, replacing the current document-heavy evidence chain (Limitation R4) with dynamic, model-based safety assurance.

Challenge 2: Granularity mismatch between models and risk analyses

A second challenge arises from the granularity mismatch between MBSE architectures and RBD analyses (Limitation M2 and R1). MBSE models represent the system across multiple abstraction layers: operational, functional, logical, and physical. Each are optimized for communication and traceability. Risk analyses, in contrast, focus on specific scenarios or failure events at a much finer level of detail, such as component malfunction, fire in a compartment, or failure of a control algorithm. These different scales of representation make direct linkage between architecture and risk models inherently difficult (Limitation M4) [15].

For example, a probabilistic flooding model may quantify the likelihood of water ingress in a particular

compartment, yet the MBSE model might only represent that compartment as part of a higher-level structural module without explicit boundaries or internal attributes. The result is a misalignment in model semantics: the risk model refers to phenomena that the MBSE architecture does not explicitly encode. This misalignment complicates automated traceability, as it becomes unclear which design element a specific hazard or risk control corresponds to [8, 57].

The issue extends beyond technical mapping. It affects how design decisions are made. When risk assessments are performed at a different level of detail than architecture models, the feedback loop between design and assurance weakens (Limitation R5)[68]. Designers cannot easily see how modifications to layout or functionality influence risk outcomes, and safety engineers cannot efficiently trace how their findings relate to specific model elements (Limitation M1). This disconnect delays the integration of safety considerations into early-stage trade-offs, which is precisely where RBD aims to add value.

Bridging this granularity gap requires defining consistent abstraction levels between system and risk models. One approach could be to establish “risk modeling views” within MBSE tools, where architecture elements are decomposed only to the level necessary for relevant hazard scenarios. Alternatively, model transformations could automatically generate risk-analysis models (e.g., fault trees or event trees) based on architecture hierarchies. Such approaches would ensure that both MBSE and RBD operate at compatible levels of resolution, allowing risk evidence to flow seamlessly through the same digital thread that connects requirements, architecture, and verification [69].

Challenge 3: Fragmented toolchains and interoperability

Integration is further hindered by fragmented toolchains (Limitation M3). MBSE environments such as Capella, Cameo, and System Composer coexist with specialized safety tools for fault-tree, event-tree, or Monte-Carlo analyses. Interfacing these platforms typically relies on ad-hoc scripts, custom profiles, or manual data transfers, which are costly to maintain and fragile over long project lifecycles (Limitation M1) [8, 70]. Despite repeated calls for standardized interoperability across engineering domains [31, 71], embedding RBD outputs directly into MBSE repositories remains technically challenging (Limitation R3, R5 and R7) [15].

Challenge 4: Different stakeholder communities

Another obstacle is the cultural and organizational separation between MBSE practitioners and risk analysts (Limitation M1, M2, M3, M4, R2, R3, R6 and R7). MBSE is typically applied by system architects and design engineers, while RBD is the domain of safety engineers, regulatory specialists, and classification societies. Each group uses distinct notations, tools, and reporting conventions [9, 72]. Bridging these communities requires not only technical interoperability but also mutual understanding and trust in shared models [64, 73]. In practice, however, regulators remain accustomed to document-based justifications, while designers increasingly rely on model-based workflows. This creates a persistent gap in communication and collaboration.

Implications for research

These challenges highlight why MBSE and RBD, despite their complementary strengths, are still practiced largely in isolation. The absence of risk reasoning as a first-class element in MBSE, the granularity mismatch between models and scenarios, fragmented toolchains, and divergent stakeholder expectations all contribute to the difficulty of integration [8, 9, 71, 72]. For naval architecture, this is particularly limiting, since innovations such as alternative materials, novel propulsion systems, or new combat configurations require both rigorous system modeling and credible risk justification. Addressing these integration challenges is therefore important to accelerate innovation while maintaining safety, and forms the core research problem of this research.

3.4. Conclusion

This chapter identified the main challenges that currently hinder the integration of MBSE and RBD in naval ship development. Although both approaches share the goal of enabling traceable, knowledge-driven design, their implementation remains disconnected.

The analysis revealed two core technical barriers. First, the absence of risk representation within MBSE models prevents the integration of hazard, probability, and mitigation data into the system architecture. As

a result, safety assurance remains external to the model, leading to fragmented evidence chains. Second, the granularity mismatch between MBSE architectures and risk analyses complicates the alignment of model elements with the detailed scenarios used in RBD. This disconnect weakens the feedback loop between design decisions and safety evaluation.

While other challenges (such as tool fragmentation and stakeholder separation) also contribute to this gap, they fall outside the primary scope of this study. The focus of the present research will therefore be on addressing the first two barriers through a targeted integration case.

4

Method

This chapter outlines the research plan for developing and evaluating a proof-of-concept integration between MBSE and RBD within Damen Naval. Specifically, it describes how elements of the RBD workflow will be modeled within Capella to demonstrate how risk reasoning can be embedded in a system architecture. This plan forms the practical foundation for testing whether MBSE can support risk-informed design in a traceable and model-based manner.

4.1. Research objective and approach

The objective of this research is to explore how elements of the RBD process can be represented and managed within an MBSE environment. The study aims to develop a proof-of-concept and evaluate a method for embedding RBD artefacts: hazard registers, performance criteria, and reference design data, directly into system architecture models. By doing so, it seeks to address the methodological gap identified in Chapter 3: the absence of native risk representation and traceability within an MBSE environment.

Both RBD and MBSE have been shown to offer complementary strengths in managing innovation in complex naval projects. RBD provides a framework for quantifying and justifying safety, while MBSE ensures traceability and consistency of design information across the system lifecycle. However, their current separation where risk analyses are performed externally to the model, leads to fragmented evidence chains and limited visibility of safety justifications during design evolution.

The central research question guiding this work is formulated as follows (*Research Question 3*):

How can the artefacts and reasoning of RBD be represented within an MBSE framework to improve traceability and reduce administrative workload in naval ship design?

To address this question, the research follows a structured, design-oriented approach combining literature review, stakeholder interviews, and model-based implementation at Damen Naval. The work bridges academic systems engineering research and naval design practice. Methodologically, it follows an iterative design process in which theoretical insights are translated into modelling solutions, evaluated, and refined with domain experts.

The research builds upon three complementary foundations:

1. **Theoretical foundation:** The background chapters (Chapter 2 and 3) provided a detailed analysis of the principles and challenges of MBSE and RBD, identifying the lack of native risk representation and the granularity mismatch between design models and risk analyses as key methodological gaps.
2. **Industrial foundation:** The work is embedded within Damen Naval's ongoing MBSE implementation and its established RBD workflow, ensuring direct relevance to current design practices and regulatory processes.
3. **Methodological foundation:** The research follows a design science strategy, where artefacts are developed, implemented, and evaluated to generate both practical and theoretical insights.

By combining these foundations, this research develops a proof-of-concept integration of RBD artefacts within an MBSE environment to demonstrate improved traceability between design decisions, identified hazards, and safety justifications. The findings are expected to inform both the methodological development of MBSE toolchains and the practical implementation of risk-based processes in naval ship design.

4.2. Research strategy and scope

The research strategy is structured around the integration of qualitative risk artefacts from the RBD process into an MBSE framework. Building on the analysis in Chapter 3, the study focuses on the methodological interface between these two domains rather than on their independent maturity or tool-specific performance. The aim is to understand how RBD reasoning can be formally represented within a system architecture model to strengthen traceability, consistency, and safety justification throughout the design process.

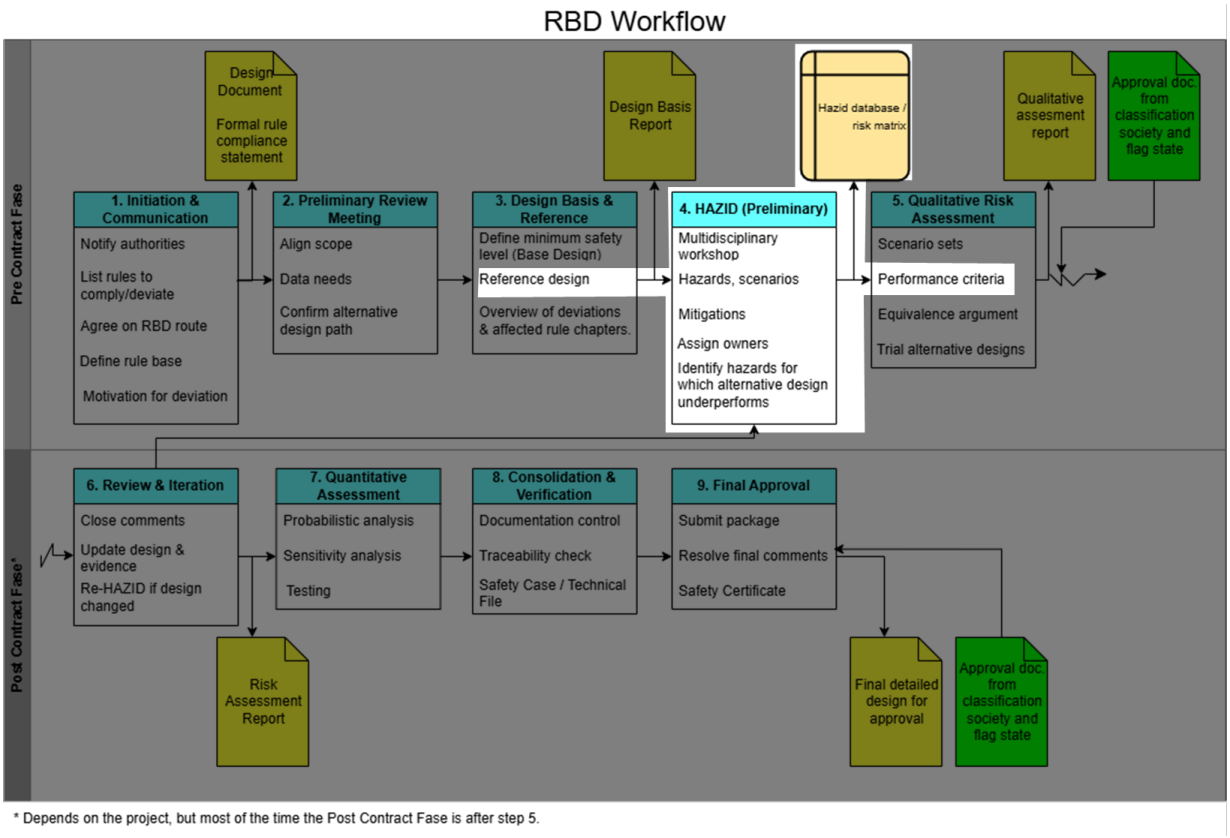


Figure 4.1: RBD workflow highlighting the phase with potential for implementation.

In figure 4.1 the part is highlighted where the focus will be on. The HAZID phase was selected as the primary focus area for several reasons. First, it represents the transition point between conceptual design and structured risk assessment, where qualitative insights are first translated into formal documentation. Second, HAZID artefacts, such as hazard descriptions, causes, consequences, and mitigations, are well-defined, traceable, and persist throughout the project lifecycle. They therefore provide a natural interface between system architecture and risk documentation. Third, discussions with RBD specialists at Damen Naval confirmed that this phase offers the highest potential for digital integration, as the HAZID register is continuously updated and referred to in subsequent risk assessments, performance validation, and approval activities. It was also noted that, due to the long duration of the process, some rules for which equivalence had already been demonstrated were sometimes forgotten, or it was no longer clear how the equivalence had been achieved. Bringing the HAZID register into a model can also contribute to a solution for this problem.

The HAZID process forms the methodological core of this study. Supporting artefacts from adjacent phases are included for context:

- The **Reference Design** from the Design Basis phase (Step 3 of the RBD workflow), which provides the benchmark against which equivalence is demonstrated;
- The **Performance Criteria** from Step 5, which define measurable thresholds for demonstrating that risks have been reduced to acceptable levels;

- The **HAZID Register**, which consolidates hazard data and mitigation status throughout the design and approval process.

Together, these artefacts form a subset of the RBD workflow that can be realistically modelled within an MBSE environment, representing a bounded and high-impact integration domain.

The scope of the research is intentionally limited to the qualitative and semi-quantitative aspects of RBD. Fully quantitative risk assessments, such as PRA or MC simulations, are acknowledged as important but remain outside the scope of this work. Similarly, the regulatory approval process and its associated documentation (e.g., Safety Case, Statement of Approval of Design Basis) are not modelled.

From an organizational perspective, the study focuses on the technical and methodological integration between MBSE and RBD rather than on the socio-organizational or managerial aspects of adoption. Challenges related to stakeholder alignment, training, or process governance are recognized but not investigated in depth. This focus ensures that the research remains concentrated on the conceptual and practical feasibility of model-based integration.

Finally, the research is situated within the industrial context of Damen Naval, which serves as both the case study environment and the validation setting. The company's active use of MBSE (through the Arcadia/Capella toolchain) and its structured application of RBD (in compliance with IMO, DNV and classification guidelines) provide a realistic basis for testing the proposed integration. The insights derived from this case are intended to contribute both to Damen's internal design methodology and to the broader academic understanding of MBSE–RBD interoperability in the naval domain.

4.3. Research Design

The research design translates the strategic focus defined in Section 4.2 into a structured plan of execution. It defines how the integration of RBD artefacts into MBSE will be explored, demonstrated, and evaluated within the industrial environment of Damen Naval. Rather than testing a predefined hypothesis, this study follows an exploratory and iterative approach aimed at constructing understanding through practical modelling and expert reflection.

4.3.1. Overall approach

The research combines two complementary modes of inquiry: (1) *process analysis (Chapter 5)*, which maps how information currently flows through Damen's RBD workflow, and (2) *model experimentation (Chapter 6)*, which tests how selected RBD artefacts can be represented within an MBSE environment. This dual approach allows the study to both explain the current separation between risk and design information and demonstrate a potential pathway for their integration.

The project is structured as a mixed-method case study, conducted within the operational context of Damen Naval. The case study format allows the investigation of a complex, multi-stakeholder engineering process in its natural setting while maintaining methodological rigor through systematic data collection, traceable modelling steps, and expert validation. The experts involved include manager product development and innovation, senior engineers and a naval architect from Damen Naval, each with between 5 and 25 years of experience in ship design, risk assessment, or systems engineering.The overall aim is not to generalize statistically but to generate transferable insights about the feasibility and benefits of model-based risk representation.

4.3.2. Structure of the research

The work is divided into three main phases. These phases are summarized conceptually in Figure 4.2.

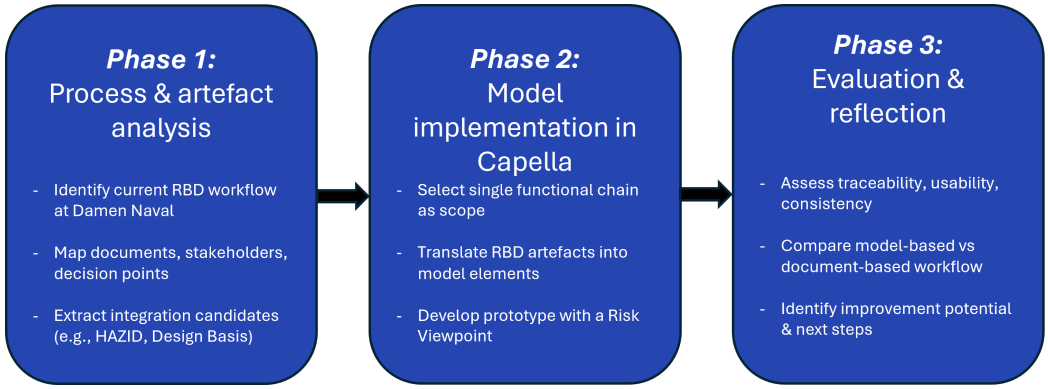


Figure 4.2: Overall structure of the research: from process analysis to model implementation and evaluation.

Phase 1 – Process and artefact analysis. This phase focuses on documenting how risk-related information is currently produced, exchanged, and validated during Damen's RBD process. Key artefacts (the design basis, reference design, HAZID report, and performance criteria) are collected and analyzed to understand their dependencies and information flow. Semi-structured interviews with RBD and MBSE specialists support this analysis by clarifying stakeholder roles and pain points. The outcome of this phase is a visual process map that highlights where the MBSE model could provide added value in terms of traceability and consistency.

Phase 2 – Model implementation in Capella. Based on the insights from Phase 1, selected artefacts (in particular the HAZID register, Reference Design elements, and performance criteria) are translated into a model-based representation. This is done within the Capella tool, which serves as Damen Naval's MBSE platform. The phase involves developing a prototype "Risk Viewpoint" that introduces dedicated model objects and relationships for hazards, mitigations, and acceptance criteria. The translation does not aim to fully automate the RBD process, but to test how qualitative risk data can be embedded within the architecture layers of an MBSE model in a traceable way. Intermediate results are discussed in review sessions with domain experts to refine both the conceptual mapping and its implementation.

Phase 3 – Evaluation and validation. The final phase assesses the feasibility and value of the proposed integration. Evaluation is performed qualitatively, through expert reviews and targeted workshops with MBSE and RBD practitioners. The assessment criteria include traceability between risk and design elements, clarity of the model representation, and expected benefits for future approval processes. The findings are synthesized into conclusions on how model-based integration can enhance risk visibility and reduce duplication across the RBD workflow. This final phase also reflects on the practical limitations observed during implementation and on potential extensions for future work, such as coupling quantitative analysis tools or embedding verification logic into the model.

4.3.3. Expected outcomes

Each phase contributes a specific output that collectively answers the research question:

- **Phase 1:** Structured description of the current RBD information flow and identification of integration opportunities.
- **Phase 2:** Prototype model in Capella representing selected RBD artefacts and demonstrating trace links between hazards, mitigations, and design elements.
- **Phase 3:** Expert evaluation results, outlining the feasibility, advantages, and limitations of embedding RBD information within MBSE.

4.4. Data Collection Methods

The research relies on multiple complementary data sources to ensure a understanding of both the existing RBD workflow and the potential for its integration into MBSE. Because the study is situated within an industrial context, the data collection process combines qualitative and technical inputs: expert knowledge,

documentary evidence, and model artefacts. Together, these sources enable triangulation between organisational practice, regulatory interpretation, and technical modelling feasibility.

4.4.1. Expert interviews

Semi-structured interviews will be conducted with specialists from three main domains within Damen Naval:

1. the RBD team responsible for risk assessment and regulatory compliance,
2. the MBSE and systems architecture team, and
3. project engineers and approval coordinators acting as interfaces with classification societies and flag administrations.

The interviews serve three purposes. First, to map the information flow and dependencies between risk documentation and system models. Second, to identify perceived inefficiencies, such as redundant data handling or inconsistent rule interpretations. Third, to explore the expectations and concerns of practitioners regarding model-based integration. The interview findings will be synthesised in the process-analysis phase and serve as input for the modelling experiment presented in Chapter 5.

Each interview follows a protocol consisting of thematic questions on workflow, tool usage, and collaboration practices. This format allows participants to elaborate on specific cases, such as recent alternative-design projects, while ensuring comparability across sessions. Interviews are documented through notes and will be permitted, anonymised transcripts. Recurring concepts identified in the interviews and internal RBD documentation are grouped into thematic categories to support later process analysis and guide their translation into model elements.

4.4.2. Document and artefact analysis

Document analysis forms the second major data source. It provides factual grounding for understanding how RBD information is currently generated, formalised, and exchanged within Damen Naval. The material to review includes:

- RBD documentation such as Design Basis and Reference Design reports, HAZID templates, and performance-criteria tables;
- internal procedures and guidelines defining the approval sequence and interactions with authorities (e.g., DNV, COMMIT);
- relevant IMO circulars and regulatory frameworks (MSC/Circ. 1002, MSC.1/Circ. 1212, MSC.1/Circ. 1455);
- MBSE artefacts such as system-architecture models, requirement databases, and Capella viewpoints currently in use.

These documents will be examined to extract recurring structures (inputs, outputs, and dependencies) that could later be represented as model relationships. Particular attention will be paid to the HAZID registers and their life-cycle updates, as these embody the continuity of risk information throughout the design process. By cross-referencing the interview data with document content, inconsistencies or data gaps will be identified, clarifying where model-based traceability could reduce manual reconciliation.

4.4.3. Modelling data

A third category of data arises from the modelling experiment itself. The proof-of-concept developed in Capella produces artefacts such as model elements, relationships, and viewpoints that serve as both analytical data and research output. During the translation of RBD artefacts into model objects, observations can be recorded regarding representational choices, tool constraints, and user-interface limitations. These modelling logs, together with exported diagrams and metadata tables, provide empirical evidence for evaluating the feasibility and usability of the proposed integration (see Section 4.6).

4.4.4. Data validation and triangulation

To ensure reliability and internal validity, findings from different data sources will be cross-checked iteratively. Preliminary interpretations from interviews are verified against official templates and reports; conversely, ambiguous document content will be clarified through follow-up discussions with experts. Intermediate model representations will also be reviewed by stakeholders from both the RBD and MBSE domains to

confirm factual accuracy and practical relevance. This triangulated approach strengthens the credibility of the conclusions by combining practitioner insight with traceable documentary and modelling evidence.

4.5. Modelling Experiment Setup

The modelling experiment represents the practical core of this research. Its purpose is to test, in a controlled but realistic setting, how selected artefacts from the RBD workflow can be represented and maintained within an MBSE environment. The experiment builds directly on the findings from the process and artefact analysis (Section 4.3) and the data collected from interviews and documentation (Section 4.4). It focuses on three key elements identified as most suitable for integration: the *Reference Design*, the *performance criteria*, and the *HAZID register*.

4.5.1. Tool environment

The experiment is conducted in Capella, Damen Naval's standard MBSE tool based on the Arcadia method. Capella provides a layered modelling framework (Operational, System, Logical, and Physical Architecture) and supports viewpoints, making it suitable for representing non-standard artefacts such as risk data. The proof-of-concept uses Capella version 6.0 with the Kitalpha Viewpoint Designer add-on to define a dedicated *Risk Viewpoint*. This viewpoint allows hazards, mitigations, and performance criterion to be instantiated as first-class model elements and linked to existing architecture components and requirements.

The modelling experiment follows a contained, sandbox approach: rather than modifying an ongoing Damen project, a representative subset of system functions is recreated to provide a safe test environment. This ensures that the experiment reflects the structure and complexity of real ship designs without interfering with confidential or classified project data. It is important that the model focuses on a single functional chain. This is a continuous sequence of functions that realizes a specific capability. Working at this level of detail allows for a meaningful connection between architectural elements and risk artefacts, providing enough granularity to capture dependencies without losing focus in system-wide complexity.

4.5.2. Scope of the model

The model scope reflects the integration focus defined in Section 4.2. It includes three interrelated artefact categories:

- **Reference Design layer:** Captures the baseline configuration of the system or subsystem under analysis. This serves as a benchmark for evaluating deviations in the risk-based process. Each element in this layer corresponds to a verified component or function within an existing design, establishing the link between conventional rule compliance and innovative alternatives.
- **Performance Criteria layer:** Defines measurable attributes or safety thresholds used to judge equivalence. Examples include maximum allowable temperature rise, flooding survival time, or probability of functional failure. These criteria are modelled as parameterised properties within Capella, connected to relevant system functions or physical components.
- **HAZID layer:** Represents the main risk artefact. Each hazard is defined as a model object with attributes for cause, consequence, likelihood, and mitigation. Hazards are linked to the architecture elements they affect (e.g., compartments, systems, or operational modes) and to performance criteria that quantify their acceptance. The resulting network of relationships provides a traceable chain from design decisions to risk evidence.

4.5.3. Implementation approach

The implementation proceeds through four sequential steps:

1. **Schema definition:** The meta-model is extended with new classes (Hazard, Mitigation, and Performance Criterion). Each class is defined with relevant attributes (e.g., likelihood, severity, verification status) and relationships to standard Arcadia elements such as Function, Component and Requirement. This structure is implemented in the Kitalpha Viewpoint Designer and deployed as a Capella add-on.
2. **Model population:** Sample data from Damen's internal HAZID templates and performance-criteria tables are transcribed into the model. Each hazard is linked to its associated system function and

the relevant performance threshold. Reference Design components are identified to indicate which hazards are already covered by existing compliance evidence.

3. **Visualization and navigation:** Custom diagrams are created to visualise the interconnections between hazards, mitigations, and architecture elements. These include matrix views linking hazards to affected functions and graphical overlays indicating coverage or equivalence achievement. The goal is to demonstrate how users could navigate from design elements to their corresponding risk information directly within the MBSE environment.
4. **Model validation and iteration:** The prototype is reviewed in short sessions with domain experts from the MBSE and RBD teams. Their feedback guides refinements to the viewpoint definitions, attribute naming, and visualization clarity. This iterative process ensures that the prototype aligns with actual workflows and terminology used at Damen Naval.

4.5.4. Evaluation setup

The final prototype serves as the primary artefact for evaluation (see Section 4.6). Evaluation focuses on three key subquestions:

- Does the model structure provide clear traceability between design elements and risk evidence?
- Can the risk information be maintained and updated efficiently as the design evolves?
- Does the integrated representation support stakeholder understanding and reduce reliance on document-based tracking?

During evaluation, screenshots, traceability matrices, and navigation sequences are recorded as empirical data. These outputs not only demonstrate technical feasibility but also support qualitative feedback on usability and workflow integration.

In summary, the modelling experiment tests the core assumption of this research: that qualitative RBD artefacts can be embedded and managed within an MBSE framework in a way that strengthens consistency, traceability, and assurance throughout the design lifecycle.

4.6. Evaluation Method

The evaluation phase assesses to what extent the proposed model-based representation of RBD artefacts effectively addresses the integration challenges identified in Chapter 3. Rather than measuring quantitative performance, the evaluation focuses on qualitative indicators of feasibility, usefulness, and alignment with industrial practice. This approach is consistent with the exploratory nature of the research, which aims to generate insights on process integration and methodological fit rather than on statistical validation.

4.6.1. Evaluation objectives

The evaluation is guided by three overarching objectives:

1. **Feasibility:** Determine whether qualitative RBD information can be represented in a structured and traceable way within an MBSE environment.
2. **Usability:** Assess whether the resulting model supports intuitive navigation, reduces duplication of information, and provides added value for engineers and approval stakeholders compared to current document-based workflows.
3. **Integration potential:** Evaluate whether the model structure can be maintained throughout the design lifecycle and interfaced with existing RBD and MBSE processes within Damen Naval.

Together, these objectives translate the high-level research question namely how RBD and MBSE can be integrated to accelerate innovation into tangible evaluation dimensions that can be assessed through expert judgement and artefact analysis.

4.6.2. Evaluation procedure

The evaluation follows a structured, two-stage procedure combining expert review sessions and analytical assessment of the model artefacts.

Stage 1 – Expert review sessions. A series of short, focused sessions is conducted with representatives from Damen's RBD, MBSE, and Approval Coordination teams. During each session, the prototype model

is demonstrated interactively, allowing participants to explore the implemented Risk Viewpoint, navigate trace links, and inspect hazard data within the Capella environment. Participants are invited to comment on three aspects:

- Conceptual alignment with their existing workflow (e.g., correspondence with HAZID templates and performance criteria);
- Practical usability of the model, including ease of navigation, data visibility, and terminology consistency;
- Perceived benefits and limitations for real-world application.

Stage 2 – Analytical model assessment. In parallel, the prototype itself is analysed using objective criteria derived from MBSE best practices and traceability metrics. These include:

- *Traceability completeness:* the proportion of hazards, mitigations, and performance criteria correctly linked to their corresponding architecture elements;
- *Model consistency:* absence of orphaned elements, redundant links, or inconsistent naming across model layers;
- *Update propagation:* ability of the model to automatically reflect changes in system structure or performance requirements;
- *Transparency:* clarity of visualisation and accessibility of information for non-technical stakeholders.

These indicators provide a semi-formal means of validating the conceptual soundness of the prototype and complement the qualitative feedback gathered from experts.

4.6.3. Evaluation criteria and interpretation

The evaluation combines qualitative and analytical results to answer three key subquestions, aligned with the research objectives:

Table 4.1: Evaluation criteria and interpretation framework.

Criterion	Evaluation Subquestion	Interpretation of Positive Outcome
Feasibility	Can RBD artefacts be modelled within Capella without loss of essential meaning?	The prototype accurately represents hazards, mitigations, and performance criteria in a structured way, maintaining their logical relationships to system architecture.
Usability	Does the model structure improve understanding and reduce reliance on static documentation?	Users can intuitively navigate between design and risk information, perceive improved overview, and consider the approach applicable in future projects.
Integration Potential	Can the proposed structure be maintained and scaled within Damen's existing MBSE processes?	The model structure aligns with existing viewpoints and data exchange formats, and experts recognise opportunities for extending it toward quantitative analysis or approval documentation.

Interpretation follows an exploratory evaluation logic: positive responses to these questions do not imply full integration readiness but indicate conceptual and practical feasibility. Limitations, contradictions, or unanticipated difficulties identified during the sessions are equally valuable, as they inform the discussion in Chapter 8 on potential extensions and research directions.

4.6.4. Validity considerations

Several measures are taken to enhance the reliability and validity of the evaluation. Expert sessions include participants from different functional backgrounds to ensure multiple perspectives. Technical, procedural and regulatory are represented. Feedback is collected using a consistent structure and coded

immediately after each session to minimise interpretation bias. The use of real artefacts (HAZID templates, performance tables) ensures ecological validity by maintaining a direct link to Damen's operational practice. Finally, all conclusions are grounded in triangulated evidence across expert insights, document content, and model observations, ensuring that findings are both credible and transferable.

4.7. Summary

This chapter has outlined the research plan and methodological approach adopted to explore how RBD artefacts can be represented and maintained within an MBSE environment. The chapter defined a structured sequence of activities designed to translate qualitative risk information into model-based representations that can support traceability, consistency, and lifecycle assurance.

The research proceeds in several interconnected stages. First, the current RBD workflow at Damen Naval is analysed to identify where risk-related information is generated, how it is documented, and how it evolves during the approval process. This phase clarifies the data dependencies between Design Basis documents, Reference Designs, performance criteria, and HAZID registers. Second, these insights are used to develop a proof-of-concept model in Capella, focusing on the artefacts that exhibit the highest integration potential (Reference Design, performance criteria, and HAZID register.) The prototype introduces a dedicated *Risk Viewpoint* in Capella, enabling hazards and mitigations to be linked directly to architecture elements and system requirements. Finally, the resulting model is evaluated through expert review sessions and structured artefact analysis to assess feasibility, usability, and integration potential.

5

Phase 1 - Analysis

This chapter addresses Research Question 4 : How can this combined MBSE-RBD approach be implemented and tested using a representative design case?

5.1. Introduction to the analysis Phase

The purpose of Phase 1 is to build a structured understanding of the current RBD workflow within Damen Naval and to identify where the process, its artefacts, and its associated information flows show structural limitations. This analysis forms the foundation for the model-based approach developed in later phases of this thesis.

This phase focuses on three core artefacts of the RBD process:

- **The Reference Design** – the baseline concept against which innovative or alternative design proposals are assessed.
- **The HAZID artefact** – the primary vehicle for identifying hazards, hazardous events, causes, consequences, and mitigations.
- **Performance Criteria** – the acceptance criteria that determine whether a design configuration is tolerable, equivalent to prescriptive requirements, or requires additional mitigation.

These artefacts form the backbone of the qualitative part of the RBD trajectory and directly influence the ability of Class (DNV) and Flag administrations to review and approve novel design solutions.

Phase 1 integrates three types of sources:

- Internal Damen documentation, including HAZID tables, meeting minutes, design assumptions, and process descriptions.
- External regulatory and verification feedback, most notably early review statements from DNV.
- Industry and academic references, including MBSE safety analyses, model-based hazard frameworks, and digital engineering trends.

By triangulating these perspectives, this phase evaluates both the content and the structure of existing artefacts, identifies systemic issues, and analyses why the RBD workflow experiences iteration cycles, inconsistencies, and delays. The goal is not to critique individual documents, but to understand the underlying patterns that limit efficiency and traceability.

The findings of Phase 1 lead directly to a structured set of requirements for an MBSE-supported RBD approach in Phase 2.

5.2. Current RBD Process at Damen Naval

5.2.1. Overall Structure of the RBD Workflow

The RBD workflow at Damen Naval is based on the IMO MSC.1/Circ.1455 framework for evaluating alternative design and arrangements. As such, it follows a systematic, stepwise procedure:

1. Establish the regulatory basis

2. Define the prescriptive and alternative design scope
3. Develop the Reference Design
4. Perform HAZID
5. Evaluate consequences and performance criteria
6. Identify risk control measures
7. Define the engineering analysis needed for equivalence
8. Perform quantitative assessments (as required)
9. Submit evidence to Class and Flag for review and approval

Within this process, the design team, Class society (DNV), Flag administration, safety specialists, and domain experts collaborate iteratively. Each step generates documents and data that feed into the next step, with the intention of progressively building a justified safety case.

5.2.2. Steps Relevant to This Thesis

Although the full RBD process spans the entire design justification pathway, this thesis focuses specifically on Steps 3, 4, and 5, where most qualitative reasoning occurs and where the largest challenges emerge.

Step 3 — Reference Design Definition
The Reference Design provides the baseline vessel or system configuration against which the alternative concept is evaluated for equivalence. In practice, this includes:

- Regulatory mapping
- Assumptions regarding materials, safety systems, and arrangements
- Applicable prescriptive requirements
- Design features serving as safety barriers
- Operational assumptions used later in the HAZID

In Damen's workflow, the Reference Design is typically captured in one or more Preliminary Design Documents. These documents evolve rapidly through review iterations and must remain aligned with subsequent safety analyses.

Step 4 — HAZID
The HAZID is executed early to identify hazards, hazardous events, initiating causes, consequences, and initial risk control measures. Workshops are guided by IMO methodology and produce a structured hazard table (see table 5.1) listing:

- Hazards and events
- Initiating causes
- Consequences and severity
- Likelihood estimates
- Existing safeguards
- Recommendations for further action

The HAZID is qualitative by nature and serves as input for developing performance criteria and further risk assessments. Its accuracy and completeness determine the validity of downstream design justifications.

Table 5.1: Key HAZID artefacts and their role and content.

Artefact	Role in process	Main content (according to MTF)
Input document set	Basis for workshop	GA, hazardous area plan, equipment layouts, operating/control/shutdown philosophy, area specific arrangement.
Node list	Structuring of analysis	Optionally utilities as separate node or as hazard.
Terms of Reference (ToR)	Upfront alignment and scoping	Purpose & scope, design description, specific hazards, method, guidewords, risk matrix & criteria, node definition, worksheet template, planning, names/roles/experience of team members.
HAZID worksheet(s)	Core record of the workshop	Per node: Hazard, Hazardous event, Cause, Consequence(s), Safeguards, Consequence level (A–C), Likelihood level (1–5), Risk ranking (Low/Med/High), Action, Responsible.
Risk matrix + criteria	Uniform assessment	3 consequence levels (A–C) × 5 likelihood levels → Low / Medium / High risk, including criteria for when something is acceptable/tolerable/unacceptable and what triggers an ALARP requirement.
HAZID report	Formal justification	Executive summary, scope, system overview, method, team, results (including discussion of high risks), conclusions (ALARP), action list, appendices (worksheets, ToR, input documents).
Action / follow-up register	Ensuring ALARP	Action number, description, link to hazard, responsible person, due date, status, evidence of completion, sign-off.

Step 5 — Performance Criteria & Qualitative Risk Assessment
Performance criteria articulate the conditions under which hazards are considered tolerable or equivalent to prescriptive requirements. These criteria include:

- Acceptable consequences
- Acceptable detection and response times
- Functional performance of barriers
- Limits on fire spread, smoke, heat, or structural degradation
- Performance criteria play a central role in determining whether the alternative design meets ALARP principles and regulatory expectations.

5.2.3. Observed Practical Limitations in the Current Workflow

Analysis of internal documents, review statements, and workshop notes reveals structural issues in how these steps are implemented in practice:

- **Fragmented information flow**
  Artefacts such as the Reference Design, HAZID, system drawings, and performance notes are stored in separate documents that evolve independently.
- **Iterative, document-based revision cycles**
  DNV and Flag reviews frequently reveal inconsistencies between design assumptions and hazard assessments, requiring repeated updates.

- **Lack of traceability**
  Relationships between hazards, functions, mitigations, and design elements are implicit rather than formally captured.
- **Heavy dependence on expert knowledge**
  The outcome of a HAZID session strongly depends on who is present, leading to inconsistent levels of detail across compartments and systems.
- **Loss of information between steps**
  Workshop discussions, assumptions, and rationales often remain undocumented or are not represented in formal artefacts.

These limitations lead to delays, ambiguity in approvals, and increased verification effort. This forms the rationale for exploring a model-based alternative in later phases.

5.3. Artefact Analysis

This section analyses the three core artefacts that define the early stages of the RBD workflow at Damen Naval: the Reference Design, the HAZID, and the Performance Criteria. These artefacts provide the qualitative foundation for alternative design justification and influence the efficiency and traceability of the overall approval process. The findings presented here are based on internal Damen documentation (including the HAZID table, design reports, and meeting of minutes), the DNV Preliminary Verification Statement, and international HAZID/MBSE guidelines.

5.3.1. Reference Design (Step 3)

Purpose and content

The Reference Design serves as the prescriptive baseline against which the alternative design is evaluated. It consolidates regulatory mappings, material assumptions, layout and arrangement features, fire protection measures, and operational assumptions. In practice, this artefact is recorded across multiple Preliminary Design Documents (e.g., Versions A and B), which evolve through iterative review cycles with Class and Flag.

Findings

Analysis of the Damen documentation reveals several structural limitations:

- **Inconsistencies across documents.** Layout drawings, ventilation plans, and boundary classifications show discrepancies, as reflected in both the DNV Preliminary Verification Statement and the Bluenose workshop minutes.
- **Ambiguity in baseline assumptions.** It is not always clear which prescriptive requirements or design features form the normative basis for equivalence assessment.
- **Lack of explicit “state-of-the-art” definition.** Different stakeholders interpret the prescriptive baseline differently, complicating the equivalence argument.
- **Missing traceability.** Many design assumptions used in the HAZID (e.g., fire boundaries, number of nozzles, detection times) are not explicitly linked to architecture elements or requirements.

Implications

The absence of a stable, traceable Reference Design undermines the consistency of subsequent hazard identification and performance evaluation. As a result, review cycles with DNV become iterative and time-consuming. A model-based representation can stabilise baseline information and ensure its reuse throughout the RBD process.

5.3.2. HAZID Artefact (Step 4)

Purpose and structure

The HAZID is the primary qualitative risk assessment step. It identifies hazards, hazardous events, initiating causes, consequences, safeguards, risk levels (severity and likelihood), and recommended actions. The formal output is captured in the *HazIdBN* document, supported by workshop discussions summarised in the minutes of meeting.

Findings
The analysis shows several recurring issues. All of them will be adressed:

- **Inconsistent level of detail.** Some compartments contain extensive hazard chains while others list only one or two hazards, indicating dependence on workshop participants rather than a standardised structure.
- **Non-normalised hazard descriptions.** Hazards interchangeably describe states, events, failure modes, or effects, reducing comparability and undermining downstream analysis (in scope).
- **Subjective and untraceable risk ratings.** Severity and likelihood assessments lack documented rationale or connection to defined acceptance criteria.
- **Mitigations not systematically linked to system functions.** Many safeguards refer to operational actions (e.g., crew response) rather than functional capabilities of the design.
- **Workshop context is lost.** The MoM contains important assumptions and clarifications that are not reflected in the HAZID table, causing loss of information between process steps.
- **No modelling of hazard propagation.** Dependencies between compartments, ventilation zones, and systems are not captured in the HAZID, limiting its system-wide validity.

Implications
These limitations reduce the robustness of the HAZID as input for performance criteria and equivalence justification. The lack of a structured, traceable hazard model is a central bottleneck in the RBD process and motivates the development of a model-based hazard viewpoint.

5.3.3. Performance Criteria (Step 5)

Purpose and content
Performance Criteria define the conditions under which hazards and scenarios are considered acceptable, and when additional mitigation is required to achieve equivalent safety. They typically cover structural performance, detection and response times, fire spread limits, smoke and heat thresholds, and ALARP-based acceptability.

Findings
Across all analysed documents, Performance Criteria are found to be:

- **Largely absent or implicit.** No explicit, formalised criteria are documented in the HAZID or related artefacts.
- **Not linked to hazards or design functions.** Criteria are not traceable to specific scenarios, barriers, or functional elements.
- **Inconsistent or insufficient for equivalence demonstration.** DNV notes in multiple comments that performance criteria are incomplete or lack quantitative thresholds.
- **Not aligned with prescriptive requirements.** There is no clear mapping between performance expectations and the prescriptive baseline.

Implications
Without explicit performance criteria, ALARP evaluations and equivalence arguments cannot be substantiated. This creates significant uncertainty in the approval trajectory and contributes to repeated review cycles. A model-based representation can make such criteria explicit, structured, and traceable.

5.4. Synthesized Findings

The analysis of the three core artefacts in Steps 3–5 of the RBD workflow (Reference Design, HAZID, and Performance Criteria) reveals a consistent pattern of structural limitations. These limitations do not stem from individual mistakes or isolated oversights; rather, they reflect systemic characteristics of a document-driven, expert-dependent, and weakly integrated design process. This section synthesises the cross-cutting issues observed across all artefacts and examines their implications for the broader RBD trajectory.

5.4.1. Recurring Issues Across Artefacts

Lack of consistency between documents
The Reference Design, HAZID, drawings, fire boundary classifications, and workshop outputs often contain conflicting information. Such inconsistencies were repeatedly highlighted in both the DNV Preliminary Verification Statement and the Bluenose meeting minutes. This undermines the reliability of downstream scenario evaluations and makes verification effort-intensive.

Fragmentation of information
Critical safety-relevant information is spread across Word documents, Excel sheets, drawings, emails, presentations, and workshop minutes. No formal mechanism exists to ensure synchronisation or visibility of dependencies between artefacts. As a result, design assumptions made in Phase 3 do not consistently propagate into the HAZID or later performance evaluations.

Limited traceability
Relationships between hazards, initiating causes, functions, components, and design assumptions are not explicitly captured. This absence of traceability makes it difficult to justify why certain hazards are included or omitted, how mitigating measures relate to functional capabilities, or how performance expectations derive from prescriptive requirements. Traceability gaps were a central concern raised by DNV during preliminary review.

Loss of contextual information
The HAZID table captures only a fraction of the reasoning expressed during the workshop. Assumptions, uncertainties, and interpretative nuances recorded in the minutes are not reflected in the formal artefacts. This leads to incomplete insight into scenario logic and threatens reproducibility in subsequent design stages.

Subjective and unstructured risk evaluation
Severity and likelihood ratings in the HAZID lack supporting criteria or documented rationale. Without explicit performance criteria or common thresholds, these assessments become expert-dependent and inconsistent, limiting their value for equivalence justification.

Dependence on individual expertise
The level of detail and quality of hazard identification varies strongly depending on which domain experts participate. Compartments analysed with different teams show substantial variation in depth, scope, and hazard definition style, reflecting a structural reliance on tacit knowledge rather than a standardised method.

Lack of system-level understanding
Hazards are identified per compartment without systematic modelling of inter-compartment interactions, ventilation effects, cascading failures, or system-level dependencies. As a result, emergent behaviours—critical for fire safety—remain outside the scope of the artefacts.

5.4.2. Impact on RBD Approval and Verification

These recurring issues collectively weaken the reliability, traceability, and justifiability of the evidence required for alternative design approval. The consequences observed in Damen documentation and review feedback include:

- **Repeated review iterations with DNV and Flag**. Missing or unclear information often forces the design team into additional cycles of revision, delaying the approval trajectory.
- **Difficulty demonstrating equivalence**. Without explicit performance criteria and consistent hazard logic, equivalence to the prescriptive baseline becomes difficult to justify.
- **Increased uncertainty**. Ambiguous assumptions and inconsistent artefacts introduce uncertainty in both the qualitative and quantitative parts of the RBD process.
- **Risk of omissions**. Fragmented artefacts increase the risk that critical hazards, interactions, or assumptions remain unaddressed.
- **Limited reusability**. Because artefacts are not structured or normalised, insights from one RBD project cannot be reused efficiently in subsequent projects.

5.4.3. Structural Nature of the Problems

The issues identified are not isolated failures of individual artefacts but they stem from intrinsic limitations of a document-based approach:

- Each artefact is created in a different tool with different structures.
- Dependencies between artefacts are implicit rather than enforced.
- Version control applies to documents, not to underlying system semantics.
- Safety reasoning depends heavily on tacit, undocumented expert knowledge.
- The process lacks mechanisms for verifying internal consistency.

Consequently, improving individual artefacts cannot fully resolve these challenges. A more fundamental shift is required toward a model-based approach that integrates architecture, hazards, performance criteria, and design assumptions into a coherent, traceable system model. This motivates the development of the model-based framework introduced in Phase 2.

5.5. Rationale for a Model-Based RBD Approach

The synthesized findings from the analysis of the Reference Design, HAZID, and Performance Criteria (Sections 5.3–5.4) indicate that the main limitations in the current RBD workflow are structural rather than incidental. These limitations arise from the inherent characteristics of a document-driven process: fragmented information, implicit dependencies, lack of formal traceability, and loss of contextual reasoning. This section provides the rationale for transitioning toward a model-based approach in Phase 2, focusing on the capabilities needed to address the shortcomings identified in Phase 1.

5.5.1. Structural Shortcomings of the Current Workflow

The analysis revealed that the current RBD artefacts suffer from three fundamental limitations:

1. **Lack of integration across artefacts.** The Reference Design, HAZID, and Performance Criteria evolve independently. Assumptions made in one artefact are not consistently propagated into the others, resulting in mismatches identified by Class and Flag.
2. **Absence of explicit system semantics.** Hazards, functions, boundaries, compartments, and performance assumptions are described textually rather than structurally. As a consequence, dependencies between system behaviour and hazard scenarios remain implicit and difficult to verify.
3. **No mechanism for ensuring internal consistency.** Document-based workflows cannot automatically detect inconsistencies between system drawings, hazard descriptions, mitigation logic, or acceptance criteria. This contributes to repeated revision cycles and delayed approval.

These issues are systemic and cannot be solved by improving individual documents. A higher level of formalism is required to ensure that hazard logic, design assumptions, and performance expectations are coherent and traceable across the entire RBD workflow.

5.5.2. Need for a Formal, Traceable Representation

A model-based representation enables the explicit capture of system behaviour, hazard relationships, assumptions, and performance expectations in a structured and interconnected way. Such an approach is expected to address the structural shortcomings identified earlier by providing:

- **A single source of truth.** Architectural elements, functions, hazards, and criteria can be managed in one integrated model rather than in separate documents.
- **Formalised semantics.** Hazards, events, causes, consequences, and mitigations are represented using well-defined modelling concepts instead of free-text descriptions, improving clarity and reproducibility.
- **Explicit traceability.** Links between hazards, system functions, design elements, and performance criteria can be encoded explicitly, supporting verification and impact analysis.
- **Consistency-by-construction.** The model enforces structural consistency across interpretations of boundaries, system behaviour, and hazard logic, reducing ambiguity during review.

- **Support for iterative refinement.** As the design evolves, updates propagate through the model systematically, minimising the risk of outdated or conflicting artefacts.

These capabilities correspond directly to the issues encountered in Damen's current RBD process and form the motivation for developing a model-based solution.

5.5.3. Expected Benefits for RBD

A model-based approach has the potential to improve the RBD workflow in several ways:

- **Improved alignment between Reference Design and hazard analysis.** Assumptions, boundaries, and design features become explicitly linked to the hazards and scenarios that depend on them.
- **More rigorous and transparent hazard logic.** Structured modelling of causes, events, and consequences reduces subjectivity and enhances reproducibility of the HAZID.
- **Explicit and traceable performance criteria.** Performance expectations can be formalised and linked to hazards, enabling a more defensible equivalence argument.
- **Reduced iteration loops during review.** Because the model provides internal consistency and clear traceability, review comments from Class and Flag are easier to address and less likely to trigger conflicting updates.
- **Foundation for quantitative analysis.** A structured hazard model provides a stable basis for downstream simulation and quantitative risk assessment.

5.5.4. Findings, implications and possible solution

The HAZID session for the Bluenose case revealed several recurring issues in the way RBD artefacts are produced, interpreted, and connected. These issues span from baseline ambiguity to fragmented data handling, and together they explain why consistent ALARP decisions and traceability remain difficult. Table 5.2 below summarises the main findings, their implications for risk-based decision-making, and the corresponding MBSE-enabled solutions.

Table 5.2: Findings from Bluenose HAZID meeting, its implications and MBSE solution.

Theme	Finding	Implication	MBSE solution
Reference Design	Uncertain baseline selection	No clear comparison with alternative designs possible	Model structural baseline scenario
HAZID quality	Discussions not recorded in worksheet	Context gets lost	Hazard viewpoint with annotations
Performance Criteria	Vague or undefined	No ALARP decisions possible	Criteria model with explicit linkage to hazards and design states
Document inconsistencies	FIP/FCP inconsistent	Extra iterations and higher risk of mistakes	Unified architecture model
Data fragmentation	Action list large and spread across artefacts	No integrated view on risk status and follow-up	Repository-based modelling

5.5.5. Conclusion

The structural shortcomings identified in Phase 1 justify exploring a model-based approach to RBD in Phase 2. By integrating key RBD artefacts into a unified system model and formalising the relationships between hazards, design functions, and performance criteria, the model-based approach aims to improve coherence, traceability, and efficiency in the approval of innovative naval design solutions.

5.6. Requirements for Phase 2: Model-Based Representation

The findings of Phase 1 highlight the need for a structured, model-based representation of key RBD artefacts to address issues of inconsistency, fragmentation, and lack of traceability in the current workflow. This section defines the requirements for Phase 2, where a model-based framework will be developed and validated using a representative testcase. The requirements are grouped into two categories:

1. conceptual requirements for the modelling framework (metamodel), and
2. process requirements for integrating the model-based approach into the RBD workflow.

5.6.1. Conceptual Requirements for the Metamodel

The metamodel used in Phase 2 shall provide the formal modelling concepts necessary to capture hazards, design assumptions, system behaviour, and performance expectations in a coherent and traceable structure. Based on the artefact analysis and synthesized findings, the following requirements are defined:

CR1: **Hazard Representation.** The model shall include explicit concepts for hazards, hazardous events, initiating causes, and consequences, with consistent semantics across all compartments and systems.

CR2: **Scenario Modelling.** The model shall support the representation of hazard propagation and event-consequence chains, including interactions between compartments, systems, and operational states.

CR3: **Link to System Architecture.** Hazards and scenarios shall be traceable to architectural elements such as functions, components, boundaries, and system behaviours.

CR4: **Traceable Design Assumptions.** The model shall allow explicit documentation of baseline and alternative design assumptions.

CR5: **Risk Control Measures (RCMs).** Mitigations shall be represented explicitly and linked to system functions, components, or operational actions, enabling systematic evaluation of their effectiveness.

CR6: **Performance Criteria.** The model shall include formal concepts for performance criteria, enabling their linkage to hazards, scenarios, and design elements.

CR7: **Requirements Traceability.** Functional and performance requirements shall be linked to their corresponding architectural and hazard-related elements.

CR8: **Consistency Constraints.** The metamodel shall support structural rules or constraints to ensure internal consistency (e.g., each hazard must have a cause, consequence, and associated criterion).

5.6.2. Process Requirements for Integration

To ensure that the model-based representation aligns with the practical demands of the RBD workflow, the following process requirements are defined:

PR1: **Input Alignment.** The modelling approach shall accept structured inputs from existing artefacts, including Reference Design documentation, HAZID workshops, and preliminary criteria notes.

PR2: **Stakeholder Transparency.** The model shall facilitate interpretation by domain experts (e.g., safety engineers, designers, and Class reviewers) through clear viewpoints and navigable structure.

PR3: **Iterative Refinement.** The modelling framework shall support updates as the design evolves, ensuring that changes propagate consistently across linked elements.

PR4: **Review Support.** The model shall provide traceable evidence to support discussions and verification activities with DNV and Flag administrations.

PR5: **Reusability.** Model structures, hazard templates, and performance criteria shall be reusable for future RBD projects, reducing effort and increasing standardisation.

PR6: **Compatibility with Existing Toolchains.** The model-based solution shall be implementable in a modelling environment available within Damen Naval (Capella), without requiring disruptive changes to the existing workflow.

PR7: **Output for Downstream Analyses.** The structure of the model shall support extraction of information for subsequent quantitative analysis or simulation where applicable.

5.6.3. Summary

The requirements defined in this section translate the structural shortcomings identified in Phase 1 into concrete modelling needs for Phase 2. Together, they form the basis for the development of a model-based RBD framework capable of supporting consistent hazard reasoning, explicit traceability, and clearer justification of alternative design solutions.

5.7. Summary of Phase 1

Phase 1 provided a structured analysis of the current RBD workflow at Damen Naval, focusing on the three artefacts underpinning the alternative design process: the Reference Design, the HAZID, and the Performance Criteria. The analysis was based on internal documentation, Class review statements, workshop outputs, and hazard identification guidelines.

The results indicate that observed limitations are structural rather than incidental. The Reference Design lacks consistent definition and traceability, the HAZID exhibits non-normalised hazard structures and loss of context, and explicit Performance Criteria are largely absent. Across all artefacts, fragmented information, document inconsistencies, reliance on tacit knowledge, and weak traceability between hazards, design assumptions, and system functions were identified.

These structural shortcomings introduce uncertainty into the approval process and contribute to iterative revisions with Class and Flag administrations. The findings suggest that incremental improvements to individual artefacts are insufficient; the underlying issue is the absence of an integrated and traceable representation of risk and system behaviour.

By translating these insights into conceptual and process requirements for a model-based framework (Section 5.6), Phase 1 establishes the foundation for the structured model implementation and evaluation carried out in Phase 2 which will be adressed in chapter 6.

6

Phase 2 - Model implementation

This chapter continues on addressing Research Question 4 : How can this combined MBSE-RBD approach be implemented and tested using a representative design case?

6.1. Purpose and scope of Phase 2

Phase 1 resulted in a set of requirements for integrating RBD artefacts into a MBSE environment. These requirements were derived from an analysis of current RBD practices and the limitations observed when risk information is captured primarily through document-based artefacts. Phase 2 addresses these requirements by implementing a model-based representation in Capella, following the Arcadia method.

The objective of Phase 2 is not to develop a complete system model of a vessel, but to demonstrate how risk-related information can be embedded within a functional design model in a structured and traceable manner. The focus is therefore on showing how hazards, acceptance criteria, and ALARP considerations can be represented as explicit model elements and linked directly to system behaviour.

To keep the implementation focused and verifiable, a single representative functional chain is selected as a pilot case: the bunkering scenario. This functional chain was chosen because it involves multiple operational handovers between ship and shore, clearly defined start and stop conditions, and several safety-critical functions such as valve control, fuel flow management, and measurement. These characteristics make it well suited to demonstrate the integration of RBD artefacts at functional level.

The scope of Phase 2 is defined as follows:

- Implementation of a functional chain for the bunkering scenario in the System Analysis layer.
- Definition and integration of Hazard objects associated with individual functions, including qualitative risk attributes such as likelihood, consequence class, risk ranking, and ALARP summary.
- Definition of Criteria objects representing measurable acceptance conditions and linking these to relevant functions and architectural elements.
- Creation of a dedicated risk-aware view in which hazards are visible in direct relation to the functional chain.

This chapter describes how the Phase 1 requirements are translated into concrete model constructs and how the model is structured to support risk-based reasoning. The evaluation of the implemented approach, including its benefits and limitations, is addressed in the subsequent chapter.

6.2. Model structure and placement within Arcadia

The implementation of Phase 2 is aligned with the Arcadia method and focuses primarily on the System Analysis layer. This layer was selected because it provides the most appropriate abstraction level for representing system behaviour, functional interactions, and operational sequences, which are central to HAZID-style risk identification. At this stage of the design, risks are typically associated with what the system does rather than with detailed component implementations.

6.2.1. Functional Chain

The model is therefore structured around a functional chain defined in the System Analysis layer, representing the bunkering scenario. The methanol system gives raise to two system actors: The bunker loading team and the fuel supplier (see figure 6.1).

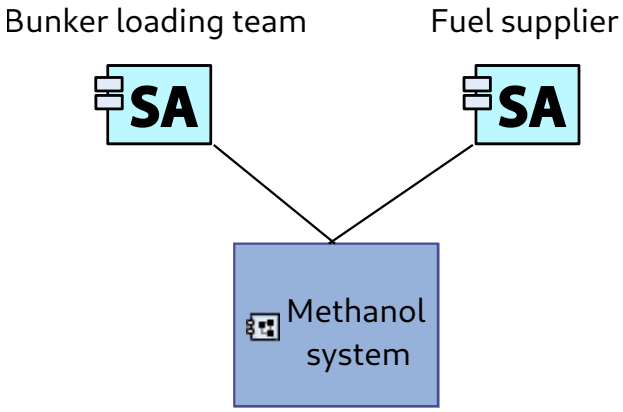


Figure 6.1: Methanol system with two actors

The functional chain captures the ordered execution of system functions involved in bunkering, including preparation, initiation, control, monitoring, and termination of fuel transfer (see figure 6.2 for the first and last step of the functional chain. To see the whole functional chain, see figure A.1 in the appendix). By using a functional chain as the backbone of the model, hazards can be directly associated with specific system behaviours and operational steps.

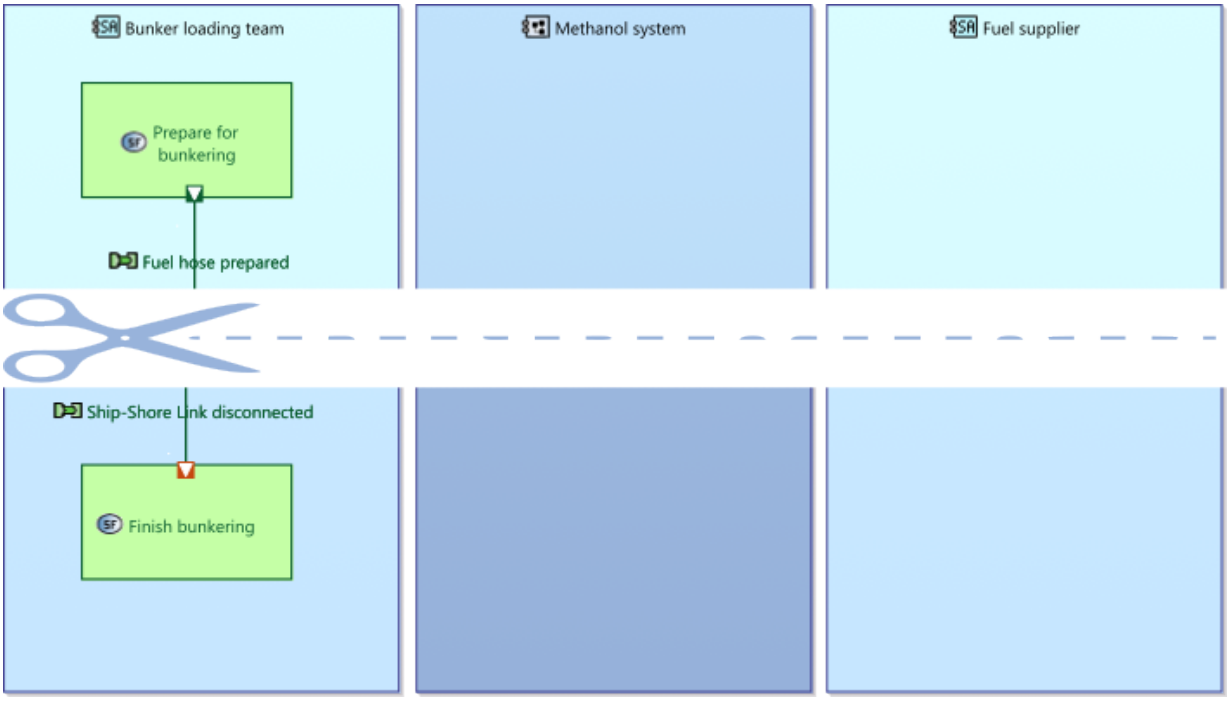


Figure 6.2: The start and end of the functional chain

6.2.2. Hazard objects

Hazard objects are introduced as explicit model elements and are linked to individual functions within the functional chain. Each Hazard object contains qualitative risk information, such as cause, consequence, likelihood, consequence class, risk ranking, and an ALARP summary. Placing hazards at the functional

level reflects common HAZID practice, where risks are identified based on operational behaviour and failure modes rather than on detailed component design. This also ensures that hazards remain valid during early design stages, when architectural details may still change.

6.2.3. Criteria objects

In addition to hazards, Criteria objects are introduced to represent measurable acceptance conditions that support risk evaluation and ALARP decision-making. Criteria are defined as separate model elements and are linked to the relevant functions and, where appropriate, to logical architectural elements. This separation allows hazards to express what can go wrong, while criteria express how acceptable system behaviour is defined and verified. Together, these elements enable a clear distinction between risk identification and risk acceptance.

6.2.4. The view

To support clarity and consistency, hazard and criteria objects are centrally managed within the model and referenced in the functional chain view. This ensures a single source of truth for risk-related information and prevents duplication or inconsistent updates across different diagrams. Scenario-based views are used to visualise the relationships between functions and hazards, while editing of hazard and criteria content is performed in their owning model packages.

This model structure enables the integration of RBD artefacts into an MBSE environment in a way that is consistent with Arcadia principles, supports early-stage risk reasoning, and remains scalable to more detailed design phases.

6.3. Hazard objects: definition and implementation

In Phase 2, hazards are represented as explicit model elements rather than as entries in external worksheets or documents. Each hazard is defined as a dedicated Hazard object containing qualitative risk information consistent with standard HAZID practice. This approach ensures that risk-related information is embedded directly in the model and can be traced to the functional behaviour to which it applies (see figure 6.3).

Each Hazard object contains the following core attributes:

- a descriptive name and textual description of the hazardous situation,
- a cause, describing the credible mechanism by which the hazard may arise,
- a consequence, describing the credible worst-case outcome if the hazard materialises,
- a likelihood class, expressed on an ordinal scale,
- a consequence class, expressing the severity of the outcome,
- a derived risk ranking based on the applied risk matrix,
- an ALARP summary indicating the acceptability status of the risk.

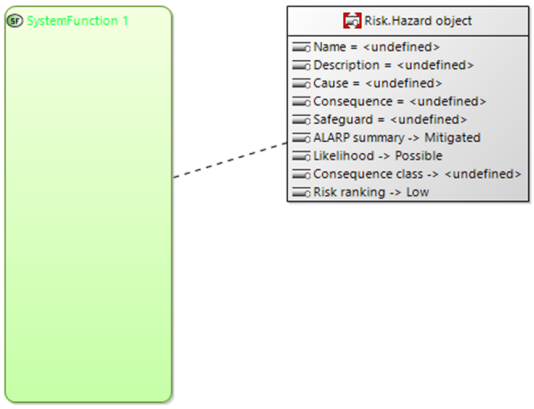


Figure 6.3: Risk.Hazard object linked to a SystemFunction

These attributes reflect common HAZID workshop outputs, but are structured in a way that allows them to be consistently interpreted and reused across the model. Likelihood and consequence class are estimated based on expert judgement, consistent with early design practice, and the resulting risk ranking is derived rather than independently assigned.

6.3.1. Definitions

1. Likelihood

Purpose: For the purpose of this research, likelihood is defined as the estimated probability that a hazardous event will occur within the defined operational context, assuming no additional safeguards beyond those explicitly modelled.
Type: Integer (ordinal scale)
Allowed values: 1–5 (see table 6.1)

Table 6.1: Likelihood values

Value	Description
1	Very unlikely – credible only under exceptional circumstances
2	Unlikely – has occurred elsewhere but not expected during normal operation
3	Possible – could occur during the system lifetime
4	Likely – expected to occur several times
5	Very likely – occurs frequently or continuously

2. Consequence class

Purpose: Consequence class represents the severity of the worst credible outcome if the hazard materialises.
Type: Enumeration (categorical)
Allowed values: A-C (see table 6.2)

Table 6.2: Consequence class values

Class	Description
A	Minor – no injury, negligible damage, no operational impact
B	Major – injury, significant damage, temporary loss of function
C	Severe – fatality, catastrophic damage, loss of vessel or mission

3. Risk ranking
Purpose: Risk ranking is the combined risk level, derived from likelihood and consequence class, using a predefined risk matrix.
Type: String
Allowed values: Low, Medium, High (see table 6.3)

Table 6.3: Risk ranking table

Consequence \Likelihood	1	2	3	4	5
A	Low	Low	Low	Medium	Medium
B	Low	Medium	Medium	High	High
C	Medium	High	High	High	High

4. ALARP summary
Purpose: Final statement to express if the hazard is mitigated, tolerable or unacceptable.
Type: String
Allowed values: Mitigated, Tolerable, Unacceptable

6.3.2. Implementation

In figure 6.4 an example is shown of how a Risk.Hazard object looks like:

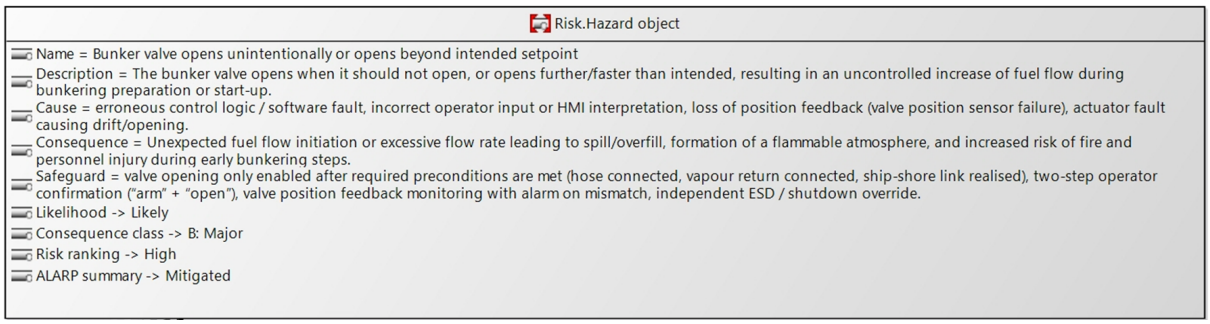


Figure 6.4: Example of what a Risk.Hazard object looks like

The Risk.Hazard objects are linked directly to the system functions in the functional chain to which they apply (see figure 6.5). This functional-level placement aligns with the nature of HAZID analyses, where risks are identified in relation to operational steps and system behaviour rather than detailed component implementations. Associating hazards with functions also ensures that they remain valid as the design evolves and architectural details change.

To maintain consistency and avoid duplication, Hazard objects are centrally managed within the model and referenced in scenario-based views, such as the risk-aware functional chain. In these views, hazards are visualised in relation to the functions they affect, while their content remains editable only in their owning package. This separation between ownership and visualisation enforces a single source of truth for risk information and supports controlled updates during iterative design.

The use of explicit Hazard objects enables hazards to function as first-class modelling elements rather than passive documentation artefacts. This supports traceability across the model, allows hazards to be reviewed in the context of system behaviour, and forms the basis for linking risk identification to acceptance criteria and ALARP decision-making in subsequent steps.

Figure 6.5: Risk.Hazard objects attached to functions of the functional chain

6.4. Criteria objects: definition and implementation

While Hazard objects capture what can go wrong and why, they do not by themselves provide a basis for determining whether a risk is acceptable or adequately mitigated. To support risk acceptance and ALARP decision-making, Criteria objects are introduced in Phase 2 as explicit model elements representing measurable acceptance conditions.

A Criteria object defines a condition that system behaviour must satisfy in order to limit or mitigate a hazard. Criteria are therefore complementary to hazards: hazards express undesired situations, whereas criteria express the conditions under which system behaviour is considered acceptable. This separation reflects common RBD practice, in which risk identification and risk acceptance are treated as distinct but related activities.

Each Criteria object contains the following key attributes:

- a descriptive name and description of the acceptance condition,
- a criterion type (e.g. functional, performance, timing, or safety),
- a measured parameter relevant to the criterion,
- a threshold value and associated unit,
- a comparison operator defining the acceptance condition,
- an acceptability class indicating whether the criterion outcome is acceptable, tolerable, or unacceptable,
- a verification method describing how compliance can be demonstrated.

6.4.1. Definitions

The properties of the Risk Criteria object are defined as follows:

Name Unique identifier of the criterion.

Criterion type Defines the nature of the constraint:

- *Performance*: numerical behaviour

- *Safety*: hazard mitigation effectiveness
- *Timing*: response times and delays
- *Functional*: correct logical behaviour

Measured parameter The physical or logical quantity being constrained (e.g. pressure, time, temperature).

Threshold value, unit, and comparison operator Together define the formal acceptance condition. For example: *Pressure* ≤ 0.3 *bar*. This explicit formulation is essential for traceability and later verification.

Acceptability class Indicates whether the criterion itself is acceptable, independent of overall risk ranking:

- *Acceptable*
- *Tolerable* (ALARP justification required)
- *Unacceptable*

Verification method Describes how compliance with the criterion will be demonstrated (e.g. analysis, simulation, test), not whether it has already been achieved.

Evidence reference Links the criterion to supporting engineering artefacts such as calculations, simulations, or test reports.

Linked hazard(s) Explicitly connects the criterion to one or more Hazard objects.

Applicable configuration Specifies whether the criterion applies to the baseline design, alternative configurations, or all configurations.

Status Supports lifecycle management of criteria throughout iterative design development.

A Risk Criteria object therefore represents a measurable constraint on system behaviour, defined by a parameter, threshold, and acceptability class, and explicitly linked to hazards and system functions to support objective ALARP decision-making.

In table 6.4 the key attributes are shown and defined by type, range and the default.

Table 6.4: Definitions of the key attributes of the criteria objects

Property	Type	Range	Default
Name	String	–	Criteria name
Description	String	–	Short description of the criterion
Criterion type	Enumeration	Performance / Safety / Timing / Functional / Environmental	Performance
Measured parameter	String	–	Pressure / Time / Temperature / Flow
Threshold value	Real	Domain-specific	–
Unit	String	–	bar / s / °C / kg/s
Comparison operator	Enumeration	$<, \leq, =, \geq, >$	$\leq$
Acceptability class	Enumeration	Acceptable / Tolerable / Unacceptable	Unacceptable
Verification method	Enumeration	Analysis / Simulation / Test / Inspection	Analysis
Evidence reference	String	–	Link to calculation, test, or report
Linked hazard(s)	Reference	Hazard objects	–
Applicable configuration	Enumeration	Baseline / Alternative / All	All
Status	Enumeration	Open / Verified / Invalidated	Open

Each Risk Criteria object captures a single, well-defined condition expressed in terms of a measurable parameter, a threshold value, and an acceptance rule. This structure enables qualitative risk assessments to be supported by explicit and verifiable criteria, without requiring full quantitative risk analysis at early design stages. The properties included in the Risk.Criteria object reflect common information already used in risk-based design practice, such as performance limits, timing constraints, or safety margins, but are formalised as model elements rather than informal statements in documentation.

The criterion type distinguishes between different categories of acceptance conditions, such as performance, safety, timing, functional, or environmental criteria. This allows criteria to be interpreted consistently across different engineering disciplines. The measured parameter, threshold value, unit, and comparison operator together define the acceptance condition in an unambiguous manner, enabling later verification through analysis, simulation, testing, or inspection.

Each Risk Criteria object is explicitly linked to a Hazard objects, making the relationship between risk identification and risk mitigation transparent. This linkage provides traceability between identified hazards and the criteria used to justify their acceptability under ALARP principles. In addition, criteria can be scoped to specific design configurations, supporting comparison between baseline and alternative solutions during design trade-off studies.

The status and evidence reference properties support lifecycle management of risk criteria. They allow criteria to be tracked from initial definition through verification and validation, while maintaining a clear link to supporting calculations, test results, or reports. By modelling risk criteria explicitly, the proposed approach enables risk acceptance decisions to be reasoned about, reviewed, and maintained within the MBSE environment, reducing reliance on external documents and improving consistency as the design evolves.

6.4.2. Implementation

In figure 6.6 an example is shown of how a Risk.Criterea object looks like.

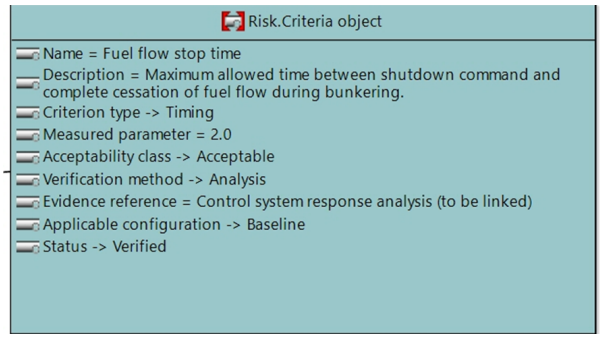


Figure 6.6: Example of what a Risk.Criterea object looks like

These Risk.Criteria objects are linked to the relevant system functions and, where applicable, to logical architectural elements to which those functions are allocated (see figure 6.7). This allows acceptance conditions to be traced from functional behaviour to the systems or components responsible for meeting them. In this way, criteria form a bridge between functional risk reasoning and architectural design decisions.

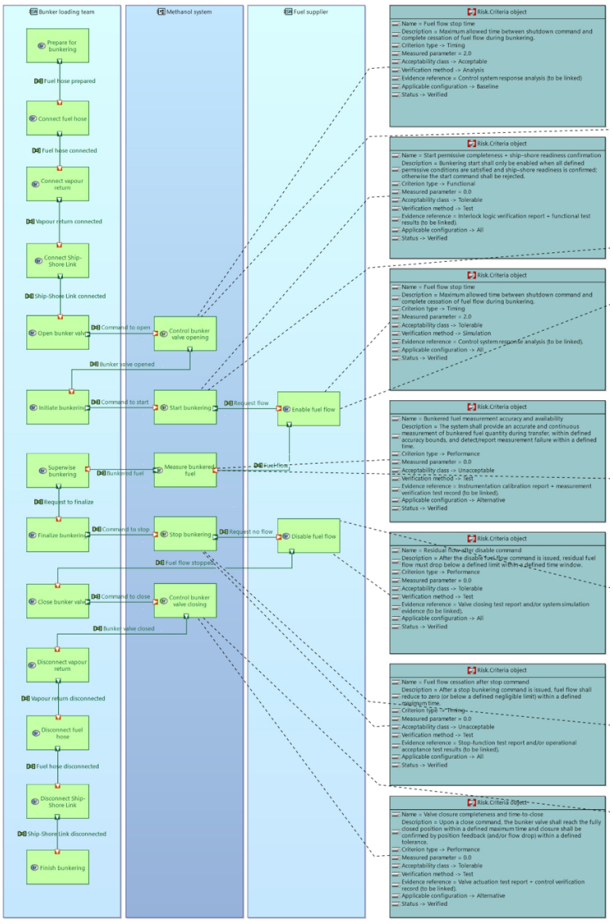


Figure 6.7: Risk.Criterea objects connected to the functional chain

In the model, criteria are used to provide objective justification for ALARP classifications assigned to hazards. For example, a hazard related to uncontrolled fuel flow may be mitigated by a criterion specifying a maximum allowable valve closing time or a residual flow limit after a stop command. By expressing such conditions explicitly in the model, ALARP decisions become traceable to measurable system behaviour rather than being based solely on qualitative judgement.

As with hazards, Criteria objects are centrally managed within the model and referenced in scenario-based views. This ensures consistency and prevents duplication of acceptance conditions across different diagrams or analyses. Criteria content is edited in its owning package, while functional chain views are used to visualise the relationship between functions, hazards, and acceptance conditions.

The explicit modelling of criteria enables a structured transition from qualitative risk identification to semi-quantitative risk evaluation. This supports more transparent design discussions, facilitates verification planning at later design stages, and reduces reliance on external documentation for demonstrating risk acceptability.

6.5. Risk-aware functional chain view

To support structured review and evaluation of risk information in relation to system behaviour, a dedicated risk-aware functional chain view is introduced in Phase 2. This view is based on the functional chain representing the bunkering scenario and is extended to visualise hazards and their relationships to individual functions.

The risk-aware functional chain view provides an integrated overview in which functional behaviour and associated hazards are shown simultaneously. A function in the chain is linked to a Hazard objects, allowing hazards to be interpreted in the context of specific operational steps rather than as isolated

entries in a list. This reflects how HAZID discussions are typically conducted, where risks are considered step-by-step along an operational sequence.

In this view, hazards are visualised as referenced model elements associated with the functions to which they apply. While the hazard content itself is centrally managed and edited in its owning package, the functional chain view serves as a read-only representation that supports inspection, discussion, and validation. This separation ensures consistency while enabling stakeholders to reason about risks in a scenario-oriented manner.

The risk-aware view supports several key aspects of the proposed RBD–MBSE integration:

- It makes explicit which hazards are associated with which system functions, improving transparency compared to document-based hazard lists.
- It supports traceability by linking hazards to functions and, indirectly, to architectural elements through functional allocation.
- It enables focused review of risk information during design discussions and HAZID-style workshops, using the functional chain as a common reference.

By embedding hazards directly within a functional chain view, risk identification becomes part of the system model rather than an external activity. This allows the model to function not only as a design artefact, but also as a structured representation of risk-related knowledge. The risk-aware functional chain therefore plays a central role in demonstrating how RBD artefacts can be integrated into an MBSE environment in a practical and reviewable manner (see figure 6.8 for a overview of the model. See figure A.2 for a detailed version in the appendix).

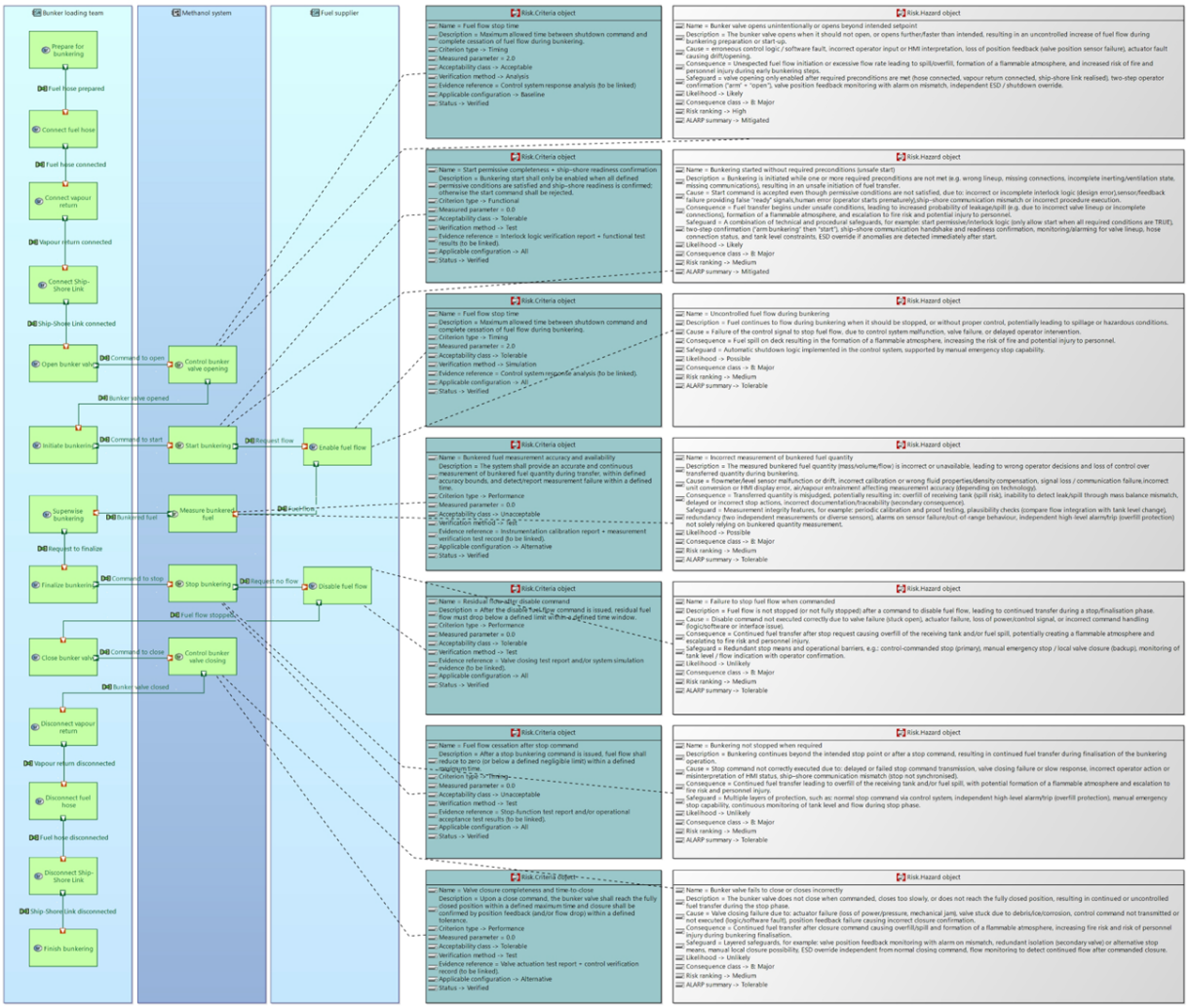


Figure 6.8: Overview of the functional chain with hazards and criterea connected to it

6.5.1. Risk reasoning in design context

In addition to reducing documentation overhead, the risk-aware functional chain view enables risk information to be interpreted in the context of the system design itself. By combining functional behaviour, architectural allocation, hazards, and mitigation criteria within a single model, risks are no longer treated as isolated items (like usually in a Hazid document), but as elements that are explicitly related to system interactions and dependencies.

This integrated representation makes it possible to reason about how hazards relate to multiple functions or how mitigation measures influence different parts of the system. For example, a hazard associated with uncontrolled fuel flow may be linked to several functions in the bunkering chain, such as valve opening, flow control, and stopping actions. In a document-based approach, such relationships are typically captured implicitly or spread across multiple worksheets, making it difficult to assess dependencies or cumulative effects. In the model-based representation, these relationships become explicit and visible within the functional chain.

Although a full analysis of interacting risks is outside the scope of this thesis, the model demonstrates the potential to extend risk-based reasoning beyond isolated hazard identification. By embedding hazards and criteria within the system model, risk evaluation can be performed in direct relation to functional interactions and architectural choices. This shows that the proposed approach does not only enable the same RBD activities with fewer documents, but also supports a more integrated and context-aware understanding of risk in early design phases.

7

Phase 3 - Evaluation and reflection

This chapter addresses Research Question 5: How does the integrated method perform in terms of approval efficiency, traceability, and design clarity compared to traditional approaches?

7.1. Evaluation approach

Phase 3 evaluates the model-based implementation developed in Phase 2 using the evaluation framework defined in Chapter 4. The functional chain model, extended with Hazard and Criteria objects, serves as the primary evaluation artefact, as introduced in Section 4.5.4. The purpose of this phase is to assess to what extent the proposed integration of RBD artefacts into an MBSE environment addresses the challenges identified in Phase 1.

The evaluation follows the qualitative and exploratory approach outlined in Sections 4.6.1–4.6.3. Rather than aiming for quantitative performance measurement or statistical validation, the focus is on assessing conceptual feasibility, practical usability, and integration potential within an industrial design context. This is consistent with the objective of the research, which is to investigate how combining RBD and MBSE can support faster and more coherent implementation of innovations.

The evaluation is structured around the three evaluation objectives defined in Section 4.6.1:

- *Feasibility*: whether qualitative RBD artefacts such as hazards, mitigations, and performance criteria can be represented in a structured and traceable manner within an MBSE model;
- *Usability*: whether the resulting model structure supports intuitive navigation, improves understanding of risk information, and reduces reliance on document-based workflows;
- *Integration potential*: whether the proposed model structure aligns with existing RBD and MBSE practices and can be maintained and extended throughout the design lifecycle.

Evaluation results are derived from a combination of model inspection, traceability analysis, and qualitative observations made during the development and review of the model. These results are interpreted using the evaluation criteria and interpretation logic defined in Section 4.6.3, recognising that positive outcomes indicate conceptual and practical feasibility rather than full integration readiness.

The evaluation explicitly assesses the requirements derived in Chapter 5, based on the challenges identified in Chapter 3, are addressed by the implemented model (table 7.1 and table 7.2).

By explicitly applying the evaluation framework defined earlier in the thesis, Phase 3 closes the methodological loop between problem analysis, model implementation, and reflective assessment. The following sections present the evaluation results per objective and discuss their implications for the integration of RBD and MBSE.

7.2. Evaluation results: feasibility, usability and integration potential

7.2.1. Feasibility

The first evaluation objective concerns the feasibility of representing qualitative RBD artefacts within an MBSE environment without loss of essential meaning. This objective addresses the question whether hazards, mitigations, and acceptance criteria can be modelled in a structured and traceable way, consistent with established HAZID practices.

Representation
The implemented prototype demonstrates that qualitative RBD artefacts can be explicitly represented as model elements within Capella. Hazards are modelled as dedicated Hazard objects and are directly linked to the system functions in the functional chain to which they apply. Each Hazard object contains structured attributes describing the hazardous situation, its cause, consequence, likelihood class, consequence class, risk ranking, and ALARP summary. This structure closely mirrors the information typically captured during HAZID workshops, while providing a more formal and consistent representation.

Association
By associating hazards with individual functions in the functional chain, risk information is anchored to system behaviour rather than to abstract system descriptions or isolated documentation artefacts. This functional placement ensures that hazards remain interpretable during early design stages, when architectural details may still evolve, and supports consistent reuse of risk information as the design progresses.

Acceptation
In addition to hazards, acceptance conditions are represented using explicit Criteria objects. These criteria express measurable or verifiable conditions under which system behaviour is considered acceptable and provide objective support for ALARP classifications. The separation between Hazard and Criteria objects preserves the distinction between risk identification and risk acceptance, while allowing explicit traceability between undesired events and their corresponding mitigation conditions.

Allocation
Traceability between RBD artefacts and design elements is achieved through explicit links within the model. Hazards are linked to functions, criteria are linked to functions and allocated architectural elements, and functions are allocated to logical components. This enables end-to-end traceability from operational behaviour to architectural responsibility without relying on external traceability matrices. Inspection of the model confirms that hazards, criteria, and functional elements can be navigated bidirectionally, supporting verification of completeness and consistency.

Summary
Overall, the results indicate that qualitative RBD artefacts can be modelled within an MBSE framework in a way that preserves their intent and structure. The prototype demonstrates conceptual feasibility by showing that hazards, mitigations, and acceptance criteria can be embedded directly in the system model, forming an integrated representation that aligns with established RBD practices.

7.2.2. Usability
The second evaluation objective concerns the usability of the proposed model-based representation, focusing on whether the structure supports intuitive navigation, improves understanding of risk information, and reduces reliance on document-based workflows. This objective addresses the practical question of whether the model adds value for engineers and stakeholders involved in RBD activities.

Interpretation
Evaluation of the prototype indicates that the integration of hazards and criteria within a functional chain significantly improves the interpretability of risk information. By visualising hazards directly in relation to system functions, risks can be reviewed in the context of specific operational steps rather than as isolated entries in a hazard list. This scenario-oriented representation aligns with how engineers typically reason about system behaviour and supports step-by-step discussion during reviews and HAZID-style sessions.

Navigation
Navigation within the model allows users to move directly between functions, associated hazards, and linked criteria without consulting external documents or traceability matrices. Compared to traditional document-based RBD workflows, this reduces the need to manually correlate information spread across multiple artefacts. As a result, the effort required to understand the rationale behind a given risk classification or mitigation measure is reduced.

Communication
The prototype also supports clearer communication between stakeholders with different backgrounds. Functional chain views provide an accessible entry point for non-specialists, while detailed hazard and criteria properties remain available for in-depth inspection. This layered access to information enables both high-level overview and detailed analysis within the same model, without duplicating content.

Indication
Qualitative feedback obtained during model walkthroughs indicates that presenting risk information in direct relation to functional behaviour improves situational awareness and supports more focused discussions. Rather than debating abstract risk levels, stakeholders are able to relate hazards and mitigations to concrete system actions and responsibilities. This shift from document-centric to behaviour-centric risk discussion represents a key usability benefit of the proposed approach.

Summary
Overall, the evaluation shows that the model-based representation enhances usability by improving navigability, reducing information fragmentation, and supporting shared understanding of risks. These benefits suggest that the approach can reduce cognitive and administrative overhead in RBD activities, while simultaneously enabling richer and more context-aware risk discussions.

7.2.3. Integration potential

The third evaluation objective concerns the integration potential of the proposed model structure within existing RBD and MBSE practices. This objective addresses whether the approach can be maintained, scaled, and aligned with current workflows in an industrial design environment, rather than functioning only as a standalone prototype.

Aligning
Evaluation of the prototype indicates that the proposed integration of RBD artefacts aligns well with existing MBSE practices based on the Arcadia method. Hazards and criteria are introduced as additional model elements without altering the underlying modelling principles or architectural layers. As a result, the approach complements existing functional and architectural modelling activities rather than replacing them.

Corresponding
From an RBD perspective, the structure corresponds closely with established HAZID workflows. The information captured in Hazard objects mirrors the content of conventional HAZID worksheets, while Criteria objects reflect performance and acceptance criteria already used in approval and assurance processes. This correspondence reduces the conceptual gap between document-based RBD artefacts and their model-based representation, supporting adoption by stakeholders familiar with current practices.

Governing and Maintaining
The separation between model ownership and visualisation further supports integration into ongoing design processes. Hazard and Criteria objects are centrally managed, while scenario-based views are used for review and discussion. This allows the same risk information to be reused across multiple views and design iterations, reducing the risk of inconsistencies as the model evolves.

Scaling
In addition, the prototype demonstrates that the model structure can accommodate incremental extension. Additional functional chains, hazards, or criteria can be introduced without restructuring the existing model, and more detailed architectural layers can be incorporated as the design matures. This suggests that the proposed approach can support both early-stage exploratory design and later-stage refinement.

Summary
Overall, the evaluation indicates that the proposed model-based representation has strong integration potential within existing RBD and MBSE workflows. It aligns with established practices, supports incremental adoption, and provides a foundation for further extension toward more detailed analysis or formal approval documentation.

Overview of adressed Conceptual requirements
Table 7.1 provides an overview of how the conceptual requirements derived in Section 5.6.1 are addressed by the Phase 2 prototype. The table explicitly links each requirement to concrete model elements and views, complementing the qualitative evaluation by making requirement coverage transparent. Partial coverage indicates requirements that are conceptually supported but not fully enforced or demonstrated in the current implementation.

Table 7.1: Coverage of conceptual requirements by the Phase 2 prototype

Req.	Requirement summary	Addressed	Evidence in model
CR1	Explicit representation of hazards and consequences	✓	Hazard objects linked to functions (Sec. 6.3)
CR2	Scenario and event–consequence modelling	◑	Functional chains with hazard context (Sec. 6.5)
CR3	Traceability to system architecture	✓	Function–component allocation (Sec. 6.2)
CR4	Traceable design assumptions	✓	Baseline vs alternative configuration scope (Sec. 6.4)
CR5	Explicit risk control measures	✓	Criteria objects linked to hazards (Sec. 6.4)
CR6	Performance criteria linked to hazards	✓	Risk Criteria object definition (Sec. 6.4)
CR7	Requirements traceability	✓	End-to-end trace links in model (Sec. 7.2.1)
CR8	Consistency constraints	◑	Structural rules defined, not enforced automatically (Sec 7.2.3.1)

Overview of adressed process requirements
Table 7.2 summarises the extent to which the process requirements defined in Section 5.6.2 are supported by the implemented modelling approach. The overview illustrates how the prototype aligns with existing RBD workflows and MBSE practices, while also highlighting areas where further validation or extension would be required in an industrial setting.

Table 7.2: Coverage of process requirements by the Phase 2 prototype

Req.	Requirement summary	Addressed	Evidence in model
PR1	Input alignment with existing RBD artefacts	✓	Mapping of HAZID inputs to model elements (Sec. 6.1)
PR2	Stakeholder transparency	✓	Risk-aware functional chain view (Sec. 6.5)
PR3	Iterative refinement support	✓	Central hazard and criteria ownership (Sec. 6.3–6.4)
PR4	Review and verification support	✓	Traceable evidence links (Sec. 7.2.3)
PR5	Reusability across projects	◑	Template-based structure, not yet validated but possible (Sec 7.2.3.1)
PR6	Compatibility with existing toolchains	✓	Implemented within Capella (Sec. 6.2)
PR7	Output for downstream analyses	◑	Conceptual support, not demonstrated (Sec 7.2.3.1)

7.2.3.1 Rationale for partial requirement coverage

Partially covered requirements reflect deliberate scoping choices rather than deficiencies of the proposed approach. For the conceptual requirements, CR2 (scenario and event–consequence modelling) is partially covered because hazards are embedded within functional chains to provide behavioural context, but systematic propagation of scenarios across logical and physical architecture layers was not implemented in this study. Similarly, CR8 (consistency constraints) is partially covered as structural modelling rules are conceptually defined, but automated rule enforcement or tool-based validation mechanisms were outside the scope of the prototype.

For the process requirements, partial coverage of PR5 (reusability across projects) results from the evaluation being limited to a single pilot case. While the model structure and artefact definitions are designed for reuse, validation across multiple projects is required to confirm standardisation potential. PR7 (output for downstream analyses) is partially covered because the model supports traceable extraction of risk and performance information, but no direct coupling to quantitative analysis or simulation tools was demonstrated within this research.

7.3. Interpretation of results

The evaluation results presented in Section 7.2 are interpreted using the interpretation framework defined in Section 4.6.3. This framework distinguishes between conceptual feasibility, practical usefulness, and readiness for broader adoption, and explicitly recognises the exploratory nature of the research.

The evaluation results can be interpreted in direct relation to the challenges identified in Chapter 3 and the conceptual and process requirements derived in Chapter 5. Chapter 3 highlighted several structural limitations of current RBD practice, including the absence of explicit risk representations within system models, fragmented traceability between design and risk artefacts, and a strong reliance on document-based workflows. These challenges formed the basis for the requirements formulated in Section 5.6.

The prototype developed in Phase 2 demonstrates that these requirements can be addressed within an MBSE environment. Hazards and acceptance criteria are represented as explicit model elements and are directly linked to functional behaviour and architectural allocation, fulfilling the requirement for integrated risk representation. The use of a single model as the authoritative source for both design and risk information addresses the identified fragmentation and reduces the need for manual traceability across documents.

Furthermore, the risk-aware functional chain view responds directly to the need for contextualised risk reasoning identified in Chapter 3. By embedding hazards within functional sequences, risks are evaluated in relation to system behaviour rather than as isolated checklist items. This confirms that the proposed method not only meets the conceptual requirements derived in Chapter 5, but does so in a way that improves coherence between design reasoning and risk-based justification.

7.3.1. Feasibility

The feasibility evaluation shows that qualitative RBD artefacts can be embedded in an MBSE model without loss of essential meaning. Hazards, criteria, and ALARP considerations are represented as structured model elements and are directly linked to functional behaviour and architectural allocation. This confirms that the proposed integration is conceptually sound and that MBSE can support RBD activities at early design stages. At the same time, feasibility in this context should be interpreted as proof of concept rather than proof of completeness or maturity.

7.3.2. Usability

The usability evaluation indicates that the model-based representation improves the accessibility and interpretability of risk information. By presenting hazards in the context of functional chains, risk discussions shift from abstract classifications to behaviour-oriented reasoning. This supports more focused design discussions and reduces the effort required to trace risk-related information across multiple artefacts. However, usability gains depend on the availability of a well-structured functional model and on stakeholder familiarity with model-based representations.

7.3.3. Integration potential

The integration potential assessment suggests that the proposed approach can be incorporated into existing RBD and MBSE workflows without requiring fundamental changes to established practices. The alignment with common HAZID artefacts and the use of Arcadia-compliant modelling constructs support incremental adoption. Nevertheless, full integration into industrial processes would require organisational alignment, modelling discipline, and agreement on how model-based risk information is used in approval and assurance activities.

7.3.4. Summary

Taken together, the results indicate that combining RBD and MBSE enables not only a reduction in documentation overhead, but also a shift toward more integrated and context-aware risk reasoning. The model-based representation makes dependencies between system behaviour, architectural elements, and risk mitigation measures explicit. This supports earlier identification of design sensitivities and provides a stronger basis for informed decision-making during innovation-driven design processes.

In accordance with the interpretation framework, these results demonstrate that the proposed approach is viable and valuable at a conceptual and practical level, while also highlighting that further validation and extension would be required for large-scale or safety-critical deployment.

8

Conclusion, Contribution and Recommendations

This chapter provides a conclusion, covers the contribution and gives an overview of the primary recommendations for the future continuation of this research project.

8.1. Conclusion

This thesis investigated how RBD artefacts can be integrated into a MBSE environment to support naval ship design. The central research question concerned whether qualitative risk information, traditionally managed through document-centric workflows, can be represented, maintained, and evaluated within a system model in a way that improves traceability, consistency, and decision-making. The novelty of this research lies in demonstrating how qualitative RBD artefacts can be embedded directly within the functional and architectural structure of an MBSE model, rather than being maintained as separate risk documentation.

The results demonstrate that such an integration is both feasible and practically meaningful. By representing hazards, risk control measures, and acceptance criteria as explicit model elements and linking them directly to system functions and architectural structures, risk information can be embedded within the design context rather than treated as an external justification activity. This represents a shift from document-based risk justification toward model-based risk reasoning embedded within the system architecture. This enables risk reasoning to be performed in relation to system behaviour and design assumptions, addressing key limitations of current RBD practice.

The implemented prototype shows that the proposed approach can reduce documentation overhead by consolidating risk and design information within a single authoritative model. In doing so, the model becomes not only a design artefact but also a carrier of the risk justification logic required for approval processes. At the same time the prototype improves transparency and traceability. Rather than replacing existing RBD practices, the approach complements them by providing a structured backbone in which risk-related artefacts can evolve consistently as the design matures.

Overall, this research confirms that combining MBSE and RBD at the model level offers a viable pathway toward more coherent, context-aware, and maintainable risk-based justification in naval ship design, particularly in domains where innovation extends beyond the coverage of prescriptive regulations. This research demonstrates how qualitative risk artefacts traditionally captured in document-based RBD processes can be embedded directly within an MBSE system model, enabling risk reasoning to be performed in the context of system architecture rather than as a separate documentation activity.

8.2. Contribution

This thesis contributes to the emerging integration of MBSE and RBD by introducing a concrete modelling approach for representing qualitative risk artefacts within system architecture models. The main contributions are:

- A structured conceptual integration of qualitative RBD artefacts into an MBSE environment, enabling hazards, mitigations, and acceptance criteria to be represented as first-class model elements.

- A modelling strategy that links hazards and mitigation logic to functional chains, enabling risk reasoning to be performed in relation to system behaviour and interactions.
- A set of conceptual and process requirements that translate documented RBD challenges into explicit modelling needs, providing a reproducible basis for future MBSE–RBD integration efforts.
- A risk-aware functional chain representation that embeds hazards within system behaviour, allowing risk reasoning to be performed in design context rather than through isolated document-based analyses.
- An evaluated model-based prototype, implemented in Capella, demonstrating how risk information can be maintained, traced, and updated consistently as design assumptions evolve.

8.3. Recommendations

The following recommendations outline directions for extending the proposed MBSE–RBD integration beyond the scope of this research. They focus on deepening analytical capability, expanding lifecycle coverage, and strengthening the role of the model as a central decision-support artefact.

8.3.1. Extension to later design phases

This research focuses on the integration of RBD artefacts into an MBSE environment, where qualitative risk assessment and functional reasoning are most relevant. A logical direction for future research is to investigate how the proposed model-based approach can be extended to later design phases, in which architectural detail and verification activities become more prominent.

In later phases of the design lifecycle, system functions are increasingly refined into physical components, subsystems, and interfaces. Extending the proposed approach would involve analysing how Hazard and Criteria objects defined at functional level can be systematically propagated to the Logical and Physical Architecture layers. This would enable risk-related information identified early in the design to remain explicitly linked to detailed design decisions, rather than being reinterpreted or duplicated in separate artefacts.

In addition, future work could explore how Criteria objects can be connected to verification and validation activities, such as simulations, tests, and inspections. By linking acceptance criteria directly to verification evidence within the model, a continuous trace can be established from early risk identification through to compliance demonstration. This has the potential to further reduce documentation overhead and improve consistency across design phases.

Such an extension would also allow investigation of how qualitative risk assessments evolve as more detailed information becomes available. Early qualitative classifications could be refined or complemented with quantitative data, while maintaining continuity within the same model structure. This would support a more integrated risk management process across the full design lifecycle.

Overall, extending the proposed RBD–MBSE integration to later design phases represents a natural continuation of this research. It offers the potential to strengthen traceability, reduce rework between design stages, and further support informed decision-making as system designs mature.

8.3.2. Integration of quantitative risk information

The approach presented in this thesis focuses on the qualitative integration of RBD artefacts into an MBSE environment, consistent with common practice in early design phases. Likelihood and consequence classes are expressed using ordinal scales and expert judgement, which is appropriate when detailed data is limited. A relevant direction for future research is the integration of quantitative risk information within the same model-based structure.

Future work could investigate how quantitative data, such as failure rates, reliability figures, and operational feedback, can be incorporated alongside existing qualitative Hazard and Criteria objects. Rather than replacing qualitative assessments, quantitative information could be used to refine or support them as the design matures. This would allow the model to evolve from an early, exploratory risk assessment tool into a more substantiated decision-support system in later design stages.

An important aspect of such an extension would be maintaining consistency between qualitative and quantitative representations. For example, quantitative probability estimates could be mapped to existing

likelihood classes, or used to validate whether qualitative classifications remain appropriate as more information becomes available. Similarly, quantitative performance data could be linked to Criteria objects to support more rigorous verification and validation activities.

Integrating quantitative risk information also opens opportunities to connect the model to operational data and feedback loops. Data from testing, commissioning, or in-service operation could be used to update risk assumptions within the model, supporting continuous improvement and learning across projects.

Overall, the integration of quantitative risk information represents a logical extension of the proposed RBD–MBSE approach. It would enhance analytical depth while preserving the structured, traceable model-based representation demonstrated in this thesis, and further strengthen the role of MBSE as a unifying framework for risk management across the system lifecycle.

8.3.3. Towards integration with Integrated Logistics Support (ILS)

While this research has focused on the integration of MBSE and RBD, an important adjacent discipline is Integrated Logistics Support (ILS). ILS aims to ensure that naval platforms meet demanding targets for availability, maintainability, and life-cycle cost by systematically addressing supportability from the earliest design stages. Its toolkit includes analyses such as FMECA, Reliability-Centered Maintenance, Maintenance Task Analysis, Level of Repair Analysis, and Life-Cycle Costing, all of which overlap conceptually with risk assessments used in RBD.

Currently, ILS is typically managed in parallel to systems engineering and RBD, with results documented in separate processes and deliverables. This separation creates duplication and weakens traceability between design decisions, risk arguments, and supportability outcomes. A future research direction is therefore to extend the MBSE–RBD integration proposed in this research to a triad that also incorporates ILS. Such an approach would enable a unified model environment that simultaneously captures functional requirements, risk justifications, and supportability considerations. The outcome would be not only safer and more innovative designs, but also vessels that are easier and more cost-effective to operate and maintain throughout their life cycle.

8.3.4. From fault tolerance to graceful degradation

A promising direction for future research is the evolution of MBSE–RBD integration from compliance-focused analysis toward cost- and lifecycle-driven optimization. Current practice in high-dependability domains, such as space and naval systems, often relies on full redundancy to guarantee safety and reliability. While effective, this strategy increases mass, cost, and complexity, and many redundant components are never actually used during operation. Bitetti et al. [38] argue that a paradigm shift is needed: from strict fault tolerance toward *graceful degradation*, in which systems are designed to continue functioning at reduced performance after faults rather than relying on complete redundancy.

To support this shift, the authors introduced an optimization tool that operates alongside Capella's reliability viewpoint. By coupling architectural models with dependability attributes, the tool systematically explores trade-offs between mass, cost, and reliability across multiple subsystem configurations. In their case studies on satellite subsystems, this approach enabled the identification of configurations that satisfied reliability targets with substantially lower mass and cost than traditional fully redundant designs.

For naval design, this perspective suggests that MBSE and RBD could evolve into a joint framework for lifecycle optimization, balancing not only performance and safety, but also affordability and operational sustainability. Integrating graceful degradation and cost-aware optimization into model-based environments would therefore extend the role of MBSE–RBD from assurance to genuine design guidance, shaping future ships that are both safer and more efficient throughout their life cycle.

8.3.5. Addressing partially fulfilled requirements

The evaluation presented in Chapter 7 includes several requirements that are marked as partially addressed in Tables 7.1 and 7.2. These cases do not indicate shortcomings of the proposed approach, but rather reflect conscious scoping decisions made in this research. The prototype demonstrates conceptual feasibility for these requirements, while full implementation or validation was beyond the intended scope of a single pilot case.

For the conceptual requirements, partial coverage primarily relates to aspects such as scenario propagation and consistency constraints. While the model structure supports the representation of event–consequence

chains within functional sequences, automated enforcement of modelling rules and systematic propagation across architecture layers were not implemented. Future work could focus on formalising such constraints through modelling guidelines, rule-based checks, or tool-supported validation mechanisms to strengthen model robustness.

Similarly, for the process requirements, partial coverage reflects areas where the approach is structurally prepared but not yet empirically validated. Reusability across projects and support for downstream analyses were demonstrated at a conceptual level, but require application in multiple case studies to assess scalability, standardisation potential, and integration with quantitative analysis workflows.

Addressing these partially fulfilled requirements represents a logical next step in the maturation of the proposed MBSE–RBD approach. Targeted follow-up studies could focus specifically on extending these aspects, thereby transforming conceptual support into fully operational capabilities while preserving the core structure demonstrated in this thesis.

References

[1] INCOSE. *Systems Engineering Vision 2020*. https://www.incose.org/sevision2020. 2007.

[2] Evangelos Boulougouris et al. “Risk-based design of naval combatants”. In: *Ocean Engineering* 65 (2013), pp. 49–61. DOI: https://doi.org/10.1016/j.oceaneng.2013.02.014. URL: https://www.researchgate.net/publication/259693221_Risk-based_design_of_naval_combatants.

[3] Hillary Sillitto et al. *Systems Engineering and System Definitions*. Tech. rep. INCOSE-TP-2019-001-01. San Diego, CA, USA: International Council on Systems Engineering (INCOSE), July 2019. URL: https://www.incose.org/docs/default-source/default-document-library/final_-se-definition.pdf.

[4] Austin A. Kana. *Systems Engineering: Lecture Slides for MT44035 - Design of Complex Specials*. Lecture slides, Faculty of Mechanical, Maritime and Materials Engineering (3mE). Delft, The Netherlands, 2024. URL: https://brightspace.tudelft.nl/d2l/le/content/682176/viewContent/4091725/View.

[5] Rashmi Jain et al. “Exploring the Impact of Systems Architecture and Systems Requirements on Systems Integration Complexity”. In: *Systems Journal, IEEE* 2 (July 2008), pp. 209–223. DOI: 10.1109/JSYST.2008.924130.

[6] International Maritime Organization. *Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process*. Tech. rep. Accessed: 9 September 2025. IMO, 2002. URL: https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/MSC-MEPC.2-Circ.12-Rev.2%20-%20Revised%20Guidelines%20For%20Formal%20Safety%20Assessment%20(Fsa)For%20Use%20In%20The%20Imo%20Rule-Making%20Proces...%20(Secretariat).pdf.

[7] Pascal Roques. *Systems Architecture Modeling with the Arcadia Method: A Practical Guide to Capella*. Elsevier, 2017.

[8] Lorenzo Bitetti et al. “Model Based Approach for RAMS Analyses in the Space Domain with Capella”. In: *International Conference on Model-Based Safety and Assessment (IMBSA)*. Vol. 11852. Lecture Notes in Computer Science. Springer, 2019, pp. 19–33. DOI: 10.1007/978-3-030-32872-6_2.

[9] K. Henderson et al. “Value and benefits of model□based systems engineering (MBSE): Evidence from the literature”. In: *Systems Engineering* 24.1 (2020), pp. 51–66. DOI: 10.1002/sys.21566.

[10] Tim Bedford et al. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2013. URL: https://books.google.nl/books?hl=nl&lr=&id=46dx50PoWcwC&oi=fnd&pg=PR13&dq=Tim+Bedford+et+al.+Probabilistic+Risk+Analysis:+Foundations+and+Methods.+Cambridge+University+Press,+2013.&ots=F3sgL8yfIZ&sig=AYa4y2LFQXPiwcCqHw_ZXLML6ug#v=onepage&q&f=false.

[11] Collidu. *Risk-Based Thinking Presentation*. Accessed: 16 September 2025. 2025. URL: https://www.collidu.com/presentation-risk-based-thinking.

[12] Evangelos Boulougouris et al. “Risk-based design of naval combatants”. In: *Ocean Engineering* 65 (2013), pp. 20–30.

[13] Christian Breinholt et al. “SAFEDOR–The Implementation of Risk-based Ship Design and Approval”. In: *Procedia - Social and Behavioral Sciences* 48 (2012). Transport Research Arena 2012, pp. 753–764. DOI: https://doi.org/10.1016/j.sbspro.2012.06.1053. URL: https://www.sciencedirect.com/science/article/pii/S1877042812027899.

[14] Brett Morris. *A Model-Based Systems Engineering Methodology to Support Early Phase Australian Off-the-Shelf Naval Ship Acquisitions*. https://hdl.handle.net/2440/119895. 2019.

[15] W. J. Tudor et al. “Virtual integration: managing complex warship design through model based engineering”. In: *Proceedings of the Engine as a Weapon International Symposium (EAAW)*. 2019. DOI: 10.24868/issn.2515-8171.2019.009.

[16] D. Brefort et al. “An architectural framework for distributed naval ship systems”. In: *Ocean Engineering* 147 (2018), pp. 375–385. DOI: 10.1016/j.oceaneng.2017.10.028.

[17] N. A. Tepper. *Exploring the use of Model-Based Systems Engineering (MBSE) to develop systems architectures in naval ship design*. http://hdl.handle.net/1721.1/61910. Master’s thesis, Massachusetts Institute of Technology. 2010.

[18] B. Lightsey. *Systems Engineering Fundamentals*. Defense Acquisition University, 2001.

[19] D. Long et al. *A Primer for Model-Based Systems Engineering*. 2nd. Vitech, 2012.

[20] K. Packham. *Time to say goodbye to documents and hello to MBSE*. https://www.rheagroup.com/time-to-say-goodbye-to-documents-and-hello-to-mbse/. 2021.

[21] P. Pearce. “A Practical Approach For Modelling Submarine Subsystem Architecture In SysML”. In: (2013).

[22] K. Odukoya et al. *Towards a semantic approach to knowledge exchange in Architectural Framework*. https://doi.org/10.13140/RG.2.2.18415.20645. 2023.

[23] D. Verma et al. *MBSE Applied*. https://esi.nl/events/2021/160421. 2021.

[24] I. Poulis. *Application of Model Based System Engineering (MBSE) with Ship Design Arrangement Tool of advanced zero emissions Power, Propulsion and Energy Systems in Maritime Technology*. Master’s thesis, Delft University of Technology, http://resolver.tudelft.nl/uuid:7faf4cc0-c493-4efb-ad3b-5046ca208288. 2022.

[25] Damen Naval. *Damen Naval*. Accessed: 9 September 2025. 2024. URL: https://www.damen.com/companies/naval.

[26] Monch. “150 years of naval shipbuilding in Vlissingen”. In: *Monch - Naval News* (2023). Accessed: 9 September 2025. URL: https://monch.com/150-years-of-naval-shipbuilding-in-vlissingen/.

[27] Manufacturing Today. “Manufacturing Today dives into the pivotal role Damen Naval plays in securing global waters”. In: *Manufacturing Today* (Apr. 2024). Accessed: 9 September 2025. URL: https://manufacturing-today.com/news/manufacturing-today-dives-into-the-pivotal-role-damen-naval-plays-in-securing-global-waters/.

[28] Egbert Kooij. “Applying Model-Based Systems Engineering to Naval Ship Design”. MSc Thesis. MA thesis. Delft University of Technology, 2022. URL: https://tudelft.on.worldcat.org/oclc/1358880136.

[29] Tim Weilkiens. *Systems Engineering with SysML/UML: Modeling, Analysis, Design*. Morgan Kaufmann, 2006.

[30] Steffen Boschert et al. “Digital Twin — The Simulation Aspect”. In: *Mechatronic Futures*. Springer, 2016, pp. 59–74.

[31] Jeffrey A. Estefan. *Survey of Model-Based Systems Engineering (MBSE) Methodologies*. Tech. rep. INCOSE, 2008.

[32] Object Management Group. *Systems Modeling Language v2 (SysML v2) Specification*. 2023. URL: https://www.omg.org/spec/SysML/2.0/.

[33] *Support Functionality in System Modelling: The Chicken or the Egg*. Vol. SNAME 14th International Marine Design Conference. SNAME International Marine Design Conference. June 2022, D021S004R004. DOI: 10.5957/IMDC-2022-272. eprint: https://onepetro.org/snameimdc/proceedings-pdf/IMDC22/IMDC22/D021S004R004/3008251/sname-imdc-2022-272.pdf. URL: https://doi.org/10.5957/IMDC-2022-272.

[34] Obeo and Thales. *Arcadia Method*. Accessed: 15 September 2025. 2025. URL: https://mbse-capella.org/arcadia.html.

[35] Pascal Roques. “MBSE with the Arcadia Method and the Capella Tool”. In: *8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)*. Accessed: 15 September 2025. Toulouse, France, 2016. URL: https://hal.science/hal-01258014/document.

[36] ANZEN Engineering and CESA. *Model-driven design and development of an electromechanical actuation system*. Capella Days 2023 Presentation. Accessed: 15 September 2025. 2023. URL: https://mbse-capella.org/.

[37] Nataliya Yakymets et al. “Model-Based Engineering, Safety Analysis and Risk Assessment for Personal Care Robots”. In: *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. 2018, pp. 6136–6141. DOI: 10.1109/IROS.2018.8594115.

[38] D. Bitetti et al. “Model Based Safety Assessment in the Space Domain with Capella”. In: *Proceedings of the 8th International Conference on Model-Based Safety and Assessment (IMBSA)*. Vol. 11093. Lecture Notes in Computer Science. Springer, 2018, pp. 1–16. DOI: 10.1007/978-3-030-00129-0_1.

[39] Rolf Skjong et al. “Risk-Based Design of Ships”. In: *Proceedings of the 10th International Symposium on Practical Design of Ships and Other Floating Structures (PRADS)*. 2007, pp. 45–56.

[40] Daozheng Huang et al. “Application of Fuzzy Logic to Safety Risk Assessment of China’s Maritime Passages”. In: *Transportation Research Record: Journal of the Transportation Research Board* 2273 (2012), pp. 112–120. DOI: 10.3141/2273-14. URL: https://www.researchgate.net/publication/270210515.

[41] International Maritime Organization. *Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process*. Tech. rep. MSC/Circ.1023–MEPC/Circ.392. IMO, 2002. URL: https://www.imo.org/en/OurWork/Safety/Pages/FormalSafetyAssessment.aspx.

[42] Makoto Ito. *Fundamentals and Applications for Risk-Based Design*. Tech. rep. 6 (□). Research Institute, ClassNK. ClassNK Technical Journal, 2022. URL: https://www.classnk.or.jp/hp/pdf/research/rd/2022/06_e04.pdf.

[43] Christos A. Kontovas. “Formal Safety Assessment: A Critical Review”. In: *Marine Policy* 44 (2014), pp. 45–53. URL: https://www.researchgate.net/publication/233651797_Formal_Safety_Assessment_A_Critical_Review.

[44] Hans Pasman et al. “Hazard Identification Methods in the Process Industries”. In: *Journal of Loss Prevention in the Process Industries* 36 (2015), pp. 77–87.

[45] Thomas Hansen et al. “Risk-Based Design in Maritime Engineering: Current Practices and Challenges”. In: *Ocean Engineering* 206 (2020), p. 107334.

[46] International Maritime Organization. *MSC/Circ.1002: Guidelines on Alternative Design and Arrangements for Fire Safety*. https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSC-Circulars/MSC-Circ.1002.pdf. Accessed: 16 September 2025. 2001.

[47] International Maritime Organization. *MSC.1/Circ.1212: Alternative Design and Arrangements for SOLAS Chapters II-1 and III – Netherlands Regulatory Framework (NeRF)*. https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSC-Circulars/MSC.1-Circ.1212.pdf. Accessed: 16 September 2025. 2007.

[48] International Maritime Organization. *MSC.1/Circ.1455: Guidelines for the Approval of Alternatives and Equivalents as Provided for in Various IMO Instruments*. https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSC-Circulars/MSC.1-Circ.1455.pdf. Accessed: 16 September 2025. 2013.

[49] International Naval Safety Association (INSA). *ANEP-77 Volume 1: Naval Ship Code, Edition 3*. Tech. rep. Allied Naval Engineering Publication, Edition 3, Part 1. Brussels, Belgium: NATO Naval Armaments Group (NNAG), July 2019. URL: https://s3-eu-west-1.amazonaws.com/s3.

spanglefish.com/s/22631/documents/safety-specifications/anep-77-pt1-edg-v3-jul19.pdf.

[50] Richard Delpizzo et al. “An Introduction to NATO Standard ANEP (Allied Naval Engineering Publication) 77 and Its Application to Naval Ships”. In: *Ciencia y tecnología de buques* 11 (Sept. 2017), p. 75. DOI: 10.25043/19098642.153.

[51] Alfredo Valcalda et al. “A Method to Assess the Impact of Safe Return to Port Regulatory Framework on Passenger Ships Concept Design”. In: *Journal of Marine Engineering and Technology* 22.3 (2023), pp. 111–122. DOI: 10.1080/20464177.2022.2031557.

[52] ClassNK. *ClassNK Technical Journal, No. 6 (2022-II): Dealing with Risk*. Tech. rep. Accessed: 2025-09-29. Nippon Kaiji Kyokai (ClassNK), 2022. URL: https://www.classnk.or.jp/hp/pdf/research/rd/2022/06_e0.pdf.

[53] Apostolos Papanikolaou et al. “State of the Art, Challenges and Future Directions in Life-Cycle Risk Management of Ships”. In: *Proceedings of the 12th International Marine Design Conference (IMDC)*. Tokyo, Japan: IMDC, 2015, pp. 417–442. URL: https://pure.tudelft.nl/ws/files/36365983/IMDC2015_SoA_LCRM_DVAP-FINAL.pdf.

[54] Andrew P. Sage et al. *Handbook of Systems Engineering and Management*. Wiley, 2009.

[55] Katy Snook et al. “Bridging the Gap Between Safety and Systems Engineering”. In: *INCOSE International Symposium* 29.1 (2019), pp. 1133–1146. URL: https://pure.tue.nl/ws/portalfiles/portal/350816190/bridging-the-gap-between-requirements-engineering-and-systems-architecting-the-elephant-specification-language.pdf.

[56] Reto Keller et al. “Integrating Reliability Modeling and System Architecture Design”. In: *Proceedings of the European Safety and Reliability Conference (ESREL)*. 2020.

[57] Yiannis Papadopoulos et al. “Towards Model-Based Safety and Dependability Analysis: Challenges and Opportunities”. In: *Reliability Engineering and System Safety* 219 (2022), p. 108166. URL: https://www.researchgate.net/publication/228622870_Model-based_safety_analysis_final_report.

[58] Mohammad Chami et al. “A Survey on MBSE Adoption Challenges”. In: (Nov. 2018). URL: https://www.researchgate.net/publication/328118976_A_Survey_on_MBSE_Adoption_Challenges.

[59] Office of the Under Secretary of Defense (R&E). *DoD Digital Engineering Strategy*. Tech. rep. U.S. Department of Defense, 2018. URL: https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf.

[60] Michel Ingham et al. “Experiences with Model-Based Systems Engineering at JPL: Challenges and Successes”. In: *INCOSE International Symposium*. 2012, pp. 1181–1198.

[61] INCOSE, IEEE, and PMI. *SEBoK: Model-Based Systems Engineering (MBSE) Overview and Challenges*. Systems Engineering Body of Knowledge, v.2.x. 2023. URL: https://www.sebokwiki.org/.

[62] Michael Bone et al. “Survey of MBSE Adoption Trends: 2015 Results”. In: *INCOSE International Symposium*. 2015, pp. 1–15. URL: https://www.researchgate.net/publication/283955091_Current_Modeling_Trends_in_Systems_Engineering.

[63] Tyson R. Browning. “Design Structure Matrix Extensions and Front-End Loading in Complex Development Projects”. In: *Systems Engineering* 19.2 (2016), pp. 158–173.

[64] Joseph Elm et al. *The Business Case for Systems Engineering: Results of a Survey of Projects in the Defense and Commercial Sectors*. Tech. rep. CMU/SEI-2012-TR-005. SEI, Carnegie Mellon University, 2012. URL: https://resources.sei.cmu.edu/.

[65] Xinyu Chen et al. “Risk Assessment Method for Maritime Autonomous Surface Ships Based on Combined Functional Analysis and HAZID”. In: *Journal of Marine Science and Engineering* 13.5 (2025), p. 970. DOI: 10.3390/jmse13050970. URL: https://www.mdpi.com/2077-1312/13/5/970.

[66] Vasileios Sideris. “Advancing Model-Based Systems Engineering (MBSE) in the Development of Systems Architecture: Exploring the Value of MBSE during Early-Stage Naval Vessel Design”.

Supervisors: A.A. Kana and J.F.J. Pruyn. MA thesis. Delft, The Netherlands: Delft University of Technology, June 2024. URL: http://resolver.tudelft.nl/uuid:42c74b48-a4e7-4542-87ae-5320d11a027b.

[67] Vasileios Sideris et al. “Advancing Model-Based Systems Engineering in the Development of Naval Vessel Systems Architecture”. In: *Journal of Ship Production and Design* (2025). In press. URL: https://repository.tudelft.nl/record/uuid:42c74b48-a4e7-4542-87ae-5320d11a027b.

[68] Nancy Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press, 2012.

[69] International Council on Systems Engineering (INCOSE). *INCOSE Systems Engineering Vision 2035*. Tech. rep. San Diego, CA: INCOSE, 2023.

[70] Johan Cederbladh et al. “A Road-Map to Readily Available Early Validation and Verification of System Behaviour in Model-Based Systems Engineering using Software Engineering Best Practices”. In: *ACM Trans. Softw. Eng. Methodol.* 34.5 (May 2025). DOI: 10.1145/3708520. URL: https://doi.org/10.1145/3708520.

[71] Tyson Browning et al. “Reducing unwelcome surprises in project management”. In: 56 (Mar. 2015), pp. 53–62. URL: https://www.researchgate.net/publication/283878132_Reducing_unwelcome_surprises_in_project_management.

[72] J. Bach et al. *Bridging Safety and Systems Engineering – Organizational Challenges in MBSA*. Tech. rep. 2018. URL: https://pure.tue.nl/ws/portalfiles/portal/350816190/bridging-the-gap-between-requirements-engineering-and-systems-architecting-the-elephant-specification-language.pdf.

[73] Tyson Browning. “The Many Views of a Process: Toward a Process Architecture Framework for Product Development Processes”. In: *Systems Engineering* 12 (Dec. 2009), pp. 69–90. DOI: 10.1002/sys.20109.

A

Appendix

On the next page you will find images of the model.

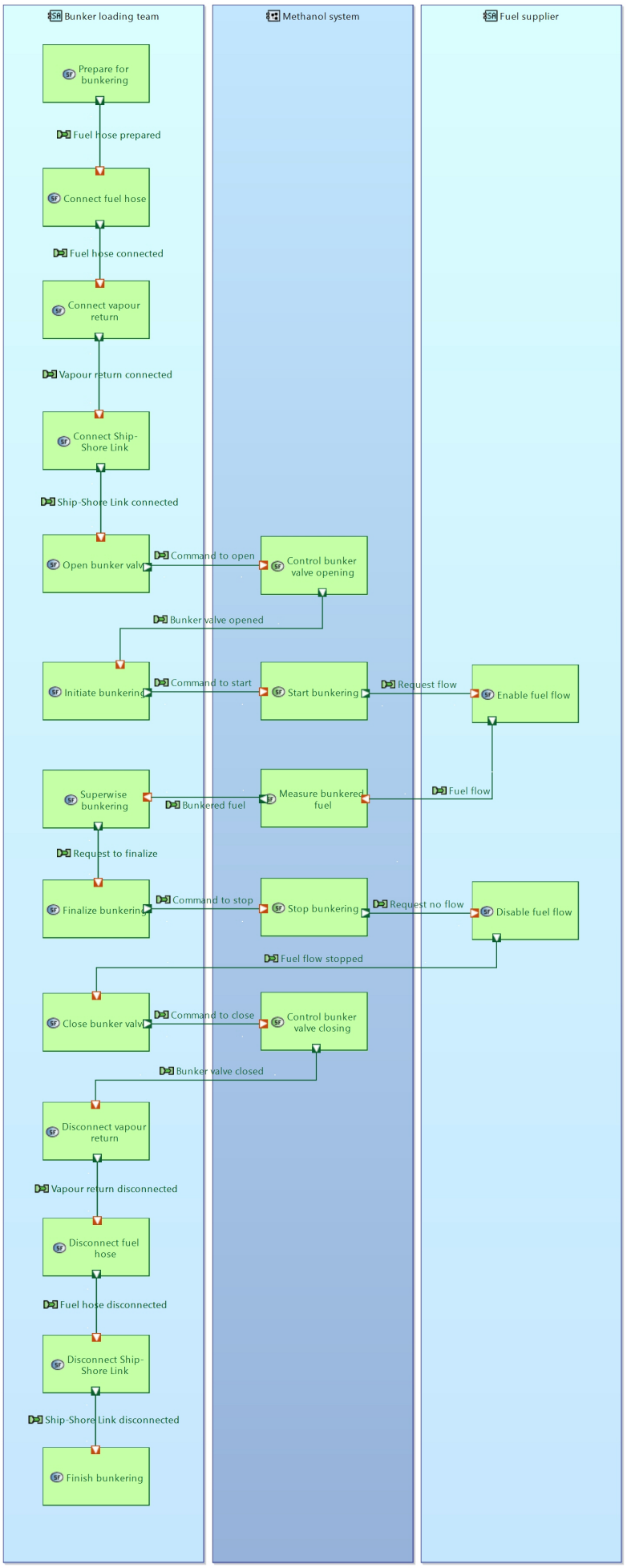


Figure A.1: The complete functional chain from top till bottom

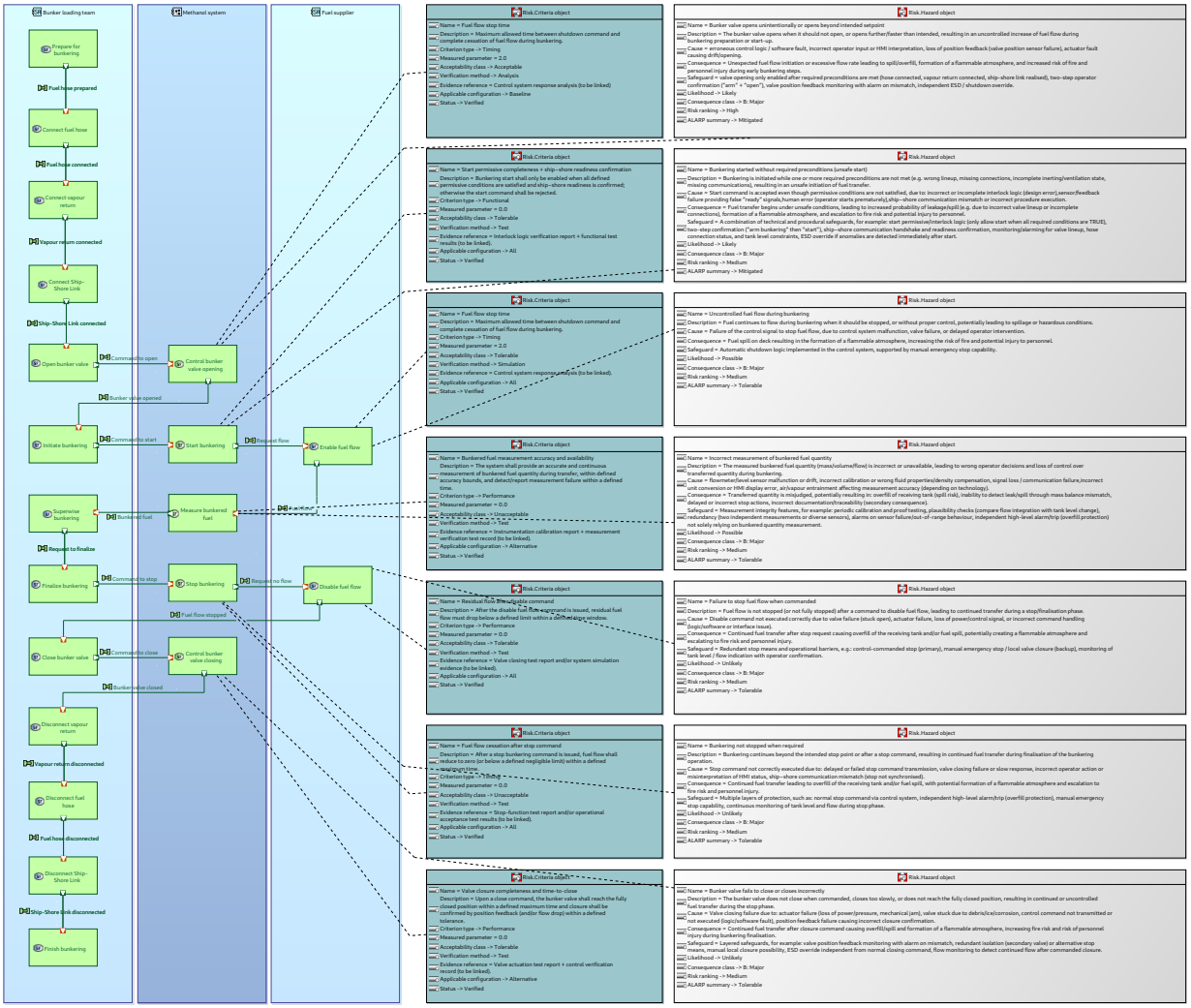


Figure A.2: Complete overview of the model with the Hazard objects and criterea objects connected to it (svg form)