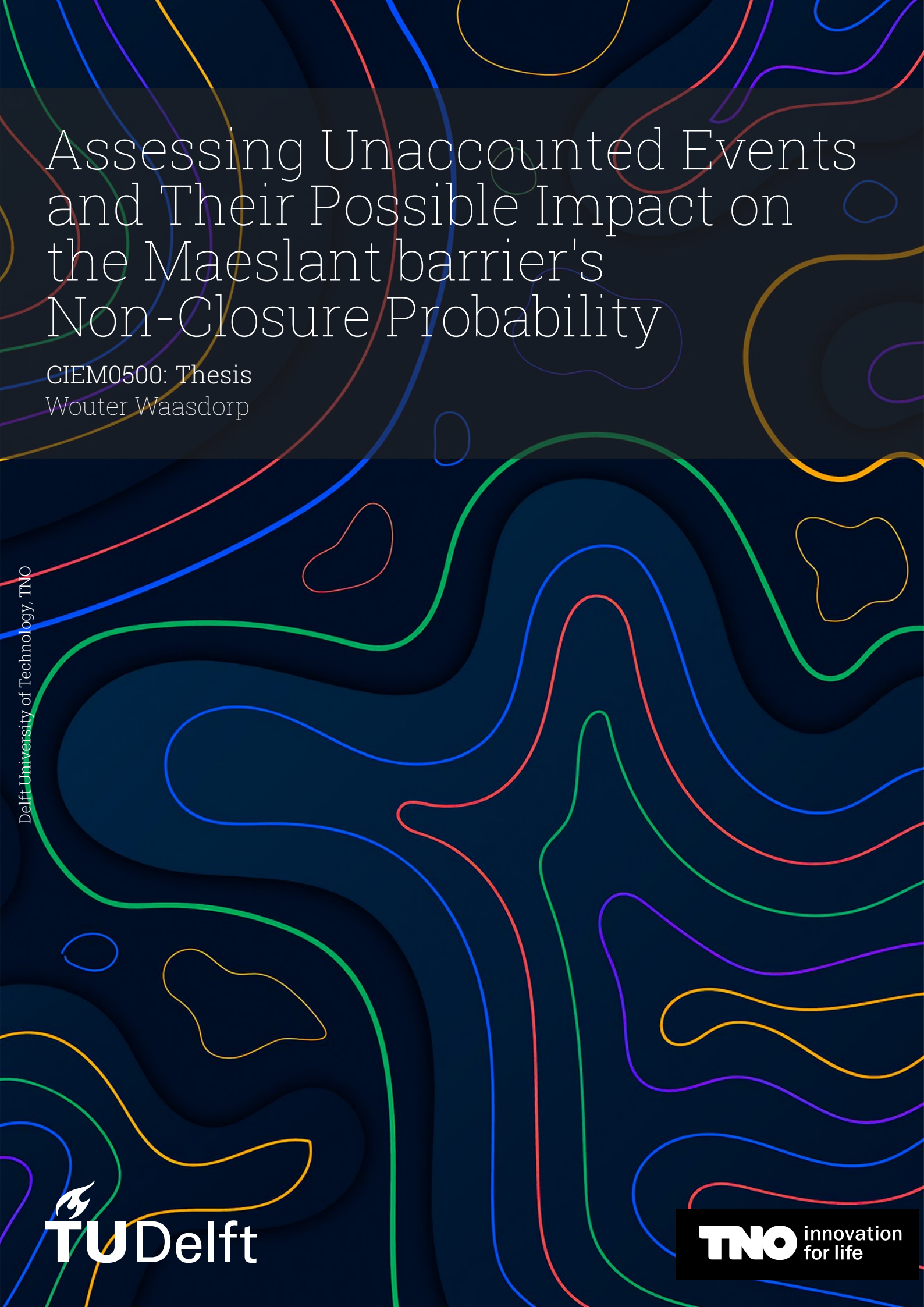
Assessing Unaccounted Events and Their Possible Impact on the Maeslant barrier's Non-Closure Probability

CIEM0500: Thesis

Wouter Waasdorp

Delft University of Technology, TNO



Assessing Unaccounted Events and Their Possible Impact on the Maeslant barrier's Non-Closure Probability

by

Wouter Waasdorp

Student Name	Student Number	Master track
Wouter Waasdorp	5383005	Hydraulic and Offshore Structures

Supervisors TU Delft:	Dr. ir. José Álvarez Antolínez
	Dr. ir. Alexander Bakker
Supervisors TNO:	Prof. dr. ir. Raphaël Steenbergen
	Dr. ir. Gina Torres Alves
Project Duration:	February 2025 - September 2025
Faculty:	Faculty of Civil Engineering and Geosciences, TU Delft
Company:	Dutch Organization for Applied Scientific Research (TNO)

Cover: Image source: Reddit, unknown artist 2021.
This thesis utilized the internal Microsoft 365 Copilot of TNO for writing Python scripts and occasionally for improving grammar and spelling

TU Delft

TNO innovation for life

Preface

This thesis marks the apotheosis of my Master's journey in Hydraulic and Offshore Structures at the TU Delft, conducted in collaboration with TNO. It explores the territory of unaccounted-for events in the Maeslant barrier's closure reliability analysis, a topic that combines engineering, uncertainty, and the importance of transparent risk assessment in flood defense.

The research was challenging but rewarding. It required navigating complex systems, engaging with experts, and developing methods to quantify what is often left unquantified. I am grateful for the guidance and support of my supervisors: Dr. ir. José Álvarez Antolínez, Dr. ir. Alexander Bakker, Prof. dr. ir. Raphaël Steenbergen, and Dr. ir. Gina Torres Alves, whose insights and encouragement were of great value throughout this process. I would also like to thank the experts who contributed their time and knowledge during the whole process. Their input formed the backbone of this work and highlighted the value of collaboration in engineering risk analysis.

Finally, after spending much time reading, talking, and thinking about the reliability and safety of one of the assets of the Dutch flood defense network, a song text from a Dutch band resonated with me. As Hang Youth said: "Geen gelul! De dijken moeten hoger." I wish any reader of this thesis the best of luck.

Wouter Waasdorp
Delft, the Netherlands, September 2025

Abstract

The Maeslant barrier is a storm surge barrier and a critical component of the Dutch coastal flood defense system. Its reliability is formally assessed through a Reliability and Availability (RA) analysis, which estimates the probability of non-closure during storm events. However, concerns have been raised regarding the completeness and transparency of this analysis, particularly the potential omission of relevant failure events. This thesis investigates whether a selected set of previously unaccounted-for events can be systematically identified and quantified to improve the accuracy of the non-closure probability.

A three-stage methodology was developed. First, a structured inventory of unaccounted-for events was constructed using HAZOP, FMEA, What-If, and external event screening techniques, mapped across four analytical dimensions. Second, the list was filtered based on estimated occurrence probability and quantifiability, resulting in a shortlist of three events: epistemically uncertain events, non-stationary component degradation, and the unverified reliability of human interventions. Third, these events were quantified using structured expert judgment, research into time-dependent fault tree modeling, and human reliability assessment.

Results indicate that these unaccounted-for events can alter the estimated non-closure probability, either increasing it by an order of magnitude or reducing it by up to 50%. Moreover, the analysis revealed limitations in the current RA analysis, including outdated reliability assumptions, a fragmented integration of human interventions, and a lack of empirical data. These findings support the need for a more transparent and adaptable RA framework. The discussion highlights that while completeness in risk assessment is theoretically unattainable, similar to the limitations of physical laws, models should strive for an optimal balance between complexity, traceability, and applicability.

Recommendations include developing a centralized component lifecycle database, maintaining a registry of previously unaccounted-for events, formally integrating the OPSCHEP model into the fault tree structure, and adopting structured human reliability verification. These changes can improve the accuracy, transparency, and credibility of the Maeslant barrier's non-closure probability and serve as a blueprint for other critical infrastructure systems.

Contents

1

Introduction

The Netherlands is a low-lying river delta known for its battle against water (Mostert, 2020). To ensure that the inhabitants of this delta are safe against flooding, an integrated network of dikes, dams, weirs, and storm surge barriers[1] is created, which is constantly under construction to ensure safety in the future. Movable storm surge barriers are a vital component of the Netherlands' flood defense system. These structures are designed not only to protect densely populated and economically critical areas from coastal flooding but also to maintain navigational access and preserve surrounding ecosystems (Walraven et al., 2022). These structures are able to do this because they consist of movable components that, under normal circumstances (e.g. no storm surge), remain open. These structures are strategically located at estuaries and are closed whenever an extreme storm surge is anticipated (L. Mooyaart & Jonkman, 2017).

One example of a storm surge barrier in the Netherlands is the Maeslant barrier, which is situated on the Nieuwe Waterweg. This barrier was built as part of the Dutch Deltaworks and has been in use since 1997 (L. Mooyaart & Jonkman, 2017). The barrier consists of two large gates housed in docks on opposite sides of the Nieuwe Waterweg. During extreme storm surges, the gates close to prevent water levels from exceeding the maximum thresholds that the inland dikes can withstand. By doing so, the Maeslant barrier safeguards approximately 2 million residents and significant areas of South Holland from potential flooding (Rijkswaterstaat, 2025a).

As sea levels rise and urban areas expand, coastal flood risk grows, prompting the need to strengthen coastal flood defenses (Hallegatte et al., 2013). The Maeslant barrier can fail in one of three ways: structurally, through overtopping and by operational errors. For the Maeslant barrier, non-closure [2] is identified as the primary failure mode (L. Mooyaart et al., 2025).

For storm surge barriers in the Netherlands, the probability of non-closure is estimated with a reliability and availability (RA) analysis (See section 2.4). The RA analysis generally uses fault and event trees (see Appendix A). In other sectors, RA analyses are known by various terms, such as probabilistic safety assessments, quantitative risk analyses, or similar combinations. These analyses are employed across diverse technological systems, including nuclear power plants, aircraft, space missions, and chemical facilities, to investigate low-probability, high-consequence events, particularly when data to quantify such risks are limited (Bier & Cox Jr, 2007) .

The report: "Wettelijke beoordeling Europoortkering I Dijktraject 208" ("Statutory Assessment of the Europoort Barrier I Dike Section 208")(Rijkswaterstaat, 2022a), questions the credibility of the

[1] A storm surge is a temporary and abnormal rise in sea level, primarily caused by strong onshore winds and low atmospheric pressure during storms. It poses a major flooding risk in low-lying coastal regions (National Ocean Service, NOAA, 2024).

[2] In the context of the Maeslant barrier, "non-closure" refers to the failure of the barrier to complete its intended closing operation when a closure request is issued during storm surge conditions.

RA analysis performed for the Maeslant barrier. Specifically, it states that the analysis cannot be independently verified due to a: “lack of transparency regarding underlying assumptions, input data, and modeling approach.” An example of this is the inability of experts to review the OPSCHEP-model (see subsection 2.4) due to modeling choices (Expert, Rijkswaterstaat & TU Delft 2025). This raises concerns about the completeness of the risk assessment, i.e. insinuating the possibility of the existence of events that are unaccounted for in the current failure to close probability calculation of the Maeslant barrier. From a scientific standpoint, the difficulty of reproduction undermines the credibility of the conclusions, which is problematic for a safety-critical system such as a movable storm surge barrier.

From a scientific perspective, these concerns expose a deeper methodological challenge: as RA models become more complex, their credibility increasingly depends on transparency, traceability, and interpretability (Aven, 2016; Mostert, 2018; Paté-Cornell, 1996; van Asselt & Renn, 2011). In safety-critical infrastructure such as the Maeslant barrier, the inability to clearly justify how risk estimates are derived, especially when they influence regulatory thresholds, constitutes a substantial risk. It is therefore not only a practical obligation but a scientific necessity to ensure that RA models remain comprehensible, justifiable, and open to critical evaluation.

Therefore, this thesis investigates the following question:

- Can a selected set of previously unaccounted-for events be systematically identified and quantified, and how can they be integrated into the non-closure probability calculation of the Maeslant barrier?

With the following sub-research questions:

- Which unaccounted events exist?
- How can these events be organized and filtered to produce a short-list for detailed analysis?
- How can these unaccounted events from the Short-list be quantified?
- How can these events be integrated in the non-closure probability calculation of the Maeslant barrier?

The thesis is structured to answer these questions as follows. Events not currently considered in the existing RA analysis and that may contribute to the barrier’s non-closure probability were first identified and compiled into a structured long-list. From this list, the top three most relevant or impactful events were selected. This is called the Short-list. These top three events were then quantitatively assessed and analyzed to evaluate their potential contribution to the overall non-closure probability. The structure of this thesis reflects this approach: Chapter 2 provides a system analysis of the Maeslant barrier, Chapter 3 outlines the methodology for making the Long-list, Short-list, and how to quantify the events on the Short-list, Chapter 4 presents the results of the lists and their analysis, and of the quantification and their analysis. Chapter 5 gives a discussion, after which Chapter 6 concludes the research and provides recommendations.

2

System analysis

This chapter presents a system analysis of the Maeslant barrier. The analysis follows a logical structure, beginning with the context and operation of the barrier itself. It then introduces the Reliability and Availability (RA) framework that Rijkswaterstaat[1] uses to assess the barrier's performance. This is followed by highlighting the limitations in the current RA analysis. These limitations motivate the need for a more complete and transparent assessment, which is the focus of the following chapters in which the research question is answered.

2.1. The Maeslant barrier

Movable storm surge barriers are a vital component of the Netherlands' flood defense system. The first of its kind in the Netherlands, the Hollandse IJssel Barrier, was completed in 1958. Since then, more than 50 storm surge barriers have been constructed worldwide (Trace-Kleeberg et al., 2023), including five in the Netherlands (L. Mooyaart & Jonkman, 2017). The global relevance of such barriers continues to grow, with at least 11 new projects underway in the United States, two barriers under construction in Belgium, and multiple similar projects being considered in Singapore (Jan De Nul Group, 2025; Lee et al., 2023; Orton et al., 2023). In response to rising sea levels and expanding urban areas, the Netherlands has continued to adapt its flood defense strategy to address both spatial and societal constraints (Hallegatte et al., 2013).

In the Netherlands, the decision to build movable storm surge barriers was often driven by the infeasibility of alternative flood defense strategies, like dams and dikes. Furthermore, reinforcing existing inland dikes, particularly in densely developed areas, was frequently deemed too complex, time-consuming, or socially disruptive (Rijkswaterstaat, 2024). During the 1980s, this was especially evident in the case of Rotterdam and Dordrecht, where strengthening existing defenses, mainly dikes, would have taken decades and required large-scale interventions in historic city centers. As a more practical solution, the Maeslant barrier was conceived. Construction began in 1991, and the barrier has been operational since 1997 (Jonkman & Merrell, 2024).

The Maeslant barrier is a component of the Dutch Delta Works, a system of dams, locks, dikes, and storm-surge barriers built in response to the North Sea Flood of 1953. Located at the mouth of the Rotterdam Harbor, the barrier plays a role in allowing uninterrupted access to one of the world's busiest ports while offering high levels of flood protection. Unlike many other barriers that remain closed or partially block waterways [2], the Maeslant barrier remains fully open under normal conditions and only

[1] Rijkswaterstaat is the executive agency of the Dutch Ministry of Infrastructure and Water Management. It is responsible for the design, construction, management, and maintenance of the main infrastructure facilities in the Netherlands, including waterways, roads, and flood defenses (Rijkswaterstaat, 2025c)

[2] Unlike the Maeslant barrier, which remains fully open under normal conditions, other Dutch storm surge barriers such as the Oosterschelde barrier and the Hartel barrier impose partial restrictions on waterways. The Oosterschelde barrier, for example, consists of sluice gates that are normally open but can close during storm surges, blocking navigation, which

closes during extreme storm surge events (Watson & Finkl, 1992). It protects approximately 2 million residents and extensive infrastructure in South Holland, making it an indispensable element of the flood protection strategy in the Netherlands (RijksWaterstaat, 2017).

After more than two decades of service, the Maeslant barrier faces a range of operational and structural challenges (Haasnoot et al., 2019). Maintaining such a complex system is demanding in both technical and logistical terms. Moreover, quantifying the reliability of the barrier over time has proven difficult, especially in light of rising sea levels, aging components, and the likelihood of more frequent closures (Jonkman & Merrell, 2024). These trends are raising questions about the future dependability of the structure and the robustness of the models used to assess its performance.

2.2. Technical overview

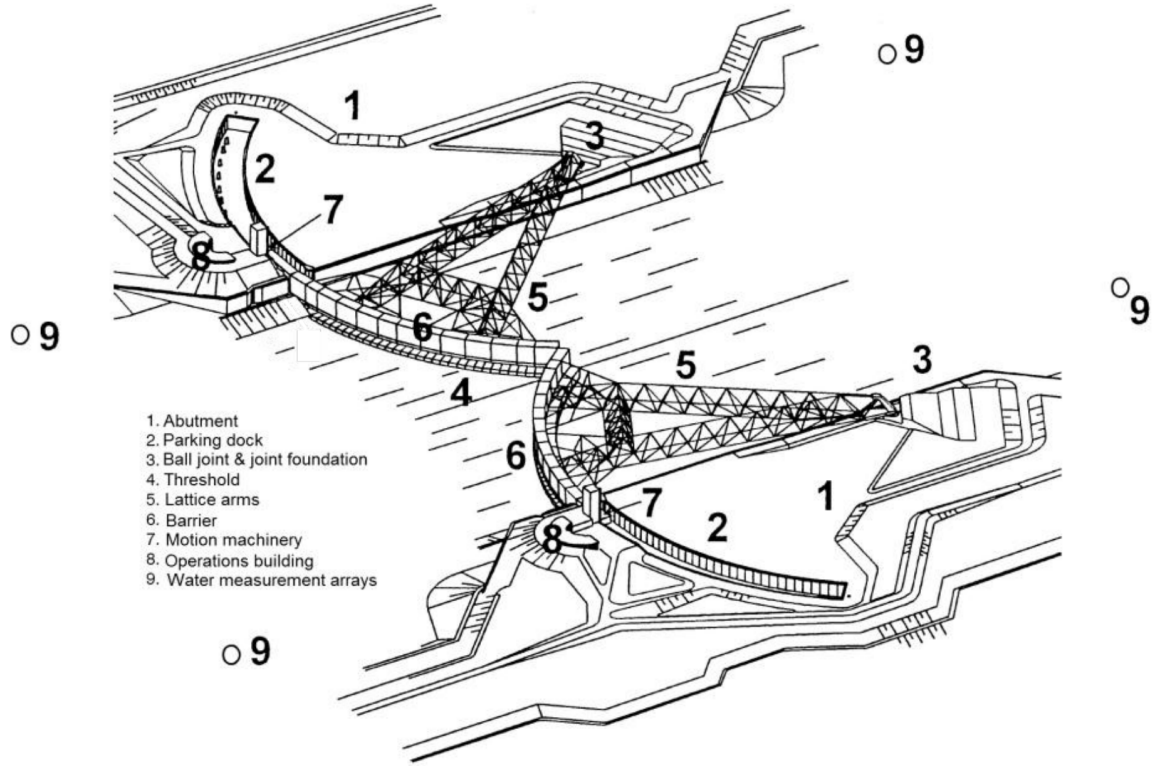


Figure 2.1: Schematic image of the Maeslant barrier and its components (Rijkswaterstaat, 2012). The numbers on the components coincide with the names listed in the legend in the left bottom corner of the figure.

Technically, the Maeslant barrier consists of two floating gates, each measuring 210 meters in length and 22 meters in height, spanning from -17 meters to +5 meters NAP[3] as shown in Figure 2.1, component number 6. These gates are anchored to the ground by a spherical bearing of 10 meters in diameter, weighing 680 tons (component number 3 in Figure 2.1) (Rijkswaterstaat, 2025a). When not in use, the gates are stored in docks on opposite sides of the waterway and rotated to position using large electric motors connected to gear systems mounted at the top of each gate, called the locomobile (respectively component numbers 2 and 7 in Figure 2.1).

Once aligned, the gates are flooded with water to sink them to the riverbed, forming a watertight seal. After the storm surge has passed, water is pumped out of the gate compartments, allowing air to enter naturally and enabling the gates to refloat and return to their docks. This unique floating-submersion mechanism enables the barrier to transition, relatively quickly, between open and closed states, while minimizing disruption to maritime traffic (World Shipping Council, 2023).

is limited to a sluice. Similarly, the Hartel barrier includes vertical lift gates that restrict both the height and width of the passage (Jonkman et al., 2016).

[3]Normaal Amsterdams Peil (NAP) is the standard reference level for measuring elevation in the Netherlands, roughly equivalent to mean sea level (Rijkswaterstaat, 2025b).

2.3. Operation and control system

The operation of the Maeslant barrier is fully automated and managed by the BOS[4], a sophisticated control system responsible for coordinating the entire Europoort barrier[5], which includes the Maeslant barrier, Hartel barrier, and Hartel sluice[6]. The BOS integrates data from multiple sources, including weather forecasts, water levels, and system status, to determine whether closure is necessary during storm surge events. When the waterlevels of 3 meters above NAP in Rotterdam and 2.9 meters in Dordrecht (Rijkswaterstaat, 2025a) are predicted, the BOS autonomously initiates the closure process. During this process, the best moment for closure is estimated. Early detection data from the meteorological station in Hoek van Holland provides sufficient lead time to prepare and execute the closure.

There are two main types of closures[7]:

- Peilsluiting (water level closure): A closure that is used when river (Rhine) discharge is within normal limits. In this case, the barrier can close when the sea water level exceeds the threshold of 2 meters above NAP without requiring special coordination regarding river flow.
- Kentering sluiting (turn-around or low water slack closure): A closure used when river discharge is high. . To make sure that the river (Rhine) discharge does not pose problems for the inland dikes, the closure is timed to coincide with tidal slack (the brief moment when water flow reverses). This coordination creates a basin in the inland water system.

Once the closure criteria are met, the movement phase is initiated controlled by the BESW(Control System Maeslant barrier), as shown in Figure 2.2. The gates are maneuvered into position using a combination of motorized rotation and buoyancy control. During this movement phase, buoyancy is carefully regulated to ensure the gates remain balanced as they are pushed forward. The locomobile drives the gates using motorized rotation during the closure sequence. The weight of the locomobile on the part of the gate that extends into the water causes the gate to lift slightly, making buoyancy regulation particularly important. Precise adjustments of the gate compartments' water content are necessary to keep the gates stable throughout this maneuvering.

[4]The BOS (Balance of System), referred to here as a decision and support system, encompasses a complex array of hardware and software components designed to monitor, analyze, and control the operation of the Maeslant barrier. This includes real-time data acquisition, predictive modeling, automated decision-making algorithms, and secure communication interfaces that collectively ensure the barrier responds accurately and autonomously to changing environmental conditions.

[5]The Europoort barrier is a collective term for a critical segment of the Dutch coastal flood defense system protecting the Rotterdam region. It includes the Maeslant barrier, the Hartel barrier, and the Hartel sluice (Rijkswaterstaat, 2013).

[6]The Hartel sluice is operated manually by personnel. While the BOS provides supporting information and coordination, the actual control of the sluice is not fully automated (Goorden et al., 2022).

[7]These two types of closures depend on the river discharge measured at Lobit, with a threshold of $6000 m^3/s$. When the discharge exceeds $6000 m^3/s$, the closure is classified as a kenteringsluiting; when it is below this threshold, it is considered a peilsluiting.

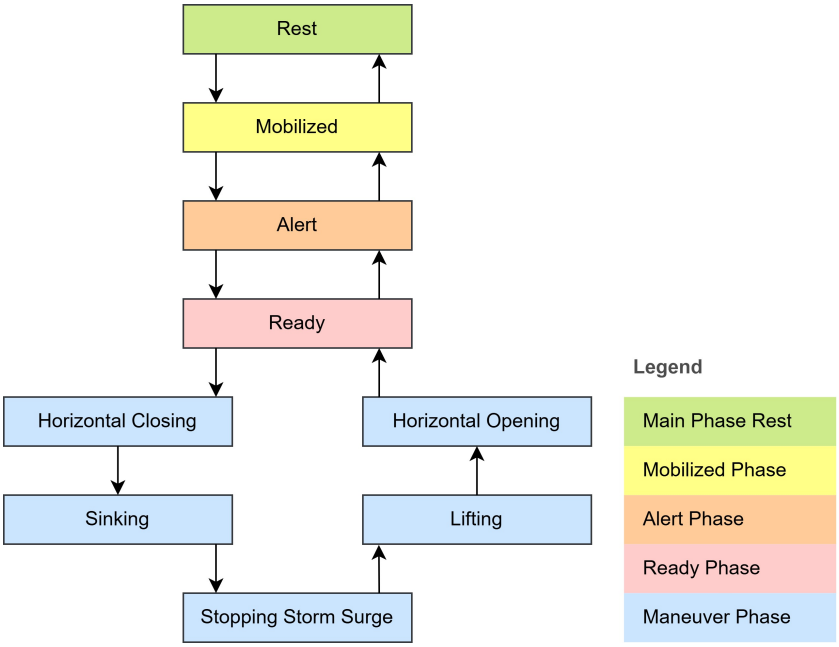


Figure 2.2: Simplified scheme of the closing sequence of the Maeslant barrier. Arrows indicate the direction of the sequence, starting from the top with "rest".

After the gates are in position, the second balancing phase is started. In this phase, the gates are carefully balanced to rest lightly on the threshold on top of the riverbed, maintaining minimal contact with the threshold while remaining nearly neutrally buoyant. This balance allows the gates to seal effectively under pressure while retaining the ability to be lifted rapidly if unexpected conditions occur. Achieving and maintaining this buoyancy near the threshold on top of the riverbed is a critical and complex part of the operation, requiring continuous fine-tuning of water levels in the gate compartments throughout the closure.

A simplified schematic overview of the BOS and the closing process of the Maeslant barrier is shown in Figure 2.3.

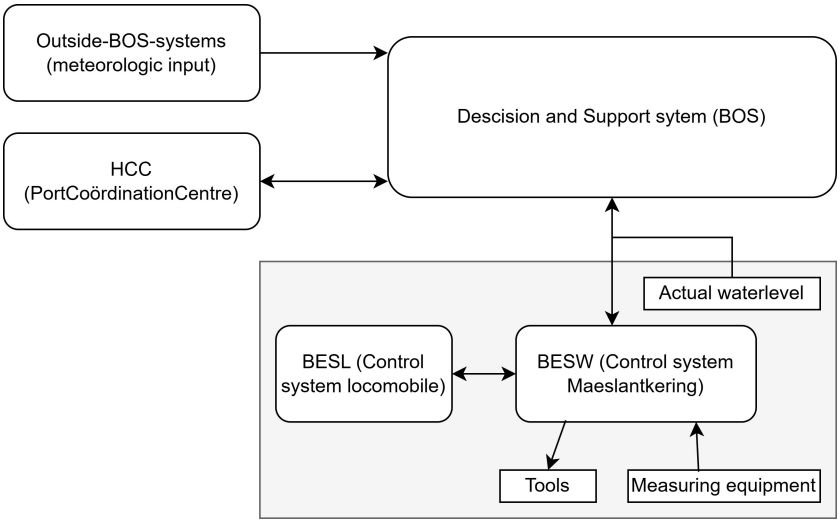


Figure 2.3: Simplified scheme of the BOS for solely the Maeslant barrier. Arrows indicate communication direction between the different systems listed, with BOS as the head-system.

2.4. Reliability and Availability (RA) Analysis

Reliability and Availability (RA) analysis' are a critical component in the engineering of movable infrastructure systems such as the Maeslant barrier. In general, reliability refers to how likely the Maeslant barrier is to function correctly when needed. Its availability is expressed as the chance of success per closure request. Availability for the Maeslant barrier refers to the probability that the barrier is fully operational and ready to respond when needed, which would be low during maintenance and high during the storm season (Trivedi & Bobbio, 2017).

Formal methodologies, such as those outlined in IEC 60300-3-1 (STANDARD & IEC, 2003), provide structured approaches for quantifying and modeling these attributes through techniques like Fault Tree Analysis (FTA) (see Appendix A). In storm surge barriers and other flood defense systems, organisations such as Rijkswaterstaat rely on RA analysis to ensure that the operational readiness remains within acceptable risk margins for non-closure and for structural integrity (Bakker, Busnach, et al., 2025; L. F. Mooyaart et al., 2023; van Maaren, 2018).

Reliability and Availability (RA) analyses rely on various inputs, including manufacturer data, historical records, estimated repair durations, and assumed failure rates derived from expert judgment. While these inputs are necessary to construct quantitative models, they can introduce uncertainties due to limited empirical validation or context-specific variability. Consequently, although RA models are a valuable tool for system assessment and decision-making, their results should be interpreted within the context of these underlying assumptions and the inherent unpredictability of real-world operational environments (Blanchard et al., 1990; Trivedi & Bobbio, 2017).

In the Netherlands, a strict form of risk-based asset management is applied to maintain the required closing probability of storm surge barriers (Kharoubi et al., 2024). The Maeslant barrier, for example, must achieve a non-closure probability of 1/100 (Government of the Netherlands, 2024). To meet this standard, Rijkswaterstaat implemented the "ProBO: Probabilistic Operations and Maintenance" framework, now referred to as "Risk-based Operations and Maintenance" (Kharoubi et al., 2023). ProBO is not part of the formal RA model but provides a broader asset management structure within which RA analyses are interpreted and acted upon. It encompasses three dimensions: technical, organizational, and contractual. The technical dimension includes risk analysis methods such as RA; the organizational dimension addresses planning, maintenance, and inspections; and the contractual dimension concerns performance-based service agreements with external parties. These dimensions are supported by the Deming cycle; Plan, Do, Check, Act, as a continuous improvement process (Kharoubi et al., 2023). Within this context, RA analysis serves as a critical input for performance evaluation, helping to prioritize interventions and ensure long-term reliability.

A RA analysis facilitates ongoing closure reliability monitoring and identifies improvement opportunities when needed (ProBO, 2017). The RA analysis usually is a highly detailed analysis that employs techniques like fault trees and event trees to evaluate all significant risks that could impact the structure's performance (see subsection A.2). This high level of detail allows for an efficient assessment of the effects of temporary changes (Bakker et al., 2022). The risks considered in the analysis are pre-defined, and if something is missing, it can still be added later (ProBO, 2017). This also means that many potential failure modes in the analysis may not have been observed yet.

In Appendix A, the key principles and computational steps of FTA are explained in detail. This includes the structure of fault trees, the logic behind gate operations, the treatment of dependencies, and the use of minimal cut sets. These explanations aim to provide a comprehensive understanding of how FTA is applied in the context of complex systems.

For the Maeslant barrier specifically, FTA is used to model and quantify the probability of non-closure by identifying combinations of component and system failures that could lead to operational failure during a closure request. This includes mechanical failures (e.g., gate movement), control system errors (e.g., BESW malfunction), and human intervention failures[8]. The resulting fault tree is used to estimate

[8]These human intervention failures are not directly in the FTA of the Maeslant barrier but, are later added to the minimal cutsets exported from the FTA. this is further explained in Section 2.4.

the overall non-closure probability under the assumption of random, independent failures (Webbers et al., 2008). In practice, however, the assumption of statistical independence between basic events is a simplification (Pinto et al., 2009). In complex systems like the Maeslant barrier, certain failures may share underlying causes or interact in unforeseen ways. While the current FTA includes shared failure causes, many potential correlations, such as those arising from aging infrastructure or deferred maintenance, are difficult to quantify and may be underrepresented (Dekker, 2016; Pinto et al., 2009; Webbers et al., 2008).

OPSCHEP model

Human intervention is a critical component in ensuring the Maeslant barrier meets its required reliability standard, particularly in situations where automated systems fail. To formally account for these human actions, Rijkswaterstaat developed the OPSCHEP (OKE Project Software for the Calculation of Human Error Probabilities) model, which contains predefined procedures and operator interventions that can be initiated during system failures or unexpected conditions (Rijkswaterstaat GPO – afdeling Instandhouding Constructies & Onderhoud (ICO), 2017). These human interventions are modeled within the RA analysis of the Maeslant barrier as follows; first, the minimal cut sets are calculated from the FTA (see Section A.3). Second, human interventions are then added, when there is a suitable human intervention, to these minimal cut sets to reduce the failure-to-close probability (Expert, Rijkswaterstaat 2025).

The inclusion of the HAD (Human Action Database) in the RA framework is intended to ensure that backup procedures are considered in the overall system reliability. These human actions act not only as reactive measures but also serve as redundancy when the BOS (Decision and Support System), the BESW (control system Maeslant barrier) or the mechanical components do not function as intended. However, the effectiveness of these interventions depends on training, procedural rigor, and operational readiness (Defensie, 2017; Hirotsu et al., 2001). While the HAD framework suggests potential reliability benefits, further investigation is needed to understand the extent to which these gains are supported by clearly defined operational standards and their consistent implementation (Rijkswaterstaat, 2022a).

2.4.1. The bathtub curve and preconditions for FTA

As mentioned before, most FTAs are limited by preconditions, the FTA of the Maeslant barrier included. These preconditions are derived from the operational state of the system, using the bathtub curve (Figure 2.4). The bathtub curve is a standard reliability model that describes how a system's or component's failure rate evolves over time (Blanchard et al., 1990). It is divided into three phases:

- A decreasing failure rate during the initial early failure period.
- A constant failure rate throughout the useful life phase.
- An increasing failure rate in the wear-out phase.

From a scientific standpoint, this conceptual model is useful but not neutral; it imposes assumptions that directly influence risk estimation (Jonker & Pennink, 2010). If the actual failure behavior deviates from the assumed phase (e.g., the system is aging but still modeled as in its useful life), the calculated probabilities may become misleading. This issue is particularly relevant for complex, aging infrastructure such as the Maeslant barrier, where transitions between life phases are uncertain and may not be adequately captured by a stationary failure model. Therefore, understanding which phase the system is in is not just a modeling formality, but a substantive determinant of whether the RA output is valid (L. Mooyaart et al., 2025; van Maaren, 2018).

Only the middle phase of the bathtub curve, where the failure rate remains approximately constant and failures occur randomly, aligns with the foundational assumptions of most FTA's. FTA typically assumes that failure probabilities are time-independent and statistically independent, which holds only if the system is in this stable "useful life" phase.

While it is theoretically possible to model different life phases using more advanced techniques, such as time-dependent reliability models or non-stationary Fault Tree Analysis (FTA), the current RA framework used for the Maeslant barrier does not implement these approaches. Instead, it is built on the

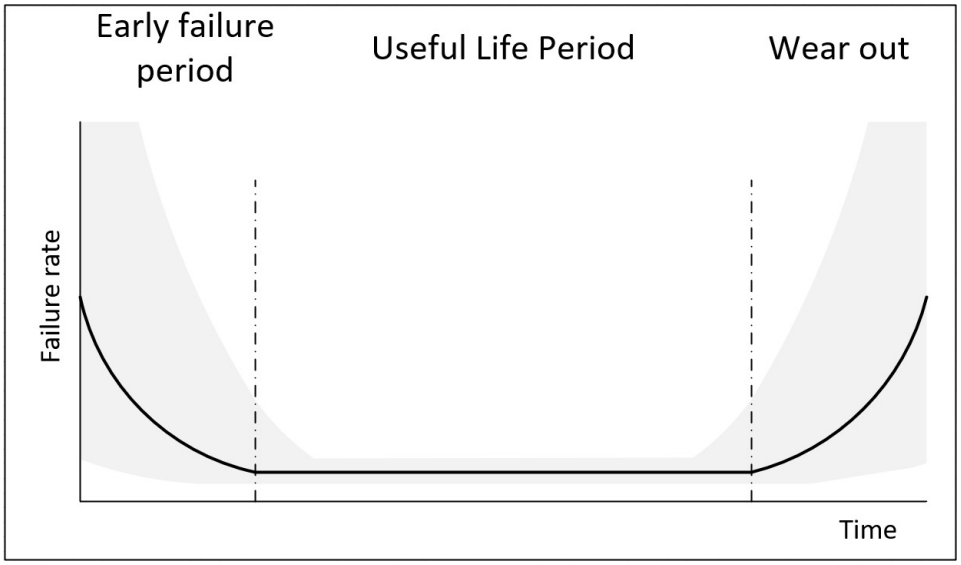


Figure 2.4: The standard bathtub curve illustrating the evolution of failure rates over time. The horizontal is depicting time, and the vertical axis is depicting the failure rate. Where the failure rate is constant is considered to be the useful life period.

assumption of stationary failure rates, where time-dependent aging effects are either considered negligible or assumed to be mitigated through routine maintenance interventions (Rijkswaterstaat, 2022a). However, this assumption introduces potential risks: as infrastructure ages, its failure behavior can deviate from the stable patterns assumed in the model. L. Mooyaart et al. (2025) highlights that the timing of transitions between life phases is often uncertain and not explicitly captured in static RA models, also shown in Figure 2.5. This underscores the importance of regularly evaluating whether the preconditions underlying the model still reflect the physical state and operational context of the system (van Maaren, 2018).

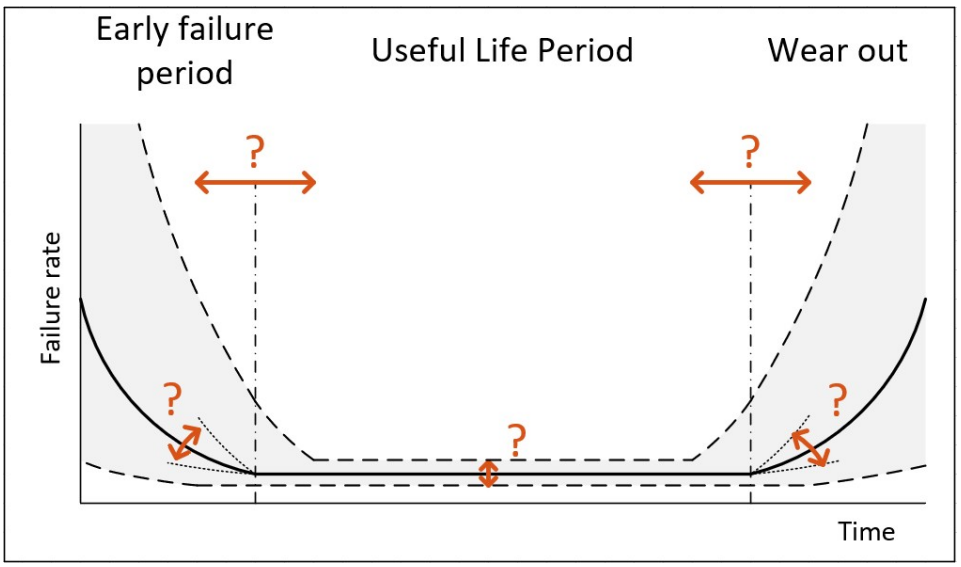


Figure 2.5: Bathtub curve uncertainty (Mooyaart, 2025). The horizontal is depicting time, and the vertical axis is depicting the failure rate. The orange arrows and question marks are depicting the uncertainty in failure rate.

If these dynamics are not reflected in the RA model, the fault tree may underestimate/overestimate failure likelihoods, leading to a warped sense of reliability. In short, adherence to these preconditions determines whether the FTA provides a realistic picture of system risk.

Another key assumption in the reliability assessment of the Maeslant Storm Surge Barrier is that the probability of non-closure is independent of the characteristics of the storm itself. This simplification is deemed necessary because the barrier is rarely operated under full storm conditions, making empirical performance data under such conditions scarce. As a result, failure probabilities are often derived from expert judgment or generalized failure databases, rather than direct observation. This introduces significant uncertainty, particularly since the barrier's operational reliability may be influenced by storm-specific factors such as wind direction, wave action, or surge dynamics. The assumption of independence allows for tractable modeling but may obscure critical dependencies that affect real-world performance, especially in extreme or compound storm events (Bakker, Busnach, et al., 2025). In addition, it is contradicted by the assumption that the failure-to-close probability decreases when a storm becomes more severe, due to a lower probability of a wrong closure decision (Expert, Rijkswaterstaat & TU Delft 2025).

2.4.2. Observations on the current FTA

The following observations were identified during the review of the current RA framework and are reported here as such. First, the analysis of current dominant failure paths showed that the dominant failure path in the current FTA is associated with software reliability. The software reliability values used in the model are derived from an outdated estimation technique, the TDT-model (van Otterloo, 2003). This technique, while once standard, has since been criticized in academic literature for its unreliable estimates (Brandt et al., 2011). A more modern approach called TOPAAS, which is already in use in Rijkswaterstaat, could provide more accurate assessments (Brandt et al., 2011).

A second observation concerns the current implementation of the OPSCHEP model in relation to the FTA. At present, these two models are separated (see Section 2.4). This post-hoc combination makes it difficult to identify truly dominant failure paths, because what appears critical in the FTA alone may in fact be mitigable through procedures already represented in OPSCHEP.

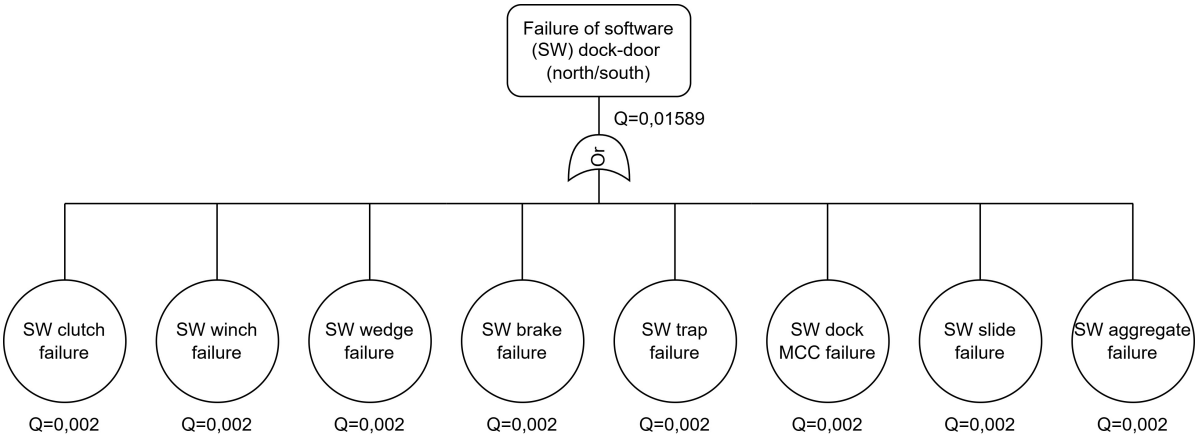
The current dominant failure path in the FTA originates from the dockdoor steering software on both the north and south sides of the Maeslant barrier (see Figure 2.6a). As previously discussed, the reliability of this software is based on an outdated guideline. When the reliability class of this software component is adjusted to one level higher [9], as shown in Figure 2.6b, the overall failure-to-close probability of the Maeslant barrier decreases from $P = 0.7$ to $P = 0.56$.

When the reliability of the dockdoor steering software is adjusted, another recurring failure path emerges as critical in the analysis. However, this is non-trivial to identify, as its complexity appears to stem from a combination of lower-level component interactions and conditional dependencies that are not immediately visible. The navigation through the tree becomes difficult due to branches. These branches emerge 10-12 layers deep when following a new dominant failure path, and all show almost the same failure probability, but the differences and their origin are non-trivial to identify.

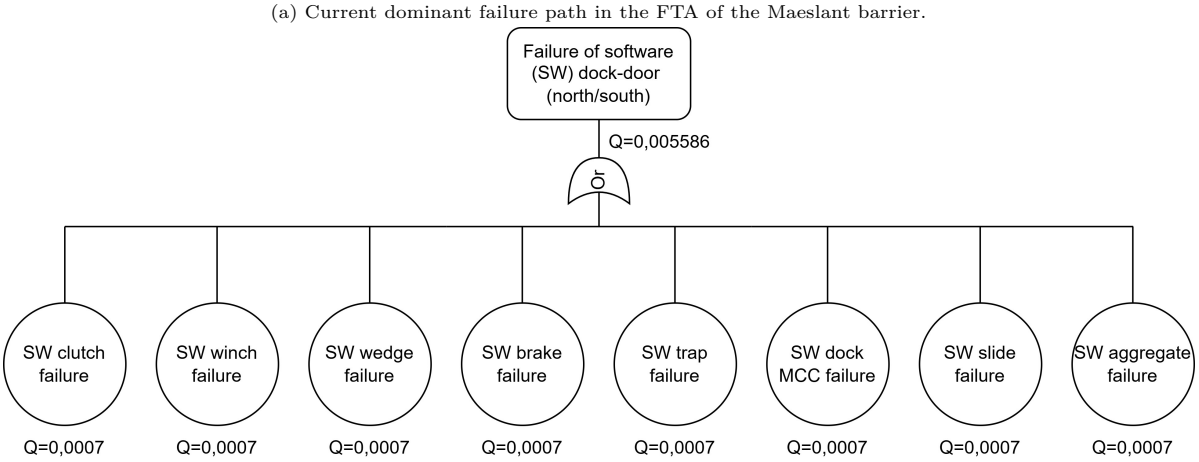
Upon closer inspection, a recurring component becomes apparent: the failure of a specific motherboard. This component appears consistently across all the new dominant branches, typically around 20 to 22 layers deep into the fault tree. This motherboard failure acts as a common node, suggesting it plays a critical role in the system's vulnerability (once the software reliability is improved). Its repeated presence across multiple paths indicates that it may be a structural weak point in the current design or modeling assumptions.

Another observation from the fault tree analysis is the presence of components with potentially unrealistic failure probabilities. In several instances, basic events are assigned a failure probability of exactly $P = 0$, implying absolute reliability, while some others are set to $P = 1$, indicating certain failure. The complex modeling of the electrical and computer systems makes it non-trivial to identify the origin of differences in failure probabilities between seemingly identical components. Without access to clearer documentation, it is difficult to determine whether these differences are intentional or the result of inconsistent modeling.

[9] The reliability of software according to the TDT-model used, is defined by different reliability classes (e.g., A, B, C...). These classes go from most reliable to least reliable, each having their own failure probability



(a) Current dominant failure path in the FTA of the Maeslant barrier.



(b) Dominant failure path with adjusted probabilities (all shifted one class lower).

Figure 2.6: Dominant failure paths in the FTA of the Maeslant barrier: (a) using current reliability assumptions, and (b) after adjusting software probabilities. The figure is an illustration from the FTA of the Maeslant barrier which is programmed in Reliability Workbench from Isograph (Ltd., 2025). The circles are basic events, where the "Q" stands for probability of occurrence of said basic event. The "Q" on top stands for failure probability of the SW of the dock-door.

In summary, these observations suggest that the current FTA includes outdated reliability assumptions, limited integration of human interventions, and potentially inconsistent treatment of component failure probabilities. Such issues may obscure the true dominant failure paths and therefore compromise the transparency and credibility of the analysis. These concerns form the basis for calling for a more complete and transparent risk analysis in the following section.

2.5. Calling for a more complete and transparent risk analysis

Very extensive, highly detailed fault trees can be difficult to work with and may lack transparency, particularly when assumptions and data inputs are not explicitly documented or verifiable (Aven, 2016; Mostert, 2018; Paté-Cornell, 1996; van Asselt & Renn, 2011; Webbers et al., 2008). This concern is not purely theoretical: Rijkswaterstaat has publicly expressed doubt regarding the operational reliability of the Maeslant barrier within the broader flood defense system in South Holland, stating that action is needed in the coming years to address these vulnerabilities (Rijkswaterstaat, 2021, 2022a, 2022b).

The issue of incompleteness in the current RA analysis has been raised by several sources like Bakker, Busnach, et al. (2025) and Webbers et al. (2008). More broadly, the completeness of risk assessments is inherently reliant on iterative expert input, multidisciplinary perspectives, and continuous re-evaluation of underlying assumptions (Pinto et al., 2009). However, observations from the current calculation (see Section 2.4.2) indicate that the current RA framework used for the Maeslant barrier may not fully align with the standards for transparency and completeness. These observations note that certain critical

assumptions are built on outdated reliability estimation techniques and that uncertainties are not always addressed in a systematic manner. CSK Review Team (2021) states that rare but high-impact failure modes may not be adequately considered, and that it is “full of mistakes”. This forms the central scientific problem addressed in this thesis: Can a selected set of previously unaccounted-for events be systematically identified and quantified, and how can they be integrated into the non-closure probability calculation of the Maeslant barrier?

In summary, the Maeslant barrier is a highly complex and critical infrastructure asset that depends on both automated systems and human intervention to operate reliably (Rijkswaterstaat, 2022a). Yet concerns about model transparency, traceability, and the potential omission of critical events reveal the need for a more complete approach. These challenges motivate the investigative methods presented in the following chapter.

3

Methodology

This chapter outlines a structured methodology to identify and quantify events not yet included in the Maeslant barrier's non-closure probability calculation. Building on the gaps in the current RA analysis (Chapter 2), the approach systematically uncovered, filtered, and quantified relevant events. It began with a broad inventory of events using HAZOP (Hazard and Operability Analysis), FMEA (Failure Modes and Effects Analysis), What-If Analysis, and External Event Screening across four analytical dimensions, supported by expert input. The list was then narrowed based on preliminary probability estimation and quantifiability, and the selected events were quantified using probabilistic techniques such as expert judgment, fault tree research, and human reliability analysis. This ensures both conceptual relevance and analytical rigor.

3.1. Overview of Methodology

The methodology of this research followed a three-stage approach (Figure 3.1). This structure was designed to systematically address the limitations identified in the current RA model for the Maeslant barrier. The process began by acknowledging and investigating potential incompleteness[1] in the existing analysis. Stage 1 involved the development of a comprehensive long-list of potentially unaccounted events, using multiple analytical inputs. In Stage 2, this list was refined into a short-list through a filtering process based on quantifiability and estimated contribution to the non-closure probability. In Stage 3, the shortlisted events were quantified using methods suited to their characteristics.

Although these stages are presented sequentially, the methodology was applied in an iterative manner. Insights gained during later stages were used to revisit earlier assumptions and refine the selection of events. For example, the quantification process in Stage 3 revealed dependencies that required re-examining the screening criteria of Stage 2. In this way, the methodology ensured that the final set of quantified events reflects both theoretical completeness and practical feasibility.

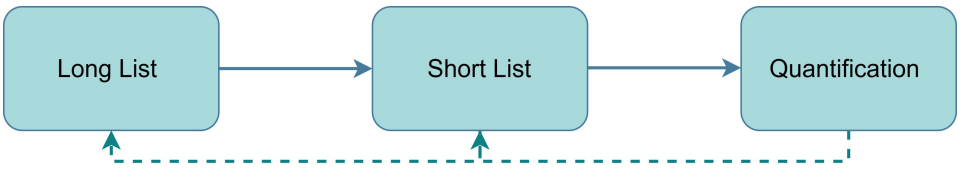


Figure 3.1: Overview of the Methodology: "Three-Stage Rocket". The methodology is followed from left to right, with the dashed arrows indicating the iterative nature of the methodology.

[1] Incompleteness refers to unaccounted events and missing data in the current RA model for the Maeslant barrier.

3.2. Stage 1: Long-List

The objective of this section was to independently identify events that may contribute to the non-closure probability of the Maeslant barrier but are currently not considered in the existing failure probability model.

The methods applied in this stage of the study, FMEA, HAZOP, What-If Analysis, and External Event Screening, are standard approaches outlined in the Red Book for systematically identifying potential failure events (Schüller et al., 1997) (see subsection 3.2.1). These methods originate from established industrial safety practices and have been formalized to ensure completeness and consistency in RA analyses. Their importance lies in structuring the identification of events in a way that minimizes the chance of overlooking events. In the context of the Maeslant barrier, using these methods helps to ensure that both common and less obvious events are captured, laying a strong foundation for a quantitative analysis.

Each technique was applied using four analytical dimensions, as shown by L. Mooyaart et al. (2025), with an added 4th axis of operation sequence, to ensure consistency and thoroughness (see Figure 3.2). Using these dimensions, each identified event exists somewhere on the analytical axis. Normally, the development of long- and short-lists is done by a team of experts to ensure a broad and thorough perspective. In this study, the process was carried out independently by a single researcher, the author, which is less common and brings some limitations, e.g. accommodating multiple roles within the event identification process where normally these roles are for different experts who try to complete each other, like a meeting leader, a structural expert, and a software expert.

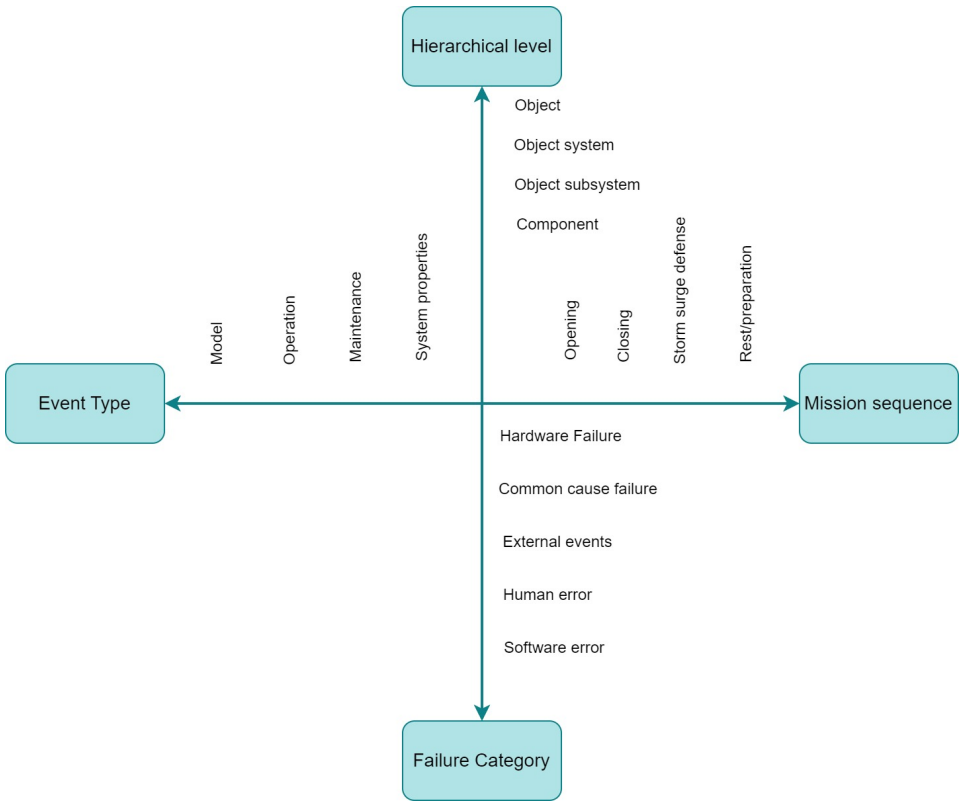


Figure 3.2: Four analytical dimensions that were used to systematically identify unaccounted events. Each axis is representing an analytical dimension. The horizontal-left axis is representing "event type", the horizontal-right is representing "mission sequence", the vertical-top axis is representing "hierarchical level", and the horizontal-bottom axis is representing "failure category".

Through this structured approach, the study develops a list of previously unaccounted-for events, enabling a more robust probabilistic modeling of the Maeslant barriers non-closure probability, shown in figure 3.3. In the following subsections, further explanations of identification methods are given, and

a step-by-step approach for event identification is provided.

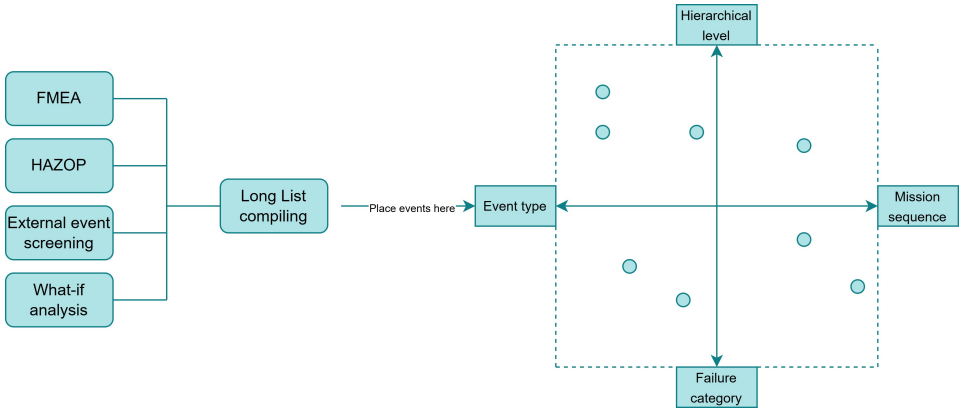


Figure 3.3: Stage 1 methodology showing how the axis are used with the identification methods. The four identification methods are used along side the four analytical dimensions ensuring overall coverage.

3.2.1. Event identification methods

The definitions for HAZOP, FMEA and What-if analysis are mostly paraphrased from the Redbook (Schüller et al., 1997) and for External event screening it is paraphrased from Rijkswaterstaat (ProBO, 2017). By combining these four methods, the analysis aimed to ensure coverage of both systematic and creative perspectives, as well as internal and external hazards. This triangulation reduced the risk of overlooking relevant unaccounted events.

Hazard and Operability Study (HAZOP)

HAZOP is a structured and systematic method for identifying potential hazards and operability problems in technical systems. It was originally developed for the chemical process industry but is now applied across a wide range of engineering domains, including infrastructure and control systems. The technique is based on examining system elements against a set of predefined guide words (e.g., “no,” “more,” “less,” “as well as”) to uncover possible deviations from intended functions (Kletz, 2018). Each deviation is then analyzed in terms of its possible causes, its consequences for system performance, and existing safeguards. The output of a HAZOP session is a structured list of deviations, their origins, and their potential impact on system safety and reliability.

In practice, HAZOP is typically conducted as a group exercise involving experts from different disciplines, which allows for both technical detail and cross-functional insight. While the method is qualitative, it often forms the foundation for more quantitative analyses, such as fault trees or event trees. No explicit equations are used in HAZOP, but its structured, tabular format lends itself to systematic documentation and later translation into probabilistic models.

The main strengths of HAZOP are its ability to (i) systematically identify a comprehensive range of deviations, including rare or unexpected interactions; (ii) highlight design and operational weaknesses early; and (iii) create a documented basis for further analysis. Its limitations are that it (i) is resource-intensive, requiring significant expert involvement; (ii) depends strongly on the knowledge and experience of participants; and (iii) does not directly provide quantitative probabilities, requiring follow-up methods to assign failure likelihoods.

In this research, HAZOP was applied as an event identification method to ensure that both technical and operational deviations of the Maeslant barrier were captured in a structured way. This was particularly important given the study’s focus on unaccounted events. By applying HAZOP, a comprehensive initial set of potential events was generated, forming the foundation for subsequent screening, prioritization, and quantification steps.

Failure Modes and Effects Analysis (FMEA)

FMEA is a systematic technique for identifying and analyzing potential failure modes of a system, their causes, and their effects on system performance (International Electrotechnical Commission, 2018;

Stamatis, 2003). It was originally developed in the aerospace industry in the 1960s and has since become a widely used reliability engineering tool across sectors such as automotive, manufacturing, and infrastructure. The process begins by listing system components or functions, identifying how each might fail (failure modes), and then assessing the consequences of those failures (effects). For each failure mode, potential causes are also identified and documented.

A key feature of FMEA is the prioritization of risks through scoring. In its traditional form, each failure mode is assigned three values: a severity (S), occurrence (O), and detection (D) rating. The product of these values forms the Risk Priority Number (RPN), calculated as:

$$RPN = S \times O \times D \tag{3.1}$$

The RPN provides a relative measure to compare failure modes and to prioritize mitigation actions. Modern adaptations of FMEA also include fuzzy logic or probabilistic extensions, but the underlying principle of structured prioritization remains the same.

The strengths of FMEA are that it (i) provides a structured approach for systematically evaluating failure modes; (ii) facilitates prioritization by highlighting the most critical issues; and (iii) promotes interdisciplinary collaboration through its team-based implementation. However, its limitations include (i) subjectivity in scoring, as ratings often depend on expert judgment; (ii) a tendency to focus on single-point failures rather than complex interactions; and (iii) limited scalability in very large or highly interdependent systems.

In this research, FMEA was applied as an event identification method to capture potential failure modes of key subsystems of the Maeslant barrier. By evaluating their possible causes and consequences, FMEA contributed to identifying unaccounted events that could influence closure reliability. The structured prioritization aspect of FMEA also helped in screening events for further quantification, complementing the broader perspectives offered by other methods.

What-if Analysis

The What-if Analysis is a qualitative risk identification method that relies on systematically asking structured "what if" questions about deviations, failures, or unexpected conditions in a system (Center for Chemical Process Safety, 2008). Typical questions include: "What if component X fails to operate?", "What if operator Y performs an incorrect action?", or "What if environmental condition Z occurs?". Each question is then analyzed to identify potential causes, consequences, and existing safeguards. The results are usually documented in tabular form, listing the initiating condition, its potential effects, and possible corrective actions.

What-if Analysis is particularly suited to the early stages of risk assessment, when system knowledge may be incomplete but brainstorming by subject matter experts can highlight vulnerabilities. Unlike structured methods such as HAZOP, it does not rely on predefined guide words; instead, it depends on the creativity, experience, and diversity of the participants.

The strengths of What-if Analysis are that it (i) is flexible and easy to apply to almost any system; (ii) encourages wide-ranging brainstorming that can reveal issues not captured by more formal methods; and (iii) requires fewer resources and less preparation than structured approaches such as HAZOP. Its limitations are that it (i) is less systematic, and therefore risks overlooking certain failure mechanisms; (ii) depends strongly on the expertise and imagination of the participants; and (iii) produces qualitative rather than quantitative results, requiring follow-up methods for probabilistic evaluation.

In this research, What-if Analysis was applied alongside other event identification methods to capture a broad range of potential unaccounted events for the Maeslant barrier. Its flexibility allowed the identification of scenarios that might not emerge through more rigid methods, particularly those related to unusual operating conditions or rare combinations of events. This ensured that the long-list of candidate events included a diverse range of possibilities before screening and prioritization.

External Event Screening

External Event Screening is a method used to identify and assess hazards that originate outside the boundaries of the technical system under study (International Atomic Energy Agency, 2003; Melchers,

1999). Such events include natural hazards (e.g., extreme weather, flooding, earthquakes), external technical failures (e.g., power supply interruptions), or human-induced factors (e.g., shipping accidents, cyber-attacks). The aim is to determine which external events are credible, how they could affect the system, and whether they should be included in further reliability analysis.

The screening process typically follows a structured sequence: (i) compile a broad list of potential external hazards using historical data, literature, and expert judgment; (ii) screen the list based on relevance, likelihood, and potential impact; and (iii) retain only those events that could plausibly contribute to the top-event probability. This process avoids overloading the fault tree or risk model with irrelevant or negligible events, while ensuring that major external influences are not overlooked.

The strengths of External Event Screening are that it (i) explicitly broadens the scope of the analysis beyond internal technical failures; (ii) ensures that low-frequency but high-consequence events are considered; and (iii) creates a structured basis for deciding which external factors to model quantitatively. Its limitations are that it (i) depends on the availability and quality of historical data; (ii) involves subjective judgments when assessing plausibility; and (iii) may still miss unknown or unprecedented events.

In this research, External Event Screening was applied to account for hazards to the Maeslant barrier that originate outside the mechanical and control subsystems, such as environmental or operational disturbances. By systematically reviewing and filtering potential external hazards, the method ensured that the long-list of unaccounted events captured influences beyond the internal system boundaries, which is essential for a comprehensive reliability assessment.

For each technique, an effort was made to systematically map insights to the relevant subsystem (e.g., hydraulics, sensors, communications), identify specific failure causes (e.g., mechanical, human, software), categorize them by physical domain (e.g., electrical, mechanical, hydraulic), and link them to their corresponding stage in the closure operation sequence. This matrixed approach tried to ensure that the entire system is looked at and that identified events are not isolated but seen in relation to their context and system dependencies.

3.2.2. Step-by-Step Procedure for Event Identification

The development of the long-list of unaccounted-for events follows a structured and iterative analysis process, visualized in Figure 3.3. The first step was to decide what parts of the system will be included in the analysis; this means both the technical parts (like machines and electronics) and the human roles (like operators). Once that's clear, a table was created to help organize the analysis. This table looks at the system from four angles: which part of the system is involved, what caused the failure, what kind of component it is, and when in the operation the issue happened. This helps make sure nothing important is missed and that everything is sorted in a clear way.

With this analytical tool in place, multiple risk identification methods were applied in parallel:

- FMEA: For each component, possible failure modes were identified and assessed using three criteria: severity (S), occurrence (O), and detectability (D). These are combined into a Risk Priority Number (RPN = S × O × D). Typical FMEA questions include, but are not limited to: "How could this component fail?" and "What would be the effect of this failure on the system?"
- HAZOP: Applied to subsystem-function pairs using structured guide words to explore deviations from normal operation. Guide words include:
  - No / Not: complete absence (e.g., no signal)
  - More / Less: quantitative deviations (e.g., more flow)
  - As Well As: additional elements present
  - Part Of: incomplete action or flow
  - Reverse: reversal of intended direction (e.g., reverse signal)

  - Late / Early: timing deviations

  These guide words stimulated systematic thinking about how each function might deviate and what the implications would be.

- External Event Analysis: Focused on risks originating outside the system boundaries. This includes natural hazards (e.g., lightning, extreme winds), infrastructure dependencies (e.g., loss of grid power), and third-party interference (e.g., shipping traffic).
- What-If Analysis: A brainstorming approach structured around hypothetical failure questions. The analyst explored edge-case scenarios using prompts like: "What if this signal is delayed?" "What if the backup doesn't activate?" or "What if environmental conditions differ from those assumed in the model?" The purpose was to capture complex interactions and rare but plausible situations.

Each of these methods generated a list of candidate failure events. These were then compiled into a consolidated event list. During compilation, events are reviewed for duplicates, mapped across the four analysis axes, and refined for clarity.

Through the combination of these methods and consistent mapping onto a shared analytical framework, the study produced a reproducible, structured, and exhaustive list of potentially unaccounted or possibly underestimated failure events. This list formed the foundation for further expert elicitation and probabilistic modeling to quantify their contribution to the overall non-closure probability.

3.3. Stage 2: Short-list

This study applied a filtering process to identify a short-list of events that are both relevant and suitable for quantification, see Figure 3.4. This was done by educated estimates and fact-checking through sources such as de Jong (2024), Rijkswaterstaat (2016), Royal Netherlands Meteorological Institute (KNMI) (2025), van Maaren (2018), and Webbers et al. (2008). The purpose of this step was to focus the subsequent quantification effort on the most relevant and feasible events, while avoiding unnecessary detail that would not contribute meaningfully to the overall reliability analysis.

The first filter was based on order of magnitude: events with an estimated probability of occurrence significantly lower than the threshold of 1/100 per operational cycle are excluded from further consideration. This aligns with the scope of the existing RA analysis, which focuses on events within this probability range. Events falling below this threshold, such as those on the order of 1/1000 or less, were considered out of scope for the current study. These probabilities were estimated by the researcher and people involved with the Maeslant barrier, after which they are consulted with the supervisor Alexander Bakker. A method explained in ProBO (2017) and van Maaren (2018).

It is essential to note that, while individual events with low probabilities, such as 1/1000 per occurrence, may seem negligible in isolation, their combined effect could, in theory, present a significant risk. However, for this thesis, which focuses on quantifying a few key events, summing an amount of low-impact individual scenarios was considered outside the scope of the analysis. This category of events could represent a form of incompleteness in the current RA analysis of the Maeslant barrier and, in principle, should be taken seriously, but unfortunately, falls out of the scope of this thesis because that is set on a set of possible high-impact events. The point is that while the Short-list is not 100% complete, it does capture a substantial portion of the relevant events.

Following this initial screening, the remaining events were evaluated for their potential to be meaningfully quantified using available data, expert input, or probabilistic modeling techniques, after which the possibility of merging events was reviewed. The outcome of this three-step selection process was a top three list of events, each of which was individually quantified and potentially incorporated into the existing failure probability model as well, to assess their impact on the non-closure probability of the Maeslant barrier.

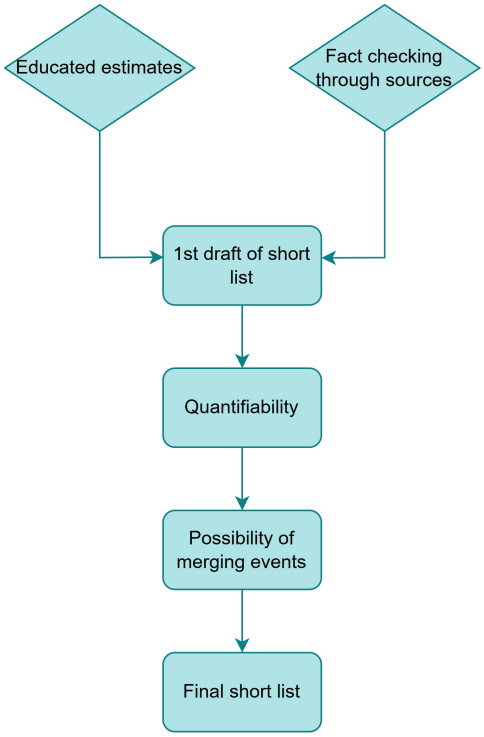


Figure 3.4: Flowchart of methodology used for creating the Short-list. Starting from the top following the direction of the arrows downward.

Step-by-Step Procedure

- Start with Long-list.
- Step 1, probability Screening:
  - Estimate the order of magnitude of each event's occurrence probability, through educated estimates and fact checking through sources.
  - Exclude all events with a probability significantly lower than 1/100 per operational cycle (e.g., events in the order of 1/1000 or lower).
- 1st draft of short-list
- Step 2, quantifiability Screening:
  - Assess each remaining event for its potential to be modeled or estimated within the scope of the thesis.
  - Discard events where no quantification method is possible within this study's time or data constraints.
- Step 3, merging of events:
  - Events that can be merged, to fit the scope of the thesis, are merged.
- Step 4, compile Top 3 Events:
  - Select the three most impactful and quantifiable events (as shown in Figure 3.5).
- Proceed to Quantification:

By applying these filters, the analysis distilled a broad and diverse long-list into a focused set of three events that balance relevance, impact, and analytical feasibility. This process ensured that the subse-

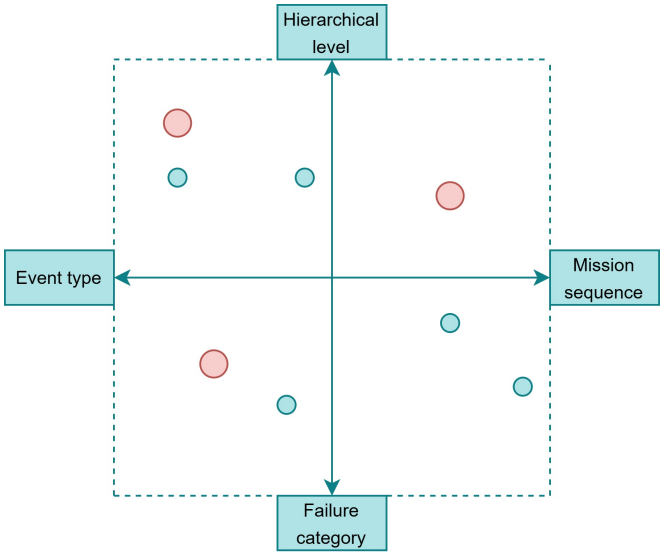


Figure 3.5: top 3 events (red dots) making up the Short-list, existing somewhere on the analytical axis, the blue dots represent events that exist but are exluded from the Short-list. The axis correspond to the four analytical dimensions, with the horizontal-left axis representing “event type”, the vertical-top axis representing “hierarchical level”, the horizontal-right axis representing “mission sequence”, and the vertical-bottom axis representing “failure category”.

quent probabilistic modeling concentrated resources on events most likely to improve the completeness and credibility of the overall risk assessment.

3.4. Stage 3: quantification

The goal of this stage was to determine the potential contribution of the identified events on the short-list to the overall non-closure probability of the Maeslant barrier. Given the absence of empirical data for many of these events, this study relied on a combination of quantification techniques. Depending on the nature of each event, these include structured expert judgement (SEJ), FTA analysis, and integration of existing human reliability data. This section outlines the methodology and tools used for quantification, followed by a detailed presentation of results.

3.4.1. Quantification Methods

In Stage 3, the shortlisted events were quantified using methods tailored to their specific characteristics. Because the three events differ substantially in nature, ranging from epistemic uncertainty to modeling assumptions and human reliability, no single quantification approach would have been sufficient. Instead, multiple methods were applied in parallel, with each chosen to best represent the underlying uncertainty while remaining feasible within the available data and resources.

Table 3.1 summarizes the mapping between the shortlisted events and the quantification methods applied.

Table 3.1: Overview of quantification methods applied to the shortlisted events.

Event type	Quantification method	Justification
Epistemically uncertain events	Expert judgment elicitation combined with probabilistic bounding	Allows the inclusion of previously unmodeled or underestimated events; experts provide probability ranges that are formalized into distributions.
Precondition of stationarity of FTA not met	Research into how to implement non-stationarity into the FTA	provides a roadmap to capturing time-dependent failure rates.
HAD not verified	Human reliability analysis (HRA), benchmarked against literature	Provides probabilistic estimates of operator actions; compensates for the lack of verification in the existing HAD by cross-checking with established HRA techniques.

This structured mapping ensured that each event was quantified with a method suited to its characteristics, while maintaining consistency across the analysis. The explicit link between event type and method increases the transparency of the overall methodology and creates a clear rationale for the probabilistic results presented in Chapter 4.

3.4.2. Epistemic uncertain events probability estimation using SDM

SEJ is a formal methodology for eliciting, aggregating, and applying expert assessments in situations where empirical data is scarce or incomplete (Cooke, 1991). Depending on its design, SEJ can serve different purposes, ranging from capturing uncertainty distributions to building consensus among experts. In this study, a simplified delphi method (SDM) was used to quantify the probabilities of events not yet represented in the RA model. The focus was not on scoring expert performance but rather on structuring the elicitation process to ensure traceability, transparency, and reproducibility of the estimates.

The Delphi method is a structured technique for collecting and refining expert opinions through a series of iterative questionnaires interspersed with controlled feedback (Linstone & Turoff, 1975). The method relies on multiple rounds of anonymous input, with experts given the opportunity to revise their estimates in light of group feedback. This process aims to reduce noise, expose reasoning differences, and facilitate convergence without confrontation or group pressure. In the context of this study, a SDM was used to collect a probability estimate for events identified in the Short-list. Although formal consensus was not the primary goal, the iterative structure helped clarify assumptions and improve the consistency of judgments across participants.

Cooke's method[2] was initially considered as a candidate for the expert judgment process, given its strengths in calibrating and weighting expert input based on objective performance metrics (Cooke, 1991). However, implementing this method requires verified "seed" questions, reference items with known outcomes, to evaluate the accuracy and informativeness of expert assessments (Colson & Cooke, 2018). As this study focused on unaccounted-for events for which no outcome data is currently available, such calibration was not feasible within the scope of the thesis. The "absence" of historical data on these previously overlooked or emergent events made it difficult to apply performance-based weighting in a meaningful way.

Given the time constraints and scope of this study, a full multi-round Delphi procedure was not feasible. Instead, a streamlined three-step process was developed, referred to as the simplified Delphi method

[2]Cooke's method, also known as the Classical Model, is a structured expert judgment technique that quantitatively weighs expert inputs based on their statistical accuracy and informativeness in response to seed questions, reference problems with known outcomes. Experts who perform better on these calibration questions receive more weight in the aggregation of probability estimates. This approach helps reduce bias and improve the reliability of expert-based quantification when empirical data are limited (Cooke, 1991).

(SDM). Experts first independently identified potential missing or underestimated events with an explanation and their contribution to the overall failure to close probability. These submissions were then consolidated into a shared list, after which experts provided their contribution estimates for each event. Unlike traditional Delphi applications, this implementation does not include multiple feedback rounds but maintains anonymity between experts. The focus was on collecting structured, traceable probability estimates on events they consider as not yet accounted for in the current RA analysis, rather than reaching formal consensus. This simplified approach was chosen to retain methodological robustness while making the process feasible within the thesis' practical limitations.

The primary objective of this elicitation session was:

- To identify potential events currently omitted or inadequately accounted for in the RA analysis.
- To quantitatively estimate their potential impact on the barrier's probability of non-closure.
- To aggregate expert judgments into a probability representing epistemic uncertain events[3].

Procedure

The expert elicitation was conducted through the SDM, shown in Figure 3.6:

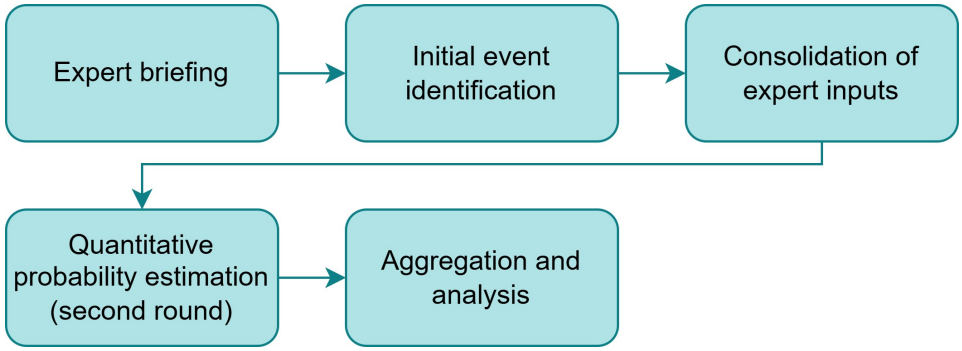


Figure 3.6: Methodology for quantification of epistemically uncertain events probability via SDM. Starting from the left-top following the directions of the arrows.

Step 1: Expert briefing. Experts were briefed individually using a structured briefing document (see appendix B.1), clearly outlining the elicitation process, expectations, and examples. Experts were instructed to:

1. Independently identify 3 to 10 events that they believe are not accounted for or are inadequately addressed in the current RA analysis.
2. Provide a short explanation for each event.
3. Estimate the lower bound, median, and upper bound of how each event might increase the probability of barrier non-closure (expressed as percentage increase[4]).

Step 2: Initial event identification. Each expert completed an Excel template structured as follows (also shown in appendix B.2):

[3] in this thesis, the term "epistemically uncertain events" refers to events or phenomena that are currently missing from the RA model, whether due to being unknown, underestimated, or dormant, and that must be assigned a probabilistic estimate to be formally integrated into the RA analysis.

[4] e.g. a 5% increase on a probability of $P = 0.01$ results in $P = 0.0105$

Rank	Event Title	Brief Explanation	Lower Bound (%)	Median (%)	Upper Bound (%)
1	Example event	Brief explanation	0.3%	0.5%	0.7%
2	Example event	Brief explanation	0.1%	0.25%	0.4%
...	...	...	...	...	...

Table 3.2: Initial event identification template.

Step 3: Consolidation of expert inputs. All individual responses were aggregated, anonymized, and combined into a unified event list. Duplicate or similar events were merged into a single coherent description. This consolidated event list was redistributed to all experts.

Step 4: Quantitative probability estimation (second round). Experts provided refined probability estimates for each event listed in the consolidated Excel sheet, including their confidence levels. The structured format used for this second round is shown in appendix B.3

Step 5: Aggregation and analysis. Responses from the second round were aggregated to derive meaningful probabilities.

Once all expert responses were collected, they were systematically analyzed to ensure consistency and traceability. Each individual estimate was incorporated into a consolidated dataset, from which a combined probability was derived. This aggregated probability represents the estimated contribution of epistemically uncertain events to the overall non-closure probability.

The Structured Expert Judgment (SEJ) exercise produced ranges of percentage increases (δ_i) to the baseline failure-to-close probability. Because individual expert responses varied, the estimates for the lower, median, and upper bounds were aggregated by simple averaging across experts. This equal-weight aggregation was chosen to ensure methodological transparency and to avoid the need for calibration or weighting schemes that were outside the scope of this study. The averaged values of δ_i formed the input for the subsequent quantification step.

To illustrate a combination of all listed events, the averaged values were integrated using a product-of-success formulation. Starting from the baseline probability $P_0 = 0.01$, each event modifies this baseline as $P_i = P_0 \cdot (1 + \delta_i)$. Assuming independence among events, the overall success probability is given by

$$P_{\text{success, total}} = \prod_{i=1}^{n} [1 - P_0 \cdot (1 + \delta_i)],$$

with the failure-to-close probability defined as its complement. This procedure was applied separately to the lower, median, and upper bound estimates, producing an aggregated range of overall failure-to-close probabilities.

Several limitations and assumptions apply to this aggregation: (i) the independence assumption between EUE and HAD may not hold in practice, as interactions could exist between technical and human reliability factors; (ii) the method relies on averaged expert judgments rather than calibrated or weighted responses, which introduces subjectivity; and (iii) the approach treats the aggregated estimates as point probabilities, without fully propagating uncertainty distributions. (iv) If the events exclude each other this method does not hold. (v) All events are assumed to weigh equally throughout the failure tree regardless their position. These simplifications mean that the aggregated outcomes should be regarded as indicative only.

3.4.3. Non-stationary FTA

A limitation of the current RA framework is that the FTA assumes stationary failure rates for all basic events. In practice, this means that component failure probabilities are treated as constant over time, which does not reflect ageing, degradation, or wear mechanisms in long-lived systems (Rijkswaterstaat,

2022a; Vesely et al., 1981). To address the shortlisted event "precondition of stationarity not met," this thesis explored how a non-stationary formulation of the FTA could be developed.

Methodologically, the approach would involve identifying components of the Maeslant barrier subject to degradation (e.g., mechanical subsystems prone to fatigue or electronic elements affected by obsolescence) and replacing their constant probabilities with time-dependent models. Embedding such models into the FTA would allow minimal cut sets and top-event probabilities to evolve over the life cycle of the system.

This type of extension has been discussed more broadly in the reliability literature as a way to improve the realism of probabilistic risk assessments for complex systems (Rausand & Høyland, 2004; Zio, 2009). Conceptually, it provides a roadmap for integrating degradation mechanisms into FTA, thereby enabling more accurate risk estimates when long-term data are available.

In practice, however, the implementation of this approach requires detailed lifetime or degradation datasets to estimate the Weibull (or other distribution) parameters. At present, such data for the Maeslant barrier are not available. Consequently, a full non-stationary quantification could not be carried out within this thesis. Instead, the contribution here is to outline a methodological framework and demonstrate, in an exploratory manner, how the FTA structure could incorporate non-stationary reliability once sufficient data become available.

This approach highlights both the importance of moving beyond stationary assumptions in critical infrastructure risk assessments and the data requirements for doing so. The methodology thus provides a foundation for future work aimed at improving the completeness and credibility of the RA model for the Maeslant barrier.

3.4.4. Verification of the HAD in RA Analysis

This section outlines the methodology developed to explore how verifying HAD could influence the non-closure reliability of the Maeslant barrier. The HAD represents a structured set of human interventions modeled within the RA framework, particularly in scenarios where automated systems such as the BOS, BESW or mechanical components fail, from now called "machine failure". While these human actions are currently included in the RA model through the OPSCHEP model (see subsection 2.4), their assumed reliability is not always supported by empirical verification or standardized training assessments (expert, Rijkswaterstaat 2025). To address this gap, a probabilistic scenario-based approach was designed to quantify the potential reliability gains associated with different levels of operator training and procedural validation. The focus was on operational human actions during closure events, as these are most critical to the barrier's real-time performance and overall non-closure probability, and as these are performed by the operators of the Maeslant barrier.

To highlight the importance of verifying human reliability assumptions, this study draws on practices from other high-reliability sectors such as the defense industry and nuclear energy industry. These industries have long recognized the critical role of human performance in system safety and have developed structured approaches to validate operator readiness, procedural adherence, and training effectiveness (Defensie, 2017; Hirotsu et al., 2001; Preischl & Hellmich, 2016). By examining how these sectors implement and verify human reliability measures, valuable insights can be gained into how the HAD framework for the Maeslant barrier might be strengthened. The following subsection outlines these cross-industry practices and highlights key lessons that inform the proposed methodology.

Verification in other industries

To better understand the potential benefits of verifying the HAD in the context of the Maeslant barrier, this section examines how human reliability is validated in other high-reliability sectors, specifically, the defense and nuclear energy industries. These sectors offer mature frameworks for ensuring that human interventions are not only modeled but also empirically supported through structured training, performance monitoring, and procedural standardization.

In the defense sector, particularly within the Dutch Ministry of Defence, human actions are embedded in rigorously defined operational protocols. Personnel undergo standardized training programs where

every critical action is practiced under realistic conditions and evaluated against strict performance criteria. Deviation from these procedures is not permitted, and operational readiness is continuously assessed through drills and simulations (Defensie, 2017). As a result, the reliability of human actions is not assumed but verified, making the associated human reliability data defensible.

Similarly, the nuclear industry has long recognized the significance of human error in both operational and maintenance contexts. Studies by Hirotsu et al. (2001) and Heo and Park (2010) show that while operational errors are less frequent, maintenance-related human errors account for a substantial portion of incidents. This has led to the development of structured HRA (Human Reliability Anlysis) methods, such as the THERP (Technique for Human Error Rate Prediction), which provide probabilistic estimates of human error based on task complexity and context (Swain & Guttmann, 1983). More recent work by Preischl and Hellmich (2013, 2016) demonstrates how empirical data from licensee event reports in German nuclear power plants can be used to derive context-specific and verifiable HEPs (Human Error Probabilities).

These industries demonstrate that human reliability can be systematically verified through a combination of structured training, performance data, and continuous validation. Most importantly, these practices are underpinned by rigorous documentation, which ensures that procedures, performance metrics, and training outcomes are traceable. This level of transparency is essential for verifying assumptions in probabilistic models and for maintaining accountability in safety-critical systems (Verma et al., 2010).

Methodology for quantifying the impact of operator training on HAD reliability

Building on insights from other industries, this section introduces a probabilistic scenario-based methodology to evaluate how the quality of operator training influences the contribution of the HAD to the Maeslant barrier's non-closure probability. This approach modeled human reliability as a distribution that varies with training level. The goal was to quantify how improvements in training and procedural rigor could reduce the likelihood of failure during critical human interventions and vice versa.

The methodology began by assuming that the current non-closure probability of the Maeslant barrier, $P_{\text{base}} = 0.01$, implicitly includes a nominal HEP based on THERP estimates (Swain & Guttmann, 1983). This baseline served as a reference point for comparing alternative training scenarios. To model the influence of training quality, three levels were considered: highly trained, nominally trained, and badly trained. For each level, kernel density estimators (KDEs) were constructed using task-specific HEPs and the conditional probability of machine failure, which triggers the need for human intervention.

To analyze the distribution of HEP's KDE. KDE is a non-parametric technique that estimates the probability density function of a random variable by smoothing individual data points using a kernel function, typically Gaussian. This method offers several advantages over histograms, including smoother visualizations, better resolution of multimodal structures, and flexibility in representing complex distributions without binning artifacts (Chen, 2017). However, KDEs are sensitive to bandwidth selection, which can lead to over- or under-smoothing, and they suffer from boundary bias and computational inefficiency in high dimensions (Gramacki, 2018). Their ability to transparently represent uncertainty and variation makes them a suitable choice for this study (Team, 2020).

The selection of human actions from THERP was based on a mapping of typical operator tasks during Maeslant barrier closure to corresponding THERP task categories. These include simple detection, routine operations, decision-making under time pressure, and execution of complex procedures. Each task type has a range of HEP values reflecting different training levels, from low (e.g., 0.001 for simple detection by a highly trained operator) to high (e.g., 0.6 for complex diagnosis by an untrained operator) (see table E.1). This mapping ensured that the modeled human reliability reflected the operational reality of the Maeslant barrier while remaining grounded in established probabilities.

Monte Carlo sampling was then applied to each KDE to generate 10 thousand realizations of added non-closure probability due to human error. These distributions were normalized such that the nominal scenario aligns with the baseline P_{base}. This ensured that all scenarios are directly comparable, regardless of differences in absolute probability levels. Normalization in this context adjusted the KDE

outputs so that the central tendency of the reference scenario matches a predefined standard, allowing the model to isolate and compare the effects of different training levels. This approach captured not only the shift in expected reliability due to training but also the uncertainty range around each scenario.

Step-by-Step Methodology

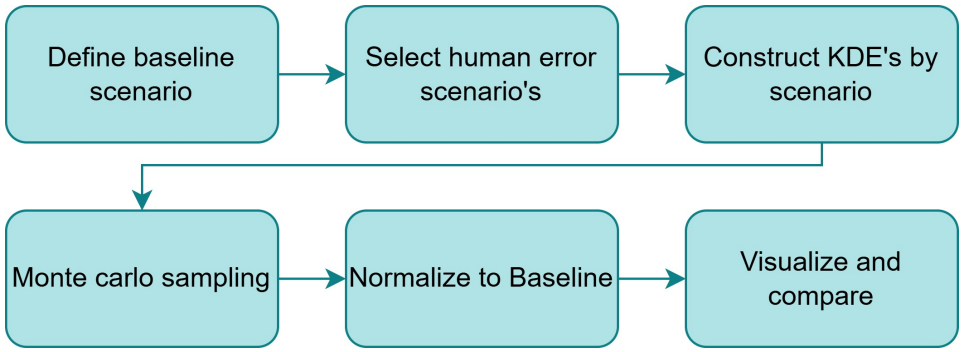


Figure 3.7: Impact of human training methodology flowchart. Starting from the left-top following the directions of the arrows.

1. Define Baseline Scenario: The non-closure probability $P_{\text{base}} = 0.01$ is considered to incorporate a nominal HEP across relevant human tasks, based on THERP estimates (see table E.1).
2. Construct KDEs by Scenario: For three training scenarios (trained, nominal, and untrained), kernel density estimators are fitted to the task-level added non-closure probabilities (i.e., $P_{\text{Machine fail}} \times P_{\text{HEP}}$).
3. Monte Carlo Sampling: From each KDE, 10 thousand samples are drawn to create representative distributions of added failure probability due to human intervention for each training level.
4. Normalize to Baseline: The mean of the nominal scenario is scaled to match $P_{\text{base}} = 0.01$. The same scaling factor is applied to the sampled distributions for the highly trained and less trained cases, maintaining their relative differences while ensuring comparability with the baseline RA model.
5. Visualize and Compare: The resulting distributions are then visualized to show how improved or degraded training influences the overall risk profile, capturing both mean shifts and uncertainty bands.

This methodology enables a robust understanding of how human reliability, driven by training quality, affects overall system reliability. The use of KDEs and probabilistic sampling captures the full spread of potential human error behavior and how it translates into operational risk.

3.5. Integration in to the non-closure probability calculation

In addition to quantifying individual events, a methodological step was developed to explore how their combined effect on the non-closure probability of the Maeslant barrier could be estimated. The approach assumes independence between the epistemically uncertain events (EUE) and the HAD verification, and combines them through a product-of-success formulation:

$$P_{\text{total}} = 1 - (1 - P_{\text{EUE}}) \cdot (1 - P_{\text{HAD}})$$

This formulation provides a simple way to estimate an aggregated failure-to-close probability by considering the joint contribution of multiple sources of uncertainty. It was applied using the lower, median, and upper bounds derived from the SDM for the EUE, combined with a range of plausible HAD values.

Several limitations and assumptions apply to this aggregation: (i) the independence assumption between EUE and HAD may not hold in practice, as interactions could exist between technical and human

reliability factors; (ii) the method relies on averaged expert judgments rather than calibrated or weighted responses, which introduces subjectivity; and (iii) the approach treats the aggregated estimates as point probabilities, without fully propagating uncertainty distributions. (iv) If the events exclude each other this method does not hold. (v) All events are assumed to weigh equally throughout the failure tree regardless their position. These simplifications mean that the aggregated outcomes should be regarded as indicative only.

It is therefore important to stress that the aggregated results derived in this way are not decision-grade estimates. They serve purely as an illustrative exercise to show how different uncertainties might interact when combined, highlighting the sensitivity of the overall non-closure probability to assumptions about human reliability and epistemic gaps in the RA model. As emphasized in the reliability literature, aggregation of expert judgments and multiple uncertainty sources requires careful treatment of dependencies and weighting schemes before results can be used to inform operational or policy decisions (Cooke, 1991; Rausand & Høyland, 2004).

In summary, the methodology presented in this chapter offers a structured and transparent approach to identifying and quantifying previously unaccounted-for events in the Maeslant barrier's RA analysis. By combining established event identification techniques with expert elicitation and probabilistic modeling, the study addresses key limitations in the current framework, particularly those related to epistemic uncertainty and human reliability. This multi-stage process lays the foundation for a more complete and evidence-informed assessment of the barrier's non-closure probability, which is further explored in the results and analysis presented in the following chapter.

3.6. Limitations and assumptions

The following limitations and assumptions underpin the methodology applied in this study:

- The long-list of potential unaccounted events was developed by the author alone, rather than through a multidisciplinary panel, which may have limited the breadth and diversity of perspectives.
- Probability estimates for infrequent or unobserved events were based primarily on expert elicitation due to the scarcity of empirical operational data.
- The structured expert judgment process was implemented in a reduced form (SDM), with only one feedback round, which may have constrained the potential for convergence of expert views.
- The human reliability assessment used THERP task categories mapped to Maeslant barrier operations without full-scale empirical validation for this specific context.
- Only events with an estimated order-of-magnitude probability near or above 1/100 per operational cycle were retained for quantification, excluding lower-probability scenarios even if their cumulative effect could be relevant.
- The aggregation calculation uses several assumptions mentioned in Section 3.4.2 and Section 3.5. Therefore, results are meant to demonstrate sensitivity to combined uncertainties, not to serve as operational or decision-grade risk estimates.

  These points are discussed in greater detail in Section 5.2.

4

Results and Analysis

This chapter presents the outcomes of the three-stage methodology used to identify and quantify previously unaccounted-for failure mechanisms in the Maeslant barrier's RA analysis. It begins with the development of a long-list of potential failure events currently not accounted for, followed by a structured filtering process to create a short-list of the most relevant and quantifiable scenarios. The final three events, epistemically uncertain events, non-stationary failure behavior, and the verification of the HAD, are each analyzed using tailored probabilistic methods.

4.1. Long-list

The resulting long-list of potential failure events is presented in Table 4.1 and presented with full descriptions in Appendix C. It consists of 58 events distributed across five categories: HAZOP (4 events), FMEA (5 events), What-If Analysis (8 events), External Event Screening (32 events), and outside the preconditions (9 events) (see subsection 4.1.2). These events were categorized according to the four analytical dimensions outlined in Figure 3.2. It is important to note that overlap across methods was limited. For example, the seiche-related failure was only identified during the FMEA. This occurred because the method's component-focused structure guided attention to specific vulnerabilities that were not directly prompted by the broader External Event Screening categories. This illustrates the value of using multiple techniques; different analytical lenses lead to different discoveries.

While the method was applied consistently and systematically, it is important to note that the single researcher, the author, conducted the analysis without subject-matter expertise in the operational or technical domains of the Maeslant barrier. As such, the Long-list should be viewed as an exploratory output, a basis for further expert review rather than a definitive catalog of failure scenarios. Where needed, expert input was sought informally to clarify uncertainties or validate assumptions.

4.1.1. Incompleteness

Both existing literature and interview findings highlight a limitation in the Reliability and Availability (RA) analysis: inherent incompleteness. Previous studies, such as Bakker, Rovers, and Mooyaart (2025), van Maaren (2018), and Webbers et al. (2008), acknowledge that RA models, while systematic, cannot capture all potential failure modes and contextual factors. This observation was reinforced by multiple interviewees, who pointed out that real-world complexities, human factors, and unforeseen interactions often fall outside the scope of standard RA frameworks. As a result, while RA analysis provides valuable insights, it should be interpreted as a partial representation of system risk rather than a fully comprehensive assessment. The long-list highlights this as well.

4.1.2. Preconditions

While performing the analysis according to the methodology (see section 3.2), events occurred that exist outside of the preconditions of the current RA analysis (see subsection 2.4.1); this is visualized in

Table 4.1: Long-list of potential unaccounted events for the Maeslant barrier (full descriptions in Appendix C).

Method	Event ID and Name		
FMEA	1.1 Seiche sea-side	1.2 Incorrect landing	1.3 Trouble with BESW
	1.4 Wrong buoyancy (heavy)	1.5 Wrong buoyancy (light)	
HAZOP	1.6 Maintenance done wrong	1.7 Weather station data wrong	1.8 Incorrect closure type
	1.9 Disobedience ship/harbor		
External Events	1.10 Temporal compound events	1.11 Long drought	1.12 High wind speeds
	1.13 Hailstorm	1.14 Heavy rain	1.15 High temperatures
	1.16 Earthquake	1.17 Snow accumulation	1.18 Extreme cold
	1.19 Flooding	1.20 Elevated water levels	1.21 Prolonged water
	1.22 Oscillating waves	1.23 Large waves	1.24 Soil movement
	1.25 Underground failure	1.26 Coastal land loss	1.27 Fire nearby
	1.28 Fire inside object	1.29 External impact	1.30 Hazardous release ext.
	1.31 Hazardous release int.	1.32 Explosion nearby	1.33 Explosion inside
	1.34 Meteor/satellite	1.35 Aircraft crash	1.36 Turbine part detachment
	1.37 Infestation	1.38 Cable/pipe damage	1.39 Debris impact
	1.40 Power outage	1.41 Sea-current shift	
What-if Analysis	1.42 More closures (SLR)	1.43 Outdated climate knowledge	1.44 Pandemic
	1.45 Ship blocking	1.46 Political hinder	1.47 Knowledge loss
	1.48 Common cause redundancy	1.49 RA incompleteness	
Outside Preconditions	2.1 Too much detail	2.2 Maintenance window missed	2.3 Lack of structure
	2.4 Lessons not implemented	2.5 Preventive replacement missed	2.6 Parts used differently
	2.7 Weather independence wrong	2.8 Stationarity not met	2.9 HAD not verified

Figure 4.1.

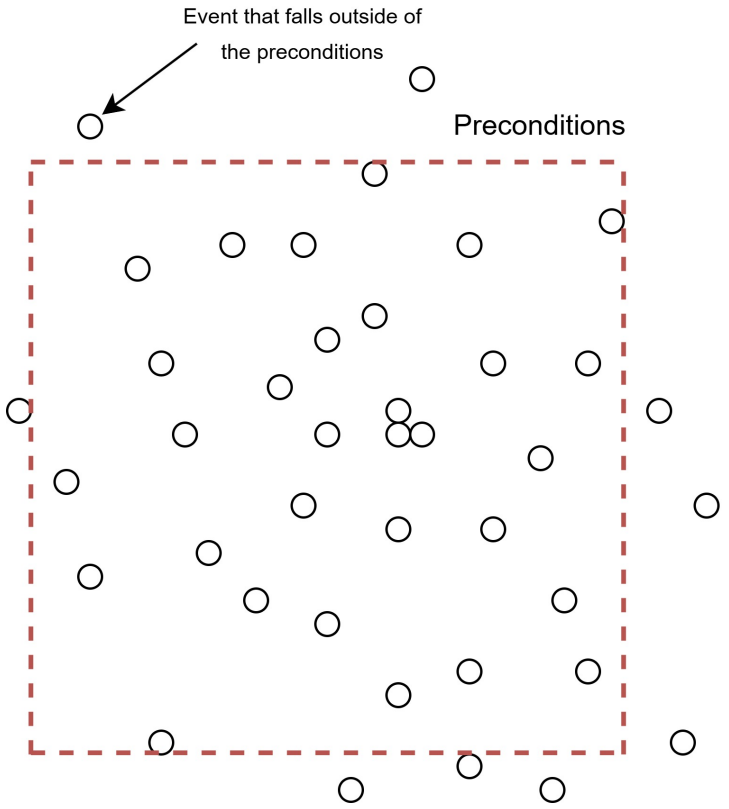


Figure 4.1: Visualization of events that exist outside of the preconditions of the current RA analysis of the Maeslant barrier. The dots represent events, where the red dotted line represent the boundary of the preconditions in which the events can exist inside or outside.

Input from multiple stakeholders confirmed that both inside and outside preconditions are critical factors that must be considered in any comprehensive analysis of the Maeslant barriers' reliability. Respondents consistently emphasized that overlooking these preconditions would result in an incomplete understanding of potential failure mechanisms. Therefore, the decision was made to add an extra category in the Long-list, named: "Outside preconditions." All events that exist outside of these preconditions have been placed in this category.

One of these events is the assumptions of constant failure rate of components within the RA analysis. Multiple stakeholders indicated that, in practice, the preconditions required to maintain a constant failure rate are not always fully met. Factors such as resource constraints, operational pressures, and unexpected system complexities can result in deferred maintenance, incomplete component replacements, or delayed renovations. This introduces periods where the system may shift out of the flat part of the bathtub curve, increasing the risk of age-related failures and challenging the validity of the FTA assumptions in real-world conditions.

In summary, the long-list development process underscores both the strengths and limitations of the current RA framework. By applying a structured, multi-method approach, this study was able to uncover a diverse range of potential failure events, some of which fall outside the assumptions and preconditions of the existing analysis. The inclusion of these "outside preconditions" events highlights the importance of continuously revisiting and expanding the boundaries of risk models to reflect real-world complexities. While the list is not exhaustive, it serves as a robust foundation for further expert validation and prioritization. The next step is to systematically filter this long-list into a focused short-list of events that are both relevant and quantifiable, as outlined in the following section.

4.2. Short-list

In this section, the Long-list, see Table 4.1 and Appendix C, was structurally shortened to a top 3 short-list.

An overview of the event selection and shortlisting process is provided in Table 4.2, summarizing how each event was assessed across the filtering stages. The table shows which events were excluded, integrated, or retained for quantification, leading to the final top three. A more detailed explanation of the rationale behind each decision is provided in the remainder of this section.

Event	Order of Magnitude Retained	Ability to Quantify Outcome	Final Top 3
1.1 Seiche (sea-side)	No	-	-
1.2 Incorrect landing	No	-	-
1.3 Trouble with control system	Yes	Excluded (sensitive nature)	-
1.4/1.5 Wrong buoyancy	No	-	-
1.6 Maintenance done wrong	Yes	Integrated into 1.44, 2.2, 2.5, 2.8	-
1.7 Weather station error	No	-	-
1.8 Incorrect closing type	No	-	-
1.9 Disobedience of ship	No	-	-
1.10 Temporal compound events	Yes	Integrated into 1.49	-
1.11-1.42 External events	No	-	-
1.43 Outdated climate knowledge	Yes	Integrated into 1.49	-
1.44 Pandemic	Yes	Integrated into 1.6, 2.2, 2.5, 2.8	-
1.46 Political hinder	Yes	Integrated into 1.49	-
1.47 Generational knowledge loss	Yes	Integrated into 1.49	-
1.48 Missed common cause	Yes	Integrated into 1.49	-
1.49 Incompleteness of RA analysis	Yes	Retained for quantification	Yes
2.1 Unverifiability of RA analysis	-	Excluded (too broad); partial addressed by 2.9	-
2.2 Maintenance not on time	-	Integrated into 1.6, 1.44, 2.5, 2.8	-
2.3 Unstructured RA analysis	-	Integrated into 1.49	-
2.4 No new knowledge in RA	-	Integrated into 1.49	-
2.5 Preventive replacement not met	-	Integrated into 1.6, 1.44, 2.2, 2.8	-
2.6 Misinterpretation of data	-	Excluded (too broad/complex)	-
2.7 Wrong assumption in RA	-	Excluded (too broad/complex)	-
2.8 Stationarity not met	-	Integrated into 1.6, 1.44, 2.2, 2.5	Yes
2.9 HAD not verified	-	Retained for quantification	Yes

Table 4.2: Comprehensive overview of event selection and integration across filtering stages. Green color representing retention, red color representing exclusion and yellow color representing integration onto other event.

4.2.1. Order of magnitude deletion

This section evaluates the order of magnitude of occurrence for each identified event, organized according to the categories defined in the Long-list. The numbering corresponds to the numbers in appendix C.

FMEA

- 1.1 Seiche (sea-side): Based on de Jong (2024), it was concluded that the occurrence rate of a moderate seiche, exceeding 0.25 meters, is observed to occur roughly once every 0.7 to 1.1 years. But the Maeslant barrier is designed to withstand critical seiche events with an annual probability of occurrence of 10^{-7} per year, corresponding to a design amplitude of approximately 1.00 meter. As a result, this scenario is considered negligible and has been excluded from further analysis.
- 1.2 Incorrect landing: Based on input an expert of Rijkswaterstaat, it was concluded that the

occurrence rate is lower than 1 in 1,000 events. As a result, this scenario is considered negligible and has been excluded from further analysis.

- 1.3 Trouble with control system (BESW): Based on input from an expert of Rijkswaterstaat, it was concluded that the occurrence rate could not be disclosed. Consequently, this scenario remains under consideration at this stage of the analysis.
- 1.4/5 Wrong buoyancy above threshold (Too heavy/light): Based on input from an expert of Rijkswaterstaat, it was concluded that the occurrence rate is lower than 1 in 100 events and could be lower than 1 in 1,000. As a result, this scenario is considered negligible and has been excluded from further analysis.

HAZOP

- 1.6 Maintenance done wrong: Based on input from two experts from Rijkswaterstaat and the TU Delft, it was concluded that the occurrence rate could not yet be determined. Consequently, this scenario remains under consideration at this stage of the analysis.
- 1.7 Prediction/data weather station done wrong: Based on input from an expert from the TU Delft and Rijkswaterstaat and general KNMI reliability data Royal Netherlands Meteorological Institute (KNMI) (2025), the probability of a critical error in weather prediction or data reporting is estimated to be between 0.001 and 0.01 per critical event. This reflects the generally high reliability of meteorological forecasting in the Netherlands, while acknowledging the inherent uncertainty during extreme weather events. Therefore, this scenario is considered negligible and excluded from further analysis.
- 1.8 Incorrect choice of closing type: Based on input from two experts from Rijkswaterstaat and TNO, and considering the high level of expertise embedded within the Maeslantkering operational team, the likelihood of selecting an incorrect type of closure is effectively negligible. This scenario can therefore be excluded from further analysis.
- 1.9 Disobedience of ship/Harbor: Based on observations during functionality closures and input from an expert from Rijkswaterstaat, it is acknowledged that disobedience by ships or harbor authorities, motivated by economic interests, can cause delays in the closure process. While strict protocols are enforced during actual storm surge events, a small but non-zero probability of delay remains. This probability is estimated to be approximately 0.001 per critical closure event, reflecting the generally high compliance but recognizing the potential for exceptional cases. Given the low estimated probability and the robust enforcement mechanisms in place, this scenario will be excluded from further analysis.

External events:

- 1.10 Temporal compound events: The impact of this finding cannot yet be quantified with sufficient certainty and is therefore retained in the analysis for further consideration.
- 1.11 to 1.40: are either already accounted for within existing operational procedures or have a probability of occurrence that is considered too low to warrant further analysis.
- 1.41 Shift in sea-current: The consequences and likelihood of this event occurring in the near future are uncertain but deemed negligible; therefore, it will not be considered in further analysis.

What if analysis:

- 1.42 Increased closing due to SLR (sea level rise): Although this could present a problem in the future, experts of Rijkswaterstaat indicate that it does not currently pose a significant risk (the sea has not risen significantly); therefore, it will not be included in further analysis.
- 1.43 Outdated understanding of climate change/the lack of implementation of new knowledge: In collaboration with an expert from Rijkswaterstaat, this event has been identified as a relevant case for possible quantitative assessment.
- 1.44 Pandemic: In consultation with an expert from TNO, aiming at the manpower shortage, this has been identified as a relevant subject for quantitative evaluation.

- 1.45 Ship blocking: Although a vessel stranding within the barrier area is theoretically possible, strict traffic control and closure protocols (Rijkswaterstaat, 2016) make this scenario extremely unlikely. Given the low probability and lack of historical precedent, it is excluded from further analysis.
- 1.46 Political hinder: A shift in political perspective could lead to reduced trust in Rijkswaterstaat's expertise, potentially complicating structural maintenance efforts. As such, changes can occur abruptly; this scenario remains relevant and is retained in the analysis.
- 1.47 Generational knowledge loss: In consultation with multiple experts from Rijkswaterstaat and TNO, this event has been identified as having significant potential impact and is retained in the analysis.
- 1.48 Missed common cause of redundant systems: In consultation with an expert from Rijkswaterstaat, this event has been identified as having significant potential impact and is retained in the analysis.
- 1.49 Icompleteness of RA analysis: This event cannot be reliably quantified based on available sources and interviews alone but, in consultation with multiple interviewees, has been assessed as significant and will therefore remain included in the analysis.

Although it is acknowledged that the combined occurrence of multiple low-probability events, each with a likelihood on the order of 1/1000, could, in aggregate, pose a significant threat, such compound scenarios fall outside the scope of this thesis. Given the focus on quantifying three events of highest relevance, these low-probability events were not considered for further analysis.

Outside preconditions:
All events classified as outside preconditions cannot be fully quantified based solely on available sources and expert input. The complexity and uncertainty surrounding these events make it difficult to establish reliable probability estimates at this stage. As a result, these events are retained in the analysis for further consideration to ensure that potential risks are not overlooked.

4.2.2. Ability/Interest to quantify deletion

This section selects events based on the suitability of the remaining for quantification, with all event numbers corresponding to those listed in appendix C. The events still under consideration are listed below. While all identified events are relevant, some fall outside the scope of this thesis for quantitative probability assessment. For these cases, a brief explanation is provided alongside each event in the list.

- 1.3 Trouble with control system: Due to the sensitive nature of this event, it will not be subject to further quantification or analysis.
- 1.6 Maintenance done wrong: Although originating from different categories, this event can be integrated with events 1.44, 2.2, 2.5, and 2.8
- 1.10 Temporal compound events: Due to insufficient available data, quantifying this event falls outside the scope of this thesis.
- 1.43 Outdated understanding of climate change/the lack of implementation of new knowledge: Considered in isolation, this event is not sufficiently significant to warrant inclusion within the scope of this thesis.
- 1.44 Pandemic: Although originating from different categories, this event can be integrated with events 1.6, 2.2, 2.5, and 2.8
- 1.46 Political hinder: Quantifying the probability of political changes that could alter funding streams and incentives related to the Maeslant barrier falls outside the scope of this thesis.
- 1.47 Generational knowledge loss: Considered in isolation, this event is not sufficiently significant to warrant inclusion within the scope of this thesis. Additionally, Rijkswaterstaat is working internally to mitigate this knowledge loss (Expert, Rijkswaterstaat 2025).

- 1.48 Missed common cause of redundant systems: According to experts from Rijkswaterstaat and the TU Delft, this represents a significant issue but should not be considered in isolation; therefore, it is incorporated into event 1.49.
- 1.49 Incompleteness of RA analysis: This event is regarded as highly significant according to an expert of Rijkswaterstaat, as well as findings from Webbers et al. (2008) and van Maaren (2018). It encompasses events 1.10, 1.43, 1.46, 1.47, 1.48, 2.3, and 2.4; therefore, it will be included for quantification.
- 2.1 Unverifiability of the RA analysis: This event is too broad in scope to be quantified within the framework of this thesis; however, event 2.9 represents a scaled-down version that could address its key aspects.
- 2.2 Precondition of on-time maintenance not met: Although originating from different categories, this event can be integrated with events 1.6, 1.44, 2.5, and 2.8
- 2.3 Unstructured RA analysis: On its own, this event is too vague to quantify; however, it contributes to the broader context of event 1.49 and will therefore be encompassed within that event.
- 2.4 No implementation of new knowledge in the RA analysis: This event is too indistinct to be quantified independently but is relevant to the scope of event 1.49 and will thus be incorporated into its assessment.
- 2.5 Precondition of preventive replacement not met: Although originating from different categories, this event can be integrated with events 1.6, 1.44, 2.2, and 2.8
- 2.6 Misinterpretation of component data: Although this is recognized as a significant issue by multiple interviewees, it is too complex and broad to be quantified within the scope of this thesis and is therefore not included for quantification.
- 2.7 Wrong assumption in RA analysis: This is considered an important problem; however, due to its complexity and the fact that it extends beyond the scope of this thesis, it will not be quantified.
- 2.8 Precondition of stationarity not met: Although originating from different categories, this event can be integrated with events 1.6, 1.44, 2.2, and 2.5
- 2.9 HAD not verified: Given the availability of sufficient data and the importance attributed to this event by multiple interviewees, it will be included for quantitative assessment.

The events selected for further analysis are consolidated and described in a ranked summary of the top three most suitable events.

It is acknowledged that, in principle, all identified events could be meaningfully quantified given sufficient data, time, and resources. However, certain events have been excluded from quantification in this study because their analysis would require a depth beyond the scope of this thesis. This does not imply that these events are irrelevant or unquantifiable.

4.2.3. Top 3

The top three events represent a focused selection of scenarios from the Long-list of potential unaccounted events. They were chosen based on their relevance, potential impact on closure reliability, and the feasibility of quantifying them within the scope of this thesis.

1. Epistemically uncertain events[1]
2. Precondition of stationarity of FTA not met

[1] In this thesis, the term “epistemically uncertain events” refers to events or phenomena that are currently missing from the RA model, whether due to being unknown, underestimated, or dormant, and that must be assigned a probabilistic estimate to be formally integrated into the RA analysis.

3. Unverified[2] reliability of human intervention (HAD: Human Action Database)

The positioning of these events along analytical dimensions is shown in Figure 4.2. The spread demonstrates that the Top 3 cover a variety of perspectives and mechanisms, ensuring input from multiple angles rather than being concentrated in one type of uncertainty.

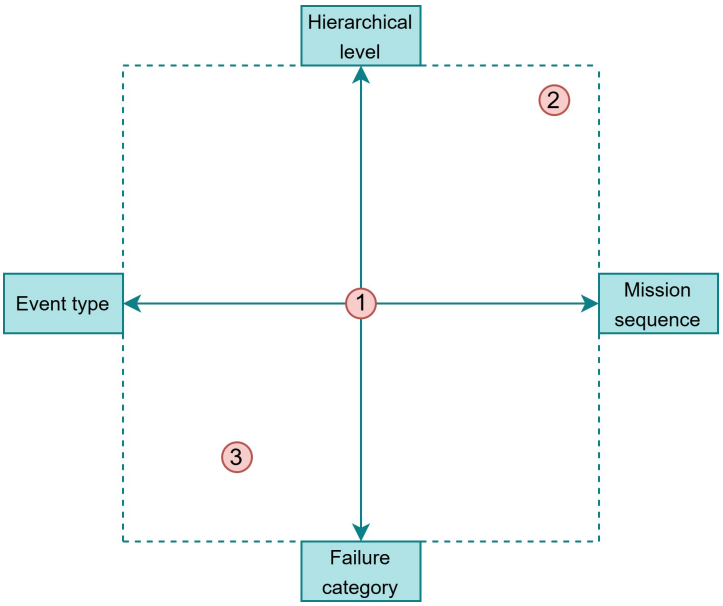


Figure 4.2: Positions of the Top 3 short-listed events (red dots) on the analytical axis. The numbers correspond to the top 3 listed events, with: 1. Epistemically uncertain events, 2. Precondition of stationarity of FTA not met, and 3. Unverified HAD. The axis correspond to the four analytical dimensions, with the horizontal-left axis representing "event type", the vertical-top axis representing "hierarchical level", the horizontal-right axis representing "mission sequence", and the vertical-bottom axis representing "failure category".

In conclusion, the shortlisting process distilled a broad and diverse set of potential failure events into a compact set of three. Together, epistemically uncertain events, the violation of the FTA stationarity assumption, and the unverified reliability of the HAD represent a balanced cross-section of analytical dimensions, forming a foundation for the quantification in the next section.

4.2.4. Relation of Top 3 Events to the Bathtub Curve

The three shortlisted events can also be interpreted in relation to the phases of the bathtub curve introduced in Section 2.4.1. This perspective illustrates that the unaccounted events identified in this study span all phases of the system life cycle.

- Epistemically uncertain events correspond to the early failure phase, since they represent phenomena that only become visible once sufficient knowledge or operational evidence accumulates.
- Violation of stationarity in the FTA aligns with the wear-out phase. Several components exhibit non-stationary degradation mechanisms, whereas the current model assumes constant failure rates.
- Unverified HAD is most relevant for the useful life phase. Human intervention reliability is assumed constant, but without verification, these values remain uncertain and can behave unpredictably, similar to random failures.

By linking the Top 3 events to the bathtub curve, it becomes clear that each phase of the curve is represented in the unaccounted events. This demonstrates that missing uncertainties are not concentrated in

[2]In this thesis, the term unverified refers to the fact that the Human Action Database (HAD) has not been validated against empirical performance data or systematic testing. The reliability values it contains are therefore based on assumptions and expert judgment, without independent confirmation that they reflect real-world operator performance under relevant conditions.

a single failure phase, but distributed across the full life cycle of the system. It further underscores the importance of integrating these events into the RA framework to ensure a comprehensive representation of closure reliability.

4.3. Quantification Results

This section presents the quantitative results for the three most critical unaccounted-for failure mechanisms identified in the shortlisting process: (1) epistemically uncertain events, (2) non-stationary failure behavior, and (3) the verification of the Human Action Database (HAD). Each of these was assessed using a tailored probabilistic method, as outlined in Chapter 3, to estimate their potential contribution to the Maeslantbarrier's non-closure probability.

4.3.1. Epistemically Uncertain events

A total of nine experts were contacted for participation in the SDM. These individuals were selected based on their experience with the Maeslant barrier or RA analysis in comparable infrastructure systems. Of the nine, four experts submitted complete first-round responses (shown in appendix D), and all four experts provided refined estimates in the second round. The second-round responses formed the basis for the quantitative analysis presented here. The experts demonstrated a wide range of perspectives (see Figure 4.3), for example, on events involving human decision-making, model assumptions, and maintenance-related uncertainties. While some events, such as "storm conditions" and "human error", were consistently rated as significant, others showed greater variability, reflecting differing interpretations of system behavior and failure probabilities.

The aggregated ranges in Figure 4.3 and Table D.6 show that while individual expert estimates varied significantly, the aggregated values seem to provide a more stable foundation for further modeling. The average lower bound across all events was approximately 1.4%, with a median of 5% and an upper bound of 13%. This spread could highlight the epistemic uncertainty inherent in the expert judgment process. Notably, events such as "storm conditions", "decision-making errors", and "model error due to incomplete data" consistently received higher median and upper-bound estimates, suggesting that these are perceived as impactful contributors to non-closure risk.

One concern raised during the SDM was the uncertainty surrounding the Maeslant barrier's performance during an actual normative storm event. The barrier has never been deployed under such conditions (Expert, Rijkswaterstaat & TU Delft 2025), leaving a gap in empirical validation. Several experts expressed concern about this lack of operational experience, with one expert even assigning an upper bound of 100% to the added failure probability associated with storm conditions. This estimate, while not representative of the group average of 63%, shows signs of unease among domain experts. It could reflect a fear that the current RA model may not capture the dynamic and potentially compounding effects of a normative storm on the Maeslant barrier's performance. The idea that such an estimate was deemed plausible by an experienced professional highlights a need for addressing these concerns through a more transparent integration of storm-related uncertainties into the RA framework.

Notably, one of the interviewed experts expressed a contrasting view compared to the rest of the panel, arguing that human decision-making may actually contribute positively to the reliability of the Maeslant barrier's closure. The expert provided negative probability ranges in their responses, suggesting that certain human decisions could reduce the overall failure to close probability (see Table D.4). As a result, some of the aggregated lower bounds in the dataset are negative, which is not physically meaningful in probabilistic terms but does highlight the presence of fundamentally different mental models[3] among the experts (see Table D.6).

The top 10 highest-rated events from the SDM predominantly reflect uncertainty stemming from a lack of knowledge (see Figure 4.4). The emphasis placed by experts on these knowledge gaps signals a distress regarding the reliability of current assessments and shows a need for targeted implementation efforts, not only to address the identified uncertainties but also to restore expert confidence in the the RA analysis.

[3] An expert's internal understanding of how the Maeslant Barrier operates and fails, shaping their judgments during elicitation.

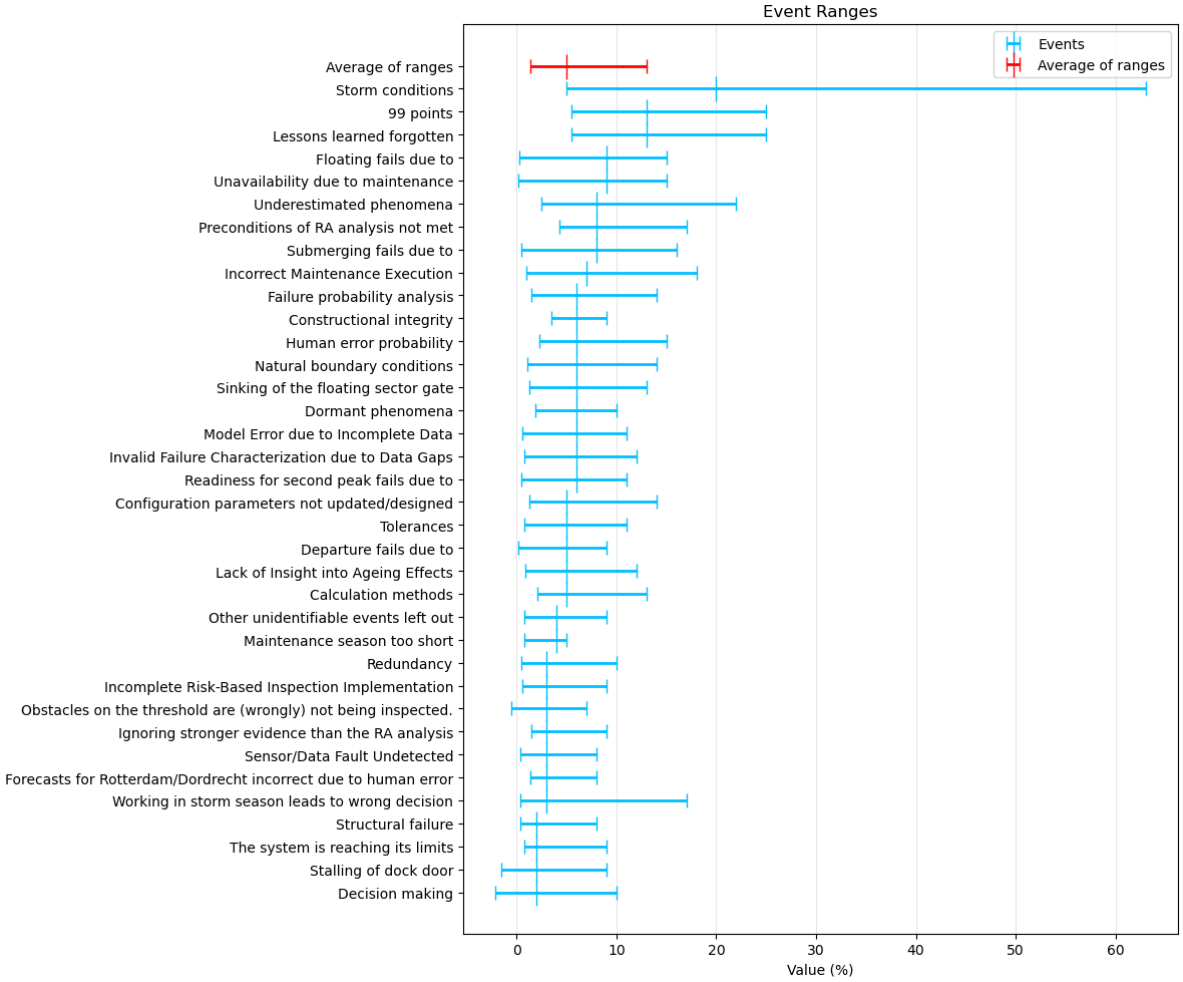


Figure 4.3: Aggregated ranges from the performed SDM. The horizontal axis shows the value of percentage increase in failure-to-close probability of $P = 0.01$. The vertical axis shows the listed events from the SDM. The blue and red bars represent the range and the median. The red bar in particular represents the average of all listed events. All explanations of the listed events on the vertical axis are given in Appendix D.

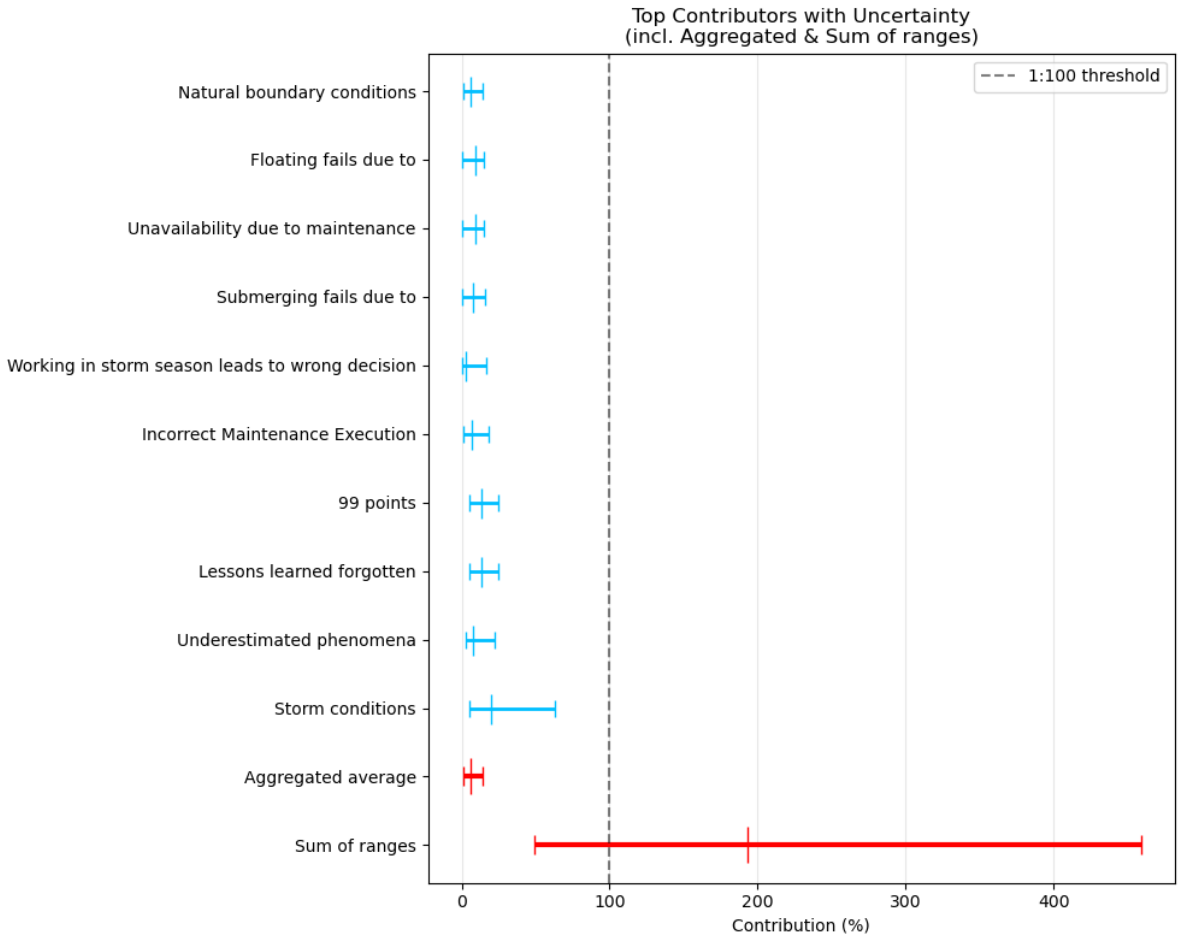


Figure 4.4: Aggregated ranges top 10 events listed by experts in the SDM. With the sum of all aggregated ranges and aggregated average in red. the horizontal axis shows the value of percentage increase in failure-to-close probability of $P = 0.01$. The vertical axis shows the top 10 listed events from the SDM. The blue and red bars represent the range and the median. The dashed line represents 100% increase in failure-to-close probability. All explanations of the listed events on the vertical axis are given in Appendix D.

The responses also show a lack of convergence between individual expert judgments. The wide spread in lower and upper bounds for several events, particularly those involving human decision-making and model assumptions, indicates differences in interpretation and confidence levels. This divergence suggests that the experts were operating with varying (mental) models of the system and its failure mechanisms. A more refined elicitation process, such as a multi-round Delphi method with structured, anonymous feedback and discussion, could help bridge these gaps. By allowing experts to reflect on the reasoning of their peers without direct confrontation, such a process fosters deeper understanding and may lead to more consistent and robust probability estimates.

A further complication in interpreting the expert input is that the summed median of all averaged event estimates exceeds 100% (see Figure 4.4), which is not physically meaningful in the context of the failure to close probability of the Maeslant barrier. This overestimation shows the challenge of aggregating epistemic uncertainty across multiple events without accounting for potential overlap or interdependence. One pragmatic way to incorporate this uncertainty into the FTA is to consolidate the expert input into a single epistemically uncertain event. By taking the median of the complete average, 5%, this event can be added as a basic node in the FTA with a failure probability of $P = 0.05$, as shown in Figure 4.5. This approach allows the uncertainty to be formally represented without inflating the overall risk estimate. A similar method was applied in the analysis of the Mareike sluice (Expert, Rijkswaterstaat & TU Delft 2025), where an epistemically uncertain event was introduced based on the judgment of a single expert. In contrast, this analysis benefits from a broader expert base, making the 5% estimate a bit more representative of collective uncertainty. The addition of this event in this way increases the probability of non-closure given by the FTA from $P = 0.07$ to $P = 0.12$. No definitive meaning can be concluded from this increase because of the OPSCHEP that needs to be added, as described in section 2.4.2.

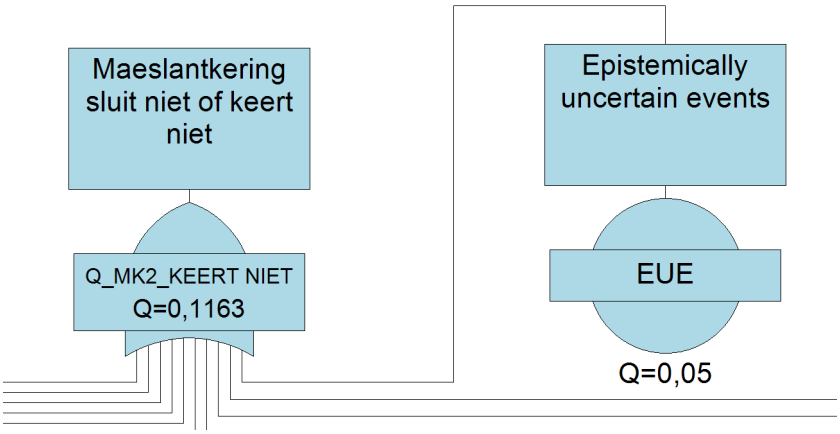


Figure 4.5: Adding of epistemically uncertain events as a basic event in the current FTA of the Maeslant barrier, done in Reliability Workbench (Ltd., 2025)

Aggregating by taking the product of success

A more comprehensive approach for interpreting the ranges obtained from the SDM is to estimate the overall failure-to-close probability of the Maeslant barrier considering all the events as described in Section 3.4.2. This was applied to three sets of values for δ_i: lower-bound, median, and upper-bound estimates derived from the SDM. The resulting aggregated failure probabilities were:

$$P_{\text{failure-to-close, total}} \in [0.307, 0.317, 0.335]$$

This is significantly higher than using only the averaged range of alle events as one event with a lower bound 1.4%, a median of 5% and an upper bound of 13% resulting in:

$$P_{\text{failure-to-close, total}} \in [0.0100, 0.0105, 0.0113]$$

These results show that: when aggregating the expert-elicited uncertainty contributions from all identified events, the overall failure-to-close probability of the Maeslant barrier increases, from the baseline of $P = 0.01$ to a range between approximately $P = 0.307$ and $P = 0.335$. This is based on a probabilistic model that assumes independence among events and applies the SDM estimates as multiplicative risk factors. The implication is that the actual non-closure probability may be underestimated by more than a factor of 30. This result should not be taken literally, due to the assumption of independence, and the method of the SDM, as discussed in Section 3.4.2 and further discussed in Section 5.2.

In stage 2 (see Section 4.2), several events were merged into a broader category of epistemically uncertain or incomplete events. Upon comparison, a number of these merged or short-listed events show clear overlap with those mentioned in the SDM. For instance, "outdated climate knowledge" aligns with "outdated natural boundary conditions", and "generational knowledge loss" corresponds to "lessons learned forgotten". Similarly, "missed common cause" relates to "redundancy", "unstructured RA analysis" matches with data gaps and "incomplete risk-based assessment", and "no new knowledge in RA analysis" reflects both "incomplete data" and "lessons learned forgotten". "Temporal compound events", merged under this broader category, were also mentioned by experts as "underestimated phenomena" and "other identifiable events left out". While temporal compound events have been identified as a relevant risk (Bakker, Rovers, & Mooyaart, 2025), they are not yet included in the current analysis.

These overlaps are not limited to the category of incompleteness or epistemic uncertainty. Several expert-identified events also align with the other two short-listed events. For instance, "HAD not verified" corresponds closely with SDM-identified events such as "human error", "incorrect maintenance", "decision making", "working in storm season", and "sensor detection". Similarly, the short-listed event "precondition of stationarity of FTA not met" reflects concerns raised in the SDM about preconditions in RA analysis, "model error due to incomplete data", "invalid failure categorization due to data gaps", "lack of insights into aging effects", and "systems reaching their limit".

Taken together, these overlaps confirm that the events identified earlier in the research are validated by expert judgment. The convergence between the short-listed items and SDM findings reinforces the relevance of the selected events and strengthens confidence in the methodology used to uncover them.

While the SDM used in this study provides valuable insights, it also has clear limitations. The absence of calibration questions and performance-based weighting means that expert input was treated uniformly, regardless of individual accuracy or informativeness. This limits the statistical robustness of the aggregated estimates and makes it difficult to quantify uncertainty with confidence. Furthermore, because there is no convergence, there has not been enough room for discussion and new estimates between and from the experts.

In earlier consultancy work, Horvadt & Partners argued that unaccounted-for events do not require explicit modeling, as their effects are implicitly captured through conservative estimates applied to other failure modes (Horvadt & Partners, 2025). However, the author argues that this reasoning is fundamentally flawed. Relying on conservatism as a blanket justification introduces a false sense of completeness and undermines the transparency and traceability of the RA analysis. While conservative estimates may buffer against known uncertainties, they do not account for unknown or emergent failure mechanisms, particularly those outside the structure of the existing fault tree. Moreover, conservatism is often applied with minimal empirical justification and relies heavily on expert judgment[4] (Expert, Rijkswaterstaat 2025), making it difficult to assess whether the degree of overestimation is appropriate or sufficient.

4.3.2. Non-stationary FTA

After research into the existing model, it became apparent that non-stationarity has, to some extent, already been incorporated into the current analysis. Specifically, for components identified as having entered the wear-out phase, an expert-derived B-Weibull function[5] is used to recalculate their failure

[4] At Rijkswaterstaat, this refers to an expert assigning a value or estimate based on their knowledge and experience, often without strict reproducibility or formal calculation.

[5] The B-Weibull distribution is a modified form of the standard Weibull distribution used in reliability engineering to model time-to-failure data. It introduces a threshold parameter B, representing the minimum time before failures can

probabilities and update them yearly (Expert, Rijkswaterstaat 2025). This approach introduces a degree of time dependence into the model, allowing for increasing failure rates as components age. However, this implementation remains limited in scope and is applied selectively, based on expert judgment. As a result, the RA model still largely operates under the assumption of stationarity, and the integration of non-stationary behavior is not reproducible. Moreover, component lifetimes are estimated without integrating condition monitoring or operational data (Expert, Rijkswaterstaat 2025).

To address these shortcomings, this thesis proposes a more robust and structured approach: the development of a centralized component lifecycle database. This database would systematically collect degradation-related data for critical components, including, but not limited to:

- Expert-judged component lifecycles
- Observed component lifecycles
- Operational stress histories
- Maintenance records
- Environmental exposure metrics

From this database, time-varying failure rate functions such as B-Weibull or other parametric models can be calibrated for each component. This creates a transparent, reproducible, and data-driven foundation for incorporating non-stationary behavior into the RA framework, but also a foundation to check the expert-judgment derived component lifetime. One expert interviewed for the SDM independently proposed such a database, further validating its feasibility (see Table D.3).

Importantly, a modeling approach that uses data and feedback does not inherently lead to a more negative risk assessment. While current expert-derived component failure rate estimates are generally conservative (Bakker et al., 2022), real-time data may reveal components are performing better than expected, e.g., due to reduced operational stress or improved maintenance practices. This could lower the estimated non-closure probability and enable more cost-effective asset management by focusing efforts where degradation is actually occurring. If condition monitoring and operational data were systematically collected and analyzed, it could reveal that certain components are performing better than expected, with longer-than-assumed lifespans. This would have a positive effect on the overall reliability of the structure, potentially reducing the estimated non-closure probability. Therefore, integrating real-time data into the RA framework not only improves accuracy but also opens the possibility for more efficient and risk-informed asset management.

The implementation of non-stationary failure modeling can be operationalized using existing tools such as Isograph's Reliability Workbench, which is already in use for the Maeslant barrier's RA analysis (Ltd., 2025). Reliability Workbench supports advanced fault tree modeling, including the assignment of time-dependent failure distributions such as the B-Weibull function (Ltd., 2025). This functionality allows analysts to simulate how component reliability evolves over time and to assess the cumulative impact of aging on system-level failure probabilities. By linking component-specific B-Weibull parameters, derived from the proposed lifecycle database, to fault tree events, the model can dynamically reflect degradation trends and maintenance effects.

To illustrate this capability, a simplified fault tree model is constructed, shown in Figure 4.6, using three basic events representing the distinct phases of the bathtub curve: early life failure, constant failure, and wear-out. These events were connected via an OR gate, indicating that system failure occurs if any of the three modes are triggered. Each event is assigned a different failure distribution: the early life phase was modeled using a Weibull distribution with a shape parameter $\beta < 1$, capturing the

occur. The probability density function is given by:

$$f(t) = \frac{\beta}{\eta}\left(\frac{t-B}{\eta}\right)^{\beta-1} e^{-\left(\frac{t-B}{\eta}\right)^{\beta}}, \quad \text{for } t > B,$$

where β is the shape parameter, η is the scale parameter, and B is the threshold time. This allows modeling of components with delayed failure onset, such as those with a burn-in period (Nguyen-Schäfer, 2016).

decreasing failure rate typical of infant mortality; the constant failure phase uses a constant failure rate, representing random failures; and the wear-out phase was modeled with a Weibull distribution where $\beta > 1$, reflecting increasing failure rates due to aging. A time-dependent analysis within the software can then be used to show the failure rate over time of the component. This is done by assigning a chance of zero to the life phase that is not considered in that timeframe.

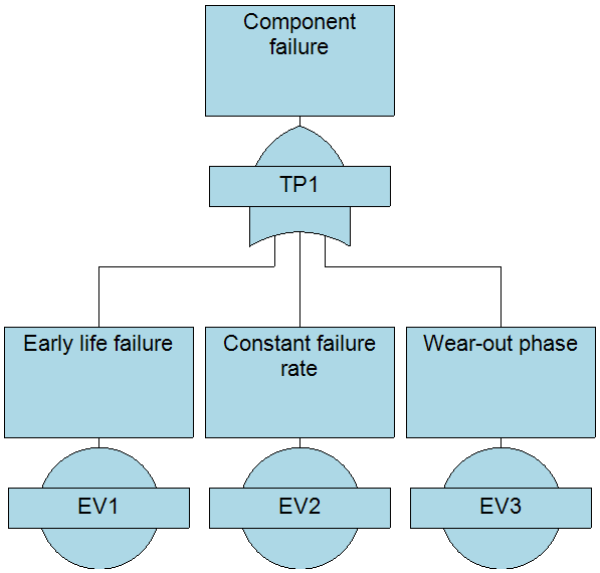


Figure 4.6: Component modeling in a non-stationary FTA, done in Reliability Workbench (Ltd., 2025)

4.3.3. Verifying HAD

To assess how different levels of training affect the Human Action Database (HAD) contribution to the overall non-closure probability of the Maeslant barrier, a probabilistic scenario comparison was performed as described in Section 3.4.4. This approach builds on the assumption that the current base non-closure probability of $P_{\text{base}} = 0.01$ already includes the nominal human error contribution, based on a representative Human Error Probability (HEP).

The resulting probability distributions for human intervention reliability differ significantly across the three training scenarios. The baseline case yields a median non-closure probability of $P = 0.01$ with a relatively narrow spread, while the trained scenario shifts the distribution downward, producing consistently lower values of non-closure probability across the range. In contrast, the untrained scenario produces a broader distribution, with the upper tail extending to $P = 0.35$, indicating substantially higher potential non-closure probabilities.

Figure 4.7 visualizes these distributions, showing limited overlap between the trained and untrained scenarios. The trained case clusters tightly around lower probabilities, whereas the untrained case is both wider and shifted upward, reflecting greater uncertainty and increased likelihood of adverse outcomes. Together, these distributions illustrate how assumptions about operator training levels translate into markedly different reliability estimates within the HAD framework.

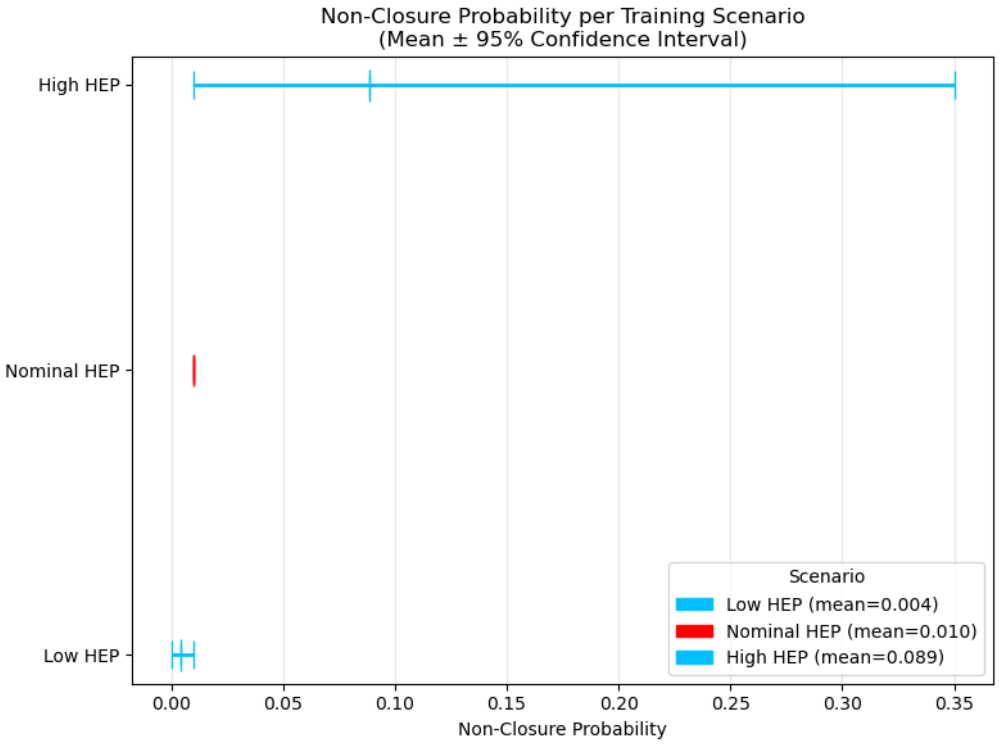


Figure 4.7: Distributions of HAD contribution to non-closure probability under different operator training levels. The horizontal axis shows the failure-to-close probability and the vertical axis shows the different training levels ranging from low, nominal and high. The bars in the graph represent the range and the median. The legend in the right-bottom corner shows the median values of the failure-to-close probability resulting from the different training levels.

This analysis demonstrates that the assumed human error rate embedded in the existing non-closure estimate substantially influences the overall risk profile, when computed as simplistically as this. The new failure to close probabilities range from:

$$P_{\text{failure-to-close, total}} \in [0.004, 0.01, 0.09]$$

If the actual training and verification processes deviate from nominal assumptions, the barrier's failure-to-close probability may be over- or underestimated. This underlines the importance of investing in verified training protocols, standard operating procedures, and regular operator assessments to reduce uncertainty in HAD performance.

The decision to use the THERP handbook as the foundation for estimating human error probabilities in this study is further validated by findings from the OPSCHEP model used by Rijkswaterstaat (Expert, Rijkswaterstaat 2025). Upon reviewing the documentation of OPSCHEP, it became clear that the human error probabilities embedded in the model are themselves derived from the THERP methodology (Rijkswaterstaat GPO – afdeling Instandhouding Constructies & Onderhoud (ICO), 2017). By adopting the same foundational data, consistency is assured with established national practices. Moreover, the use of THERP allows for transparent error modeling, using widely available documentation.

During the SDM, several experts expressed concerns regarding the current status of the Human Action Database (HAD). A theme was the lack of empirical validation of the reliability values, which are presently based on assumptions rather than systematic performance data. Experts also noted that the database does not sufficiently reflect context-dependent factors such as stress, time pressure, and operational complexity, all of which can strongly influence human error probabilities (see Section 4.3.1). In addition, as described in Section 2.4.2, the documentation of the HAD implementation in the FTA is incomplete, making it difficult to trace how reliability values were originally derived. These concerns

underline the wide range of uncertainty reflected in the probability estimates reported above, and illustrate why HAD verification remains a critical open issue in the RA framework.

The nuclear- and defense industry demonstrate that human reliability can be systematically verified through a combination of structured training, empirical performance data, and continuous validation (Defensie, 2017; Khalaquzzaman et al., 2010). Applying similar principles to the Maeslant barrier, such as scenario-based training, performance audits, and integration of operational feedback, could significantly enhance the credibility of the HAD component within the RA framework. Applying similar principles to the Maeslant barrier, such as scenario-based training, performance audits, and integration of operational feedback, could significantly enhance the credibility of the HAD component within the RA framework. The next subsection explores how this insight is translated into a probabilistic methodology tailored to the Maeslant barrier context.

Furthermore, research in the nuclear industry has shown that a significant proportion of human errors stem not from operational mistakes, but from maintenance-related issues (Heo & Park, 2010; Hirotsu et al., 2001). For the Maeslant barrier, it became apparent that these errors often remain latent and undetected until the affected component is called upon during a critical moment (Expert, Rijkswaterstaat 2025). An example is the failure of a water pump that had undergone maintenance but was not functionally verified afterward. The fault only became apparent when the pump was needed, revealing a gap in the verification process (Expert, Rijkswaterstaat 2025). This exposes a systemic issue: maintenance activities are assumed to restore full functionality, yet in practice, verification from the operators is often limited (Expert, Rijkswaterstaat 2025). Without structured post-maintenance testing or condition monitoring, as done in the nuclear- and defense industry, such latent failures could propagate unnoticed through the system.

4.4. Aggregated results

By combining the failure-to-close probabilities from both epistemically uncertain events (EUE) and the Human Action Database (HAD) verification, the total aggregated risk increases slightly beyond the individual contributions. Using the formula from section 3.5:

Table 4.3: Combined Failure-to-Close Probabilities from EUE and HAD Sources. Follwing the mathodology explained in Section 3.5. The vertical-left column shows the failure-to-close probability from the HAD and the horizontal-top colomn shows the failure-to-close probabilities from the EUE.

HAD \ EUE	0.307	0.317	0.335
0.004	0.310	0.319	0.337
0.010	0.313	0.322	0.342
0.090	0.365	0.375	0.393

The aggregated results presented in Table 4.3 illustrate how the combined failure-to-close probability of the Maeslant barrier evolves when accounting for both EUE and uncertainties in human intervention reliability (HAD). The table shows that even small increases in the HAD-related failure probability can meaningfully elevate the total risk. For instance, when the HAD contribution is as low as 0.004, the combined failure probability ranges from $P = 0.310$ to $P = 0.337$, depending on the EUE estimate. However, when the HAD contribution increases to 0.09, the total risk rises significantly, reaching up to $P = 0.393$. This is illustrative, due to the assumptions on the aggregation of the SDM ranges. Therefore, this result should not be taken literally but indicative.

5

Discussion

This thesis investigated whether previously unaccounted events could be systematically identified, quantified and integrated into the Maeslant barrier's non-closure probability calculation. The approach was exploratory: structured identification and quantification were applied to broaden the scope of the current RA, but the resulting estimates are indicative rather than definitive. This limitation arises from both methodological constraints, such as the SDM, and the reliance on human reliability data drawn from other high-risk domains such as the nuclear and defense industries.

More broadly, the research demonstrates how structured methods can produce insights while also revealing tensions between model-based outputs and expert perspectives. Such tensions are valuable, as they expose blind spots in both approaches and highlight areas where further evidence is required. The estimates reported here should therefore be understood as signposts rather than final answers, pointing toward potential risk drivers and priority areas for future investigation, while keeping the overarching goal in view: safeguarding flood safety through credible and transparent reliability assessments.

5.1. Comparison with other studies

Compared to previous studies on the reliability of the Maeslant barrier, such as those by Webbers et al. (2008), and L. Mooyaart et al. (2025), this thesis takes a distinctly exploratory and integrative approach by explicitly targeting unaccounted-for events. While earlier work has acknowledged the limitations of fault tree assumptions (e.g. Bakker, Busnach, et al. (2025)) and the challenges of modeling human interventions, it often remained without quantitative outcome. This study tries to systematically identify and quantify these events. Moreover, whereas the current analyses relies on expert judgment, that is almost never reproducible, this thesis applies SDM to show differing mental models and quantify uncertainty ranges. The inclusion of negative probability estimates and the lack of convergence among experts, as observed in this study, not only highlight a broader fragmentation of opinions not addressed in earlier work but also suggest that the elicitation instructions may not have been sufficiently explicit to prevent such issues. Additionally, the proposed integration of OPSCHEP into the fault tree and the use of time-dependent modeling tools like Reliability Workbench represent methodological advancements beyond the (almost) static assumptions of the current RA analyses (Ltd., 2025). In doing so, this thesis not only complements but also challenges existing literature by advocating for a more transparent, adaptive, and data-informed RA analysis.

5.2. Limitations and assumptions

As outlined in Section 3.6, this study operates under several methodological constraints and modeling assumptions. Here, these are discussed in more detail, including their potential influence on results and implications for future work.

A limitation of this study is that the identification of previously unaccounted-for events was conducted

solely by the author. While the applied techniques are standard in RA analyses, they are typically carried out by multidisciplinary teams to capture diverse perspectives and minimize bias. The absence of such a collaborative setting may have constrained the breadth of identified events and increased the risk of overlooking certain failure modes. Although informal expert input was used to validate assumptions, the lack of a structured group elicitation process reduces the robustness and reproducibility of this stage. As such, the resulting long-list should be viewed as a preliminary foundation for further expert review rather than a definitive inventory.

A further limitation arises from the shortlisting process, in which only three events were selected for quantification. This restriction was dictated by the scope and time constraints of the thesis, including the limited period available for expert engagement, data collection, and probabilistic modeling. While this focused approach enabled in-depth analysis of the selected cases, it also meant that many potentially relevant events were excluded, most often because their estimated probability of occurrence was below the inclusion threshold of approximately 1/100 per operational cycle, due to limited data availability, or because modeling them would have been too complex within the available timeframe. These omissions do not imply irrelevance; in a complete and transparent risk assessment, all identified events should ultimately be reviewed, validated, and, where appropriate, integrated into the RA analysis.

Another limitation of this study lies in the SDM used to quantify epistemically uncertain events. Due to time and resource constraints, a simplified, Delphi method was used. Experts were asked to estimate how much each event might increase the failure-to-close probability using 5%–95% ranges and a median value. However, without standardized seed questions or performance-based weighting, as in Cooke's method Cooke (1991), the reliability of individual inputs could not be assessed. Moreover, asking for percentage contributions to a probability, rather than estimates in absolute or measurable units, was unconventional and may have introduced ambiguity. Previous studies on expert elicitation caution that the format of probability questions can strongly influence both accuracy and consistency of responses (Colson & Cooke, 2018; Morgan & Henrion, 1990; O'Hagan et al., 2006). In particular, relative probability formats can lead to greater interpretation variability between experts, especially when baseline probabilities are not explicitly defined. The responses showed a notable lack of convergence, with wide variability in how events were interpreted and quantified. Some experts even submitted negative probability ranges, reflecting fundamentally different mental models of the system. This divergence highlights the difficulty of aggregating expert opinions without structured consensus-building and may have introduced additional uncertainty into the final estimates.

Beyond these methodological concerns, it became clear that the SDM, in its current form, can only serve a signal or exploratory function. This is due to the structural separation between human intervention and technical failure in the existing RA analysis of the Maeslant barrier, and the mere complexity of said RA analysis. The question posed to experts, how much the failure-to-close probability increases due to specific events, lacked the precision needed to align with the granularity of the fault tree model. While this relative framing was chosen to simplify expert engagement, it may have sacrificed specificity and traceability; without clearly defining whether the increase was relative to the total system probability, a specific subsystem, or an individual cut set, experts may have interpreted the question differently. Literature on expert elicitation highlights that probability questions should mirror the architecture and logic of the underlying model to improve comparability and integration (Colson & Cooke, 2018; Morgan & Henrion, 1990; O'Hagan et al., 2006). In the context of the Maeslant barrier fault tree, a more compatible approach might involve eliciting absolute probabilities for individual basic events or minimal cut sets, ideally framed in measurable units such as "failures per closure request" or "probability per operational cycle." Another alternative would be to present experts with relevant portions of the fault tree and request conditional probabilities given the state of parent nodes. While such approaches demand more time, model familiarity, and cognitive effort from participants, a staged hybrid process, starting with broad probability ranges to identify high-impact events, followed by targeted elicitation at the fault tree level, could balance feasibility and precision. Although the expert responses in this study offer valuable insights, they remain subjective and are based on varying interpretations of the RA framework. The aggregation level of the SDM results is therefore too high to draw definitive conclusions. Before any integration into the RA model can be considered, the interaction between the expert-identified events and the fault tree must be made explicit. Only then can these insights evolve from exploratory signals into actionable inputs. As such, the SDM results should be interpreted

as indicative rather than definitive, and future work should adopt a more rigorous, model-aligned elicitation protocol to improve their direct applicability to the RA model.

This study also faced several data-related limitations that influenced both the identification and quantification of unaccounted-for events. Many of the failure probabilities used in the current RA model are based on expert judgment or outdated assumptions, with limited empirical validation. In particular, the lack of a centralized, structured dataset on component degradation, maintenance history, and operational performance constrained the ability to model time-dependent failure behavior accurately. Similarly, the absence of detailed, verifiable data on human interventions in the Maeslant barrier limited the HAD analysis. While some expert-derived probabilities were used to approximate these uncertainties, the lack of real-world performance data introduces a degree of speculation into the results.

The aggregation approach adopted comes with several limitations that shape how the results should be interpreted. First, the assumption of independence between EUE and HAD, and between the events of SDM is unlikely to hold strictly, since technical reliability and human reliability often interact in practice and the events mentioned in the SDM show overlap. Second, reliance on averaged expert judgments, without calibration or weighting, introduces an element of subjectivity into the estimates. Third, the treatment of aggregated values as point probabilities neglects the propagation of uncertainty distributions. Fourth, the method breaks down if the events are mutually exclusive. Finally, the approach assumes that all events carry equal weight in the failure tree, regardless of their position or relative influence. Taken together, these simplifications mean the results should be regarded as illustrative rather than definitive. The outputs are not decision-grade estimates but rather an exploratory exercise to demonstrate how different uncertainties combine and how sensitive the overall non-closure probability is to assumptions about human reliability and epistemic gaps in the RA model. As highlighted in the reliability literature, proper aggregation of expert judgment and uncertainty requires explicit treatment of dependencies and weighting before results can credibly support operational or policy decision-making (Cooke, 1991; Rausand & Høyland, 2004).

In addition, another important consideration in the context of RA analysis is the extent to which completeness should be pursued. It is said that completeness in physical laws is unattainable, as demonstrated by the inherent limitations in formal systems and the presence of assumptions and constraints. In physics, every law is subject to boundary conditions and idealizations, which limit its applicability to real-world scenarios (Weingartner, 2005). Therefore, rather than striving for absolute completeness, it may be more appropriate to aim for an optimal level of complexity, one that balances generality, transparency, and applicability. In the context of RA analysis, this implies that models should explicitly state their assumptions and constraints, and focus on traceability and adaptability rather than exhaustive coverage. Such an approach acknowledges the limitations of modeling complex systems and supports the development of reliable and interpretable risk assessments.

The divergence between the events identified in this study and those currently incorporated in the RA analysis of the Maeslant barrier could be attributed to both structural and procedural factors. The existing RA analysis is built around a predefined fault tree structure, which is currently maintained by a single individual. While this ensures consistency, it also introduces the risk of tunnel vision, where assumptions and modeling choices remain unchallenged over time.

5.3. Interpretation of results

Beyond the expected outcomes of the quantification exercises, several findings emerged that were not anticipated at the outset of this study. These findings are valuable because they expose structural weaknesses in the current RA framework and suggest directions for improvement.

First, the epistemically uncertain events (EUE) were found to exert a larger influence on the non-closure probability than expected (see Section 4.3.1). Experts have shown concern by assigning large influences on omitted events. This demonstrates that the omission of epistemically uncertain events from the current RA framework may not be a marginal issue, but could be a source of underestimation.

Second, the Human Action Database (HAD) verification results showed that assumptions about training

levels drive differences in non-closure probability (see Section 4.3.3). The spread between the trained and untrained scenarios spans nearly two orders of magnitude, underscoring how sensitive the RA is to human performance assumptions. This outsized effect illustrates the risks of relying on an unverified database: without empirical validation, the reliability of human intervention remains one of the largest unknowns in the analysis.

Third, the fault tree analysis revealed that once software reliability values were updated, certain hardware components re-emerged as dominant contributors (see Section 2.4.2). In particular, a specific motherboard appeared repeatedly as a common node deep within the new dominant failure paths. This was unexpected, as earlier analyses emphasized software as the critical driver. One take could be that the result suggests that current model assumptions may be masking vulnerabilities in hardware and system interactions, which only become visible under different parameterizations. Another take could be that the software and computer reliability is marked as most important while modern computers and software can be made extremely reliable, looking at the capabilities of, for example, the European Space Agency (ESA) (European Space Agency, 2025).

It is also important to note that the experts consulted in this study expressed greater concern about certain vulnerabilities than is reflected in the current FTA. Whereas the FTA highlights software and computer components as dominant contributors, experts emphasized broader systemic and human-related uncertainties, particularly those linked to operator performance and unverified HAD values. This divergence suggests that the present RA framework may underestimate areas of concern that practitioners perceive as critical, further reinforcing the need to align model assumptions with expert judgment and operational realities.

Taken together, these findings challenge several aspects of current RA practice. The reliance on outdated software reliability data risks, and extensiveness within modeling, misdirecting attention toward components that may not be the true weak points. The incomplete integration of OPSCHEP into the FTA structure obscures the role of human interventions in mitigating technical failures (see Section 2.4.2). And the absence of systematic treatment of epistemic uncertainty means that potentially important events remain outside the scope of the model. Each of these issues undermines the credibility of the RA and highlights the need for a more comprehensive, data-driven, and integrated approach.

5.4. Implications for the Legal 1/100 Standard

As described in Section 2.4, a central benchmark in the Dutch flood defense system is the legal requirement that the Maeslant barrier achieves a non-closure probability of at most 1/100 per closure request (Government of the Netherlands, 2024). The results of this thesis indicate that the inclusion of previously unaccounted-for events may influence whether this requirement is actually satisfied. The findings regarding, EUE and HAD demonstrate that the margin between the modeled non-closure probability and the legal requirement is sensitive to methodological choices and assumptions. While the current RA framework may report compliance, the omission of the events studied here introduces a risk of underestimation.

Therefore, the influence on the legal 1/100 requirement is twofold. First, the actual non-closure probability may already be closer to or above the threshold than official analyses suggest. Second, the credibility of compliance claims is weakened if uncertainties remain outside the formal RA model.

5.5. Societal impact

The Maeslant barrier is not only an engineering asset but also a cornerstone of societal security in the Netherlands. Its performance directly influences the safety of over two million residents, the protection of critical infrastructure, and the continuity of economic activities in one of the country's most densely populated and economically vital regions (Jonkman & Merrell, 2024; Rijkswaterstaat, 2025c). Any compromise in its reliability would have cascading social, economic, and political consequences, from displacement of communities and loss of livelihoods, to disruptions in trade and transport through the Port of Rotterdam (Hallegatte et al., 2013).

The uncertainty and incompleteness identified in this study's review of the RA analysis have implications

that extend beyond technical accuracy. A perceived lack of transparency or confidence in the barrier's reliability can erode public trust in flood defense governance (Mostert, 2020; Terpstra, 2011), complicate policy decisions, and provoke public debate about investment priorities. In a country where water safety is part of the societal contract between citizens and government (van Buuren et al., 2016), maintaining that trust is as critical as the physical integrity of the barrier itself.

Addressing the identified gaps, such as by improving data traceability, integrating human reliability verification, and maintaining a registry of unaccounted-for events, strengthens not only the analytical framework but also the accountability of the institutions responsible for flood protection. These measures provide policymakers with defensible, evidence-based risk assessments (Kasperson et al., 1988), give communities confidence that safety systems adapt to new knowledge, and support long-term resilience planning in the face of climate change (Haasnoot et al., 2019; IPCC, 2022).

In this sense, the societal impact of this thesis lies in reframing reliability analysis not merely as a technical task, but as a public responsibility whose outcomes influence social stability, economic security, and collective preparedness for extreme events.

5.6. Future work

First, additional empirical data on human reliability during barrier operations, particularly under stress conditions, is required to replace assumptions with evidence-based estimates. Second, the incorporation of time-dependent effects into fault tree models should be expanded beyond selective expert judgment. Third, the SDM would benefit from refinement, ideally through iterative or multi-round SEJ formats to improve calibration and convergence.

Beyond methodological development, the primary challenge lies in translating these insights into practice. This includes embedding them into decision support systems, maintenance strategies, and policy frameworks without introducing unnecessary complexity. The objective is not to construct perfect models, but to develop models that clearly communicate their limitations. This approach supports trust, adaptability, and improved engineering practice.

While the dedication and expertise of the engineers currently responsible for the Maeslant barrier should be acknowledged and commended, the complexity of the existing RA analysis limits the effectiveness of incremental improvements. This study shows that issues, such as undocumented assumptions, limited transparency in the OPSCHEP integration, and the omission of certain failure modes, are rooted in the structure of the current model itself rather than in isolated data or parameter choices. In such a framework, small adjustments may correct individual branches or input values, but they cannot address the deeper architectural limitations, meaning that the same problems may persist in future updates.

As difficult as the conclusion may seem, it is the opinion of the author that the most effective path forward is to reduce complexity by taking a step back and developing a new RA model from the ground up. This is a significant undertaking, but it would allow the integration of all lessons learned to date, adoption of a modular and transparent architecture, and early embedding of human reliability modeling and non-stationary effects. Such a redesign should also incorporate clear documentation of all assumptions, open access to the modeling logic where possible, and a framework for periodic review and update as new empirical data become available. Although the initial effort and resource investment would be considerable, the payoff would be a model that is easier to audit, more adaptable to future climate and operational changes, and capable of sustaining stakeholder trust over the long term. This approach would also align the Maeslant barrier's RA process with best practices from other high-reliability sectors, where model rebuilds are periodically undertaken to prevent the accumulation of opaque assumptions and outdated structures.

6

Conclusions and Recommendations

6.1. Conclusions

This thesis set out to investigate if a selected set of previously unaccounted-for events can be systematically identified and quantified, and how they can be integrated into the non-closure probability calculation of the Maeslant barrier. The study was structured into three stages, identification, shortlisting, and quantification. The conclusions below are organized around the research questions posed in this study.

6.1.1. RQ1: Which unaccounted events exist?

A comprehensive long-list of potential events was developed using four complementary methods: HAZOP, FMEA, What-if analysis, and External Event Screening. Each method contributed a different perspective, structured hazard analysis, failure mode logic, creative scenario exploration, and rare-event consideration, together ensuring broad coverage. This approach demonstrated that unaccounted events can be systematically identified.

6.1.2. RQ2: How can these events be organized and filtered to produce a short-list for detailed analysis?

The Long-list was reduced to a short-list through screening criteria that emphasized (i) expected contribution to the non-closure probability and (ii) quantifiability within the scope of this study. This process distilled the list into three priority events:

1. Epistemically uncertain events (EUE),
2. Precondition of stationarity of FTA not met,
3. Unverified reliability of human intervention (HAD: Human Action Database).

These three events span all phases of the reliability bathtub curve, ensuring coverage of early-life, useful-life, and wear-out uncertainties. The shortlisting process therefore provided a balanced cross-section of missing events.

6.1.3. RQ3: How can these unaccounted events from the short-list be quantified?

Each shortlisted event was quantified using methods suited to its characteristics. Epistemically uncertain events were explored through structured expert judgment (SEJ) using the SDM framework, revealing wide uncertainty ranges and fragmentation of expert opinion. For the non-stationary FTA, an illustrative methodology was developed that would allow time-dependent modeling once degradation data become available; current data gaps prevent full application. The HAD verification was examined through scenario-based training levels, demonstrating that the quality of training strongly shifts the non-closure probability. Together, these quantifications were exploratory, not definitive, but they show

the pathways by which such events can be brought into the RA framework.

6.1.4. RQ4: How can these events be integrated in the non-closure probability calculation of the Maeslant barrier?

Using a simple independence-based aggregation, indicative combined probabilities were calculated for EUE and HAD. These showed that even modest increases in HAD-related uncertainty could meaningfully elevate total risk, from baseline estimates around $P = 0.31$ to as high as $P = 0.39$. While the aggregation relied on strong assumptions (e.g., independence, linearity) (see Section 3.6 and Section 5.2), the exercise demonstrates how multiple unaccounted events can interact to shift the system-level risk estimate.

6.1.5. Overall insights

This study leads to several insights regarding the current RA framework of the Maeslant barrier:

- Epistemic uncertainty is not marginal; knowledge gaps and unmodelled phenomena can have an influence on overall reliability outcomes, and experts express concern regarding these events.
- Human reliability is a sensitive factor in the analysis. The results indicate that training quality in particular may have a stronger effect on non-closure probability than currently represented in the RA model. Moreover, because human intervention is not explicitly embedded within the FTA structure, it cannot be scrutinized with the same transparency as technical components, which further complicates validation.
- The contrast between model outcomes and expert concerns suggests that current RA practices may convey greater confidence than is justified, particularly where outdated data sources or simplifying assumptions are applied.

Taken together, these findings suggest that the RA of the Maeslant barrier is incomplete rather than incorrect. By systematically identifying and exploring unaccounted events, this thesis shows that the present reliability estimate may understate the true range of uncertainty. More broadly, the work illustrates the need for a reliability framework that is transparent about its assumptions, adaptive to new evidence, and continuously updated as data and methods improve.

6.2. Recommendations

In light of the findings presented in this thesis, several recommendations are proposed to improve the completeness, transparency, and reliability of the Maeslant barrier's RA framework. These recommendations aim to address the identified gaps in the current analysis and support the development of a more robust and adaptive risk assessment process, particularly as the system continues to age and faces increasing environmental and operational pressures.

To strengthen the empirical foundation of SEJ, it is recommended that Rijkswaterstaat initiate the development of a dataset documenting previously unaccounted-for events that were later incorporated into FTAs across storm surge barriers and other critical infrastructure. Such a dataset would enable the application of more rigorous SEJ methodologies, including Cooke's method. This approach would allow for a more defensible quantification of epistemically uncertain events and their contribution to the Maeslant barrier's non-closure probability. Moreover, the resulting framework could be generalized across Rijkswaterstaat's infrastructure, offering a systematic and transparent way to "put a number on uncertainty" and enhance the credibility of risk assessments organization-wide.

To address the limitations of the current stationarity assumption in fault tree modeling, a centralized component lifecycle database is recommended. This database should include expert-judged and observed component lifetimes, operational stress histories, maintenance records, and environmental exposure data. Such a resource would enable the systematic application of non-stationary failure models and support the validation of previous failure probabilities determined through expert judgment.

The current RA model includes human interventions via the Human Action Database (HAD), but lacks

transparency on formal verification of training levels, procedural adherence, and operational readiness. It is recommended that Rijkswaterstaat adopt structured human reliability verification practices from high-reliability sectors such as nuclear energy and defense. This includes scenario-based training, post-maintenance functional testing, quality control, and more regular performance audits. Quantifying the impact of training quality on non-closure probability, as demonstrated in this thesis, shows the possible increase in reliability.

Another recommendation is the integration of the OPSCHEP model directly into the FTA. Currently, the interaction between these two components is limited, which restricts the ability to easily trace how human interventions influence dominant failure paths. By embedding OPSCHEP into the FTA structure, it should become possible to identify dominant failure paths more transparently and address them more effectively. Additionally, it is recommended to revise the current reliability assessment of the software systems within the FTA. The existing evaluation is outdated and does not reflect the capabilities of modern software reliability assessment tools. Updating this component would not only improve the accuracy of the RA model but also ensure that software-related risks are appropriately represented in the overall non-closure probability.

Finally, recommendations can be made for subsequent student projects. The Structured Decision-Making (SDM) approach used in this thesis can be refined with clearer elicitation instructions and perhaps calibration exercises to avoid unrealistic outcomes. Quantification can be extended by piloting non-stationary reliability models if suitable data become available, or by developing simulation-based approaches to human reliability. Above all, future work should prioritise clarity and traceability over complexity. A reliability model that is understandable to both experts and practitioners will ultimately have greater impact than one that is technically sophisticated but opaque. This reflects earlier observations that transparency and communicability are essential for risk models to inform decision-making effectively (Aven, 2016; Mostert, 2018; Paté-Cornell, 1996; van Asselt & Renn, 2011).

Taken together, these recommendations point to a common direction: future RA of the Maeslant barrier should be more transparent, adaptive, and empirically grounded. Only by combining improved data collection with methodological advances can the RA evolve into a tool that is both technically credible and societally robust.

This thesis has shown that even in a system as thoroughly engineered as the Maeslant barrier, blind spots can still exist, events and uncertainties that escape the current RA framework. Through structured identification and expert elicitation, this thesis explores how epistemic uncertainty and unverified human reliability could significantly influence the estimated non-closure probability. The recommendations made, ranging from integrating OPSCHEP into the fault tree to adopting structured human reliability verification and building a component lifecycle database, are not just technical upgrades but steps toward a more transparent and resilient risk assessment. The persistent unrest surrounding the RA analysis, echoed in both expert feedback and the SDM results, underscores the need for this shift. And if software reliability continues to dominate the failure paths, it could be a possibility to look beyond the traditional circles. Organizations like the European Space Agency have decades of experience building software that simply cannot fail (European Space Agency, 2025). If they are to land probes on comets, why not involve them in safeguarding Dutch flood defenses? After all, the stakes are just as high. This thesis doesn't claim to have all the answers, but it is a step toward finding them.

References

Andrews, J., & Moss, T. (2002). Reliability and risk assessment. Professional Engineering Publishing.

Andrews, J., & Lunt, S. (2012). Introduction to fault tree analysis. 2012 Annual Reliability and Maintainability Symposium. USA, 1–3.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bakker, A., Busnach, T., Nagelhout, M., Mooyaart, L., & Hamerslag, E. J. (2025). A qualitative model of the reliability-maintenance cost relation of critical hydraulic structures in support of complex modeling and communication of model results [Accessed: 2025-07-21]. Proceedings of the 33rd European Safety and Reliability & 33rd Society for Risk Analysis Europe Conference (ESREL-SRA-E 2025). https://doi.org/10.3850/981-973-0000-00-0

Bakker, A., Mooyaart, L., Hamerslag, E. J., & van Gijzen, L. (2022). Towards probablistic asset management of storm surge barriers under rapidly changing circumstances (tech. rep.). EasyChair.

Bakker, A., Rovers, D. L., & Mooyaart, L. F. (2025). Storm surge clusters, multi-peak storms and their effect on the performance of the maeslant storm surge barrier (the netherlands). Journal of Marine Science and Engineering, 13(2), 298.

Bier, V. M., & Cox Jr, L. A. (2007). 15 probabilistic risk analysis for engineered systems. Cambridge University Press New York.

Blanchard, B. S., Fabrycky, W. J., & Fabrycky, W. J. (1990). Systems engineering and analysis (Vol. 4). Prentice hall Englewood Cliffs, NJ.

Brandt, E., Di Bucchianico, A., van Ekris, J., Groote, J., Geurts, W., Heslinga, G., & Kolk, G. (2011). Topaas : Een structurele aanpak voor faalkansanalyse van software intensieve systemen. Rijkswaterstaat. Ministerie van Verkeer en Waterstaat.

Center for Chemical Process Safety. (2008). Guidelines for hazard evaluation procedures (3rd). American Institute of Chemical Engineers.

Chen, Y.-C. (2017). A tutorial on kernel density estimation and recent advances. arXiv preprint arXiv:1704.03924. https://arxiv.org/abs/1704.03924

Colson, A. R., & Cooke, R. M. (2018). Expert elicitation: Using the classical model to validate experts' judgments. Review of Environmental Economics and Policy.

Cooke, R. M. (1991). Experts in uncertainty: Opinion and subjective probability in science. Oxford University Press.

CSK Review Team. (2021, January). Internal Review Report: Analysis of Failure Probability Modeling Issues in Change Proposal WV490 (Technical Report) (Confidential internal document). Rijkswaterstaat (RWS).

de Jong, M. (2024). Seiche-statistiek maeslantkering: Overzicht van voorgaande studies, toepassing vergrote meetdataset en vooruitblik (tech. rep. No. 11210307-000-HYE-0001) (In opdracht van Rijkswaterstaat, rapportdatum 28 oktober 2024). Deltares. Delft, The Netherlands.

Defensie. (2017). Opwerken volgens sarc [Accessed: 2025-05-05]. Alle Hens, Ministerie van Defensie. https://magazines.defensie.nl/allehens/2017/01/03_opwerken-volgens-sarc

Dekker, S. (2016). Drift into failure: From hunting broken components to understanding complex systems. CRC press.

European Space Agency. (2025). European space agency official website [Accessed: 2025-07-23]. https://www.esa.int/

Goorden, M., van de Mortel-Fronczak, J., van Eldik, K., Fokkink, W., & Rooda, J. (2022). Lessons learned in the application of formal methods to the design of a storm surge barrier control system∗. IFAC-PapersOnLine, 55(28), 93–99.

Government of the Netherlands. (2024). Waterwet (water act) [Accessed: 2025-01-24]. https://wetten.overheid.nl/BWBR0025458/2024-01-01

Gramacki, A. (2018). Nonparametric kernel density estimation and its computational aspects (Vol. 37). Springer. https://doi.org/10.1007/978-3-319-71688-6

Haasnoot, M., Diermanse, F., Kwadijk, J., de Winter, R., & Winter, G. (2019). Strategieën voor adaptatie aan hoge en versnelde zeespiegelstijging: Een verkenning. Deltares Delft, The Netherlands.

Hallegatte, S., Green, C., Nicholls, R. J., & Corfee-Morlot, J. (2013). Future flood losses in major coastal cities. Nature climate change, 3(9), 802–806.

Heo, G., & Park, J. (2010). A framework for evaluating the effects of maintenance-related human errors in nuclear power plants. Reliability Engineering and System Safety, 95(8), 797–805. https://doi.org/10.1016/j.ress.2010.03.001

Hirotsu, Y., Suzuki, K., Kojima, M., & Takano, K. (2001). Multivariate analysis of human error incidents occurring at nuclear power plants: Several occurrence patterns of observed human errors. Cognition, Technology & Work, 3(2), 82–91. https://doi.org/10.1007/s101110100032

Horvadt & Partners. (2025). Horvadt & partners – engineering consultancy [Accessed: 2025-07-11]. https://horvat.nl/

IEC, I. (2006). Fault tree analysis (fta). IEC, 61025, 2007.

Inc., P. (2025). Common cause analysis [Accessed: 2025-06-17]. https://support.ptc.com/help/wrr/r12.0.2.0/en/index.html#page/wrr/PractitionersGuide/CommonCauseAnalysis.html

International Atomic Energy Agency. (2003). External events hazards — screening and analysis.

International Electrotechnical Commission. (2018). Iec 60812:2018 — failure modes and effects analysis (fmea and fmeca) [IEC, Geneva].

IPCC. (2022). Climate change 2022: Synthesis report. contribution of working groups i, ii and iii to the sixth assessment report of the intergovernmental panel on climate change [Edited by Lee, H., Romero, J., and Others]. https://doi.org/10.59327/IPCC/AR6-9789291691647

Jan De Nul Group. (2025). Storm surge barrier protects belgium from natural disasters [Accessed: 2025-07-21]. https://www.jandenul.com/storm-surge-barrier-protects-belgium-natural-disasters

Jonker, J., & Pennink, B. W. (2010). The essence of research methodology: A concise guide for master and phd students in management science. Springer. https://link.springer.com/chapter/10.1007/978-3-540-71659-4_3

Jonkman, S. N., & Merrell, W. J. (2024). Discussion of "coastal defense megaprojects in an era of sea-level rise: Politically feasible strategies or army corps fantasies?" Journal of Water Resources Planning and Management, 150(4), 07024002.

Jonkman, S. N., Voortman, H. G., Klerk, W. J., & van Vuren, S. (2016). Developments in the management of flood defences and hydraulic infrastructures in the netherlands. In Life-cycle of engineering systems: Emphasis on sustainable civil infrastructure (pp. 65–78). CRC Press.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X., & Ratick, S. (1988). The social amplification of risk: A conceptual framework. Risk Analysis.

Khalaquzzaman, M., Kang, H. G., Kim, M. C., & Seong, P. H. (2010). Quantification of unavailability caused by random failures and maintenance human errors in nuclear power plants. Nuclear Engineering and Design, 240, 1606–1613. https://doi.org/10.1016/j.nucengdes.2010.03.011

Kharoubi, Y., van den Boomen, M., Hertogh, M., & van den Bogaard, J. (2023). Foundation for risk-based asset management for storm surge barriers. In Life-cycle of structures and infrastructure systems (pp. 3214–3221). CRC Press.

Kharoubi, Y., van den Boomen, M., van den Bogaard, J., & Hertogh, M. (2024). Asset management for storm surge barriers: How and why? Structure and Infrastructure Engineering, 1–15.

Kletz, T. A. (2018). Hazop & hazan: Identifying and assessing process industry hazards. CRC Press.

Lee, S. T. T., Xu, S., & Kua, I. (2023). How the tiny island city-state of singapore fights rising sea levels [Accessed: 2025-07-21]. TIME. https://time.com/6322111/singapore-fights-rising-sea-levels-climate-change/

Linstone, H. A., & Turoff, M. (1975). The delphi method: Techniques and applications [Reprinted online: http://is.njit.edu/pubs/delphibook/]. Addison-Wesley.

Ltd., I. (2025). Reliability workbench [Accessed: 2025-06-22].

Melchers, R. E. (1999). Structural reliability: Analysis and prediction (2nd). John Wiley & Sons.

Mooyaart, L. F., Bakker, A., van den Bogaard, J. A., Rijcken, T., & Jonkman, S. N. (2023). Economic optimization of coastal flood defence systems including storm surge barrier closure reliability. Journal of Flood Risk Management, 16(3), e12904.

Mooyaart, L., Bakker, A., van den Bogaard, J., Jorissen, R., Rijcken, T., & Jonkman, S. (2025). Storm surge barrier performance—the effect of barrier failures on extreme water level frequencies. Journal of Flood Risk Management, 18(1), e13048.

Mooyaart, L., & Jonkman, S. N. (2017). Overview and design considerations of storm surge barriers. Journal of Waterway, Port, Coastal, and Ocean Engineering, 143(4), 06017001.

Morgan, M. G., & Henrion, M. (1990). Uncertainty: A guide to dealing with uncertainty in quantitative risk and policy analysis. Cambridge University Press.

Mostert, E. (2018). An alternative approach for socio-hydrology: Case study research. Hydrology and Earth System Sciences, 22(1), 317–329.

Mostert, E. (2020). Water and national identity in the netherlands; the history of an idea. Water History, 12(3), 311–329.

National Ocean Service, NOAA. (2024). What is storm surge? [Accessed: 2025-06-20]. https://oceanservice.noaa.gov/facts/stormsurge-stormtide.html

Nguyen-Schäfer, H. (2016). Reliability using the weibull distribution. In Computational design of rolling bearings (pp. 141–170). Springer. https://doi.org/10.1007/978-3-319-27131-6_7

O'Connor, P., & Kleyner, A. (2012). Practical reliability engineering (5th). Wiley.

O'Hagan, A., Buck, C. E., Daneshkhah, A., Eiser, J. R., Garthwaite, P. H., Jenkinson, D. J., Oakley, J. E., & Rakow, T. (2006). Uncertain judgements: Eliciting experts' probabilities. John Wiley & Sons.

Orton, P., Ralston, D., van Prooijen, B., Secor, D., Ganju, N., Chen, Z., Fernald, S., Brooks, B., & Marcell, K. (2023). Increased utilization of storm surge barriers: A research agenda on estuary impacts. Earth's Future, 11(3). https://doi.org/10.1029/2022EF002991

Paté-Cornell, E. (1996). Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering & System Safety, 54(2-3), 95–111. https://doi.org/10.1016/S0951-8320(96)00067-1

Pinto, A., Nunes, I. L., & Ribeiro, R. A. (2009). Framework for ensuring risk assessment completeness in construction industry. 17th IEA Congress, Beijing, China.

Preischl, W., & Hellmich, M. (2013). Human error probabilities from operational experience of german nuclear power plants. Reliability Engineering and System Safety, 109, 150–159. https://doi.org/10.1016/j.ress.2012.08.004

Preischl, W., & Hellmich, M. (2016). Human error probabilities from operational experience of german nuclear power plants, part ii. Reliability Engineering and System Safety, 148, 44–56. https://doi.org/10.1016/j.ress.2015.11.011

ProBO, S. (2017, September). Handreiking externe gebeurtenissen - screening (Handreiking) (Definitief). RWS GPO – afdeling Instandhouding Constructies & Onderhoud (ICO). mailto:probo@rws.nl WW RWS Nummer: 5501.

Rausand, M., & Høyland, A. (2004). System reliability theory: Models, statistical methods, and applications (2nd). Wiley.

Rauzy, A. (2001). Mathematical foundations of minimal cutsets. IEEE Transactions on Reliability, 50(4), 389–396.

RijksWaterstaat. (2017). Prestatiepeilenmodel oosterscheldekering 2017 (tech. rep.). Rijkswaterstaat.

Rijkswaterstaat. (2012). Basic documentation maeslant barrier (tech. rep.) (Accessed: 2025-07-21). Rijkswaterstaat. https://www.rijkswaterstaat.nl/en/projects/iconic-structures/maeslant-barrier

Rijkswaterstaat. (2013). Europoortkering [Archived from the original on March 3, 2013. Accessed June 23, 2025]. https://web.archive.org/web/20130303014455/http://www.rijkswaterstaat.nl/water/feiten_en_cijfers/dijken_en_keringen/europoortkering/

Rijkswaterstaat. (2016). Operation of the maeslant barrier [Accessed: 2025-05-03]. Ministry of Infrastructure and Water Management, Netherlands. https://www.rijkswaterstaat.nl

Rijkswaterstaat. (2021, October). Bestuurlijke rapportage beoordeling dijktraject 209, europoortkering ii [Government report].

Rijkswaterstaat. (2022a, June). Wettelijke beoordeling europoortkering i dijktraject 208 (Technical Report) (Definitief). Rijkswaterstaat West-Nederland Zuid.

Rijkswaterstaat. (2022b, July). Bestuurlijke rapportage beoordeling normtraject 210, hollandsche ijsselkering [Government report].

Rijkswaterstaat. (2024). Besluit tot wijziging van het Waterbesluit in verband met actualisatie van de normen voor primaire waterkeringen [Accessed via the Internet Archive].

Rijkswaterstaat. (2025a). Maeslantkering [Consulted on January 16 2025]. Retrieved January 16, 2025, from https://www.rijkswaterstaat.nl/water/waterbeheer/bescherming-tegen-het-water/waterkeringen/deltawerken/maeslantkering

Rijkswaterstaat. (2025b). Normaal amsterdams peil (nap) [Open data portal, accessed 10 June 2025].

Rijkswaterstaat. (2025c). Over ons [Accessed: 2025-06-23]. https://www.rijkswaterstaat.nl/over-ons

Rijkswaterstaat GPO – afdeling Instandhouding Constructies & Onderhoud (ICO). (2017, September). Handreiking kwantificering menselijk handelen met gebruik van het opschep model (Technical Report No. 5532) (Definitieve versie). Rijkswaterstaat (RWS). Netherlands.

Royal Netherlands Meteorological Institute (KNMI). (2025). Weather forecasting and meteorological data [Accessed: 2025-05-03]. Royal Netherlands Meteorological Institute. https://www.knmi.nl

Schüller, J., Brinkman, J., van Gestel, P., & van Otterloo, R. (1997). Methods for determining and processing probabilities (Committee for the Prevention of Disasters, Ed.; Second Edition) [Publication Series on Dangerous Substances (PGS 4) – formerly CPR 12E (Red Book)]. Ministry of Social Affairs; Employment, The Netherlands.

Stamatis, D. (2003). Failure mode and effect analysis: Fmea from theory to execution (2nd). ASQ Quality Press.

STANDARD, B., & IEC, B. (2003). Part 3-1: Application guide—analysis techniques for dependability—guide on methodology.

Swain, A. D., & Guttmann, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications (tech. rep. No. NUREG/CR-1278) (THERP Handbook). Sandia National Laboratories. Albuquerque, NM, U.S. Nuclear Regulatory Commission.

Team, R. C. (2020). Kernel estimator and bandwidth selection for density and its derivatives [R package vignette]. https://free-cd.stat.unipd.it/web/packages/kedd/vignettes/kedd.pdf

Terpstra, T. (2011). Flood risk perception and the public: The role of trust and knowledge in the netherlands. International Journal of Water Resources Development, 27(4), 527–540.

Trace-Kleeberg, S., Haigh, I. D., Walraven, M., & Gourvenec, S. (2023). How should storm surge barrier maintenance strategies be changed in light of sea-level rise? a case study. Coastal Engineering, 184, 104336.

Trivedi, K. S., & Bobbio, A. (2017). Reliability and availability engineering: Modeling, analysis, and applications. Cambridge University Press.

van Asselt, M. B., & Renn, O. (2011). Risk governance. Journal of Risk Research, 14(4), 431–449. https://doi.org/10.1080/13669877.2011.553730

van Buuren, A., Driessen, P. P., Teisman, G. R., & van Rijswick, M. (2016). Adaptation to climate change-related flood risks in dutch urban areas: Lessons from practice. Journal of Environmental Planning and Management, 59(3), 331–350.

van Maaren, A. (2018, March). Guidelines on performance-based risk analyses (pra): Enabling asset management based on system performance (B. Inframan, Ed.) [HWN, HVWN, HWS networks]. Version 1.0.1. ProBo Support Desk. Netherlands, ProBo Support Desk.

van Otterloo, R. (2003, March). Methodiek ter bepaling van de betrouwbaarheid van software modules t.b.v. oke (Technisch rapport No. OKE-2005-250-T / 20813/02.54186/C) (In opdracht van Rijkswaterstaat. Beoordeeld en goedgekeurd door Ir. J.C.H. Schüller. Vertrouwelijk.). NRG. Arnhem.

Verma, A. K., Srividya, A., & Karanki, D. R. (2010). Reliability and safety engineering [Chapter on Probabilistic Safety Assessment]. Springer. https://doi.org/10.1007/978-1-84882-637-5

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). Fault tree handbook. U.S. Nuclear Regulatory Commission, NUREG-0492.

Walraven, M., Vrolijk, K., & Kothuis, B. B. (2022). Design, maintain and operate movable storm surge barriers for flood risk reduction. In Coastal flood risk reduction (pp. 271–286). Elsevier.

Watson, I., & Finkl, C. W. (1992). Simplified technical summary of the complete delta works, including the eastern scheldt/eenvoudige technische samenvatting van de gehele deltawerken, inclusief de oosterschelde/vereinfachte technische darstellung des gesamten deltaplans, einschliesslich der ostschelde. Journal of Coastal Research, 1–56.

Webbers, P., van den Bogaard, J., van Manena, S., & van Akkeren, J. (2008). Probabilistic maintenance and asset management on moveable storm surge barriers.

Weingartner, P. (2005). Completeness and reliability. In Physical laws and their limitations. Springer. https://doi.org/10.1007/3-540-23803-X_15

World Shipping Council. (2023). Top 50 ports — world shipping council. https://www.worldshipping.org/top-50-ports

Zio, E. (2009). Reliability engineering: Old problems and new challenges. Reliability Engineering & System Safety, 94(2), 125–141. https://doi.org/10.1016/j.ress.2008.06.002

A

Appendix A

A.1. Fault Tree Analysis

FTA is a deductive, top-down method that systematically investigates the causes of system-level failures. Originally developed for the aerospace and nuclear industries (Andrews & Lunt, 2012), FTA remains a fundamental technique within reliability and safety engineering. It focuses on modeling the logical relationships between basic component failures and a critical system failure, known as the top event. Using Boolean logic gates such as AND and OR, the fault tree identifies how combinations of failures at the component level can propagate upward to cause the top event.

The FTA process begins by clearly defining the top event, which represents the failure scenario of interest. For example, in the case of a storm surge barrier, the top event could be defined as "the barrier fails to close during a storm." From this point, the immediate causes that could lead directly to the top event are identified. Each of these causes is then recursively decomposed into more basic failure events until no further breakdown is practical. This stepwise expansion creates a logical tree structure that visualizes how failures interact within the system.

Within the fault tree, different types of logic gates represent various combinations of failures. An OR gate indicates that the top event will occur if any of the input events occur. For example, a hydraulic system failure could happen if a hydraulic pump fails or there is a hydraulic fluid leak. In contrast, an AND gate indicates that the top event will occur only if all input events occur simultaneously. For instance, a mechanical obstruction in a barrier system might require both the presence of debris and the failure of a sensor to detect that debris. More complex gates, such as Priority AND and Inhibit gates, exist but are used less frequently in standard analyses.

Once the fault tree is constructed, a quantitative analysis can be performed to estimate the probability of occurrence of the top event. Probabilities are assigned to the basic events based on empirical data, historical records, or expert judgment. In Fault Tree Analysis, basic event combinations are typically modeled using Boolean logic gates. For statistically independent events:

- An AND gate represents a scenario where all input events must occur for the output event to occur. The probability is the product of the individual event probabilities:

$$P_{\text{AND}} = P(A) \times P(B)$$

- An OR gate represents a scenario where at least one of the input events must occur for the output event to occur. The probability is calculated as:

$$P_{\text{OR}} = 1 - (1 - P(A)) \times (1 - P(B))$$

For example, consider two independent failure events within a hydraulic system: a pump failure with

a probability of $P = 0.01$, and a fluid leak with $P = 0.02$. The probability of system failure through an OR gate is:

$$P_{\text{system}} = 1 - (1 - 0.01)(1 - 0.02) = 1 - (0.99 \times 0.98) = 1 - 0.9702 = 0.0298$$

Thus, the probability of hydraulic system failure in this example is approximately 2.98% (IEC, 2006). It is important to note that this method assumes each basic event appears only once in the fault tree and that all events are statistically independent. In more complex systems, such as storm surge barriers, basic events often appear in multiple branches, which can cause simple calculations to overestimate failure probabilities. To address this, Boolean algebra and minimal cut set analysis are used to identify unique combinations of failures and ensure that the probability of occurrence of the top event is calculated accurately (Rauzy, 2001) (see subsubsection A.4).

Fault Tree Analysis offers several important advantages. It provides a clear and logical visualization of failure mechanisms and helps prioritize risk mitigation strategies by identifying dominant failure paths. It is widely supported by engineering standards such as IEC 61025 (IEC, 2006) and various reliability engineering software tools. However, the method is not without limitations. It often assumes that failures are statistically independent unless explicitly modeled otherwise, an assumption that may not always hold in complex real-world systems (Dekker, 2016). Furthermore, fault trees can become too complex and difficult to manage for large systems involving hundreds or thousands of components (Andrews & Moss, 2002). Accurate fault tree construction also heavily depends on the quality of the failure rate data available, which is often incomplete or uncertain (Andrews & Moss, 2002).

Despite these limitations, FTA remains an indispensable tool for analyzing and improving the reliability of critical infrastructure. In systems like storm surge barriers, where failure consequences are severe, Fault Tree Analysis not only helps identify technical vulnerabilities but also supports decision-making in design, maintenance planning, and operational risk management (O'Connor & Kleyner, 2012).

A.2. Illustration of Fault Tree vs. Event Tree Analysis

To clarify the distinction between Fault Tree Analysis (FTA) and Event Tree Analysis (ETA), Figure A.1 presents a side-by-side schematic (Vesely et al., 1981). These methods are both fundamental tools in reliability and availability analysis but serve different purposes:

- Fault Tree Analysis (FTA): A deductive method that starts with a top-level undesired event (e.g., system failure) and works backward to identify the combinations of component failures or faults that could cause it.
- Event Tree Analysis (ETA): An inductive approach that starts from an initiating event (e.g., BOS malfunction) and explores possible outcomes based on the success or failure of subsequent safety functions or responses.

FTA focuses on uncovering root causes, while ETA evaluates potential consequences. Together, they offer a complementary view of system reliability.

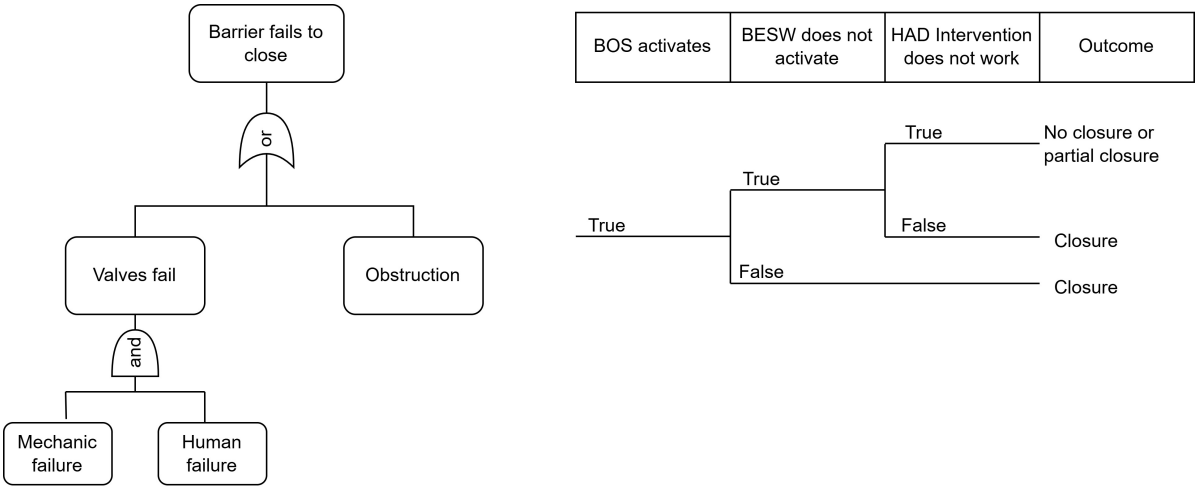


Figure A.1: Comparison between a Fault Tree (left) and Event Tree (right) schematic for illustrating system failure and response outcomes.

A.2.1. Example: FTA of a Storm Surge Barrier Failure

The following calculation is intentionally kept very simple and serves solely to illustrate the absolute basics of Fault Tree Analysis (FTA). It provides a straightforward example to demonstrate how basic events combine through logical gates to influence the probability of a top event. This example should be viewed as purely illustrative and not representative of the full complexity in real-world FTA applications such as storm surge barriers.

The following fault tree illustrates the top event "Barrier fails to close during storm," along with its primary causes (A.2):

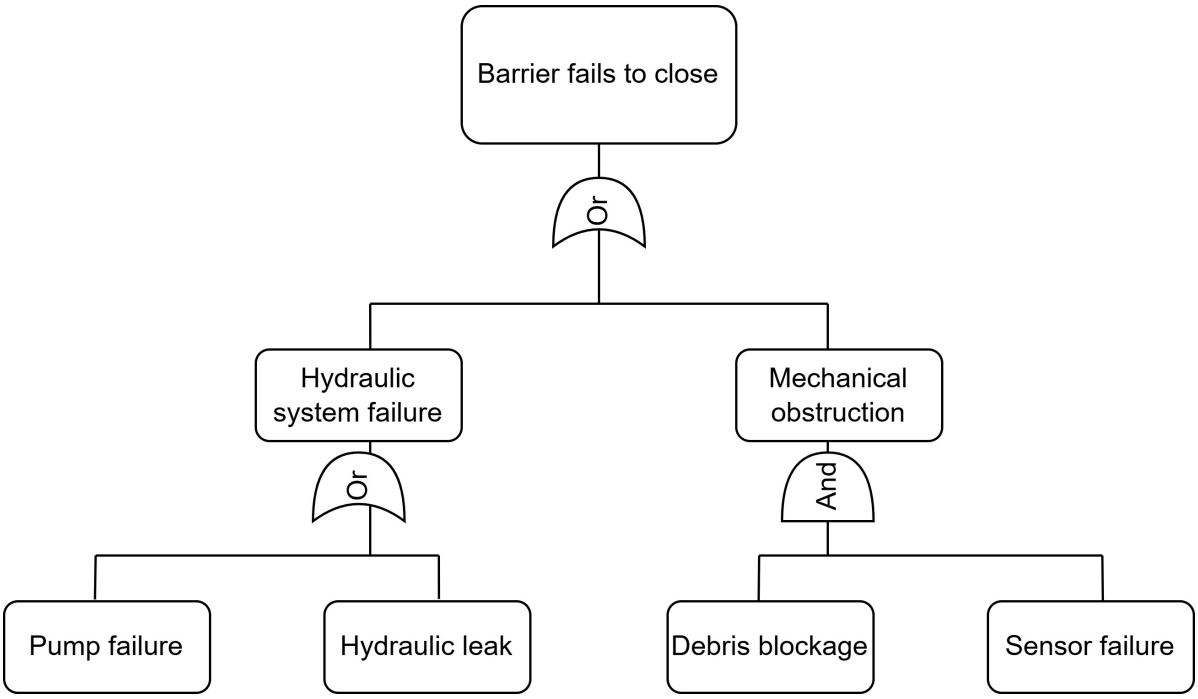


Figure A.2: FTA illustrating the top event: "Barrier fails to close during storm" along with its primary causes.

Assume the following basic event failure probabilities:

- Pump failure: $P_{\text{pump}} = 0.01$
- Hydraulic leak: $P_{\text{leak}} = 0.02$
- Debris blockage: $P_{\text{debris}} = 0.03$
- Sensor failure: $P_{\text{sensor}} = 0.01$

The probability of Hydraulic system failure (OR gate) is calculated as:

$$P_{\text{hydraulic}} = 1 - (1 - P_{\text{pump}})(1 - P_{\text{leak}})$$

$$P_{\text{hydraulic}} = 1 - (1 - 0.01)(1 - 0.02) = 1 - (0.99 \times 0.98) = 1 - 0.9702 = 0.0298$$

The probability of Mechanical obstruction (AND gate) is calculated as:

$$P_{\text{obstruction}} = P_{\text{debris}} \times P_{\text{sensor}}$$

$$P_{\text{obstruction}} = 0.03 \times 0.01 = 0.0003$$

Finally, the probability of the Top Event (OR gate) is:

$$P_{\text{top}} = 1 - (1 - P_{\text{hydraulic}})(1 - P_{\text{obstruction}})$$

$$P_{\text{top}} = 1 - (1 - 0.0298)(1 - 0.0003) = 1 - (0.9702 \times 0.9997) = 1 - 0.9699 = 0.0301$$

Thus, the overall probability of the barrier failing to close during a storm event is approximately 3.01%.

A.3. Minimal Cut Sets

While the above probability calculation gives a basic overview of how event probabilities propagate through the fault tree, another useful concept in Fault Tree Analysis is that of minimal cut sets. A minimal cut set is the smallest combination of basic events that, if they occur together, will lead to the top event.

For the example fault tree shown above, the minimal cut sets are:

- Pump failure
- Hydraulic leak
- Debris blockage, Sensor failure

This means that either a pump failure alone, a hydraulic leak alone, or the combination of a debris blockage and sensor failure can cause the barrier to fail to close. These sets are minimal in the sense that removing any event from the set would no longer lead to the top event.

A.4. Common Cause Failure (CCF) Analysis

In reliability modeling, it is often assumed that component failures occur independently. However, in real-world systems, multiple components may fail simultaneously due to a shared underlying cause—such as a power outage, environmental stress, or a software malfunction. These are referred to as common cause failures (CCFs). To account for such dependencies, several modeling approaches have been developed, including the Beta Factor model, the Multiple Greek Letter (MGL) model, the Alpha model, and the Beta-Binomial Failure Rate (BFR) model.

To illustrate how CCFs are handled in a fault tree, consider a group of four components: A, B, C, and D. If these components are susceptible to a shared failure mechanism, we must consider not only their individual failures but also all combinations of joint failures caused by the common cause. These

combinations include pairs (e.g., AB, AC), triplets (e.g., ABC), and even all four failing together (ABCD).

In the fault tree, each original basic event (e.g., A) is replaced by an OR gate that includes both its individual failure and all CCF combinations that involve it. For example, the event A is replaced by an OR gate with the following inputs: A (individual), AB, AC, AD, ABC, ABD, ACD, and ABCD. This ensures that all possible ways A could fail—including due to a shared cause—are captured.

The following parameters are typically used in CCF modeling:

- Q_t: Total unavailability of each basic event in the CCF group.
- Q_k: Unavailability of the CCF event of order k, i.e., a common cause failure involving k components.
- n: Number of basic events in the CCF group.

This structured approach allows analysts to more accurately estimate system failure probabilities in the presence of shared vulnerabilities, ensuring that the fault tree reflects both independent and dependent failure mechanisms (Inc., 2025).

A.5. Example: FTA of a Storm Surge Barrier Failure with Common Cause Failure

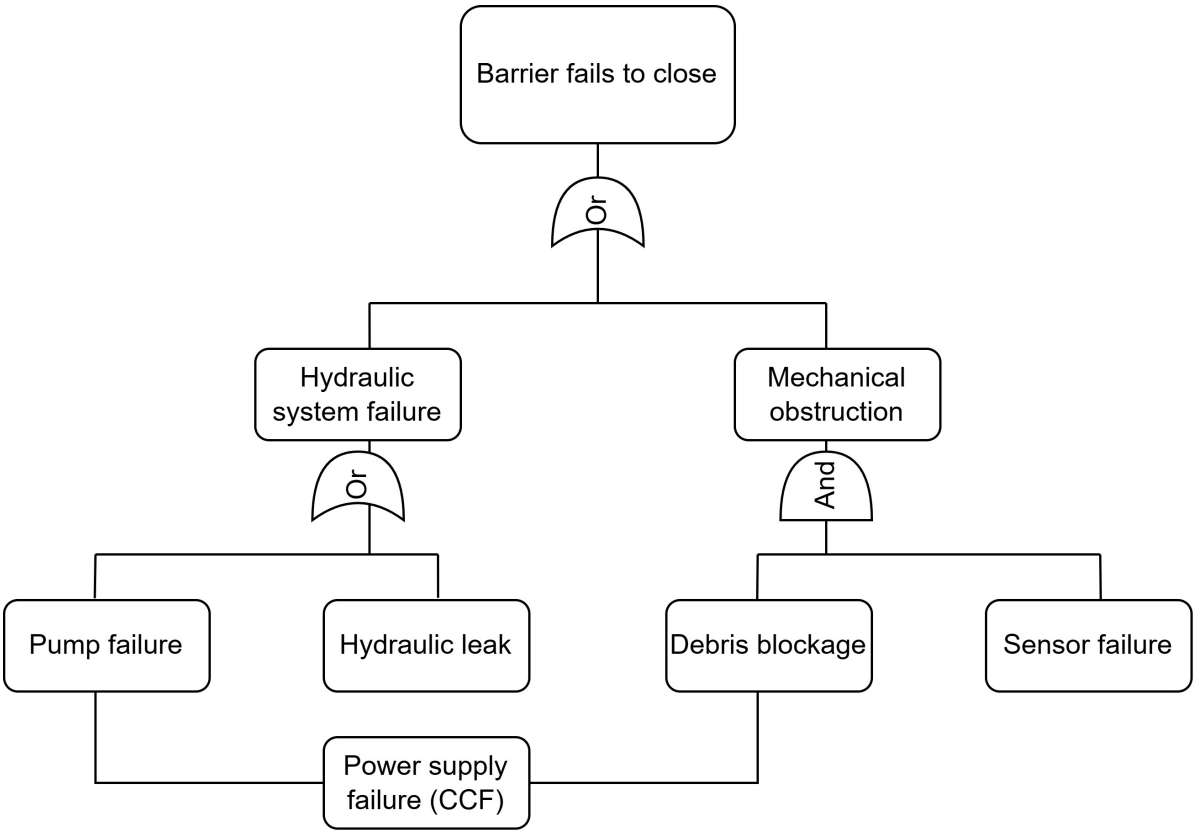


Figure A.3: FTA illustrating the top event: “Barrier fails to close during storm” along with its primary causes.

Assume the following basic event failure probabilities:

- Pump failure: $P_{\text{pump}} = 0.01$

- Hydraulic leak: $P_{\text{leak}} = 0.02$
- Debris blockage: $P_{\text{debris}} = 0.03$
- Sensor failure: $P_{\text{sensor}} = 0.01$
- Power supply failure (common cause): $P_{\text{power}} = 0.005$

We assume that the power supply failure can simultaneously cause both the pump and the sensor to fail. To model this, we use the β-factor model, where a fraction β of the failure probability is attributed to the common cause. Let $\beta = 0.3$.

The adjusted independent failure probabilities become:

$$P_{\text{pump,ind}} = (1-\beta) \cdot P_{\text{pump}} = 0.7 \cdot 0.01 = 0.007$$
$$P_{\text{sensor,ind}} = (1-\beta) \cdot P_{\text{sensor}} = 0.7 \cdot 0.01 = 0.007$$

The probability of Hydraulic system failure (OR gate):

$$\begin{aligned} P_{\text{hydraulic}} &= 1 - (1 - P_{\text{pump,ind}})(1 - P_{\text{leak}}) \\ &= 1 - (1 - 0.007)(1 - 0.02) = 1 - (0.993 \cdot 0.98) = 1 - 0.97314 = 0.02686 \end{aligned}$$

The probability of Mechanical obstruction (AND gate):

$$P_{\text{obstruction}} = P_{\text{debris}} \cdot P_{\text{sensor,ind}} = 0.03 \cdot 0.007 = 0.00021$$

Now we include the common cause failure path:

$$P_{\text{CCF}} = P_{\text{power}} \cdot \beta^2 = 0.005 \cdot 0.09 = 0.00045$$

Finally, the probability of the Top Event (OR gate over three disjoint paths):

$$\begin{aligned} P_{\text{top}} &= 1 - (1 - P_{\text{hydraulic}})(1 - P_{\text{obstruction}})(1 - P_{\text{CCF}}) \\ &= 1 - (1 - 0.02686)(1 - 0.00021)(1 - 0.00045) \\ &= 1 - (0.97314 \cdot 0.99979 \cdot 0.99955) \\ &= 1 - 0.97249 = 0.02751 \end{aligned}$$

Thus, the overall probability of the top event increases slightly to approximately 2.75% when accounting for the common cause failure.

B

Appendix B

B.1. Expert briefing document

Expert Elicitation: Assessing Incompleteness in RA Analysis for the Maeslantbarrier

Structured Delphi method

Waasdorp, W.J. (Wouter)

Delft university of technology and TNO

Introduction

The Maeslantbarrier is a critical component of the Dutch flood defense system. Located near the mouth of the Rotterdam Harbor, it is a movable storm surge barrier designed to protect over two million people and vital economic infrastructure in South Holland from extreme storm surges. It is a key part of the broader Delta Works system and plays a dual role: maintaining open access to one of the world's busiest ports during normal conditions and providing full closure protection during severe storms.

To ensure this essential infrastructure functions as intended, a Reliability and Availability (RA) analysis is conducted. This RA analysis assesses the likelihood that the barrier will perform its intended function, namely, closing successfully when required. It supports long-term asset management, regulatory compliance, and maintenance planning by identifying critical failure paths and estimating non-closure probabilities.

Despite, or perhaps due to, the high level of detail in the current RA framework, there remains a risk of incompleteness, particularly in the identification and quantification of all potential failure modes. **The objective of this expert session is to explore this residual uncertainty. We aim to identify events that may have been overlooked or insufficiently represented in the existing RA model for the non-closure probability, and quantify their contribution to the overall non-closure probability.**

Objectives

The primary objectives of this expert session are as follows:

- Identify potential events that may currently be missing from, or underrepresented in, the existing Reliability and Availability (RA) analysis of the Maeslantbarrier.
- Estimate the likelihood and potential impact of these events on the barrier's non-closure probability, based on expert insight and experience.
- Translate expert judgments into quantitative probability distributions that can be incorporated into a probabilistic framework for further analysis.

Procedure

The expert session will follow a structured, three-step process:

- **Step 1: Individual Event Identification**
  Each expert will independently identify between 3 and 10 potential events that contribute most to the probability of failure per request (request of closing of the Maeslantbarrier)**.** For each event, experts are asked to provide a brief description and a preliminary estimate of the event's potential influence on the barrier's non-closure probability.
- **Step 2: Consolidation of Events**
  All individual submissions will be compiled into a single anonymized list. This consolidated list will ensure that duplicate or similar events are grouped, while preserving the diversity of expert perspectives.
- **Step 3: Probability Estimation**
  Experts will then be asked to individually provide probability estimates for each event in the consolidated list. These estimates will be used to construct aggregated probability distributions for each event, which can be integrated into a probabilistic model for further analysis.

Instructions to Experts

Please follow the steps below when preparing your input:

1. **Work independently**
   Identify potential events on your own without consulting other experts during this stage. This ensures the integrity and independence of the individual judgments.
2. **Describe each event clearly**
   For each identified event, provide a brief but clear description. Include a short explanation of why you believe this event is relevant or potentially underestimated in the current RA analysis. If no event comes to mind try to think of the question: "If the Maeslant barrier fails to close when needed, what are the ten most likely causes and what are their probabilities?"
3. **Estimate its impact**
   For each event, provide an initial estimate, expressed as a percentage (%), of how much you believe it could realistically increase the probability of the Maeslantbarrier failing to close when required. This can be a rough, order-of-magnitude estimate based on your experience.
4. **Submit your responses by [insert deadline]**
   Please return your completed input by **10-06-2025**, so that we can proceed with compiling and analyzing the results.

Example

To guide your input, here is a simple illustrative example of what is expected:

Rank	Event	Brief explanation	Percentage lower bound (5%)	Percentage Medium	Percentage upper bound (95%)
1	Maintenance scheduling error	Maintenance delayed beyond recommended timelines.	~0.2%	~0.5%	~0.75%

This table format can be used as a reference for your own event descriptions and estimates.

For the 5% lower and 95% upper bounds, consider the numbers you cannot imagine the probability being lower or higher than.

For the order of magnitude percentage estimate think of: 1, 1/2 , 1/5, 1/10, 1/20, 1/50, 1/100 etc.

Submission instructions

Please complete the Excel file titled *Expert_Elicitation_(NAME)_(DATE).xlsx*, which has been provided separately. This file is designed to collect your input on potentially overlooked or underestimated events related to the non-closure probability of the Maeslantbarrier. Once completed, kindly email the file to: **wouter.waasdorp@tno.nl**
Deadline for submission: *10-06-2025*.
If you have any questions or require clarification, feel free to reach out in advance.

B.2. Excell round 1

Rank	Event	Brief explanation	Estimated probability lower bound (5%)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11	Other unidentifyable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable	

Estimated probability medium	Estimated probability upper bound (95%)

B.3. Excell round 2

Rank	Event	Brief explanation	Estimated probability lower bound (5%)
1			1
2			1
3			1
4			1
5			1
6			1
7			1
8			1
9			1
10			1
11	Other unidentifyable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable	

Estimated probability medium	Estimated probability upper bound (95%)
5	10
5	10
5	10
5	10
5	10
5	10
5	10
5	10
5	10
5	10

Your estimated probability lower bound (5%)	Your estimated probability median

Your estimated probability higher bound (95%)

C

Appendix C

C.1. Long-list

List of potentially overlooked events in the current failure to close probability calculation of the Maeslant barrier

The list is set up in a structured way according to the methodology. The events not taken into account in the current failure-to-close analysis of the Maeslant barrier can be divided into two groups: those that occur within the preconditions and those that occur outside the preconditions. The events that exist within the preconditions are split up into 4 categories, namely: Failure Modes and Effects Analysis (FMEA), Hazard and Operability Analysis (HAZOP), External Event Screening, and a What-If Analysis. These are the methods used to list events in a structural manner, and make the list more complete. For the set of events outside the preconditions, no structured methods were used.

Inside preconditions

FMEA

1.1 **Seiche sea-side**: During the lowering of the barrier a seiche at the sea-side is created. In the calculation, it only seemed possible at higher decays than observed. Knowledge about this is missing, possibly hindering the operation.

1.2 **Incorrect landing**: The gates are lowered to the threshold (drempel) in the wrong way. The control system is not suitable for storm and water current conditions. 20 lowering types are programmed, meaning that the operating system chooses the wrong lowering type for the closing situation.

1.3 **Trouble with control system (BESW)**: After the renewal of the control system, the control system is not working as desired (specifics are classified, and I got denied the information). The added failure probability has not been verified.

1.4 **Wrong buoyancy above threshold (Too heavy)**: The gates are balanced too heavily on the threshold, after which it cannot be raised quickly enough in the event of rising waters on the inland side.

1.5 **Wrong buoyancy above threshold (Too light)**: the gates are balanced too lightly above the threshold, causing too much water to flow into the system.

HAZOP

1.6 **Maintenance done wrong**:. The introduction of wrong fuel, misplacement of electrical components, or other human maintenance errors could cause unforeseen problems. If this is implemented in too much detail the chances of missing certain events can get bigger.

1.7 **Prediction/data weather station is wrong**: Causing an incorrect chain of decisions or lack of it.

1.8 **Incorrect choice of closing type:** Due to the incorrect closing type decision within the circumstances, unexpected water levels in the river or the sea, the barrier is unable to close. This is due to the changing nature of the system for which the barrier and the BOSS is designed(Like at the Rampspol barrier where the system is behaving very differently than what it was designed for) (kenteringsluiting/peilsluiting).

1.9 **Disobedience of ship/Harbor**: Due to the economic interest of the harbor or a ship, there is disobedience causing delays in the process of closing. This has been observed during functionality closures.

External events

1.10 **Temporal compound events**: These should be taken into account due to climate change (Bakker et al. 2025). Climate change increases the chance of closing operations of the Maeslant barrier in short periods of time, which leaves less room for maintenance needed due to the previous closing.
1.11 **Long periods of drought**: These can, for example, lead to subsidence or too low water levels.
1.12 **High wind speeds**: These can cause damage to structures or materials, and delay/hinder corrective actions.
1.13 **Hailstorm**: causing physical damage, as predicted by TNO (Botzen et al. 2010).
1.14 **Heavy rain**: causing leakage, flooding, or water ingress.
1.15 **High ambient temperatures**: affecting operations or equipment.
1.16 **Earthquakes**: or tremors causing structural damage.
1.17 **Snow accumulation:** causing overloading or roof collapse.
1.18 **Extreme cold**: affecting materials and equipment, including freezing of components.
1.19 **Flooding:** originating from outside the object or occurring within the object due to system failure.
1.20 **Elevated water levels**: due to tide, storms, or astronomical phenomena that have not been taken into account in the design.
1.21 **Prolonged water presence:** causing material degradation, on the inside and the outside of the structure.
1.22 **Oscillating waves**: in enclosed or semi-enclosed water bodies.
1.23 **Large waves**: caused by underwater disturbances.
1.24 **Large-scale movement of soil**: impacting structures.
1.25 **Sudden failure of underground spaces:** related to point 1.24
1.26 **Loss of coastal land:** affecting nearby infrastructure.
1.27 **Fire originating near the object**: such as nearby building fires.
1.28 **Fire starting within the object:** due to technical faults.
1.29 **Impact by external objects**: such as ships-, vehicles- or shipping container accidents.
1.30 **External release of hazardous materials:** affecting the object.
1.31 **Internal release of hazardous substances.**
1.32 **Explosion nearby:** impacting the object.
1.33 **Explosion**: within the object.
1.34 **Meteor or satellite fragment impact.**
1.35 **Crash of aircraft:** on or near the object.
1.36 **Parts of turbines**: detaching and impacting surroundings.
1.37 **Infestation:** by pests, fungi, or bacteria.
1.38 **Damage to cables and pipes**: due to digging work.
1.39 **Waste or debris**: impacting infrastructure or operations.
1.40 **Power outage**: affecting systems and operations.
1.41 **Shift in sea-current**: giving consequences that are unknown.

What if analysis

1.42 **Increased closing due to SLR (sea level rise)**: From Non-linear extreme value analysis, it is derivable that the closing due to storm frequency of the Maeslant barrier is going to increase compared to stationary sea levels. Water levels might change or might differ from current design sea levels.

1.43 **Outdated understanding of climate change/ the lack of implantation of new knowledge**: Our understanding of climate change has increased drastically. Therefore, there is the possibility that the design is not ready for the number of closings in the near future.

1.44 **Pandemic**: A pandemic could cause a shortage of manpower to operate the barrier. (This is a reality for a lot of barriers, even until now)

1.45 **Ship blocking**: Unforeseen circumstances could cause a ship to strand in the middle of the barrier (as happened with the Evergreen in the Suez Canal).

1.46 **Political hinder**: A different to now political view could lead to disbelieve in the experts at Rijkswaterstaat, increasing difficulty in the structural maintenance.

1.47 **Generational knowledge loss**: The engineers that worked on the Maeslant barrier when it was built are not in operation anymore. This, together with the scattered documentation on the Maeslant barrier, could lead to a knowledge loss with unknown consequences.

1.48 **Missed common cause of redundant systems**: For example, north power supply not independent of south power supply.

1.49 **Incompleteness of RA analysis**: cases like non redundant energy supply and gravitational pull of Greenland icesheets give rise to the question: What assumptions taken in the analysis could, as well, be incorrect?

Outside preconditions

2.1 **Too much detail:** Due to the high level of detail and the unverifiability of the RA analysis, the RA analysis is prone to mistakes, big or small.

2.2 **Precondition of on-time maintenance is not met**: Due to problems in society or the closing of maintenance window.

2.3 **Current analysis done without structure:** Raising the chances of missing events.

2.4 **lessons learned:** after close to 30 years of operation are not implemented in the analysis, causing the structure to still be in the ‘teething problem/infant mortality’ phase.

2.5 Precondition of preventive replacement is not met.

2.6 **Differently used parts:** Parts used for the structure are used differently than what they are made for. An example is that the pumps are designed to be wet all the time, yet they are only used once a month.

2.7 **Wrong assumption of independence in weather phenomena:** The failure to close probability is not independent of the weather conditions as assumed (wrong assumption, goes hand in hand with point 1.49)

2.8 **Precondition of stationarity (bathtub curve) is not met:** Due to the precondition of optimal performance according to the bathtub curve, where there is a constant failure rate, the RA analysis is considered stationary. If this precondition is not met, non-stationarity could play a role in the reliability and availability of the barrier.

2.9 **Human Action Database (HAD) not verified:** no clear evidence of verification was found in the portion of data available for this study. Specifically, there was no detailed information on whether training guidelines or standards for human intervention are in place or being followed. Additionally, the dataset offered little insight into how operational teams are structured or how the necessary skills are established and maintained to support critical operations.

D

Appendix D

D.1. Combined Table of input from SEJ 1st round

Table D.1: Combined Table of input from SEJ 1st round

Rank	Failure Mode	Description	Low	Medium	High
1	Decision making	The wrong decision is made by the operators while in operation	5%	10%	15%
1	Working in storm season leads to wrong decision	It can be too much for people to oversee	1%	5.50%	10%
1	Human error probability	Do the people have the right background, education, and training? ... Knowledge strategy is failing	1%	5.50%	10%
1	Forecasts for Rotterdam/Dordrecht incorrect due to human error	BOS incorrectly selects closure timing due to software error and complex water level pattern. Seiche or pipe surge influences the decision.	1%	5.50%	10%
1	Sensor/Data Fault Undetected	Sensor data leads to incorrect decisions; may go undetected if redundancy/diagnostics are insufficient.	0.20%	1%	5%
2	Structural integrity	The effects of losing sand is unknown	5%	10%	15%
2	Sinking of the floating sector gate	Failures during test storms can damage the barrier permanently in rare cases. Estimated storm frequency: 10^{-2}/year.	0.00000001%	0.0001%	0.001%
2	Dormant phenomena	Condition of retaining structures, condition of drainage, condition of cofferdam, condition of HWK, damaged anchor rods corrosion, Wear on Hempaquick hinge Hinge control is failure-prone, groundwater behavior may be abnormal	1%	5.5%	10%
2	Obstacles on the threshold are (wrongly) not being inspected.	-	1%	5%	10%
2	Stalling of dock door	In stormy weather, the catch can end up on the wrong side of the rail. Limit switches not triggered due to excessive load during opening caused by heavy waves and drop control system failure due to	1%	5.5%	10%

Rank	Failure Mode	Description	Low	Medium	High
2	Configuration parameters not updated/designed	Can lead to undesirable and unexpected behavior think of sinking matrices, fenders, and trim correction	1%	5.5%	10%
2	Tolerances	Deformation of the KW may be underestimated, truss arms bouncing on the sill	1%	5.5%	10%
2	The system is reaching its limits	Very high flows will only be partially held back by the barrier during certain storms, the barrier will not fully submerge. Multiple failing valves also limit its use	1%	5.5%	10%
2	Natural boundary conditions	Sea level rise of more than 25 cm Correlation between wind setup and discharge at Lobith greater than expected Longer storm durations seiches, new insights into, for example, probability distributions or suction forces. This can have both positive and negative effects stiffness of the retaining wall is sometimes quite low	1%	5.5%	10%
2	Redundancy	Locomobile and “Pennebaan” single point of failure	1%	5.5%	10%
2	Structural failure	There is sometimes leeway here because a conservative approach is taken when estimating mechanisms. Better to be a bit safer than on the edge. Better to allow some margin than to calculate endlessly. Structurally, the barrier consists of parallel and series systems. Assumptions have been made for this. Verifying these is worthwhile.	1%	5.5%	10%
2	Departure fails due to	Truss arms and sill make contact due to contact between consoles and seats Resonance of water in the dock entanglement of cables from shore to locomotive	1%	5.5%	10%
2	Submerging fails due to	Incorrect matrix causing valves not to open incorrect matrix causing the barrier to submerge too unevenly or too quickly brief outlier in inclinometers Unjustified or incorrect human intervention Too much sediment on the bottom	1%	5.5%	10%
2	Floating fails due to	Unjustified or incorrect human intervention pre-tension not reduced in time due to pre-tension reduced asymmetrically due to retaining wall floats up too unevenly due to	1%	5.5%	10%

Rank	Failure Mode	Description	Low	Medium	High
2	Readiness for second peak fails due to	Docking (tolerances), closing dock gate, to rest position	1%	5.5%	10%
3	Invalid failure characterization due to data gaps	Failures are modeled using assumed or outdated data; field behavior (e.g., wear-out) diverges from model assumptions	0.5%	2%	6%
3	Model error due to incomplete data	Failure behavior of components is incorrectly modeled due to unavailability of detailed degradation or diagnostic data.	0.3%	1.5%	4%
3	Incomplete risk-based inspection implementation	RBI principles not fully embedded; inspection frequency or method not adjusted to risk profile, leading to insufficient PF interval knowledge.	0.2%	1%	3%
3	Lack of insight into ageing effects	Long-term degradation mechanisms (e.g., fatigue, corrosion under insulation, seal aging) not well understood or incorporated into performance modeling.	0.3%	1%	4%
3	Ignoring stronger evidence than the RA analysis.	The RA analysis seems to have a more important role in decision-making than real evidence (damages, test results, etc). Given the weaknesses of RA analysis (based on not-representative data), this likely results in decision errors (P=1). Whether decision errors result in a flood is not that likely (P=10-5). Very uncertain about this risk.	$1E^{-}9\%$	0.001%	1%
3	Preconditions of RA analysis not met	Assumptions from the RA (Risk Assessment) are not being followed Probo not properly executed Spare parts are a bit of an issue	1%	5.5%	10%
3	99 points	Represents all findings related to the closures. Some have been resolved, some have not and/or seem to be floating (unresolved) The question is whether analysis capacity within RWS is sufficient	1%	5.5%	10%
3	Lessons learned forgotten	For example, BesW Many problems were encountered with synchronization, timing, and communication. These aspects are often underestimated in the sector. The risk is that these are not properly accounted for in design and testing.	1%	5.5%	10%

Rank	Failure Mode	Description	Low	Medium	High
3	Calculation methods	Model accuracy not included in the calculations, Affects MHW (Mean High Water) and flood probabilities and risks Cutsets are truncated at 3 levels, which may lead to underestimation This was corrected for Hartel Forecast inaccuracy for Rotterdam is increasing	1%	5.5%	10%
3	Failure probability analysis	Example: Influence of temperature on failure rate not included Failure data is outdated Failure-predictive indicators are no longer being analyzed, which means impending failures go unnoticed	1%	5.5%	10%
4	Storm conditions	it's unknown how the MK functions in a normative storm	15%	20%	25%
4	Underestimated phenomena	Mystery force: Integral calculation has never been finished	1%	5.5%	10%
5	Incorrect Maintenance Execution	Errors or shortcuts in maintenance activities introduce or leave latent faults that impair future performance. errors made during maintenance that were not discovered during testing	0.1%	7.55%	15%
5	Unavailability due to maintenance	Parts of the barrier are unavailable during "not-storm season" Every 25 years an important item of for instance the locomobile not on site (1/25), probability of storm being in the summer (1/100)	0.0004%	0.04%	0.4%
5	Maintenance season too short	Too little time to restore the barrier, or job done improperly (/under stress), resulting in a higher failure probability. Because there is no report on the HAT I do not know the current estimate on this. Current probability of a failure to close (1/100) x percentage hardware failure (50%) / conservatism (factor 10) x maintenance error percentage (50%) x factor for more stress (2)	$1E^{-}4\%$	0.02%	0.1%
-	Other unidentifiable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable. Happened in the past as well where "new" phenomona's have been identified. How do we know we have everything?	5%	10%	15%

D.2. Tables of input from SEJ 2nd round

Table D.2: Table of input from SEJ 2nd round 1st respondent

Rank	Failure Mode	Description	Remark	Low	Medium	High
1	Decision making	The wrong decision is made by the operators while in operation	-	0.1%	1%	10%
1	Working in storm season leads to wrong decision	It can be too much for people to oversee	Als je overweegt om in het stormseizoen risicovol werk uit te gaan voeren dan neem je een risico: werk niet op tijd klaar of storm komt onverwacht of is hoger dan verwacht of geen tijd meer om iets te herstellen (voorbeeld: black-out test: risico op schade is best groot: niet doen dan zou je zeggen). Om juiste besluiten te nemen heb je een hoop kennis nodig. Meer gebruik maken van event-trees. Maar: misschien heeft RWS hier al een systeem voor.	1%	5%	20%
1	Human error probability	Do the people have the right background, education, and training? ... Knowledge strategy is failing	Mensen kunnen fouten maken bij onderhoud. De zijn latente fouten hierbij zijn het meest vervelend (vorm van onmerkbaar falen). Daarnaast is de mens hard nodig om herstelacties uit te voeren.	5%	10%	20%
1	Forecasts for Rotterdam/Dordrecht incorrect due to human error	BOS incorrectly selects closure timing due to software error and complex water level pattern. Seiche or pipe surge influences the decision.	-	0.5%	1%	10%

Rank	Failure Mode	Description	Remark	Low	Medium	High
1	Sensor/Data Fault Undetected	Sensor data leads to incorrect decisions; may go undetected if redundancy/diagnostics are insufficient.	-	1%	10%	20%
2	Structural integrity	The effects of losing sand is unknown	-	5%	10%	15%
2	Sinking of the floating sector gate	Failures during test storms can damage the barrier permanently in rare cases. Estimated storm frequency: 10^{-2}/year.	"Dit is een lastige. We hebben al een aantal keren "geluk" gehad. Er zijn echter nog geen gebeurtenissen opgetreden die direct tot niet-beschikbaarheid hebben geleid. Kans op in slaap sussen is best groot. Zonder kering wordt de maatgevend hoogwaterstand (MHW) ongveer eens per100 jaar overschreden"	5%	25%	50%
2	Dormant phenomena	Condition of retaining structures, condition of drainage, condition of cofferdam, condition of HWK, damaged anchor rods corrosion, Wear on Hempaquick hinge Hinge control is failure-prone, groundwater behavior may be abnormal	-	1%	10%	15%
2	Obstacles on the threshold are (wrongly) not being inspected.	-	Het gaat om obstakels op de drempel (=sill) die onder het sediment liggen. We houden rekening met 2 meter sediment lokaal op de drempel	1%	10%	15%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Stalling of dock door	In stormy weather, the catch can end up on the wrong side of the rail. Limit switches not triggered due to excessive load during opening caused by heavy waves and drop control system failure due to	De openmelding wordt gemaakt m.b.v. 3 magneetschakelaars. Deze schakelaars zitten op de dokdeur. Als ze een “stoel op de kesp” passeren wordt het signaal gemaakt. De afstand tussen schakelaar en stoel mag niet te groot worden want dan werkt het niet meer. De bovenkant van de stoel kan op en neer en bhoort in de hoogste positie te worden vastgezet. Dat is weleens mis gegaan	1%	10%	15%
2	Configuration parameters not updated/designed	Can lead to undesirable and unexpected behavior think of sinking matrices, fenders, and trim correction	-	1%	5%	30%
2	Tolerances	Deformation of the KW may be underestimated, truss arms bouncing on the sill	Afgelopen jaren is een FEM model ontwikkeld waarmee de vervormingen kunnen worden berekend. In theorie kun je dan ook de ruimte (tolerantie) berekenen tussen vakwekarmen en de kesp. Hoever dit model is en of er al mee gerekend is weet ik niet	1%	10%	30%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	The system is reaching its limits	Very high flows will only be partially held back by the barrier during certain storms, the barrier will not fully submerge. Multiple failing valves also limit its use	In de risicoanalyse is rekening gehouden met faalmechanismen die tot een mindere prestatie lijden. De kans op zo'n mechanisme en de bijbehorende prestatie kun je met elkaar vermenigvuldigen (simpel gezegd). Een slechte prestatie met een kleine kans kan even goed zijn als een grote prestatie met een grote kans	0%	1%	10%
2	Natural boundary conditions	Sea level rise of more than 25 cm Correlation between wind setup and discharge at Lobith greater than expected Longer storm durations seiches, new insights into, for example, probability distributions or suction forces. This can have both positive and negative effects stiffness of the retaining wall is sometimes quite low	-	1%	10%	30%
2	Redundancy	Locomobile and "Pennebaan" single point of failure	-	0.1%	1%	5%
2	Structural failure	There is sometimes leeway here because a conservative approach is taken when estimating mechanisms. Better to be a bit safer than on the edge. Better to allow some margin than to calculate endlessly. Structurally, the barrier consists of parallel and series systems. Assumptions have been made for this. Verifying these is worthwhile.	-	0.02%	0.1%	1%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Departure fails due to	Truss arms and sill make contact due to contact between consoles and seats Resonance of water in the dock entanglement of cables from shore to locomotive	-	0.1%	1%	5%
2	Submerging fails due to	Incorrect matrix causing valves not to open incorrect matrix causing the barrier to submerge too unevenly or too quickly brief outlier in inclinometers Unjustified or incorrect human intervention Too much sediment on the bottom	-	0.1%	5%	10%
2	Floating fails due to	Unjustified or incorrect human intervention pre-tension not reduced in time due to pre-tension reduced asymmetrically due to retaining wall floats up too unevenly due to	-	1%	5%	10%
2	Readiness for second peak fails due to	Docking (tolerances), closing dock gate, to rest position	-	0.1%	1%	2%
3	Invalid failure characterization due to data gaps	Failures are modeled using assumed or outdated data; field behavior (e.g., wear-out) diverges from model assumptions	Ik zou willen pleiten voor een “landelijk” programma waarbij je faaldata gaat updaten a.d.h.v. de praktijk. RWS heeft heel veel objecten, dus heel veel data. Idem aandacht voor de storingsvoorspellende grootheden. Hiermee kun je faalgedrag en faalmoment voorspellen. Zie ook volgende punt	1%	10%	20%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Model error due to incomplete data	Failure behavior of components is incorrectly modeled due to unavailability of detailed degradation or diagnostic data.	-	1%	10%	20%
3	Incomplete risk-based inspection implementation	RBI principles not fully embedded; inspection frequency or method not adjusted to risk profile, leading to insufficient PF interval knowledge.	-	1%	5%	10%
3	Lack of insight into ageing effects	Long-term degradation mechanisms (e.g., fatigue, corrosion under insulation, seal aging) not well understood or incorporated into performance modeling.	-	5%	20%	40%
3	Ignoring stronger evidence than the RA analysis.	The RA analysis seems to have a more important role in decision-making than real evidence (damages, test results, etc). Given the weaknesses of RA analysis (based on not-representative data), this likely results in decision errors (P=1). Whether decision errors result in a flood is not that likely (P=10-5). Very uncertain about this risk.	Ra analyse zou je moeten toetsen aan wat je in de praktijk waarneemt, je moet kijken naar de kans op falen gegeven een sluitvraag. Als je echt een grote kans op menselijke beslisfouten hebt dan zal dit getal stuk groter moeten zijn	5%	10%	20%
3	Preconditions of RA analysis not met	Assumptions from the RA (Risk Assessment) are not being followed Probo not properly executed Spare parts are a bit of an issue	-	10%	15%	30%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	99 points	Represents all findings related to the closures. Some have been resolved, some have not and/or seem to be floating (unresolved) The question is whether analysis capacity within RWS is sufficient	-	10%	20%	40%
3	Lessons learned forgotten	For example, BesW Many problems were encountered with synchronization, timing, and communication. These aspects are often underestimated in the sector. The risk is that these are not properly accounted for in design and testing.	-	10%	20%	40%
3	Calculation methods	Model accuracy not included in the calculations, Affects MHW (Mean High Water) and flood probabilities and risks Cutsets are truncated at 3 levels, which may lead to underestimation This was corrected for Hartel Forecast inaccuracy for Rotterdam is increasing	Het is niet gezegd dat deze groter wordt, maar ALS deze groter wordt is dat een vervelende waar je iets mee moet	5%	10%	40%
3	Failure probability analysis	Example: Influence of temperature on failure rate not included Failure data is outdated Failure-predictive indicators are no longer being analyzed, which means impending failures go unnoticed	-	5%	10%	20%
4	Storm conditions	it's unknown how the MK functions in a normative storm	-	15%	20%	25%

Rank	Failure Mode	Description	Remark	Low	Medium	High
4	Underestimated phenomena	Mystery force: Integral calculation has never been finished	Onder bescheiden condities lijkt het mee te vallen. De combinatie met golven en wind is nog niet uitvoerig onderzocht	1%	10%	20%
5	Incorrect Maintenance Execution	Errors or shortcuts in maintenance activities introduce or leave latent faults that impair future performance. errors made during maintenance that were not discovered during testing	-	5%	20%	40%
5	Unavailability due to maintenance	Parts of the barrier are unavailable during “not-storm season” Every 25 years an important item of for instance the locomobile not on site (1/25), probability of storm being in the summer (1/100)	Kan, er is een eis opgenomen; zomerseizoen, kans op niet beschikbaarheid niet meer dan eens per 10 jaar. Omgerekend eens per 10 jaar mar de kering 3 maanden niet beschikbaar zijn in de zomermaanden. (nalezen in contract BD-001)	0.1%	1%	5%
5	Maintenance season too short	Too little time to restore the barrier, or job done improperly (/under stress), resulting in a higher failure probability. Because there is no report on the HAT I do not know the current estimate on this. Current probability of a failure to close (1/100) x percentage hardware failure (50%) / conservatism (factor 10) x maintenance error percentage (50%) x factor for more stress (2)	-	1%	5%	10%

Rank	Failure Mode	Description	Remark	Low	Medium	High
-	Other unidentifiable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable. Happened in the past as well where “new” phenomona’s have been identified. How do we know we have everything?	1%	5%	10%	

Table D.3: Table of input from SEJ 2nd round 2nd respondent

Rank	Failure Mode	Description	Remark	Low	Medium	High
1	Decision making	The wrong decision is made by the operators while in operation	-	1%	3%	10%
1	Working in storm season leads to wrong decision	It can be too much for people to oversee	-	0.2%	1%	5%
1	Human error probability	Do the people have the right background, education, and training? ... Knowledge strategy is failing	-	2%	5%	10%
1	Forecasts for Rotterdam/Dordrecht incorrect due to human error	BOS incorrectly selects closure timing due to software error and complex water level pattern. Seiche or pipe surge influences the decision.	-	0.2%	1%	5%
1	Sensor/Data Fault Undetected	Sensor data leads to incorrect decisions; may go undetected if redundancy/diagnostics are insufficient.	-	0.2%	1%	5%
2	Structural integrity	The effects of losing sand is unknown	-	2%	5%	10%
2	Sinking of the floating sector gate	Failures during test storms can damage the barrier permanently in rare cases. Estimated storm frequency: 10^{-2}/year.	-	0.01%	0.2%	2%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Dormant phenomena	Condition of retaining structures, condition of drainage, condition of cofferdam, condition of HWK, damaged anchor rods corrosion, Wear on Hempaquick hinge Hinge control is failure-prone, groundwater behavior may be abnormal	-	0.5%	2%	6%
2	Obstacles on the threshold are (wrongly) not being inspected.	-	-	1%	2%	5%
2	Stalling of dock door	In stormy weather, the catch can end up on the wrong side of the rail. Limit switches not triggered due to excessive load during opening caused by heavy waves and drop control system failure due to	-	1%	2%	5%
2	Configuration parameters not updated/designed	Can lead to undesirable and unexpected behavior think of sinking matrices, fenders, and trim correction	-	2%	6%	10%
2	Tolerances	Deformation of the KW may be underestimated, truss arms bouncing on the sill	-	0.1%	0.5%	2%
2	The system is reaching its limits	Very high flows will only be partially held back by the barrier during certain storms, the barrier will not fully submerge. Multiple failing valves also limit its use	-	0.3%	1.5%	4%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Natural boundary conditions	Sea level rise of more than 25 cm Correlation between wind setup and discharge at Lobith greater than expected Longer storm durations seiches, new insights into, for example, probability distributions or suction forces. This can have both positive and negative effects stiffness of the retaining wall is sometimes quite low	-	0.2%	1%	3%
2	Redundancy	Locomobile and “Pennebaan” single point of failure	-	1%	2%	5%
2	Structural failure	There is sometimes leeway here because a conservative approach is taken when estimating mechanisms. Better to be a bit safer than on the edge. Better to allow some margin than to calculate endlessly. Structurally, the barrier consists of parallel and series systems. Assumptions have been made for this. Verifying these is worthwhile.	-	0.01%	1%	2%
2	Departure fails due to	Truss arms and sill make contact due to contact between consoles and seats Resonance of water in the dock entanglement of cables from shore to locomotive	-	0.1%	1%	5%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Submerging fails due to	Incorrect matrix causing valves not to open incorrect matrix causing the barrier to submerge too unevenly or too quickly brief outlier in inclinometers Unjustified or incorrect human intervention Too much sediment on the bottom	-	0.5%	2%	3%
2	Floating fails due to	Unjustified or incorrect human intervention pre-tension not reduced in time due to pre-tension reduced asymmetrically due to retaining wall floats up too unevenly due to	-	0.5%	2%	6%
2	Readiness for second peak fails due to	Docking (tolerances), closing dock gate, to rest position	-	0.5%	2%	6%
3	Invalid failure characterization due to data gaps	Failures are modeled using assumed or outdated data; field behavior (e.g., wear-out) diverges from model assumptions	-	0.5%	2%	6%
3	Model error due to incomplete data	Failure behavior of components is incorrectly modeled due to unavailability of detailed degradation or diagnostic data.	-	0.3%	1.5%	4%
3	Incomplete risk-based inspection implementation	RBI principles not fully embedded; inspection frequency or method not adjusted to risk profile, leading to insufficient PF interval knowledge.	-	0.2%	1%	3%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Lack of insight into ageing effects	Long-term degradation mechanisms (e.g., fatigue, corrosion under insulation, seal aging) not well understood or incorporated into performance modeling.	-	0.3%	1%	4%
3	Ignoring stronger evidence than the RA analysis.	The RA analysis seems to have a more important role in decision-making than real evidence (damages, test results, etc). Given the weaknesses of RA analysis (based on not-representative data), this likely results in decision errors (P=1). Whether decision errors result in a flood is not that likely (P=10-5). Very uncertain about this risk.	-	0.001%	0.01%	1%
3	Preconditions of RA analysis not met	Assumptions from the RA (Risk Assessment) are not being followed Probo not properly executed Spare parts are a bit of an issue	-	1%	4%	10%
3	99 points	Represents all findings related to the closures. Some have been resolved, some have not and/or seem to be floating (unresolved) The question is whether analysis capacity within RWS is sufficient	-	?%	?%	?%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Lessons learned forgotten	For example, BesW Many problems were encountered with synchronization, timing, and communication. These aspects are often underestimated in the sector. The risk is that these are not properly accounted for in design and testing.	-	?%	?%	?%
3	Calculation methods	Model accuracy not included in the calculations, Affects MHW (Mean High Water) and flood probabilities and risks Cutsets are truncated at 3 levels, which may lead to underestimation This was corrected for Hartel Forecast inaccuracy for Rotterdam is increasing	-	0.2%	1%	5%
3	Failure probability analysis	Example: Influence of temperature on failure rate not included Failure data is outdated Failure-predictive indicators are no longer being analyzed, which means impending failures go unnoticed	-	0.3%	1%	4%
4	Storm conditions	it's unknown how the MK functions in a normative storm	-	?%	?%	?%
4	Underestimated phenomena	Mystery force: Integral calculation has never been finished	-	?%	?%	?%

Rank	Failure Mode	Description	Remark	Low	Medium	High
5	Incorrect Maintenance Execution	Errors or shortcuts in maintenance activities introduce or leave latent faults that impair future performance. errors made during maintenance that were not discovered during testing	-	0.1%	0.3%	1.5%
5	Unavailability due to maintenance	Parts of the barrier are unavailable during "not-storm season" Every 25 years an important item of for instance the locomobile not on site (1/25), probability of storm being in the summer (1/100)	-	0.04%	0.04%	0.04%
5	Maintenance season too short	Too little time to restore the barrier, or job done improperly (/under stress), resulting in a higher failure probability. Because there is no report on the HAT I do not know the current estimate on this. Current probability of a failure to close (1/100) x percentage hardware failure (50%) / conservatism (factor 10) x maintenance error percentage (50%) x factor for more stress (2)	-	2%	5%	7%
-	Other unidentifiable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable. Happened in the past as well where "new" phenomona's have been identified. How do we know we have everything?	-	0.3%	1%	4%

Table D.4: Table of input from SEJ 2nd round 3rd respondent

Rank	Failure Mode	Description	Remark	Low	Medium	High
1	Decision making	The wrong decision is made by the operators while in operation	Although I think wrong decisions in the operation are likely, I don't think this is very likely to result in a coastal flood. Rather, my estimate is that the current analysis is conservative regarding closure decisions. Based on an old analysis, I expect the current contribution to be approximately 5%, my estimate is that this is almost neglegible, thus: -5% of the current estimate of approx. 1/100 per request.	-10%	-5%	0%
1	Working in storm season leads to wrong decision	It can be too much for people to oversee	I have some difficulties with the event description, what is wrong? I expect that the undesired event is something like: maintenance is executed while a storm is approaching, which can either be in summer or winter. My estimate for unavailability due to maintenance in summer was 4% of 1/100. To include winter I increase this with 1%.	0.05%	5%	40%
1	Human error probability	Do the people have the right background, education, and training? ... Knowledge strategy is failing	People having the "right" background, education and training is relevant for both operation and maintenance. Previously I estimated 2% for maintenance problems due to stress. This seems to have a higher impact (x2)	0.04%	4%	20%

Rank	Failure Mode	Description	Remark	Low	Medium	High
1	Forecasts for Rotterdam/Dordrecht incorrect due to human error	BOS incorrectly selects closure timing due to software error and complex water level pattern. Seiche or pipe surge influences the decision.	-	1%	5.5%	10%
1	Sensor/Data Fault Undetected	Sensor data leads to incorrect decisions; may go undetected if redundancy/diagnostics are insufficient.	-	0.2%	1%	5%
2	Structural integrity	The effects of losing sand is unknown	I have too little information to judge this risk	?%	?%	?%
2	Sinking of the floating sector gate	Failures during test storms can damage the barrier permanently in rare cases. Estimated storm frequency: 10^{-2}/year.	-	0.00000001%	0.0001%	0.001%
2	Dormant phenomena	Condition of retaining structures, condition of drainage, condition of cofferdam, condition of HWK, damaged anchor rods corrosion, Wear on Hempaquick hinge Hinge control is failure-prone, groundwater behavior may be abnormal	-	?%	?%	?%
2	Obstacles on the threshold are (wrongly) not being inspected.	-	Leidraad Kunstwerken: 10-2 per request. I estimate that this is a factor 100 smaller for the Maeslant barrier due to its “vacuum” function (floating above sediment) and its size	0.01%	1%	5%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Stalling of dock door	In stormy weather, the catch can end up on the wrong side of the rail. Limit switches not triggered due to excessive load during opening caused by heavy waves and drop control system failure due to	I estimate that the dock door can likely be removed in case of emergency. I expect the current estimate to be conservative here. I assume 10% of the current estimate to be due to failures of the dock door.	-10%	-10%	0%
2	Configuration parameters not updated/designed	Can lead to undesirable and unexpected behavior think of sinking matrices, fenders, and trim correction	-	1%	5.5%	10%
2	Tolerances	Deformation of the KW may be underestimated, truss arms bouncing on the sill	I recognize the importance of this, and addressing this could improve maintenance. However, I think this is very unlikely to result in a coastal flood	0%	0.01%	1%
2	The system is reaching its limits	Very high flows will only be partially held back by the barrier during certain storms, the barrier will not fully submerge. Multiple failing valves also limit its use	I think this is very unlikey to result in a flood	0%	0%	0%
2	Natural boundary conditions	Sea level rise of more than 25 cm Correlation between wind setup and discharge at Lobith greater than expected Longer storm durations seiches, new insights into, for example, probability distributions or suction forces. This can have both positive and negative effects stiffness of the retaining wall is sometimes quite low	This is - principally - not included in the current RA - analysis, it would need a different approach, like Bakker et al. (2025). At this moment, this is impossible for me to estimate.	?%	?%	?%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Redundancy	Locomobile and “Pennebaan” single point of failure	-	1%	2%	3%
2	Structural failure	There is sometimes leeway here because a conservative approach is taken when estimating mechanisms. Better to be a bit safer than on the edge. Better to allow some margin than to calculate endlessly. Structurally, the barrier consists of parallel and series systems. Assumptions have been made for this. Verifying these is worthwhile.	I think conservatism should only be allowed to keep modelling efforts low. I am not able to quantify this as a risk.	?%	?%	?%
2	Departure fails due to	Truss arms and sill make contact due to contact between consoles and seats Resonance of water in the dock entanglement of cables from shore to locomotive	What is meant here? Not clear how this results in a coastal flood.	?%	?%	?%
2	Submerging fails due to	Incorrect matrix causing valves not to open incorrect matrix causing the barrier to submerge too unevenly or too quickly brief outlier in inclinometers Unjustified or incorrect human intervention Too much sediment on the bottom	What I find relevant here is that initial damages and issues are not being used to improve the current sinking matrix. This makes this risk relatively likely, at least more likely than in the current estimate. The current RA analysis does assume something for failing to submerge, but is this enough? I assume that the ballast system currently accounts for approximately 20% of the total failure probability. I expect this to be doubled by the current approach.	0.2%	20%	40%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Floating fails due to	Unjustified or incorrect human intervention pre-tension not reduced in time due to pre-tension reduced asymmetrically due to retaining wall floats up too unevenly due to	But how does this result in a flood?	?%	?%	?%
2	Readiness for second peak fails due to	Docking (tolerances), closing dock gate, to rest position	But how does this result in a flood?	?%	?%	?%
3	Invalid failure characterization due to data gaps	Failures are modeled using assumed or outdated data; field behavior (e.g., wear-out) diverges from model assumptions	I think this is a major deficiency of the current analysis, and a major motivation to rebuild the RA analysis. I can't put a number on it…	?%	?%	?%
3	Model error due to incomplete data	Failure behavior of components is incorrectly modeled due to unavailability of detailed degradation or diagnostic data.	-	1%	5.5%	10%
3	Incomplete risk-based inspection implementation	RBI principles not fully embedded; inspection frequency or method not adjusted to risk profile, leading to insufficient PF interval knowledge.	Another issue related to this: it is not know how well RBI principles are applied at those structures from which the data originate. Therefore, impossible to quantify.	?%	?%	?%
3	Lack of insight into ageing effects	Long-term degradation mechanisms (e.g., fatigue, corrosion under insulation, seal aging) not well understood or incorporated into performance modeling.	-	1%	5.5%	10%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Ignoring stronger evidence than the RA analysis.	The RA analysis seems to have a more important role in decision-making than real evidence (damages, test results, etc). Given the weaknesses of RA analysis (based on not-representative data), this likely results in decision errors (P=1). Whether decision errors result in a flood is not that likely (P=10-5). Very uncertain about this risk.	-	0.00000001%	0.001%	1%
3	Preconditions of RA analysis not met	Assumptions from the RA (Risk Assessment) are not being followed Probo not properly executed Spare parts are a bit of an issue	I don't think the influence of ProBo is easy to quantify. I am not able to, at least.	?%	?%	?%
3	99 points	Represents all findings related to the closures. Some have been resolved, some have not and/or seem to be floating (unresolved) The question is whether analysis capacity within RWS is sufficient	See above	?%	?%	?%
3	Lessons learned forgotten	For example, BesW Many problems were encountered with synchronization, timing, and communication. These aspects are often underestimated in the sector. The risk is that these are not properly accounted for in design and testing.	See above	?%	?%	?%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Calculation methods	Model accuracy not included in the calculations, Affects MHW (Mean High Water) and flood probabilities and risks Cutsets are truncated at 3 levels, which may lead to underestimation This was corrected for Hartel Forecast inaccuracy for Rotterdam is increasing	-	1%	5.5%	10%
3	Failure probability analysis	Example: Influence of temperature on failure rate not included Failure data is outdated Failure-predictive indicators are no longer being analyzed, which means impending failures go unnoticed	-	1%	5.5%	10%
4	Storm conditions	it's unknown how the MK functions in a normative storm	Oh, so true! So difficult to quantify… I estimate 20%, but very wide uncertainty bounds…	0.02%	20%	100%
4	Underestimated phenomena	Mystery force: Integral calculation has never been finished	I think this is part of some of my intitial estimates.	?%	?%	?%
5	Incorrect Maintenance Execution	Errors or shortcuts in maintenance activities introduce or leave latent faults that impair future performance. errors made during maintenance that were not discovered during testing	I think these are included in the data	0%	0%	0%

Rank	Failure Mode	Description	Remark	Low	Medium	High
5	Unavailability due to maintenance	Parts of the barrier are unavailable during "not-storm season" Every 25 years an important item of for instance the locomobile not on site (1/25), probability of storm being in the summer (1/100)	-	0.0004%	0.04%	0.4%
5	Maintenance season too short	Too little time to restore the barrier, or job done improperly (/under stress), resulting in a higher failure probability. Because there is no report on the HAT I do not know the current estimate on this. Current probability of a failure to close (1/100) x percentage hardware failure (50%) / conservatism (factor 10) x maintenance error percentage (50%) x factor for more stress (2)	-	0.00001%	0.02%	0.1%
-	Other unidentifiable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable. Happened in the past as well where "new" phenomona's have been identified. How do we know we have everything?	We don't :-). In general, this is a limitation of almost every approach, and an RA analysis is probably the only way to deal with that. Important note: The idea is that if there is a functional decomposition everything within that function is addressed. The current RA analysis is not set-up like that. I don't know how to quantify this	0.3%	1%	4%

Table D.5: Table of input from SEJ 2nd round 4th respondent

Rank	Failure Mode	Description	Remark	Low	Medium	High
1	Decision making	The wrong decision is made by the operators while in operation	-	0.5%	10%	20%
1	Working in storm season leads to wrong decision	It can be too much for people to oversee	-	0.5%	1%	1.5%
1	Human error probability	Do the people have the right background, education, and training? ... Knowledge strategy is failing	-	2%	5%	8%
1	Forecasts for Rotterdam/Dordrecht incorrect due to human error	BOS incorrectly selects closure timing due to software error and complex water level pattern. Seiche or pipe surge influences the decision.	-	4%	7%	10%
1	Sensor/Data Fault Undetected	Sensor data leads to incorrect decisions; may go undetected if redundancy/diagnostics are insufficient.	-	0.1%	0.5%	1%
2	Structural integrity	The effects of losing sand is unknown	-	5%	6%	8%
2	Sinking of the floating sector gate	Failures during test storms can damage the barrier permanently in rare cases. Estimated storm frequency: 10^{-2}/year.	-	0.1%	0.5%	1%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Dormant phenomena	Condition of retaining structures, condition of drainage, condition of cofferdam, condition of HWK, damaged anchor rods corrosion, Wear on Hempaquick hinge Hinge control is failure-prone, groundwater behavior may be abnormal	-	5%	7%	10%
2	Obstacles on the threshold are (wrongly) not being inspected.	-	-	0.1%	1%	2%
2	Stalling of dock door	In stormy weather, the catch can end up on the wrong side of the rail. Limit switches not triggered due to excessive load during opening caused by heavy waves and drop control system failure due to	-	2%	7%	10%
2	Configuration parameters not updated/designed	Can lead to undesirable and unexpected behavior think of sinking matrices, fenders, and trim correction	-	1%	3%	5%
2	Tolerances	Deformation of the KW may be underestimated, truss arms bouncing on the sill	-	2%	8%	10%
2	The system is reaching its limits	Very high flows will only be partially held back by the barrier during certain storms, the barrier will not fully submerge. Multiple failing valves also limit its use	-	2%	4%	6%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Natural boundary conditions	Sea level rise of more than 25 cm Correlation between wind setup and discharge at Lobith greater than expected Longer storm durations seiches, new insights into, for example, probability distributions or suction forces. This can have both positive and negative effects stiffness of the retaining wall is sometimes quite low	-	2%	7%	10%
2	Redundancy	Locomobile and “Pennebaan” single point of failure	-	0.5%	5%	6%
2	Structural failure	There is sometimes leeway here because a conservative approach is taken when estimating mechanisms. Better to be a bit safer than on the edge. Better to allow some margin than to calculate endlessly. Structurally, the barrier consists of parallel and series systems. Assumptions have been made for this. Verifying these is worthwhile.	-	1%	5%	10%
2	Departure fails due to	Truss arms and sill make contact due to contact between consoles and seats Resonance of water in the dock entanglement of cables from shore to locomotive	-	0.5%	5%	7%

Rank	Failure Mode	Description	Remark	Low	Medium	High
2	Submerging fails due to	Incorrect matrix causing valves not to open incorrect matrix causing the barrier to submerge too unevenly or too quickly brief outlier in inclinometers Unjustified or incorrect human intervention Too much sediment on the bottom	-	0.5%	2%	3%
2	Floating fails due to	Unjustified or incorrect human intervention pre-tension not reduced in time due to pre-tension reduced asymmetrically due to retaining wall floats up too unevenly due to	-	1%	5%	10%
2	Readiness for second peak fails due to	Docking (tolerances), closing dock gate, to rest position	-	1%	5%	25%
3	Invalid failure characterization due to data gaps	Failures are modeled using assumed or outdated data; field behavior (e.g., wear-out) diverges from model assumptions	-	1%	5%	10%
3	Model error due to incomplete data	Failure behavior of components is incorrectly modeled due to unavailability of detailed degradation or diagnostic data.	-	0.5%	5%	10%
3	Incomplete risk-based inspection implementation	RBI principles not fully embedded; inspection frequency or method not adjusted to risk profile, leading to insufficient PF interval knowledge.	-	0.5%	2%	5%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Lack of insight into ageing effects	Long-term degradation mechanisms (e.g., fatigue, corrosion under insulation, seal aging) not well understood or incorporated into performance modeling.	-	0%	2%	7%
3	Ignoring stronger evidence than the RA analysis.	The RA analysis seems to have a more important role in decision-making than real evidence (damages, test results, etc). Given the weaknesses of RA analysis (based on not-representative data), this likely results in decision errors (P=1). Whether decision errors result in a flood is not that likely (P=10-5). Very uncertain about this risk.	-	1%	1.5%	2%
3	Preconditions of RA analysis not met	Assumptions from the RA (Risk Assessment) are not being followed Probo not properly executed Spare parts are a bit of an issue	-	2%	5%	10%
3	99 points	Represents all findings related to the closures. Some have been resolved, some have not and/or seem to be floating (unresolved) The question is whether analysis capacity within RWS is sufficient	-	1%	5%	10%

Rank	Failure Mode	Description	Remark	Low	Medium	High
3	Lessons learned forgotten	For example, BesW Many problems were encountered with synchronization, timing, and communication. These aspects are often underestimated in the sector. The risk is that these are not properly accounted for in design and testing.	-	1%	5%	10%
3	Calculation methods	Model accuracy not included in the calculations, Affects MHW (Mean High Water) and flood probabilities and risks Cutsets are truncated at 3 levels, which may lead to underestimation This was corrected for Hartel Forecast inaccuracy for Rotterdam is increasing	-	1%	5%	10%
3	Failure probability analysis	Example: Influence of temperature on failure rate not included Failure data is outdated Failure-predictive indicators are no longer being analyzed, which means impending failures go unnoticed	-	1%	5%	10%
4	Storm conditions	it's unknown how the MK functions in a normative storm	-	10%	20%	25%
4	Underestimated phenomena	Mystery force: Integral calculation has never been finished	-	1%	5%	10%

Rank	Failure Mode	Description	Remark	Low	Medium	High
5	Incorrect Maintenance Execution	Errors or shortcuts in maintenance activities introduce or leave latent faults that impair future performance. errors made during maintenance that were not discovered during testing	-	1%	2%	5%
5	Unavailability due to maintenance	Parts of the barrier are unavailable during "not-storm season" Every 25 years an important item of for instance the locomobile not on site (1/25), probability of storm being in the summer (1/100)	-	0.01%	1%	2%
5	Maintenance season too short	Too little time to restore the barrier, or job done improperly (/under stress), resulting in a higher failure probability. Because there is no report on the HAT I do not know the current estimate on this. Current probability of a failure to close (1/100) x percentage hardware failure (50%) / conservatism (factor 10) x maintenance error percentage (50%) x factor for more stress (2)	-	0.01%	1%	2%
-	Other unidentifiable events left out	Inherent incompletenes of current RA-analysis due to things that are not yet identifyable. Happened in the past as well where "new" phenomona's have been identified. How do we know we have everything?	-	1%	5%	10%

D.3. Averaged ranges per scenario with equal weighting given to all the experts

Event	Lower bound	Median	Higher bound
Decision making	-2.1%	2%	10%
Working in storm season leads to wrong decision	0.4%	3%	17%
Human error probability	2.3%	6%	15%
Forecasts for Rotterdam/Dordrecht incorrect due to human error	1.4%	4%	9%
Sensor/Data Fault Undetected	0.4%	3%	8%
constructional integrity	3.5%	6%	9%
Sinking of the floating sector gate	1.3%	6%	13%
Dormant phenomena	1.9%	6%	10%
Obstacles on the threshold are (wrongly) not being inspected.	0.5%	4%	7%
Stalling of dock door	-1.5%	2%	8%
Configuration parameters not updated/designed	1.3%	5%	14%
Tolerances	0.8%	5%	11%
The system is reaching its limits	0.8%	2%	7%
Natural boundary conditions	1.1%	6%	14%
Redundancy	0.5%	3%	5%
Structural failure	0.4%	2%	4%
Departure fails due to	0.2%	2%	5%
Submerging fails due to	0.5%	8%	16%
Floating fails due to	0.7%	6%	12%
Readiness for second peak fails due to	0.5%	3%	11%
Invalid Failure Characterization due to Data Gaps	0.8%	6%	12%
Model Error due to Incomplete Data	0.6%	6%	11%
Incomplete Risk-Based Inspection Implementation	0.6%	3%	6%
Lack of Insight into Ageing Effects	1.8%	8%	17%
Ignoring stronger evidence than the RA analysis	1.5%	3%	6%
Preconditions of RA analysis not met	4.3%	8%	17%
99 points	5.5%	13%	25%
Lessons learned forgotten	5.5%	13%	25%
Calculation methods	2.1%	5%	18%
Failure probability analysis	2.1%	5%	11%
storm conditions	5%	20%	63%
Underestimated phenomena	1%	8%	15%
Incorrect Maintenance Execution	2%	7%	16%
Unavailability due to maintenance	0.0%	1%	2%
Maintenance season too short	0.8%	3%	5%
Other unidentifiable events left out	0.8%	4%	8%
Sum of ranges	49.2%	193%	459%
Average of ranges	1.4%	5%	13%

Table D.6: Averaged ranges per scenario with equal weighting given to all the experts

E

Appendix E

E.1. HEP tables

Table E.1: THERP human error probabilities for different task types.

Task Type	Low HEP	Nominal HEP	High HEP
Simple detection	0.0010	0.010	0.03
Simple operation (e.g., button press)	0.0004	0.003	0.01
Routine operation	0.0010	0.010	0.10
Decision-making under time pressure	0.0100	0.100	0.30
Complex procedure execution	0.0100	0.200	0.50
Diagnosis of unfamiliar problem	0.0500	0.200	0.60
Omission of step in procedure	0.0030	0.010	0.10

Table E.2: Added Non-Closure Probabilities as calculated according to the methodology in Section 3.4.4

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.00	Simple detection	Low HEP	0.0010	0.000000
0.00	Simple detection	Low-Mid HEP	0.0055	0.000000
0.00	Simple detection	Nominal HEP	0.0100	0.000000
0.00	Simple detection	Mid-High HEP	0.0200	0.000000
0.00	Simple detection	High HEP	0.0300	0.000000
0.00	Simple operation	Low HEP	0.0004	0.000000
0.00	Simple operation	Low-Mid HEP	0.0017	0.000000
0.00	Simple operation	Nominal HEP	0.0030	0.000000
0.00	Simple operation	Mid-High HEP	0.0065	0.000000
0.00	Simple operation	High HEP	0.0100	0.000000
0.00	Routine operation	Low HEP	0.0010	0.000000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.00	Routine operation	Low-Mid HEP	0.0055	0.000000
0.00	Routine operation	Nominal HEP	0.0100	0.000000
0.00	Routine operation	Mid-High HEP	0.0550	0.000000
0.00	Routine operation	High HEP	0.1000	0.000000
0.00	Decision-making under time pressure	Low HEP	0.0100	0.000000
0.00	Decision-making under time pressure	Low-Mid HEP	0.0550	0.000000
0.00	Decision-making under time pressure	Nominal HEP	0.1000	0.000000
0.00	Decision-making under time pressure	Mid-High HEP	0.2000	0.000000
0.00	Decision-making under time pressure	High HEP	0.3000	0.000000
0.00	Complex procedure execution	Low HEP	0.0100	0.000000
0.00	Complex procedure execution	Low-Mid HEP	0.1050	0.000000
0.00	Complex procedure execution	Nominal HEP	0.2000	0.000000
0.00	Complex procedure execution	Mid-High HEP	0.3500	0.000000
0.00	Complex procedure execution	High HEP	0.5000	0.000000
0.00	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.000000
0.00	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.000000
0.00	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.000000
0.00	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.000000
0.00	Diagnoses of unfamiliar problem	High HEP	0.6000	0.000000
0.00	Omission of step in procedure	Low HEP	0.0030	0.000000
0.00	Omission of step in procedure	Low-Mid HEP	0.0065	0.000000
0.00	Omission of step in procedure	Nominal HEP	0.0100	0.000000
0.00	Omission of step in procedure	Mid-High HEP	0.0550	0.000000
0.00	Omission of step in procedure	High HEP	0.1000	0.000000
0.05	Simple detection	Low HEP	0.0010	0.000050
0.05	Simple detection	Low-Mid HEP	0.0055	0.000275
0.05	Simple detection	Nominal HEP	0.0100	0.000500
0.05	Simple detection	Mid-High HEP	0.0200	0.001000
0.05	Simple detection	High HEP	0.0300	0.001500
0.05	Simple operation	Low HEP	0.0004	0.000020
0.05	Simple operation	Low-Mid HEP	0.0017	0.000085
0.05	Simple operation	Nominal HEP	0.0030	0.000150
0.05	Simple operation	Mid-High HEP	0.0065	0.000325
0.05	Simple operation	High HEP	0.0100	0.000500
0.05	Routine operation	Low HEP	0.0010	0.000050
0.05	Routine operation	Low-Mid HEP	0.0055	0.000275
0.05	Routine operation	Nominal HEP	0.0100	0.000500
0.05	Routine operation	Mid-High HEP	0.0550	0.002750

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.05	Routine operation	High HEP	0.1000	0.005000
0.05	Decision-making under time pressure	Low HEP	0.0100	0.000500
0.05	Decision-making under time pressure	Low-Mid HEP	0.0550	0.002750
0.05	Decision-making under time pressure	Nominal HEP	0.1000	0.005000
0.05	Decision-making under time pressure	Mid-High HEP	0.2000	0.010000
0.05	Decision-making under time pressure	High HEP	0.3000	0.015000
0.05	Complex procedure execution	Low HEP	0.0100	0.000500
0.05	Complex procedure execution	Low-Mid HEP	0.1050	0.005250
0.05	Complex procedure execution	Nominal HEP	0.2000	0.010000
0.05	Complex procedure execution	Mid-High HEP	0.3500	0.017500
0.05	Complex procedure execution	High HEP	0.5000	0.025000
0.05	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.002500
0.05	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.006250
0.05	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.010000
0.05	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.020000
0.05	Diagnoses of unfamiliar problem	High HEP	0.6000	0.030000
0.05	Omission of step in procedure	Low HEP	0.0030	0.000150
0.05	Omission of step in procedure	Low-Mid HEP	0.0065	0.000325
0.05	Omission of step in procedure	Nominal HEP	0.0100	0.000500
0.05	Omission of step in procedure	Mid-High HEP	0.0550	0.002750
0.05	Omission of step in procedure	High HEP	0.1000	0.005000
0.10	Simple detection	Low HEP	0.0010	0.000100
0.10	Simple detection	Low-Mid HEP	0.0055	0.000550
0.10	Simple detection	Nominal HEP	0.0100	0.001000
0.10	Simple detection	Mid-High HEP	0.0200	0.002000
0.10	Simple detection	High HEP	0.0300	0.003000
0.10	Simple operation	Low HEP	0.0004	0.000040
0.10	Simple operation	Low-Mid HEP	0.0017	0.000170
0.10	Simple operation	Nominal HEP	0.0030	0.000300
0.10	Simple operation	Mid-High HEP	0.0065	0.000650
0.10	Simple operation	High HEP	0.0100	0.001000
0.10	Routine operation	Low HEP	0.0010	0.000100
0.10	Routine operation	Low-Mid HEP	0.0055	0.000550
0.10	Routine operation	Nominal HEP	0.0100	0.001000
0.10	Routine operation	Mid-High HEP	0.0550	0.005500
0.10	Routine operation	High HEP	0.1000	0.010000
0.10	Decision-making under time pressure	Low HEP	0.0100	0.001000
0.10	Decision-making under time pressure	Low-Mid HEP	0.0550	0.005500

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.10	Decision-making under time pressure	Nominal HEP	0.1000	0.010000
0.10	Decision-making under time pressure	Mid-High HEP	0.2000	0.020000
0.10	Decision-making under time pressure	High HEP	0.3000	0.030000
0.10	Complex procedure execution	Low HEP	0.0100	0.001000
0.10	Complex procedure execution	Low-Mid HEP	0.1050	0.010500
0.10	Complex procedure execution	Nominal HEP	0.2000	0.020000
0.10	Complex procedure execution	Mid-High HEP	0.3500	0.035000
0.10	Complex procedure execution	High HEP	0.5000	0.050000
0.10	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.005000
0.10	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.012500
0.10	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.020000
0.10	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.040000
0.10	Diagnoses of unfamiliar problem	High HEP	0.6000	0.060000
0.10	Omission of step in procedure	Low HEP	0.0030	0.000300
0.10	Omission of step in procedure	Low-Mid HEP	0.0065	0.000650
0.10	Omission of step in procedure	Nominal HEP	0.0100	0.001000
0.10	Omission of step in procedure	Mid-High HEP	0.0550	0.005500
0.10	Omission of step in procedure	High HEP	0.1000	0.010000
0.15	Simple detection	Low HEP	0.0010	0.000150
0.15	Simple detection	Low-Mid HEP	0.0055	0.000825
0.15	Simple detection	Nominal HEP	0.0100	0.001500
0.15	Simple detection	Mid-High HEP	0.0200	0.003000
0.15	Simple detection	High HEP	0.0300	0.004500
0.15	Simple operation	Low HEP	0.0004	0.000060
0.15	Simple operation	Low-Mid HEP	0.0017	0.000255
0.15	Simple operation	Nominal HEP	0.0030	0.000450
0.15	Simple operation	Mid-High HEP	0.0065	0.000975
0.15	Simple operation	High HEP	0.0100	0.001500
0.15	Routine operation	Low HEP	0.0010	0.000150
0.15	Routine operation	Low-Mid HEP	0.0055	0.000825
0.15	Routine operation	Nominal HEP	0.0100	0.001500
0.15	Routine operation	Mid-High HEP	0.0550	0.008250
0.15	Routine operation	High HEP	0.1000	0.015000
0.15	Decision-making under time pressure	Low HEP	0.0100	0.001500
0.15	Decision-making under time pressure	Low-Mid HEP	0.0550	0.008250
0.15	Decision-making under time pressure	Nominal HEP	0.1000	0.015000
0.15	Decision-making under time pressure	Mid-High HEP	0.2000	0.030000
0.15	Decision-making under time pressure	High HEP	0.3000	0.045000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.15	Complex procedure execution	Low HEP	0.0100	0.001500
0.15	Complex procedure execution	Low-Mid HEP	0.1050	0.015750
0.15	Complex procedure execution	Nominal HEP	0.2000	0.030000
0.15	Complex procedure execution	Mid-High HEP	0.3500	0.052500
0.15	Complex procedure execution	High HEP	0.5000	0.075000
0.15	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.007500
0.15	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.018750
0.15	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.030000
0.15	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.060000
0.15	Diagnoses of unfamiliar problem	High HEP	0.6000	0.090000
0.15	Omission of step in procedure	Low HEP	0.0030	0.000450
0.15	Omission of step in procedure	Low-Mid HEP	0.0065	0.000975
0.15	Omission of step in procedure	Nominal HEP	0.0100	0.001500
0.15	Omission of step in procedure	Mid-High HEP	0.0550	0.008250
0.15	Omission of step in procedure	High HEP	0.1000	0.015000
0.20	Simple detection	Low HEP	0.0010	0.000200
0.20	Simple detection	Low-Mid HEP	0.0055	0.001100
0.20	Simple detection	Nominal HEP	0.0100	0.002000
0.20	Simple detection	Mid-High HEP	0.0200	0.004000
0.20	Simple detection	High HEP	0.0300	0.006000
0.20	Simple operation	Low HEP	0.0004	0.000080
0.20	Simple operation	Low-Mid HEP	0.0017	0.000340
0.20	Simple operation	Nominal HEP	0.0030	0.000600
0.20	Simple operation	Mid-High HEP	0.0065	0.001300
0.20	Simple operation	High HEP	0.0100	0.002000
0.20	Routine operation	Low HEP	0.0010	0.000200
0.20	Routine operation	Low-Mid HEP	0.0055	0.001100
0.20	Routine operation	Nominal HEP	0.0100	0.002000
0.20	Routine operation	Mid-High HEP	0.0550	0.011000
0.20	Routine operation	High HEP	0.1000	0.020000
0.20	Decision-making under time pressure	Low HEP	0.0100	0.002000
0.20	Decision-making under time pressure	Low-Mid HEP	0.0550	0.011000
0.20	Decision-making under time pressure	Nominal HEP	0.1000	0.020000
0.20	Decision-making under time pressure	Mid-High HEP	0.2000	0.040000
0.20	Decision-making under time pressure	High HEP	0.3000	0.060000
0.20	Complex procedure execution	Low HEP	0.0100	0.002000
0.20	Complex procedure execution	Low-Mid HEP	0.1050	0.021000
0.20	Complex procedure execution	Nominal HEP	0.2000	0.040000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.20	Complex procedure execution	Mid-High HEP	0.3500	0.070000
0.20	Complex procedure execution	High HEP	0.5000	0.100000
0.20	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.010000
0.20	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.025000
0.20	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.040000
0.20	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.080000
0.20	Diagnoses of unfamiliar problem	High HEP	0.6000	0.120000
0.20	Omission of step in procedure	Low HEP	0.0030	0.000600
0.20	Omission of step in procedure	Low-Mid HEP	0.0065	0.001300
0.20	Omission of step in procedure	Nominal HEP	0.0100	0.002000
0.20	Omission of step in procedure	Mid-High HEP	0.0550	0.011000
0.20	Omission of step in procedure	High HEP	0.1000	0.020000
0.25	Simple detection	Low HEP	0.0010	0.000250
0.25	Simple detection	Low-Mid HEP	0.0055	0.001375
0.25	Simple detection	Nominal HEP	0.0100	0.002500
0.25	Simple detection	Mid-High HEP	0.0200	0.005000
0.25	Simple detection	High HEP	0.0300	0.007500
0.25	Simple operation	Low HEP	0.0004	0.000100
0.25	Simple operation	Low-Mid HEP	0.0017	0.000425
0.25	Simple operation	Nominal HEP	0.0030	0.000750
0.25	Simple operation	Mid-High HEP	0.0065	0.001625
0.25	Simple operation	High HEP	0.0100	0.002500
0.25	Routine operation	Low HEP	0.0010	0.000250
0.25	Routine operation	Low-Mid HEP	0.0055	0.001375
0.25	Routine operation	Nominal HEP	0.0100	0.002500
0.25	Routine operation	Mid-High HEP	0.0550	0.013750
0.25	Routine operation	High HEP	0.1000	0.025000
0.25	Decision-making under time pressure	Low HEP	0.0100	0.002500
0.25	Decision-making under time pressure	Low-Mid HEP	0.0550	0.013750
0.25	Decision-making under time pressure	Nominal HEP	0.1000	0.025000
0.25	Decision-making under time pressure	Mid-High HEP	0.2000	0.050000
0.25	Decision-making under time pressure	High HEP	0.3000	0.075000
0.25	Complex procedure execution	Low HEP	0.0100	0.002500
0.25	Complex procedure execution	Low-Mid HEP	0.1050	0.026250
0.25	Complex procedure execution	Nominal HEP	0.2000	0.050000
0.25	Complex procedure execution	Mid-High HEP	0.3500	0.087500
0.25	Complex procedure execution	High HEP	0.5000	0.125000
0.25	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.012500

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.25	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.031250
0.25	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.050000
0.25	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.100000
0.25	Diagnoses of unfamiliar problem	High HEP	0.6000	0.150000
0.25	Omission of step in procedure	Low HEP	0.0030	0.000750
0.25	Omission of step in procedure	Low-Mid HEP	0.0065	0.001625
0.25	Omission of step in procedure	Nominal HEP	0.0100	0.002500
0.25	Omission of step in procedure	Mid-High HEP	0.0550	0.013750
0.25	Omission of step in procedure	High HEP	0.1000	0.025000
0.30	Simple detection	Low HEP	0.0010	0.000300
0.30	Simple detection	Low-Mid HEP	0.0055	0.001650
0.30	Simple detection	Nominal HEP	0.0100	0.003000
0.30	Simple detection	Mid-High HEP	0.0200	0.006000
0.30	Simple detection	High HEP	0.0300	0.009000
0.30	Simple operation	Low HEP	0.0004	0.000120
0.30	Simple operation	Low-Mid HEP	0.0017	0.000510
0.30	Simple operation	Nominal HEP	0.0030	0.000900
0.30	Simple operation	Mid-High HEP	0.0065	0.001950
0.30	Simple operation	High HEP	0.0100	0.003000
0.30	Routine operation	Low HEP	0.0010	0.000300
0.30	Routine operation	Low-Mid HEP	0.0055	0.001650
0.30	Routine operation	Nominal HEP	0.0100	0.003000
0.30	Routine operation	Mid-High HEP	0.0550	0.016500
0.30	Routine operation	High HEP	0.1000	0.030000
0.30	Decision-making under time pressure	Low HEP	0.0100	0.003000
0.30	Decision-making under time pressure	Low-Mid HEP	0.0550	0.016500
0.30	Decision-making under time pressure	Nominal HEP	0.1000	0.030000
0.30	Decision-making under time pressure	Mid-High HEP	0.2000	0.060000
0.30	Decision-making under time pressure	High HEP	0.3000	0.090000
0.30	Complex procedure execution	Low HEP	0.0100	0.003000
0.30	Complex procedure execution	Low-Mid HEP	0.1050	0.031500
0.30	Complex procedure execution	Nominal HEP	0.2000	0.060000
0.30	Complex procedure execution	Mid-High HEP	0.3500	0.105000
0.30	Complex procedure execution	High HEP	0.5000	0.150000
0.30	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.015000
0.30	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.037500
0.30	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.060000
0.30	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.120000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.30	Diagnoses of unfamiliar problem	High HEP	0.6000	0.180000
0.30	Omission of step in procedure	Low HEP	0.0030	0.000900
0.30	Omission of step in procedure	Low-Mid HEP	0.0065	0.001950
0.30	Omission of step in procedure	Nominal HEP	0.0100	0.003000
0.30	Omission of step in procedure	Mid-High HEP	0.0550	0.016500
0.30	Omission of step in procedure	High HEP	0.1000	0.030000
0.35	Simple detection	Low HEP	0.0010	0.000350
0.35	Simple detection	Low-Mid HEP	0.0055	0.001925
0.35	Simple detection	Nominal HEP	0.0100	0.003500
0.35	Simple detection	Mid-High HEP	0.0200	0.007000
0.35	Simple detection	High HEP	0.0300	0.010500
0.35	Simple operation	Low HEP	0.0004	0.000140
0.35	Simple operation	Low-Mid HEP	0.0017	0.000595
0.35	Simple operation	Nominal HEP	0.0030	0.001050
0.35	Simple operation	Mid-High HEP	0.0065	0.002275
0.35	Simple operation	High HEP	0.0100	0.003500
0.35	Routine operation	Low HEP	0.0010	0.000350
0.35	Routine operation	Low-Mid HEP	0.0055	0.001925
0.35	Routine operation	Nominal HEP	0.0100	0.003500
0.35	Routine operation	Mid-High HEP	0.0550	0.019250
0.35	Routine operation	High HEP	0.1000	0.035000
0.35	Decision-making under time pressure	Low HEP	0.0100	0.003500
0.35	Decision-making under time pressure	Low-Mid HEP	0.0550	0.019250
0.35	Decision-making under time pressure	Nominal HEP	0.1000	0.035000
0.35	Decision-making under time pressure	Mid-High HEP	0.2000	0.070000
0.35	Decision-making under time pressure	High HEP	0.3000	0.105000
0.35	Complex procedure execution	Low HEP	0.0100	0.003500
0.35	Complex procedure execution	Low-Mid HEP	0.1050	0.036750
0.35	Complex procedure execution	Nominal HEP	0.2000	0.070000
0.35	Complex procedure execution	Mid-High HEP	0.3500	0.122500
0.35	Complex procedure execution	High HEP	0.5000	0.175000
0.35	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.017500
0.35	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.043750
0.35	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.070000
0.35	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.140000
0.35	Diagnoses of unfamiliar problem	High HEP	0.6000	0.210000
0.35	Omission of step in procedure	Low HEP	0.0030	0.001050
0.35	Omission of step in procedure	Low-Mid HEP	0.0065	0.002275

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.35	Omission of step in procedure	Nominal HEP	0.0100	0.003500
0.35	Omission of step in procedure	Mid-High HEP	0.0550	0.019250
0.35	Omission of step in procedure	High HEP	0.1000	0.035000
0.40	Simple detection	Low HEP	0.0010	0.000400
0.40	Simple detection	Low-Mid HEP	0.0055	0.002200
0.40	Simple detection	Nominal HEP	0.0100	0.004000
0.40	Simple detection	Mid-High HEP	0.0200	0.008000
0.40	Simple detection	High HEP	0.0300	0.012000
0.40	Simple operation	Low HEP	0.0004	0.000160
0.40	Simple operation	Low-Mid HEP	0.0017	0.000680
0.40	Simple operation	Nominal HEP	0.0030	0.001200
0.40	Simple operation	Mid-High HEP	0.0065	0.002600
0.40	Simple operation	High HEP	0.0100	0.004000
0.40	Routine operation	Low HEP	0.0010	0.000400
0.40	Routine operation	Low-Mid HEP	0.0055	0.002200
0.40	Routine operation	Nominal HEP	0.0100	0.004000
0.40	Routine operation	Mid-High HEP	0.0550	0.022000
0.40	Routine operation	High HEP	0.1000	0.040000
0.40	Decision-making under time pressure	Low HEP	0.0100	0.004000
0.40	Decision-making under time pressure	Low-Mid HEP	0.0550	0.022000
0.40	Decision-making under time pressure	Nominal HEP	0.1000	0.040000
0.40	Decision-making under time pressure	Mid-High HEP	0.2000	0.080000
0.40	Decision-making under time pressure	High HEP	0.3000	0.120000
0.40	Complex procedure execution	Low HEP	0.0100	0.004000
0.40	Complex procedure execution	Low-Mid HEP	0.1050	0.042000
0.40	Complex procedure execution	Nominal HEP	0.2000	0.080000
0.40	Complex procedure execution	Mid-High HEP	0.3500	0.140000
0.40	Complex procedure execution	High HEP	0.5000	0.200000
0.40	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.020000
0.40	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.050000
0.40	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.080000
0.40	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.160000
0.40	Diagnoses of unfamiliar problem	High HEP	0.6000	0.240000
0.40	Omission of step in procedure	Low HEP	0.0030	0.001200
0.40	Omission of step in procedure	Low-Mid HEP	0.0065	0.002600
0.40	Omission of step in procedure	Nominal HEP	0.0100	0.004000
0.40	Omission of step in procedure	Mid-High HEP	0.0550	0.022000
0.40	Omission of step in procedure	High HEP	0.1000	0.040000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.45	Simple detection	Low HEP	0.0010	0.000450
0.45	Simple detection	Low-Mid HEP	0.0055	0.002475
0.45	Simple detection	Nominal HEP	0.0100	0.004500
0.45	Simple detection	Mid-High HEP	0.0200	0.009000
0.45	Simple detection	High HEP	0.0300	0.013500
0.45	Simple operation	Low HEP	0.0004	0.000180
0.45	Simple operation	Low-Mid HEP	0.0017	0.000765
0.45	Simple operation	Nominal HEP	0.0030	0.001350
0.45	Simple operation	Mid-High HEP	0.0065	0.002925
0.45	Simple operation	High HEP	0.0100	0.004500
0.45	Routine operation	Low HEP	0.0010	0.000450
0.45	Routine operation	Low-Mid HEP	0.0055	0.002475
0.45	Routine operation	Nominal HEP	0.0100	0.004500
0.45	Routine operation	Mid-High HEP	0.0550	0.024750
0.45	Routine operation	High HEP	0.1000	0.045000
0.45	Decision-making under time pressure	Low HEP	0.0100	0.004500
0.45	Decision-making under time pressure	Low-Mid HEP	0.0550	0.024750
0.45	Decision-making under time pressure	Nominal HEP	0.1000	0.045000
0.45	Decision-making under time pressure	Mid-High HEP	0.2000	0.090000
0.45	Decision-making under time pressure	High HEP	0.3000	0.135000
0.45	Complex procedure execution	Low HEP	0.0100	0.004500
0.45	Complex procedure execution	Low-Mid HEP	0.1050	0.047250
0.45	Complex procedure execution	Nominal HEP	0.2000	0.090000
0.45	Complex procedure execution	Mid-High HEP	0.3500	0.157500
0.45	Complex procedure execution	High HEP	0.5000	0.225000
0.45	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.022500
0.45	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.056250
0.45	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.090000
0.45	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.180000
0.45	Diagnoses of unfamiliar problem	High HEP	0.6000	0.270000
0.45	Omission of step in procedure	Low HEP	0.0030	0.001350
0.45	Omission of step in procedure	Low-Mid HEP	0.0065	0.002925
0.45	Omission of step in procedure	Nominal HEP	0.0100	0.004500
0.45	Omission of step in procedure	Mid-High HEP	0.0550	0.024750
0.45	Omission of step in procedure	High HEP	0.1000	0.045000
0.50	Simple detection	Low HEP	0.0010	0.000500
0.50	Simple detection	Low-Mid HEP	0.0055	0.002750
0.50	Simple detection	Nominal HEP	0.0100	0.005000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.50	Simple detection	Mid-High HEP	0.0200	0.010000
0.50	Simple detection	High HEP	0.0300	0.015000
0.50	Simple operation	Low HEP	0.0004	0.000200
0.50	Simple operation	Low-Mid HEP	0.0017	0.000850
0.50	Simple operation	Nominal HEP	0.0030	0.001500
0.50	Simple operation	Mid-High HEP	0.0065	0.003250
0.50	Simple operation	High HEP	0.0100	0.005000
0.50	Routine operation	Low HEP	0.0010	0.000500
0.50	Routine operation	Low-Mid HEP	0.0055	0.002750
0.50	Routine operation	Nominal HEP	0.0100	0.005000
0.50	Routine operation	Mid-High HEP	0.0550	0.027500
0.50	Routine operation	High HEP	0.1000	0.050000
0.50	Decision-making under time pressure	Low HEP	0.0100	0.005000
0.50	Decision-making under time pressure	Low-Mid HEP	0.0550	0.027500
0.50	Decision-making under time pressure	Nominal HEP	0.1000	0.050000
0.50	Decision-making under time pressure	Mid-High HEP	0.2000	0.100000
0.50	Decision-making under time pressure	High HEP	0.3000	0.150000
0.50	Complex procedure execution	Low HEP	0.0100	0.005000
0.50	Complex procedure execution	Low-Mid HEP	0.1050	0.052500
0.50	Complex procedure execution	Nominal HEP	0.2000	0.100000
0.50	Complex procedure execution	Mid-High HEP	0.3500	0.175000
0.50	Complex procedure execution	High HEP	0.5000	0.250000
0.50	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.025000
0.50	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.062500
0.50	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.100000
0.50	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.200000
0.50	Diagnoses of unfamiliar problem	High HEP	0.6000	0.300000
0.50	Omission of step in procedure	Low HEP	0.0030	0.001500
0.50	Omission of step in procedure	Low-Mid HEP	0.0065	0.003250
0.50	Omission of step in procedure	Nominal HEP	0.0100	0.005000
0.50	Omission of step in procedure	Mid-High HEP	0.0550	0.027500
0.50	Omission of step in procedure	High HEP	0.1000	0.050000
0.60	Simple detection	Low HEP	0.0010	0.000600
0.60	Simple detection	Low-Mid HEP	0.0055	0.003300
0.60	Simple detection	Nominal HEP	0.0100	0.006000
0.60	Simple detection	Mid-High HEP	0.0200	0.012000
0.60	Simple detection	High HEP	0.0300	0.018000
0.60	Simple operation	Low HEP	0.0004	0.000240

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.60	Simple operation	Low-Mid HEP	0.0017	0.001020
0.60	Simple operation	Nominal HEP	0.0030	0.001800
0.60	Simple operation	Mid-High HEP	0.0065	0.003900
0.60	Simple operation	High HEP	0.0100	0.006000
0.60	Routine operation	Low HEP	0.0010	0.000600
0.60	Routine operation	Low-Mid HEP	0.0055	0.003300
0.60	Routine operation	Nominal HEP	0.0100	0.006000
0.60	Routine operation	Mid-High HEP	0.0550	0.033000
0.60	Routine operation	High HEP	0.1000	0.060000
0.60	Decision-making under time pressure	Low HEP	0.0100	0.006000
0.60	Decision-making under time pressure	Low-Mid HEP	0.0550	0.033000
0.60	Decision-making under time pressure	Nominal HEP	0.1000	0.060000
0.60	Decision-making under time pressure	Mid-High HEP	0.2000	0.120000
0.60	Decision-making under time pressure	High HEP	0.3000	0.180000
0.60	Complex procedure execution	Low HEP	0.0100	0.006000
0.60	Complex procedure execution	Low-Mid HEP	0.1050	0.063000
0.60	Complex procedure execution	Nominal HEP	0.2000	0.120000
0.60	Complex procedure execution	Mid-High HEP	0.3500	0.210000
0.60	Complex procedure execution	High HEP	0.5000	0.300000
0.60	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.030000
0.60	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.075000
0.60	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.120000
0.60	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.240000
0.60	Diagnoses of unfamiliar problem	High HEP	0.6000	0.360000
0.60	Omission of step in procedure	Low HEP	0.0030	0.001800
0.60	Omission of step in procedure	Low-Mid HEP	0.0065	0.003900
0.60	Omission of step in procedure	Nominal HEP	0.0100	0.006000
0.60	Omission of step in procedure	Mid-High HEP	0.0550	0.033000
0.60	Omission of step in procedure	High HEP	0.1000	0.060000
0.65	Simple detection	Low HEP	0.0010	0.000650
0.65	Simple detection	Low-Mid HEP	0.0055	0.003575
0.65	Simple detection	Nominal HEP	0.0100	0.006500
0.65	Simple detection	Mid-High HEP	0.0200	0.013000
0.65	Simple detection	High HEP	0.0300	0.019500
0.65	Simple operation	Low HEP	0.0004	0.000260
0.65	Simple operation	Low-Mid HEP	0.0017	0.001105
0.65	Simple operation	Nominal HEP	0.0030	0.001950
0.65	Simple operation	Mid-High HEP	0.0065	0.004225

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.65	Simple operation	High HEP	0.0100	0.006500
0.65	Routine operation	Low HEP	0.0010	0.000650
0.65	Routine operation	Low-Mid HEP	0.0055	0.003575
0.65	Routine operation	Nominal HEP	0.0100	0.006500
0.65	Routine operation	Mid-High HEP	0.0550	0.035750
0.65	Routine operation	High HEP	0.1000	0.065000
0.65	Decision-making under time pressure	Low HEP	0.0100	0.006500
0.65	Decision-making under time pressure	Low-Mid HEP	0.0550	0.035750
0.65	Decision-making under time pressure	Nominal HEP	0.1000	0.065000
0.65	Decision-making under time pressure	Mid-High HEP	0.2000	0.130000
0.65	Decision-making under time pressure	High HEP	0.3000	0.195000
0.65	Complex procedure execution	Low HEP	0.0100	0.006500
0.65	Complex procedure execution	Low-Mid HEP	0.1050	0.068250
0.65	Complex procedure execution	Nominal HEP	0.2000	0.130000
0.65	Complex procedure execution	Mid-High HEP	0.3500	0.227500
0.65	Complex procedure execution	High HEP	0.5000	0.325000
0.65	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.032500
0.65	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.081250
0.65	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.130000
0.65	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.260000
0.65	Diagnoses of unfamiliar problem	High HEP	0.6000	0.390000
0.65	Omission of step in procedure	Low HEP	0.0030	0.001950
0.65	Omission of step in procedure	Low-Mid HEP	0.0065	0.004225
0.65	Omission of step in procedure	Nominal HEP	0.0100	0.006500
0.65	Omission of step in procedure	Mid-High HEP	0.0550	0.035750
0.65	Omission of step in procedure	High HEP	0.1000	0.065000
0.70	Simple detection	Low HEP	0.0010	0.000700
0.70	Simple detection	Low-Mid HEP	0.0055	0.003850
0.70	Simple detection	Nominal HEP	0.0100	0.007000
0.70	Simple detection	Mid-High HEP	0.0200	0.014000
0.70	Simple detection	High HEP	0.0300	0.021000
0.70	Simple operation	Low HEP	0.0004	0.000280
0.70	Simple operation	Low-Mid HEP	0.0017	0.001190
0.70	Simple operation	Nominal HEP	0.0030	0.002100
0.70	Simple operation	Mid-High HEP	0.0065	0.004550
0.70	Simple operation	High HEP	0.0100	0.007000
0.70	Routine operation	Low HEP	0.0010	0.000700
0.70	Routine operation	Low-Mid HEP	0.0055	0.003850

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.70	Routine operation	Nominal HEP	0.0100	0.007000
0.70	Routine operation	Mid-High HEP	0.0550	0.038500
0.70	Routine operation	High HEP	0.1000	0.070000
0.70	Decision-making under time pressure	Low HEP	0.0100	0.007000
0.70	Decision-making under time pressure	Low-Mid HEP	0.0550	0.038500
0.70	Decision-making under time pressure	Nominal HEP	0.1000	0.070000
0.70	Decision-making under time pressure	Mid-High HEP	0.2000	0.140000
0.70	Decision-making under time pressure	High HEP	0.3000	0.210000
0.70	Complex procedure execution	Low HEP	0.0100	0.007000
0.70	Complex procedure execution	Low-Mid HEP	0.1050	0.073500
0.70	Complex procedure execution	Nominal HEP	0.2000	0.140000
0.70	Complex procedure execution	Mid-High HEP	0.3500	0.245000
0.70	Complex procedure execution	High HEP	0.5000	0.350000
0.70	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.035000
0.70	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.087500
0.70	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.140000
0.70	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.280000
0.70	Diagnoses of unfamiliar problem	High HEP	0.6000	0.420000
0.70	Omission of step in procedure	Low HEP	0.0030	0.002100
0.70	Omission of step in procedure	Low-Mid HEP	0.0065	0.004550
0.70	Omission of step in procedure	Nominal HEP	0.0100	0.007000
0.70	Omission of step in procedure	Mid-High HEP	0.0550	0.038500
0.70	Omission of step in procedure	High HEP	0.1000	0.070000
0.75	Simple detection	Low HEP	0.0010	0.000750
0.75	Simple detection	Low-Mid HEP	0.0055	0.004125
0.75	Simple detection	Nominal HEP	0.0100	0.007500
0.75	Simple detection	Mid-High HEP	0.0200	0.015000
0.75	Simple detection	High HEP	0.0300	0.022500
0.75	Simple operation	Low HEP	0.0004	0.000300
0.75	Simple operation	Low-Mid HEP	0.0017	0.001275
0.75	Simple operation	Nominal HEP	0.0030	0.002250
0.75	Simple operation	Mid-High HEP	0.0065	0.004875
0.75	Simple operation	High HEP	0.0100	0.007500
0.75	Routine operation	Low HEP	0.0010	0.000750
0.75	Routine operation	Low-Mid HEP	0.0055	0.004125
0.75	Routine operation	Nominal HEP	0.0100	0.007500
0.75	Routine operation	Mid-High HEP	0.0550	0.041250
0.75	Routine operation	High HEP	0.1000	0.075000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.75	Decision-making under time pressure	Low HEP	0.0100	0.007500
0.75	Decision-making under time pressure	Low-Mid HEP	0.0550	0.041250
0.75	Decision-making under time pressure	Nominal HEP	0.1000	0.075000
0.75	Decision-making under time pressure	Mid-High HEP	0.2000	0.150000
0.75	Decision-making under time pressure	High HEP	0.3000	0.225000
0.75	Complex procedure execution	Low HEP	0.0100	0.007500
0.75	Complex procedure execution	Low-Mid HEP	0.1050	0.078750
0.75	Complex procedure execution	Nominal HEP	0.2000	0.150000
0.75	Complex procedure execution	Mid-High HEP	0.3500	0.262500
0.75	Complex procedure execution	High HEP	0.5000	0.375000
0.75	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.037500
0.75	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.093750
0.75	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.150000
0.75	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.300000
0.75	Diagnoses of unfamiliar problem	High HEP	0.6000	0.450000
0.75	Omission of step in procedure	Low HEP	0.0030	0.002250
0.75	Omission of step in procedure	Low-Mid HEP	0.0065	0.004875
0.75	Omission of step in procedure	Nominal HEP	0.0100	0.007500
0.75	Omission of step in procedure	Mid-High HEP	0.0550	0.041250
0.75	Omission of step in procedure	High HEP	0.1000	0.075000
0.80	Simple detection	Low HEP	0.0010	0.000800
0.80	Simple detection	Low-Mid HEP	0.0055	0.004400
0.80	Simple detection	Nominal HEP	0.0100	0.008000
0.80	Simple detection	Mid-High HEP	0.0200	0.016000
0.80	Simple detection	High HEP	0.0300	0.024000
0.80	Simple operation	Low HEP	0.0004	0.000320
0.80	Simple operation	Low-Mid HEP	0.0017	0.001360
0.80	Simple operation	Nominal HEP	0.0030	0.002400
0.80	Simple operation	Mid-High HEP	0.0065	0.005200
0.80	Simple operation	High HEP	0.0100	0.008000
0.80	Routine operation	Low HEP	0.0010	0.000800
0.80	Routine operation	Low-Mid HEP	0.0055	0.004400
0.80	Routine operation	Nominal HEP	0.0100	0.008000
0.80	Routine operation	Mid-High HEP	0.0550	0.044000
0.80	Routine operation	High HEP	0.1000	0.080000
0.80	Decision-making under time pressure	Low HEP	0.0100	0.008000
0.80	Decision-making under time pressure	Low-Mid HEP	0.0550	0.044000
0.80	Decision-making under time pressure	Nominal HEP	0.1000	0.080000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.80	Decision-making under time pressure	Mid-High HEP	0.2000	0.160000
0.80	Decision-making under time pressure	High HEP	0.3000	0.240000
0.80	Complex procedure execution	Low HEP	0.0100	0.008000
0.80	Complex procedure execution	Low-Mid HEP	0.1050	0.084000
0.80	Complex procedure execution	Nominal HEP	0.2000	0.160000
0.80	Complex procedure execution	Mid-High HEP	0.3500	0.280000
0.80	Complex procedure execution	High HEP	0.5000	0.400000
0.80	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.040000
0.80	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.100000
0.80	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.160000
0.80	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.320000
0.80	Diagnoses of unfamiliar problem	High HEP	0.6000	0.480000
0.80	Omission of step in procedure	Low HEP	0.0030	0.002400
0.80	Omission of step in procedure	Low-Mid HEP	0.0065	0.005200
0.80	Omission of step in procedure	Nominal HEP	0.0100	0.008000
0.80	Omission of step in procedure	Mid-High HEP	0.0550	0.044000
0.80	Omission of step in procedure	High HEP	0.1000	0.080000
0.85	Simple detection	Low HEP	0.0010	0.000850
0.85	Simple detection	Low-Mid HEP	0.0055	0.004675
0.85	Simple detection	Nominal HEP	0.0100	0.008500
0.85	Simple detection	Mid-High HEP	0.0200	0.017000
0.85	Simple detection	High HEP	0.0300	0.025500
0.85	Simple operation	Low HEP	0.0004	0.000340
0.85	Simple operation	Low-Mid HEP	0.0017	0.001445
0.85	Simple operation	Nominal HEP	0.0030	0.002550
0.85	Simple operation	Mid-High HEP	0.0065	0.005525
0.85	Simple operation	High HEP	0.0100	0.008500
0.85	Routine operation	Low HEP	0.0010	0.000850
0.85	Routine operation	Low-Mid HEP	0.0055	0.004675
0.85	Routine operation	Nominal HEP	0.0100	0.008500
0.85	Routine operation	Mid-High HEP	0.0550	0.046750
0.85	Routine operation	High HEP	0.1000	0.085000
0.85	Decision-making under time pressure	Low HEP	0.0100	0.008500
0.85	Decision-making under time pressure	Low-Mid HEP	0.0550	0.046750
0.85	Decision-making under time pressure	Nominal HEP	0.1000	0.085000
0.85	Decision-making under time pressure	Mid-High HEP	0.2000	0.170000
0.85	Decision-making under time pressure	High HEP	0.3000	0.255000
0.85	Complex procedure execution	Low HEP	0.0100	0.008500

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.85	Complex procedure execution	Low-Mid HEP	0.1050	0.089250
0.85	Complex procedure execution	Nominal HEP	0.2000	0.170000
0.85	Complex procedure execution	Mid-High HEP	0.3500	0.297500
0.85	Complex procedure execution	High HEP	0.5000	0.425000
0.85	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.042500
0.85	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.106250
0.85	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.170000
0.85	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.340000
0.85	Diagnoses of unfamiliar problem	High HEP	0.6000	0.510000
0.85	Omission of step in procedure	Low HEP	0.0030	0.002550
0.85	Omission of step in procedure	Low-Mid HEP	0.0065	0.005525
0.85	Omission of step in procedure	Nominal HEP	0.0100	0.008500
0.85	Omission of step in procedure	Mid-High HEP	0.0550	0.046750
0.85	Omission of step in procedure	High HEP	0.1000	0.085000
0.90	Simple detection	Low HEP	0.0010	0.000900
0.90	Simple detection	Low-Mid HEP	0.0055	0.004950
0.90	Simple detection	Nominal HEP	0.0100	0.009000
0.90	Simple detection	Mid-High HEP	0.0200	0.018000
0.90	Simple detection	High HEP	0.0300	0.027000
0.90	Simple operation	Low HEP	0.0004	0.000360
0.90	Simple operation	Low-Mid HEP	0.0017	0.001530
0.90	Simple operation	Nominal HEP	0.0030	0.002700
0.90	Simple operation	Mid-High HEP	0.0065	0.005850
0.90	Simple operation	High HEP	0.0100	0.009000
0.90	Routine operation	Low HEP	0.0010	0.000900
0.90	Routine operation	Low-Mid HEP	0.0055	0.004950
0.90	Routine operation	Nominal HEP	0.0100	0.009000
0.90	Routine operation	Mid-High HEP	0.0550	0.049500
0.90	Routine operation	High HEP	0.1000	0.090000
0.90	Decision-making under time pressure	Low HEP	0.0100	0.009000
0.90	Decision-making under time pressure	Low-Mid HEP	0.0550	0.049500
0.90	Decision-making under time pressure	Nominal HEP	0.1000	0.090000
0.90	Decision-making under time pressure	Mid-High HEP	0.2000	0.180000
0.90	Decision-making under time pressure	High HEP	0.3000	0.270000
0.90	Complex procedure execution	Low HEP	0.0100	0.009000
0.90	Complex procedure execution	Low-Mid HEP	0.1050	0.094500
0.90	Complex procedure execution	Nominal HEP	0.2000	0.180000
0.90	Complex procedure execution	Mid-High HEP	0.3500	0.315000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.90	Complex procedure execution	High HEP	0.5000	0.450000
0.90	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.045000
0.90	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.112500
0.90	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.180000
0.90	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.360000
0.90	Diagnoses of unfamiliar problem	High HEP	0.6000	0.540000
0.90	Omission of step in procedure	Low HEP	0.0030	0.002700
0.90	Omission of step in procedure	Low-Mid HEP	0.0065	0.005850
0.90	Omission of step in procedure	Nominal HEP	0.0100	0.009000
0.90	Omission of step in procedure	Mid-High HEP	0.0550	0.049500
0.90	Omission of step in procedure	High HEP	0.1000	0.090000
0.95	Simple detection	Low HEP	0.0010	0.000950
0.95	Simple detection	Low-Mid HEP	0.0055	0.005225
0.95	Simple detection	Nominal HEP	0.0100	0.009500
0.95	Simple detection	Mid-High HEP	0.0200	0.019000
0.95	Simple detection	High HEP	0.0300	0.028500
0.95	Simple operation	Low HEP	0.0004	0.000380
0.95	Simple operation	Low-Mid HEP	0.0017	0.001615
0.95	Simple operation	Nominal HEP	0.0030	0.002850
0.95	Simple operation	Mid-High HEP	0.0065	0.006175
0.95	Simple operation	High HEP	0.0100	0.009500
0.95	Routine operation	Low HEP	0.0010	0.000950
0.95	Routine operation	Low-Mid HEP	0.0055	0.005225
0.95	Routine operation	Nominal HEP	0.0100	0.009500
0.95	Routine operation	Mid-High HEP	0.0550	0.052250
0.95	Routine operation	High HEP	0.1000	0.095000
0.95	Decision-making under time pressure	Low HEP	0.0100	0.009500
0.95	Decision-making under time pressure	Low-Mid HEP	0.0550	0.052250
0.95	Decision-making under time pressure	Nominal HEP	0.1000	0.095000
0.95	Decision-making under time pressure	Mid-High HEP	0.2000	0.190000
0.95	Decision-making under time pressure	High HEP	0.3000	0.285000
0.95	Complex procedure execution	Low HEP	0.0100	0.009500
0.95	Complex procedure execution	Low-Mid HEP	0.1050	0.099750
0.95	Complex procedure execution	Nominal HEP	0.2000	0.190000
0.95	Complex procedure execution	Mid-High HEP	0.3500	0.332500
0.95	Complex procedure execution	High HEP	0.5000	0.475000
0.95	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.047500
0.95	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.118750

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
0.95	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.190000
0.95	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.380000
0.95	Diagnoses of unfamiliar problem	High HEP	0.6000	0.570000
0.95	Omission of step in procedure	Low HEP	0.0030	0.002850
0.95	Omission of step in procedure	Low-Mid HEP	0.0065	0.006175
0.95	Omission of step in procedure	Nominal HEP	0.0100	0.009500
0.95	Omission of step in procedure	Mid-High HEP	0.0550	0.052250
0.95	Omission of step in procedure	High HEP	0.1000	0.095000
1.00	Simple detection	Low HEP	0.0010	0.001000
1.00	Simple detection	Low-Mid HEP	0.0055	0.005500
1.00	Simple detection	Nominal HEP	0.0100	0.010000
1.00	Simple detection	Mid-High HEP	0.0200	0.020000
1.00	Simple detection	High HEP	0.0300	0.030000
1.00	Simple operation	Low HEP	0.0004	0.000400
1.00	Simple operation	Low-Mid HEP	0.0017	0.001700
1.00	Simple operation	Nominal HEP	0.0030	0.003000
1.00	Simple operation	Mid-High HEP	0.0065	0.006500
1.00	Simple operation	High HEP	0.0100	0.010000
1.00	Routine operation	Low HEP	0.0010	0.001000
1.00	Routine operation	Low-Mid HEP	0.0055	0.005500
1.00	Routine operation	Nominal HEP	0.0100	0.010000
1.00	Routine operation	Mid-High HEP	0.0550	0.055000
1.00	Routine operation	High HEP	0.1000	0.100000
1.00	Decision-making under time pressure	Low HEP	0.0100	0.010000
1.00	Decision-making under time pressure	Low-Mid HEP	0.0550	0.055000
1.00	Decision-making under time pressure	Nominal HEP	0.1000	0.100000
1.00	Decision-making under time pressure	Mid-High HEP	0.2000	0.200000
1.00	Decision-making under time pressure	High HEP	0.3000	0.300000
1.00	Complex procedure execution	Low HEP	0.0100	0.010000
1.00	Complex procedure execution	Low-Mid HEP	0.1050	0.105000
1.00	Complex procedure execution	Nominal HEP	0.2000	0.200000
1.00	Complex procedure execution	Mid-High HEP	0.3500	0.350000
1.00	Complex procedure execution	High HEP	0.5000	0.500000
1.00	Diagnoses of unfamiliar problem	Low HEP	0.0500	0.050000
1.00	Diagnoses of unfamiliar problem	Low-Mid HEP	0.1250	0.125000
1.00	Diagnoses of unfamiliar problem	Nominal HEP	0.2000	0.200000
1.00	Diagnoses of unfamiliar problem	Mid-High HEP	0.4000	0.400000
1.00	Diagnoses of unfamiliar problem	High HEP	0.6000	0.600000

Machine Failure Probability	Task Type	HEP Level	HEP Value	Added Non-Closure Probability
1.00	Omission of step in procedure	Low HEP	0.0030	0.003000
1.00	Omission of step in procedure	Low-Mid HEP	0.0065	0.006500
1.00	Omission of step in procedure	Nominal HEP	0.0100	0.010000
1.00	Omission of step in procedure	Mid-High HEP	0.0550	0.055000
1.00	Omission of step in procedure	High HEP	0.1000	0.100000