Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P188-cd

Quantitative Risk Assessment of a Periodically Unattended Bridge

Mert Yildiz[1a], Manfred Constapel[1b], Hans-Christoph Burmeister[1c]
[1a] *Fraunhofer CML, Germany. E-mail: mert.yildiz@cml.fraunhofer.de*
[1b] *Fraunhofer CML, Germany. E-mail: manfred.constapel@cml.fraunhofer.de*
[1c] *Fraunhofer CML, Germany. E-mail: hans-christoph.burmeister@cml.fraunhofer.de*

Lennart Swoboda[2a], Athalie Njabou[2b], Karl-Heinz Warnstedt[2c]
[2a] *Schulte Group, Germany. E-mail: lennart.swoboda@schultegroup.com*
[2b] *Federal Maritime and Hydrographic Agency of Germany, Germany. E-mail: athalie.njabou@bsh.de*
[2c] *Federal Maritime and Hydrographic Agency of Germany, Germany. E-mail: karl-heinz.warnstedt@bsh.de*

A periodically unattended bridge is a likely use case, often cited with regards to Maritime Autonomous Surface Ship (MASS) technologies. The German-funded B ZERO project aims to develop and demonstrate capabilities which are needed for navigating a cargo ship for up to 8 hours within a predefined operational envelope. From a risk perspective, MASS technology, and thus the implementation of B ZERO must be as safe as conventional technology, which is why a safety assessment of the B ZERO concept is executed according to the International Maritime Organization Formal Safety Assessment guidelines. This paper outlines the results from the hazard identification and risk analysis executed along the Bow-Tie Model. The risk analysis focuses on quantitative methods such as Fault and Event Tree Analysis Modeling, for relative comparison of conventional (attended) bridge and unattended bridge instead of qualitative expert-based ratings in risk matrices. It includes insights into how risks associated with MASS can be modeled by identifying reasonable probabilities from literature.

Keywords: Fault Tree Analysis, Event Tree Analysis, Formal Safety Assessment, Risk Assessment, Bow-Tie Model

1. Introduction

Maritime Autonomous Surface Ships (MASS) are becoming a reality, aiming to revolutionize transportation by providing safer, more efficient, and cost-effective means of transportation. These vessels offer several benefits, such as reducing the risks associated with human error, increasing efficiency, and lowering operating costs (Burmeister et al. (2014)). However, implementing autonomous technology in maritime operations requires caution and a thorough understanding of the involved risks. As trustworthiness (Floridi (2019); Wing (2021)) and explicitness of Artificial Intelligence (AI) are becoming as important as the capabilities of AI systems, that are designed to interact with the real world, conducting a risk analysis of autonomous vessels is essential.

The B ZERO project, funded by the German government, aims to develop and demonstrate the capabilities of autonomous navigation for cargo ships. The project aims to navigate a cargo ship for up to 8 hours within a predefined operational envelope (Ugé and Hochgeschurz (2021)). To ensure the safety of this technology, a Formal Safety Assessment (FSA) of the B ZERO concept is being executed according to the International Maritime Organization's (IMO) guidelines (IMO (2018)).

The objective of the B ZERO project is to enable a vessel to perform at least one navigational watch autonomously, without an officer-of-the-watch (OOW) being on the bridge. In line with IMO (2021) and ISO 23860:2022 (2022) definitions, the B ZERO system is an *autonomous ship system* for unattended bridge operations allowing up to *Degree Four* within its *operational envelope*. Please note that we use the term unattended instead of uncrewed, as the crew is still onboard.

Therefore, a relative risk comparison between a conventional watch (not unattended) with an OOW on the bridge and the periodically (and conditionally) unattended bridge is needed to assess if the periodically unattended bridge in general, and the B ZERO system specifically, can achieve safer navigation. In this risk assessment, we have adapted and extended the FSA methodology proposed by Rødseth and Burmeister (2015) for a dry bulk carrier in the MUNIN project. Please note that we are assuming that the principal magnitude of the consequences are not changing, as we don't fundamentally change ship design, nor oil bunkering or the number of persons on board. Thus, the risk assessment conducted is only investigating the changes in the frequency of *collision* and foundering events.

Our contributions are as follows: The paper starts in section 2 with a brief overview on methods used for risk assessment in the maritime domain. Section 2 also outlines our methodology, which starts with identifying the hazards of the B ZERO system by drawing logical connections between subsystems of the autonomous navigation system. The identified hazards are later analyzed using a Bow-Tie model (Nielsen (1971)), which combines Fault Tree Analysis (FTA) (Ericson and Ll (1999)) and Event Tree Analysis (ETA)(Ericson et al. (2015)). We conclude the paper in Section 3 by providing results and provided insight into the individual failure nodes and events that have a relatively more significant impact on the overall system, highlighting areas for potential improvements to reduce risks.

2. Background

2.1. *Formal Safety Assessment*

As the maritime industry witnessed an increase of autonomous approaches for navigation, evaluating safety concerns associated with MASS and related technologies has become an urgent priority, including at the IMO level (IMO (2021)). FSA is a structured and systematic approach that is crucial for identifying, evaluating, and mitigating the risks associated with maritime operations, including those of autonomous vessels. Several methods have been proposed for conducting risk assessment of technological systems, such as Fault Tree Analysis (Lee et al. (2021)), Fuzzy Bayesian Networks (FBN) (Zhang et al. (2019)), Reliability Block Diagrams (RBDs) (Jakkula et al. (2020); Li et al. (2020)), and Monte Carlo Simulation (MCS) (BahooToroody et al. (2022)). These methods require certain assumptions on complex Markov models and often rely on expert opinions or literature values to quantify the risks of potential outcomes, such as collision or foundering. However, the complexity of maritime situations varies spatially and temporally, making it challenging to realistically identify the risks associated with autonomous vessels. Moreover, the lack of available data specific to autonomous systems adds another layer of complexity to the risk assessment process. To address this challenge, the AUTOSHIP project conducted an expert-based assessment of safety, security, and cybersecurity hazards for an autonomous inland waterways ship during its preliminary design phase (Bolbot et al. (2021)). This assessment aimed to bridge the data gap and provide valuable insights into the risk landscape of autonomous vessel operations.

In a similar vein, the MUNIN project proposes a framework that tackles the challenges of risk assessment for autonomous vessels by providing a relative risk assessment between autonomous and conventional vessels. By utilizing FTA and ETA, the MUNIN project's framework provides an opportunity to examine the causal relationships and impacts of various hazards within the system. With this framework, MUNIN project aims to quantify the advantages and disadvantages of autonomous vehicles in terms of risk (Rødseth and Burmeister (2015)). In line with these efforts, this study leverages the MUNIN project's framework and applies it to the B ZERO project, contributing to the ongoing exploration of risk assessment methodologies in the context of autonomous vessels.

The development of FSA was initially prompted by the Piper Alpha catastrophe that occurred in 1988. Now it is an official part of the IMO rule making process. FSA consists of the following five steps (IMO (2018)):

(i) Hazard Identification
(ii) Risk Assessment
(iii) Risk Control Options
(iv) Cost-Benefit Assessment
(v) Decision-making Recommendations

In this work, first two steps of the FSA process will be presented, with a focus on the frequency changes, as consequences are assumed to be similar. To gain deeper insights into the outcomes of the ”Risk Assessment” step, we also utilized the subgraph centrality metric and Sobol sensitivity analysis.

2.2. *Hazard Identification*

We conducted the hazard identification process using a combination of methods, including reviewing relevant literature and regulations, consulting with subject matter experts, and using brainstorming and scenario-based techniques. We put the identified hazards into categories based on the subsystems of B ZERO that they belong to. Subsequently, we placed special focus on hazards related to manual takeover of the watch from the autonomous navigation system.

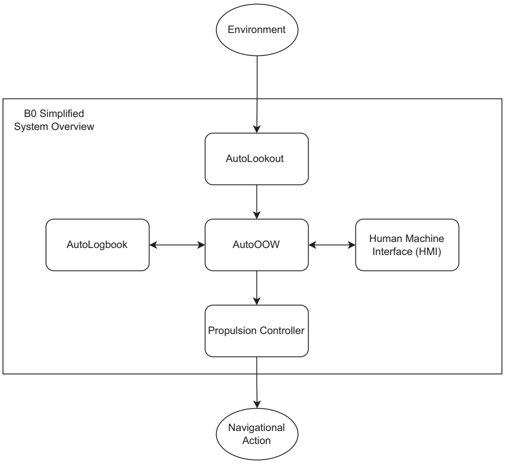


Fig. 1.: B ZERO System Overview
AutoLookout is the module responsible for sensing the environment. AutoOOW is the module responsible for autonomous decision making. AutoLogbook is the digital logbook of the B ZERO system. HMI is the interaction module of human operator with B ZERO.

Based on the B ZERO autonomous system overview provided in Figure 1, most impacting hazards are identified and documented based on the following keywords:

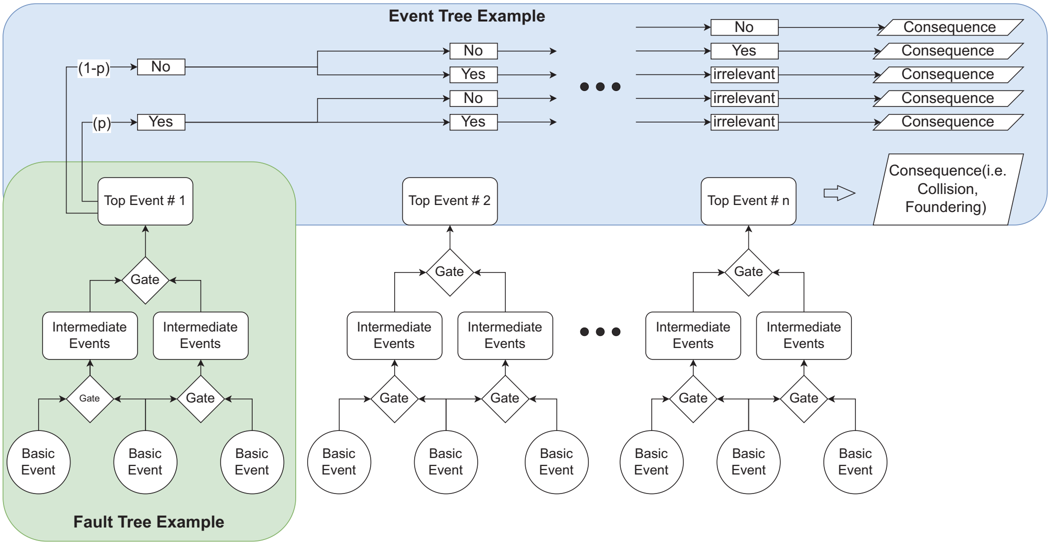
- Subsystem: A subsystem is a smaller part of a larger system that performs a specific function or task within that system. It is a self-contained unit that can be separated from the rest of the system for analysis or modification.
- Hazardous Element: A hazardous element is any component or object within a system that has the potential to cause harm or damage to people, equipment, or the environment.
- Hazardous Condition: A hazardous condition is a situation or circumstance within a system that can lead to a hazardous event. It can include factors such as environmental conditions, operational procedures, or equipment failures that increase the risk of harm or damage.
- Cause: A cause is the reason or factor that leads to a hazardous event. It can include things like design flaws, human error, or equipment malfunction that contribute to the hazardous condition.
- Possible Consequence: A possible consequence is the potential outcome of a hazardous event.

2.3. *Bow-Tie Analysis*

Bow-Tie analysis provides a graphical representation of potential hazards and their consequences. Many variations of Bow-Tie can be found in literature (de Ruijter and Guldenmund (2016)). In our work, we use the variation introduced by Nielsen (1971). We combine Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) techniques to identify the critical hazards (Top events), their causes, and the potential consequences. Top events create the sequences in the event trees which lead to occurrence of a hazard. Figure 2 presents an overview of the Bow-Tie method implemented in this paper for the calculation of occurrence probability estimates of *collision* and *foundering* consequences. *Collision* and *foundering* are specifically chosen as they were identified as the most probable hazardous consequences associated with the B ZERO voyage plan which only covers open sea navigation.

Following the Bow-Tie Analysis briefly explained in Figure 2, Fault Tree Analysis (FTA) is used to calculate occurrence probability estimates of top events that take part in the event trees. For the creation of Fault Trees, we used a subset

Fig. 2.: Bow-Tie Analysis



Fault Trees (green), are used to estimate probabilities of top events based on the *AND* & *OR* logical gates. Event trees (blue) presents linear sequences of events based on keywords such as *yes*, meaning the top event happened, *no* meaning the top event did not happen, and *irrelevant*, meaning it does not matter if the top event happened or not for the propagation of probability in that branch. ”p” refers to the the probability estimate of the top event calculated by the Fault Trees.

of standard fault tree analysis symbols defined by the Nuclear Regulatory Commission (NRC) in NUREG-0492 (Vesely et al. (1981)).

2.4. *Fault Tree Analysis*

Fault Tree Analysis is a widely used systematic and quantitative approach for analyzing and evaluating the reliability and safety of complex systems. FTA delivers graphical representations of logical relationships among various components or events that may lead to the occurrence of an undesired event, called the *top event*. The fault tree comprises a series of logic gates, such as AND, OR, NOT and events (i.e. component failures). Performing FTA can identify the critical components or events that are most likely to lead to the top event, providing insights into how to improve system reliability and safety.

According to the IMO FSA guidelines an iterative process is required to see how risk control options can change the overall reliability of the designed system. However, traditional FTA approaches are often time-consuming and resource-intensive since they require manual construction and evaluation of the fault trees. Therefore, automated tools and techniques are necessary to at least automate the calculation of manually created fault trees. For this purpose, we have developed a Python library to define FTA as a graph network analysis.

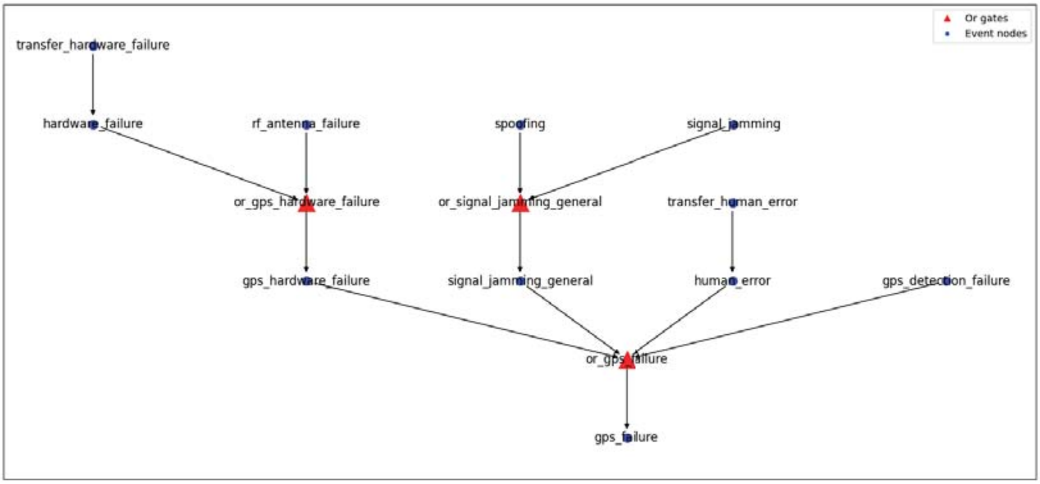
2.5. *Event Tree Analysis*

Event Tree Analysis (ETA) is a systematic and quantitative approach for analyzing and evaluating the potential outcomes of logical sequences of critical events. The event tree consists of a series of branches, each representing a possible sequence of events that may occur following the starting event. The branches are interconnected to represent the probability and consequences of each event.

By following the framework given in Jensen (2015), starting events given in Table 1 are used for the relative risk comparison of the unattended and the conventional bridge.

For the describing the probability propagation

Fig. 3.: Example of a GPS Failure Fault Tree



of branches, following keywords have been used:

- Yes: Meaning that the corresponding top event occurred. Contribution to the probability propagation equals to the probability of the top event
- No: Meaning that the corresponding top event didn't occur. Contribution to the probability propagation equals to complement of the probability of the top event
- Irrelevant: Meaning that it doesn't affect the probability propagation if the event occurs or not. Therefore, irrelevant keyword does not create a new branch in the event tree.

Since, we are using the conventional bridge event trees created in Jensen (2015), B ZERO system event trees is designed in a way that, sequence and nature of the top events of both attended and unattended bridge align on a logical level. This alignment was necessary to successfully conduct the relative risk comparison. This alignment is presented in the Figure 4 which shows the complete event trees including the top events based on the proposed starting events for both attended and unattended bridges.

Blackout and *Machinery Failure* starting events have both *Yes* and *No* branches (Figure 2), as the *Yes* branch shows the event sequence led by the starting event, *No* branch shows the event sequence in absence of the start event. Thus, B ZERO system is expected to steer the vessel and make navigational decisions. These branches which have *No* for the ”blackout” and ”machinery failure”, show the event sequences that start with ”Other ship on collision course”. This provides valuable insight to how B ZERO system copes with vessel-to-vessel collision, when the system has full control over the steering and decision making.

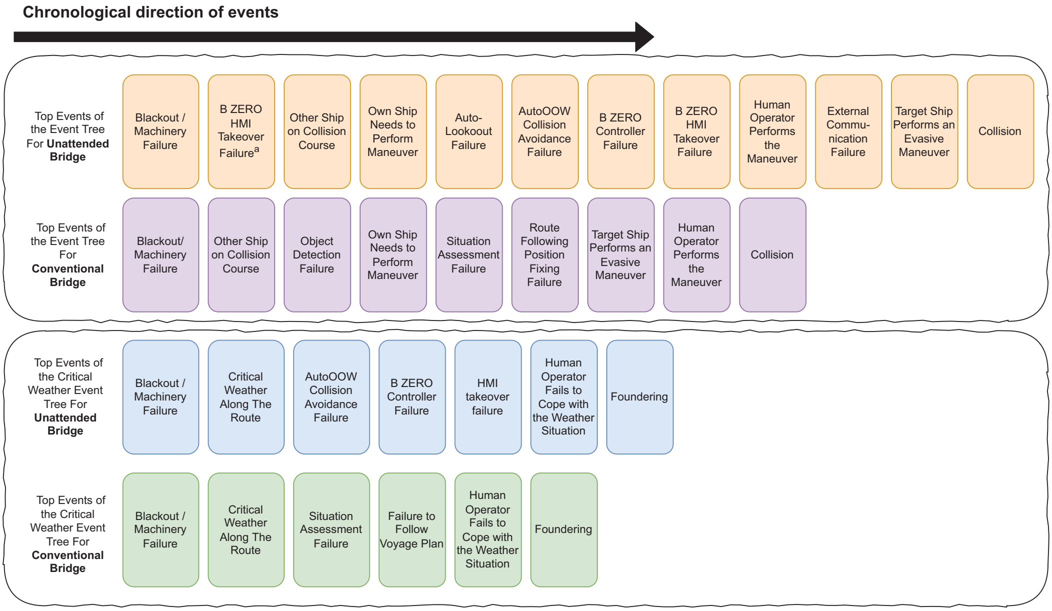
Table 1.: Potential outcomes (consequences) based on starting events

Starting Event	Consequence	Explanation
Blackout	Collision	All B ZERO systems are down and not functioning.
Machinery Failure	Collision	All propulsion of the vessel is lost.
Critical Weather Encountering	Foundering	In case the vessel finds herself in a critical weather situation according to MSC (2007a)

2.5.1. *Sensitivity Analysis*

In the context of event tree analysis, sensitivity analysis can help identifying the input parameters

Fig. 4.: Event Trees of conventional (attended) and unattended bridges


Chronological direction of events
Top Events of the Event Tree For **Unattended Bridge**
Blackout / Machinery Failure
B ZERO HMI Takeover Failure[a]
Other Ship on Collision Course
Own Ship Needs to Perform Maneuver
Auto-Lookout Failure
AutoOOW Collision Avoidance Failure
B ZERO Controller Failure
B ZERO HMI Takeover Failure
Human Operator Performs the Maneuver
External Commu-nication Failure
Target Ship Performs an Evasive Maneuver
Collision
Top Events of the Event Tree For **Conventional Bridge**
Blackout/ Machinery Failure
Other Ship on Collision Course
Object Detection Failure
Own Ship Needs to Perform Maneuver
Situation Assessment Failure
Route Following Position Fixing Failure
Target Ship Performs an Evasive Maneuver
Human Operator Performs the Maneuver
Collision
Top Events of the Critical Weather Event Tree For **Unattended Bridge**
Blackout / Machinery Failure
Critical Weather Along The Route
AutoOOW Collision Avoidance Failure
B ZERO Controller Failure
HMI takeover failure
Human Operator Fails to Cope with the Weather Situation
Foundering
Top Events of the Critical Weather Event Tree For **Conventional Bridge**
Blackout / Machinery Failure
Critical Weather Along The Route
Situation Assessment Failure
Failure to Follow Voyage Plan
Human Operator Fails to Cope with the Weather Situation
Foundering

[a] This event only exists for trees which have ”Machinery Failure” as starting event.

that have the most significant impact on the outcomes of the event tree. By doing so, it guides the decision-making process towards the events that require more attention when developing risk management strategies.

SALib (Hermans et al. (2017)) provides a range of sensitivity analysis methods, including Sobol method which is a variance-based method that decomposes the variance of the model output into contributions from individual input variables and their interactions, which allow for the analysis of both main effects and interaction effects among the input parameters.

2.5.2. *Subgraph Centrality Analysis*

Subgraph centrality (Estrada and Rodriguez-Velazquez (2005)) is a measure of centrality in network analysis that quantifies the importance of a node within a subgraph. Nodes that are highly connected within a particular subgraph but not well-connected to other parts of the network will have lower subgraph centrality scores. This metric is used on the fault tree network structure of B ZERO system to identify the importance of each event based on the number and size of its connected subgraphs thus events that have the most influence on the system and are critical for its overall reliability, are obtained.

2.6. *Critical Weather Modelling*

For the creation of event trees with the ”foundering” outcome, an estimation on critical weather encountering probability has been made using the Pilot-Charts and historical-AIS data of the B ZERO Vessel. For this estimation, methodology proposed in MUNIN project has been followed and adapted to the B ZERO navigation plan.

Due to lack of very detailed weather data for the relevant sea areas for the B ZERO project, weather data obtained from Pilot-Charts for the North Atlantic Ocean (Agency (2002)) have been used. These Pilot-Charts provide wind roses which provides insight to a 5° grid box. Extracted wind powers on the cardinal directions have been used to identify which of the critical weather phenomena stated in MSC.1/Circ.1228 of the IMO, can be encountered in B ZERO vessel’s voyage plan. Critical weather encountering occurrence probability estimate is calculated according to the criteria specified in MSC (2007a). Required vessel specific dimension information have been acquired from the project partners, whereas information such as average vessel speed and average vessel heading in between legs of the voyage have been extracted from the historical AIS data.

Table 2.: Navigation System Hazards of B ZERO System and Supplementary Basic Events

Hazardous Element	Probability
AutoLookout Sensors Failure	1.29E-04
AutoLookout Fusion Algorithm Failure	1.68E-04
AutoLookout Object Detection Failure	2.29E-04
AutoLookout Object Association Failure	4.21E-04
AutoLookout General Failure	3.28E-04
AutoLookout Object Tracker Failure	4.21E-04
AutoOOW Situational Awareness Failure	2.39E-02
AutoOOW Collision Avoidance Failure	2.58E-02
AutoOOW Switch-over Module Failure	5.41E-04
AutoOOW Collision Avoidance Trajectory Prediction Failure	2.54E-02
AutoLogbook Monitoring Failure	5.81E-04
AutoOOW General Failure	2.76E-02
B ZERO Controller Failure	3.80E-04
B ZERO Controller Motion Sensor Failure	5.41E-04
B ZERO Controller Weather Sensor Failure	5.41E-04
HMI Take-over Failure (Regular & emergency)	4.79E-02
HMI Alarm Failure	1.08E-03
Radar Failure	1.04E-03
AIS Failure	2.78E-02
Bridge Network Failure	4.21E-04
CCTV Camera Failure	3.45E-03
External Communication Failure	2.35E-02
Human Error	2.32E-02
GPS Failure	2.85E-02
Gyro Failure	1.40E-03
General Hardware Failure	3.86E-02
General Software Failure	1.61E-04
Camera Hardware Failure[a]	2.60E-03
GPS Detection Failure[b]	5.00E-02

[a] Supplementary basic event identified in literature, in addition to those outlined in the basic events report by MUNIN project (2015), [b] Estimated based on IMO (2000)

3. Results and Discussion

Quantitative assessment of the risks associated with unattended bridge operations in the context of MASS safety assurance is a complex task, primarily due to the limited availability of data specifically focused on MASS. To address this challenge, our approach in designing the B ZERO autonomous system was to confine MASS-specific risks mostly to the software level. The estimation of software-related probabilities of occurrences relied on preliminary test results of the components and expert opinions. For the remaining probabilities of failures, which are common to both unattended and conventional bridge operations, we relied on literature sources. Specific statistical probability of failures as well as equipment failure rates data of the basic events used in this study are mostly acquired from Haugen (1993), Beliczey and Schulz (1987), OREDA (2002), Van Sciver (1989), Asami and Kaneko (2013), MSC (2007b), Baker and McCafferty (2005), Antao and Guedes Soares (2006), Rebaiaia et al. (2012). Table 3 presents most of the basic events used in this work and their respective literature sources.

Following the hazard identification 27 hazardous conditions are identified related to the B ZERO system. 63 fault trees have been created to calculate occurrence probability estimates associated with the hazardous conditions. Table 2 presents these hazards and their respective occurrence probabilities. Same procedure for unattended vessel is directly adapted from Jensen (2015), after changing certain fault tree components to comply with the hardware of B ZERO test vessel. Most of basic event occurrence probabilities used in this study were obtained from the work by MUNIN project (2015), which presents a comprehensive list of events and their corresponding references. However, as part of the hazard identification process, additional basic events necessary for the B ZERO system were identified and are presented at the end of Table 2.

The results of the risk assessment based on the proposed methodology have shown that both unattended and conventional bridge operations are susceptible to *collision* and *foundering* events. The *collision* and *foundering* occurrence probabilities for the starting events of machinery failure and blackout have been presented in Table 4.

Comparing the probabilities for *collision* and foundering outcomes between unattended and attended bridges, it is evident that for the unattended bridge, occurrence probability estimates of *collision* and foundering are one order of magnitude lower compared to attended bridge according to the executed methodology, as shown in Table 4. Only for the starting even blackout and the consequence *collision*, the probability is in the same order of magnitude and relatively higher for the unattended bridge. The reason for this is, since

Table 3.: Basic event probabilities acquired from Jensen (2015) and corresponding references

Basic Events
Accident, Asleep, Alcohol, Distraction - Haugen (1993)
Action of other ship expected, crew: detection failure, crew: extinguishing failure, failure to identify maintenance need, faulty/incomplete information, interpretation failure, limited capabilities/misjudgement, manual control failure, no backup components, no command (operator), operating error (heading), operating error (velocity), radar failure, wrong command (operator) - Asami and Kaneko (2013)
Antenna damage (waves), antenna damage (wind), blade fouling, blade fracture, broken crankshaft, clogged filters (LO-system), hacking, impeller fouling, impeller fracture, incorrect data from other object, leakage (water), lube oil impurities (old), pump failure(water), rudder stuck, sensor misjudgement, short circuit (permanent), spoofing, stern tube failure, thrust block failure, turbocharger failure - MSC (2007b) - Internal MUNIN Deliverable D6
Antenna turning equipment (motor) failure, powder ext. system failure, shaft motor internal failure, water ext. system failure, - Van Sciver (1989)
Bearings, broken coupling bolts, camera hardware, drive shaft fracture, failure generator protection, failure to receive data (by own ship), internal failure generator, over worn bearings, receiver failure, sender failure, sensor failure - de Boer (2004)
Communication failure (VTS) - Antao and Guedes Soares (2006)
Detection system failure - flame, detection system failure - heat, detection system failure - smoke, diesel oil pump failure, failure hydraulic pump, PC failure, pump failure (LO), random breakdown - OREDA (2002)
Fuel oil piping broken, leakage (fuel), leakage (LO-system), leakage hydraulic system, lube oil piping broken, - Beliczey and Schulz (1987)
Shaft, coupling - Baker and McCafferty (2005)
RF antenna failure, - Rebaiaia et al. (2012)

B ZERO systems are not functioning during the ”blackout”, crew of the vessel is not being informed on time regarding a possible vessel on collision course.

Based on the combined collision and foundering probability for both ”blackout” and ”machinery failure” starting events, it is evident that unattended bridge provides lower risk compared to the conventional (attended) bridge. The reason for this is, the failure of an attended bridge may depend solely on the human crew, while that of an unmanned bridge equipped with the B ZERO system requires the failure of both the autonomous navigation system and the crew since B ZERO alarms for a takeover by the human operator during hazardous situations that the system cannot solve on its own. Consequently, the risk of failure for an unmanned bridge is lower than that of an attended bridge. In summary, B ZERO system acts as an additional barrier to prevent risky events, and its reliance on human intervention further reduces the likelihood of failure.

These results suggest that the implementation of autonomous vessels could significantly reduce the risk of collision and foundering events and ensure an operation at least as safe as conventional operation. However, it is essential to note that this risk assessment is based on the assumption that all the safety measures and technologies for autonomous vessels are adequately implemented and maintained. Therefore, it is necessary to establish comprehensive safety regulations and guidelines for autonomous vessels to ensure their safe and reliable operation.

Figure 5 and Figure 6 presents sensitivity analysis, based on the Sobol method, of *collision* outcome for the starting events ”blackout” and ”machinery failure”. Starting events are excluded from the graph to highlight effects of the B ZERO system components.

Both graphs show that ”other object on collision course”, ”own vessel needs to perform a maneuver”, ”human operator performs the maneuver” and ”target ship performs evasive maneuver” are the most important top events defining the probability of *collision*. This makes sense because during either a blackout or machinery failure, B ZERO systems cannot steer the ship, therefore human factor has the utmost importance.

Note that events related to B ZERO system such as ”AutoOOW collision avoidance failure”

Table 4.: Results of the event trees for starting events of ”Blackout” and ”Machinery Failure” for conventional and unattended bridge

	Collision Probability		Foundering Probability	
Starting Event	Unattended Bridge	Conventional Bridge	Unattended Bridge	Conventional Bridge
Blackout	3.44E-07	**1.17E-07**	**3.79E-04**	3.16E-03
Machinery Failure	**3.70E-07**	1.11E-06	**3.78E-04**	4.79E-03
Sum	**7.14E-07**	1.22E-06	**7.57E-04**	7.96E-03

exists in the graphs even though during a blackout or machinery failure B ZERO system cannot steer the ship. Reason for this is, as explained in the subsection 2.5, while event trees are created, branch that is starting with a ”No” for the starting events are also implemented. Therefore, sensitivity analysis of these event trees actually includes event sequences from the normal operation (without blackout or machinery failure). During normal operation, the probability of a collision is lower because all components of the B ZERO steering system are functioning properly, thus we have less *irrelevant* keywords in these branches.

Based on the results, it can also be stated that, most important B ZERO system component in both starting events is ”B ZERO HMI takeover failure” which is the fault tree that defines the probability of failure for the successful switchover between B ZERO system and human operator. This also makes sense, since either during the situations following the starting events or during normal operation if other components of the B ZERO system are unable to prevent a collision, it becomes critical to switch controls to the human operator to ensure safe navigation.

Table 5 shows the top 10 events with the highest occurrence probability estimates according to the designed fault trees. Based on these results, it can be deducted that sensor failure probabilities of GPS” and ”AIS” are as likely as the other B ZERO systems. Among the B ZERO sub systems, ”HMI Takeover Module” and ”B ZERO Controller Module” are estimated to be B ZERO system hazards with the highest probability of happening.

Fig. 5.: Sensitivity Analysis of Blackout Starting Event

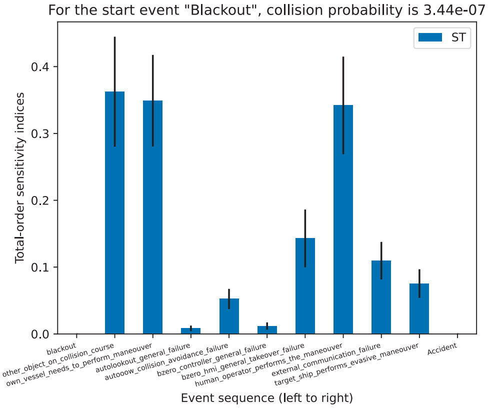


Fig. 6.: Sensitivity Analysis of Machinery Failure Starting Event

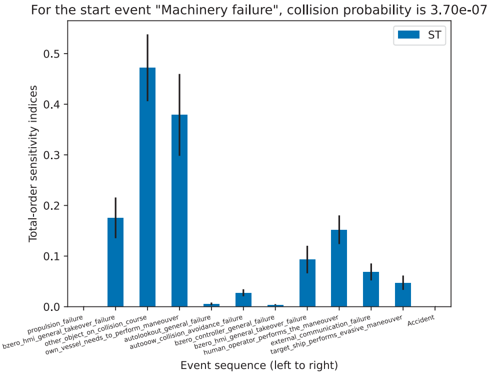


Table 6 shows top events with the highest subgraph centrality scores which rank the nodes based on their outreach capabilities in the network. As expected, ”Hardware General Failure” and ”Software General Failure” top events has the highest reach potential since they are affecting many fault trees as random error sources. On the third place, AutoOOW general failure presents itself as the most important failure node of the B ZERO failure network. On the fourth place, ”human error” is found to have similar subgraph centrality score with the ”AutoOOW general failure”. This suggests that in the B ZERO autonomous system, human error still has a huge impact on

Table 5.: Top 10 events with respect to the occurrence probabilities

Event Name	Occurrence Probability
B ZERO HMI General Takeover Failure	4.79E-02
B ZERO Controller General Failure	3.86E-02
GPS Failure	2.85E-02
AIS Failure	2.78E-02
External Failure	2.77E-02
AutoOOW General Failure	2.76E-02
AutoOOW Collision Avoidance Failure	2.58E-02
AutoOOW Collision Avoidance Trajectory Prediction Failure	2.54E-02
B ZERO HMI Emergency Takeover Failure	2.48E-02
AutoOOW Situational Awareness Failure	2.39E-02

the reliability of whole operation. Note that human error can present itself in many ways such as inputting wrong configuration, incorrect installation of the system or equipment, failures in takeover scenarios etc.

Table 6.: Subgraph Centrality Results

Failure Type	Centrality Score
Hardware General Failure	16.21
Software General Failure	14.49
AutoOOW General Failure	8.80
Human Error	8.30
AutoOOW Monitoring Failure	6.52
AutoLookout Object Tracker Failure	6.16
Gyro Failure	6.15
Antenna Failure	6.07
External Factors	5.90
AutoOOW Collision Avoidance Trajectory Prediction Failure	5.49
GPS Failure	5.43
B ZERO Controller General Failure	5.33
B ZERO HMI Alarm Failure	5.24
AutoOOW Takeover Failure	5.17
AutoOOW Situational Awareness Failure	5.09
B ZERO Controller Weather Sensor Failure	5.07
B ZERO Controller Motion Sensor Failure	5.07
Bridge Network Failure	5.05
AutoLookout General Failure	4.68

4. Conclusion

As part of the Formal Safety Assessment of the B ZERO project, identified hazardous events related to ”unattended” and ”conventional” bridge are employed in the quantitative risk assessment using a Bow-Tie model. Relative risk assessment of the B ZERO unattended bridge system has shown that it provides lower occurrence probability estimates thus safer navigation for ”collision” and ”foundering” consequences compared to conventional operations. The Sobol method and subgraph centrality analysis have provided insight into the individual failure nodes and events that have a relatively more significant impact on the overall system, highlighting areas for potential improvements to reduce risks. The development of a Python library for defining the fault trees as graph networks has enabled a more detailed analysis of the fault nodes, leading to recommendations for improvements in the B ZERO system. Overall, the results of this study have demonstrated the importance of conducting a thorough risk assessment when implementing autonomous technology in maritime operations to ensure the safety and reliability of the system.

It is important to note that our study focuses on a relative comparison between unattended and attended bridge operations. The periodic nature of this comparison, with attended bridge voyages followed by unattended voyages, and vice versa, allows us to maintain a consistent and balanced approach. By logically keeping the fault trees and event trees for both scenarios on the same level, we ensure a fair and meaningful comparison of the quantitative risk associated with these operations.

It is noteworthy that the hazards presented in table 5 exhibit similarities with the most critical hazards identified in another recent MASS project, AUTOSHIP (Bolbot et al. (2021)). These shared hazards include, among others, B ZERO’s situational awareness failure, AUTOSHIP’s situational awareness failure, B ZERO’s HMI takeover failure, AUTOSHIP’s ship losing communication with the remote center, and B ZERO’s collision avoidance failure, which aligns with AUTOSHIP’s ship being on a collision track with other ships. The specific probabilities of occurrence for the similar hazards may vary due to differences in methodologies, data sources, or other factors. Nonetheless, the shared highlighted hazards emphasize their importance and underscores the need for further research, collaboration, and continuous improvement in ensuring the safety and reliability of unattended bridge operations.

References

Agency, N. G.-I. (2002). Atlas of pilot charts north atalantic ocean.

Antao, P. and C. Guedes Soares (2006). Fault-tree models of accident scenarios of ropax vessels. *International Journal of Automation and com-*

puting 3, 107–116.

Asami, M. and F. Kaneko (2013). Development of vessel collision model based on naturalistic decision making model. *Collision and Grounding of Ships and Offshore Structures*, 49–56.

BahooToroody, A., M. M. Abaei, O. V. Banda, J. Montewka, and P. Kujala (2022). On reliability assessment of ship machinery system in different autonomy degree; a bayesian-based approach. *Ocean Engineering 254*, 111252.

Baker, C. and D. McCafferty (2005). Accident database review of human element concerns: What do the results mean for classification. In *Proc. Int Conf.'Human Factors in Ship Design and Operation, RINA Feb*. Citeseer.

Beliczey, S. and H. Schulz (1987). The probability of leakage in piping systems of pressurized water reactors on the basis of fracture mechanics and operating experience. *Nuclear engineering and design 102*(3), 431–438.

Bolbot, V., G. Theotokatos, L. Andreas Wennersberg, J. Faivre, D. Vassalos, E. Boulougouris, Ø. Jan Rødseth, P. Andersen, A.-S. Pauwelyn, and A. Van Coillie (2021). A novel risk assessment process: Application to an autonomous inland waterways ship. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 1748006X211051829.

Burmeister, H.-C., W. Bruhn, Ø. J. Rødseth, and T. Porathe (2014). Autonomous unmanned merchant vessel and its contribution towards the e-navigation implementation: The munin perspective. *International Journal of e-Navigation and Maritime Economy 1*, 1–13.

de Boer, R. (2004). *Zuverlässigkeitstechnische Systemanalyse für schiffstechnische Systeme am Beispiel der elektrischen Energieversorgung*. Shaker.

de Ruijter, A. and F. Guldenmund (2016). The bowtie method: A review. *Safety science 88*, 211–218.

Ericson, C. A. et al. (2015). *Hazard analysis techniques for system safety*. John Wiley & Sons.

Ericson, C. A. and C. Ll (1999). Fault tree analysis. In *System Safety Conference, Orlando, Florida*, Volume 1, pp. 1–9.

Estrada, E. and J. A. Rodriguez-Velazquez (2005). Subgraph centrality in complex networks. *Physical Review E 71*(5), 056103.

Floridi, L. (2019). Establishing the rules for building trustworthy ai. *Nature Machine Intelligence 1*(6), 261–262.

Haugen, S. (1993). Probabilistic evaluation of frequency of collision between ships and offshore platforms.

Hermans, F., B. Schrauwen, and T. Dhaene (2017). Sensitivity analysis using salib. *Journal of Open Source Software 2*(9), 97.

IMO (2000). Adoption of the revised performance standards for shipborne combined gps/glonass receiver equipment.

IMO (2018). Revised guidelines for formal safety assessment (fsa) for use in the imo rule-making process.

IMO, M. (2021). Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (mass).

ISO 23860:2022 (2022, May). Ships and marine technology — Vocabulary related to autonomous ship systems. Standard, International Organization for Standardization, Geneva, CH.

Jakkula, B., G. R. Mandela, and M. C. SN (2020). Reliability block diagram (rbd) and fault tree analysis (fta) approaches for estimation of system reliability and availability–a case study. *International Journal of Quality & Reliability Management 38*(3), 682–703.

Jensen, F. (2015). Hazard and risk assessment of unmanned dry bulk carriers on the high seas. Master's thesis, Technical University of Hamburg, Hamburg, Germany.

Lee, P., V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos (2021). Fault tree analysis of the autonomous navigation for maritime autonomous surface ships. In *1st International Conference on the Stability and Safety of Ships and Ocean Vehicles*.

Li, Z., Z. WAng, Y. Ren, D. YAng, and X. Lv (2020). A novel reliability estimation method of multi-state system based on structure learning algorithm. *Eksploatacja i Niezawodność 22*(1), 170–178.

MSC, I. (2007a). 1/circ. 1228 revised guidance to the master for avoiding dangerous situations in adverse weather and sea conditions. *International Maritime Organization, London*.

MSC, I. (2007b). 83/inf. 2 formal safety assessment consolidated text of msc/circ. 1023-mepc/circ. 392. *International Maritime Organisation*.

MUNIN project (2015). D9-3: Quantitative assessment. `http://www.unmanned-ship.org/munin/wp-content/uploads/2015/10/MUNIN-D9-3-Quantitative-assessment-CML-final.pdf`. Accessed on 30 Mar. 2023.

Nielsen, D. S. (1971). *The cause/consequence diagram method as a basis for quantitative accident analysis*. Risø National Laboratory.

OREDA, A. (2002). *OREDA: Offshore Reliability Data Handbook*. OREDA.

Rebaiaia, M.-L., D. Ait-Kadi, and D. Page (2012, 10). Modélisation et évaluation de la fiabilité d'un réseau gouvernemental de radio télécommunication.

Rødseth, Ø. J. and H.-C. Burmeister (2015). Risk assessment for an unmanned merchant ship. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 9*(3), 357–364.

Ugé, C. and S. Hochgeschurz (2021). Learning to swim-how operational design parameters determine the grade of autonomy of ships. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 15*(3).

Van Sciver, G. R. (1989). Guidelines for process equipment reliability data by ccps. In *Reliability Data Collection and Use in Risk and Availability Assessment: Proceedings of the 6th EuReDatA Conference Siena, Italy, March 15–17, 1989*, pp. 104–114. Springer.

Vesely, W. E., F. F. Goldberg, N. H. Roberts, and D. F. Haasl (1981). Fault tree handbook. Technical report, Nuclear Regulatory Commission Washington DC.

Wing, J. M. (2021, sep). Trustworthy ai. *Commun. ACM 64*(10), 64–71.

Zhang, X., Q. Zhang, J. Yang, Z. Cong, J. Luo, and H. Chen (2019). Safety risk analysis of unmanned ships in inland rivers based on a fuzzy bayesian network. *Journal of Advanced Transportation 2019*, 1–15.