CASE STUDY: TESTING OF REDUNDANT OPERATIONAL TECHNOLOGY SYSTEM

Lappeenranta–Lahti University of Technology LUT

Degree Programme in Computational Engineering, Bachelor's thesis

2025

Nea Vilanen

Examiners: Professor Lasse Lensu, D.Sc. (Tech.)

Abstract

Lappeenranta–Lahti University of Technology LUT

LUT School of Engineering Science

Degree Programme in Computational Engineering

Nea Vilanen

Case Study: Testing of redundant Operational Technology system

Bachelor's thesis

2025

39 pages, 11 figures and 3 tables

Examiner: Professor Lasse Lensu, D.Sc. (Tech.)

Keywords: NAPA, NAPA Emergency Computer, NAPA Stability, Redundancy, Redundant environment

The objective of this work is to test the functionality of the NAPA Emergency Computer (NAPA EC) and NAPA Stability in a redundant environment. The study evaluates system performance and data transfer in simulated scenarios where selected NAPA services are intentionally shut down. The work is carried out as a case study of a previous system failure that caused a redundancy error.

Two virtual machines were configured with NAPA EC and NAPA Stability, each running the required services. The test environment simulated realistic vessel conditions in order to evaluate system responses under operationally relevant failures. Eight scenarios were executed by disconnecting services, and system responses, redundancy activation, and synchronization between the primary and secondary systems were analyzed.

The results show that backup systems operated as intended, maintaining reliable data transfer and continuous operation without software errors. NAPA software was therefore found to function reliably under redundant configurations, and, thus, it was not the cause of the studied failure. However, a deeper understanding of the case could be gained through further testing, including integration with vessel automation systems and multiple redundant environments. Overall, the tests confirm the robustness of NAPA software in redundant operation.

Tiivistelmä

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUTin insinööritieteiden tiedekunta

Laskennallisen tekniikan koulutusohjelma

Nea Vilanen

Case-tutkimus: Varajärjestelmällä varustetun operatiivisen teknologiajärjestelmän testaus

Kandidaatintyö

2025

39 sivua, 11 kuvaa and 3 taulukkoa

Tarkastaja: Professori Lasse Lensu, TkT

Avainsanat: NAPA, NAPA Emergency Computer, NAPA Stability, Kahdennettu ympäristö

Tämän työn tavoitteena on testata NAPA Emergency Computerin ja NAPA Stability -ohjelmiston toiminnallisuutta kahdennetussa ympäristössä. Tutkimuksessa tarkastellaan ohjelmiston suorituskykyä ja tiedonsiirtoa simuloiduissa tilanteissa, joissa osa ohjelmistoista on estetty toimimasta. Työ toteutetaan tapaustutkimuksena aiemmasta järjestelmäviasta, joka aiheutti virheen kahdennetussa ympäristössä.

Kaksi virtuaalikonetta asennettiin NAPA EC- ja NAPA Stability -ohjelmistoilla, ja niissä suoritettiin kaikki tarvittavat palvelut. Testiympäristö simuloi realistisia aluksen olosuhteita, jotta järjestelmän toimintaa voitiin arvioida käytännön kannalta merkityksellisissä vikatilanteissa. Kahdeksan skenaariota toteutettiin sulkemalla palveluita, ja järjestelmän vasteet, kahdennuksen aktivoituminen sekä synkronointi ensisijaisen ja toissijaisen järjestelmän välillä analysoitiin.

Tulokset osoittavat, että varajärjestelmät toimivat suunnitellusti ja tiedonsiirto säilyi luotettavana, mikä varmisti keskeytymättömän toiminnan ilman ohjelmistovirheitä. NAPA-ohjelmiston havaittiin siis toimivan luotettavasti kahdennetussa kokoonpanossa, ja sen osallisuus tutkittuun vikaan voitiin sulkea pois. Kuitenkin tapauksen syvällisempää ymmärrystä voitaisiin parantaa edelleen laajentamalla testejä esimerkiksi aluksen automaatiojärjestelmän integroinnilla ja useampien kahdennettujen ympäristöjen arvioinnilla. Yhteenvetona suoritetut testit vahvistavat NAPA-ohjelmiston toimintavarmuuden kahdennetussa ympäristössä.

Abbreviations

Abbreviations

CBS	Computer Based Systems
CMF	Common Mode Failure
DSS	Decision Support System
EC	NAPA Emergency Computer
IMO	International Maritime Organization
IT	Information Technology
NSIA	Norwegian Safety Investigation Authority
OCIMF	Oil Companies International Marine Forum
OT	Operational Technology
SOLAS	Safety of Life at Sea
SPOF	Single Point of Failure
SRtP	Safe Return to Port
VM	Virtual Machine
WTD	Watertight Door

Table of contents

List of Figures

List of Tables

1 Introduction

The maritime passenger industry is experiencing significant growth, with cruise ships, ferries, and other vessels carrying millions of travelers around the world, as presented in Figure 1. This surge in demand highlights the popularity of cruise travel as a preferred form of leisure and underscores the importance of safety, efficiency, and reliability in maritime operations (CLIA, 2025). As ships become larger and more technologically complex, ensuring uninterrupted performance of onboard systems is critical to maintaining operational safety and passenger confidence.

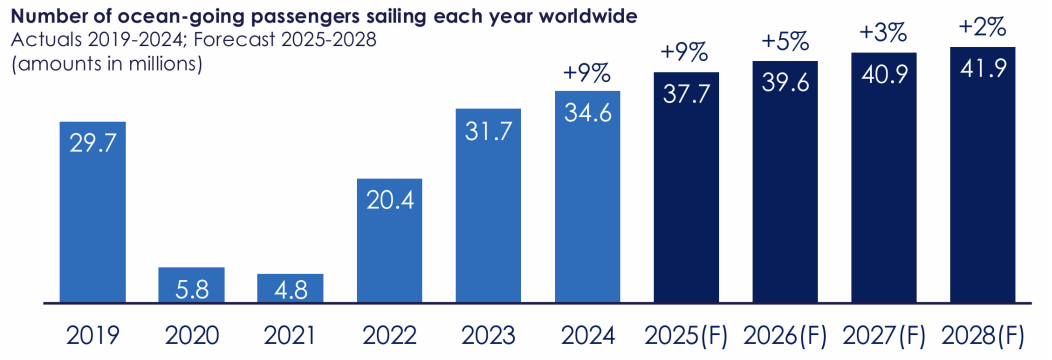

Figure 1: The growth and forecast of ocean-going passengers (Association, 2025).

Despite the deployment of advanced technologies, machine failures, including power losses and blackouts, remain frequent causes of maritime incidents, particularly on passenger vessels where thousands of passengers and crew are affected (Marine Safety Consultants, 2024). To reduce these risks, ships are equipped with decision support systems (DSS) and redundant technical architectures. DSS solutions provide real-time situational awareness and guidance to crew (Sauter, 2010), while redundancy ensures that vital systems, such as propulsion, power generation and stability management, continue to operate even if one component fails (Downer, 2009). High-profile incidents such as the Viking Sky blackout in 2019 (Ibrion, Paltrinieri & Nejad, 2021) and the Dali collision in Baltimore in 2024 (Marine Safety Consultants, 2024) illustrate that even these safeguards do not always guarantee resilience in practice, highlighting the need for further research on redundancy implementation and DSS performance.

In this context, applications such as NAPA Emergency Computer and NAPA Stability, developed by NAPA Ltd., play a crucial role in monitoring ship status, identifying vulnerabilities, and supporting operational decision-making. By providing reliable information, these systems help crew maintain safety and manage risks during both routine operations and emergencies. This thesis focuses on evaluating the performance of such systems under redundancy scenarios to ensure continuous functionality and robust decision support during

critical onboard operations.

1.1 Background

NAPA is a Finnish software and data company that delivers digital solutions to the global marine industry. Established in 1989 and with its headquarters in Helsinki, the company has become a leading provider of ship design, stability management, and operational safety tools. Its products cover stability management, emergency support, voyage and stowage planning, and fleet efficiency optimization. These solutions are designed to support both routine vessel operations and critical situations, such as flooding or stability loss, by providing reliable data for safe and efficient decision-making. With a worldwide presence and customers ranging from shipowners and operators to classification institutions and shipyards, NAPA has an important role in enhancing safety, sustainability and efficiency in the maritime sector. (NAPA, 2025.)

NAPA systems are designed to operate in redundant environments, where multiple machines ensure continuous and reliable functionality. However, in certain situations, vessels may experience failures when a primary machine loses connection and the system does not seamlessly transfer to a secondary or redundant unit. Such malfunctions can lead to operational delays, illustrating how even minor disruptions in redundancy mechanisms can have significant consequences for overall performance. Such events emphasize the importance of comprehensive testing to verify that NAPA systems maintain uninterrupted performance, effectively manage service failures, and consistently support vessel safety within redundant configurations.

Previous research on NAPA software redundancy was carried out internally by NAPA, focusing mainly on NAPA Stability, which runs on a single server. Although the tests included three redundant systems instead of two, the evaluations did not indicate any critical issues. NAPA Emergency Computer (NAPA EC) is dependent on multiple interconnected services, making its redundancy more complex. This highlights the need to include NAPA EC in independent testing, as failures in any component can disrupt the overall operation of the system. The case studied in this thesis involved redundancy issues with NAPA EC, emphasizing the importance of a thorough evaluation to ensure reliable performance and decision support during critical onboard situations.

1.2 Research objectives and delimitations

This thesis focuses on NAPA software, specifically NAPA Emergency Computer and additionally NAPA Stability, which are decision support systems designed to facilitate decision-

making onboard vessels during emergencies. These NAPA systems operate within a redundant environment, where multiple machines are configured to ensure continuous operation even if one unit fails. The objective of this research is to

- test different types of scenarios that replicate realistic failure conditions, such as loss of connection or system switchover delays
- evaluate how reliably the NAPA software maintains functionality under redundancy.

The study aims to evaluate not only the ability of the software to provide accurate and timely support to the crew, but also the effectiveness of its redundancy mechanisms in preventing service disruptions during emergencies.

The thesis does not include testing of the ship's automation system, nor does it extend beyond the evaluation of the NAPA software itself. This study uses actual ship-specific data. However, detailed information, including the identity of the vessel and any elements that could reveal it, is not disclosed due to confidentiality requirements.

1.3 Structure of the thesis

This thesis begins with a review of the background literature in Chapter 2, introducing key concepts such as redundancy, vulnerabilities in the maritime domain, and the NAPA software applied in this research. Chapter 3 then presents the methodology of the testing process, including the tools used, the test environment, and the test scenarios. Following this, Chapter 4 introduces the results of the testing process, which are analyzed and discussed in Chapter 5. Finally, Chapter 6 concludes the thesis by summarizing the findings and reflecting on their implications.

2 Literature Review

In this chapter, the concept of redundancy is introduced, with a focus on its role in the maritime industry, its benefits, and the challenges associated with it. Common vulnerabilities related to redundancy issues have been examined, supported by examples of past maritime accidents. Furthermore, the chapter has discussed decision support systems and introduced the NAPA software, which will play a central role in the upcoming testing process.

2.1 Redundancy in maritime systems

Redundancy refers to the use of multiple backup environments to which a system can connect in case of failure (Downer, 2009). In such setup, if the primary environment becomes unavailable, for example, due to a communication error, the system automatically switches over to the next available redundant environment in the sequence, which is illustrated in Figure 2. This ensures continuity of operations. Depending on the design, two or more redundant environments can be configured to provide backup. Redundancy is established through the installation of additional components or systems, or through alternative approaches that ensure the same function can still be carried out. (Wärtsilä, n.d.; Giddings, 2013.)

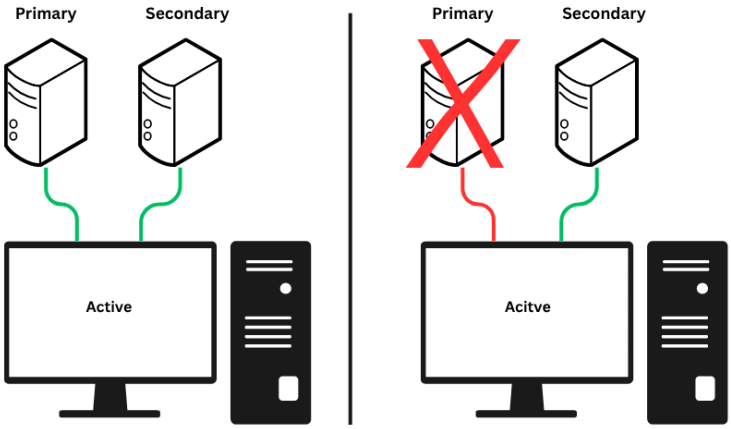

Figure 2: Redundancy with one backup system.

This type of arrangement, where a system is supported by a secondary environment, is called standby redundancy. In this setup, the backup components remain inactive until a failure occurs in the active component, at which point the standby component takes over. Standby configurations can be divided into three categories: cold standby, warm standby, and hot

standby, also known as active-active replication (Nintex, n.d.). The difference between them lies in the possibility of failure while on standby and in their level of readiness to take over. Cold standby describes a situation where the component is completely inactive and cannot fail while idle, activating only after the active component fails. Warm standby refers to a partially active component that runs in the background in a limited state, allowing a faster takeover but still carrying some risk of failure during standby. Hot standby, in contrast, is fully operational in parallel with the active component, meaning it can fail while on standby, but also ensures the fastest possible switchover with minimal disruption (Yang & Wu, 2021). These are presented in Figure 3 below.

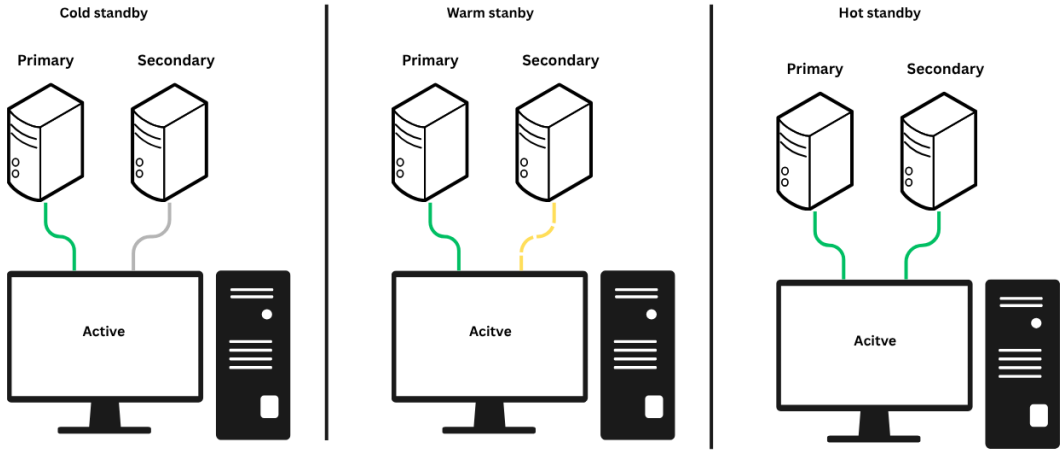

Figure 3: Different types of standbys in redundancy.

2.1.1 Relevance of redundancy

"Imagine being on a ship in a storm at night along a rocky coast. Then you lose all power. A total blackout! For this reason, power systems aboard vessels are often split into parallel redundant units to ensure power production and the ship's safety" (The Switch, n.d.)

Redundancy is important because, as a system, it can reduce the likelihood of failure (Downer, 2009). However, as described by Gardner (2022a), it is important to remember that redundancy itself does not prevent failures. Rather, it means that the vessel is equipped with multiple systems, which are typically required to ensure operational reliability and maintain service continuity. In other words, redundancy may not eliminate failures, but it can significantly improve the overall reliability of a system (Eriksen & Lützen, 2022.)

2.1.2 Standards and regulations

The International Maritime Organization (IMO) established an international maritime treaty called SOLAS, which stands for the Safety of Life at Sea. The purpose of SOLAS is to establish minimum safety regulations in the maritime industry to protect vessels, crew, and passengers (International Maritime Organization, n.d.; International Maritime Organization, 1974). Under SOLAS, a concept known as Safe Return to Port (SRtP) was introduced. This concept applies mainly to cruise ships and addresses situations such as flooding or fires. Its central idea is that even after such an accident, the vessel should be able to return safely to port under its own power, without requiring passengers or crew to abandon the ship. (Gardner, 2022b; Red Ensign Group, n.d.)

SRtP sets specific regulations on machine redundancy to ensure that critical systems remain operational even after a disaster. These systems include

- steering
- propulsion and fuel systems
- navigational systems
- key internal and external communication systems
- fire detection and firefighting systems
- bilge and ballast systems
- flooding detection systems
- power-operated watertight and semi-watertight doors
- systems supporting safe areas
- other equipment essential for damage control.

As mentioned earlier and in previous sources (Gardner, 2022b; Gardner, 2022a), redundancy itself does not prevent blackouts, rather, the SRtP requirements are designed to increase the reliability of these systems within a redundant environment.

2.1.3 Challenges in redundancy

Even with the additional safety provided by redundancy, multiple Common Mode Failures (CMFs) threaten the effectiveness of such systems and may prevent them from achieving the intended level of reliability. These failures may be the result of multiple factors, such as power supply disruptions, software bugs, environmental conditions, or human error (Lerus, 2024). CMFs have the potential to completely compromise redundancy, leading to varying

degrees of operational delay. Such delays can include postponed departures, which in turn may cause customer dissatisfaction, perceived unreliability, and reputational damage. In addition, CMFs can introduce cybersecurity vulnerabilities, increase safety risks, and even result in loss of control of the vessel. In the worst-case scenario, they can contribute to the loss of life at sea if critical data and decision support systems fail to function as required. (Lerus, 2024; Aksoy, 2025; Red Ensign Group, n.d.)

Although redundancy is critical for improving safety and reliability, it also introduces greater complexity into the overall system architecture. Adding additional components inevitably requires more physical space and complicates both installation and maintenance. Furthermore, increasing structural and operational complexity can make it more difficult for operators and engineers to fully understand, verify, and monitor the communication pathways and functionality of the system. (The Switch, n.d.; Downer, 2009.)

2.2 Failure scenarios in Maritime Information Technology and Control systems

Maritime IT and control systems are critical to modern ship operations, enabling propulsion, navigation, cargo handling, and communication. Although these technologies improve efficiency and situational awareness, they also introduce potential vulnerabilities. When triggered, whether by technical failures or cyber incidents, such weaknesses can disrupt operations, endanger safety, and compromise security. This section highlights the most common vulnerabilities, classified into engineering and operational risks and cybersecurity risks, and sets the stage for the following section, which examines real-world cases and the impacts of these failures.

2.2.1 Common vulnerabilities in Maritime

Maritime vessels rely on complex engineering systems to manage propulsion, navigation, power distribution, and control. Although these systems are designed for reliability, they are not immune to failures. The most critical vulnerabilities include blackouts (see Figure 9), single point of failure (SPOF), and limited redundancy, all of which can threaten safety and disrupt operations if not adequately addressed. (Marine Safety Consultants, 2024.)

A blackout is defined as a complete loss of electrical power within the main distribution system of a vessel, usually resulting in the failure of propulsion, steering, and other essential systems. Blackouts can occur due to mechanical failures, such as engine or fuel system malfunctions, electrical faults in generators or switchboards, operational errors, or design shortcomings that limit system resilience. The consequences are severe: vessels can lose

maneuverability, communications and navigational capabilities, increasing the risk of collisions, groundings, or other accidents while also disrupting operations and causing financial losses. (American Bureau of Shipping, 2024.)

Closely connected to blackout risks are single point of failure. A SPOF occurs when the failure of one component can cause an entire system to stop functioning, potentially creating hazardous situations or accidents. These failures may arise from predictable causes, such as design flaws, incorrect installation, poor maintenance, or human errors, as well as unpredictable causes such as manufacturing defects. Examples include mechanical breakdowns, electrical faults, fires, explosions, or flooding, any of which could result in the loss of propulsion or other critical system functions (Oil Companies International Marine Forum (OCIMF), 2018.)

To reduce the risk of SPOFs, ships often use redundancy, duplicating critical systems so that a backup can take over if the main system fails. However, redundancy has limits. Many backups share the same infrastructure, so a single problem can affect all of them. Backups can also fail at the same time due to design flaws, environmental stress, or human error. Regular testing and maintenance are needed to catch hidden problems. Even with redundancy, ships can still fail if hidden SPOFs exist or if too much depends on one operator. (Phillips, 1998; Bambach, 2018.)

While these physical vulnerabilities remain serious, modern ships must also face growing cybersecurity threats. As highlighted by GTMaritime (2022): ships are among the most vulnerable assets imaginable when it comes to cyber threats, since many onboard systems were not originally designed with digital risks in mind. Digital systems now control essential functions, and a successful cyberattack could have effects similar to physical malfunctions, potentially causing blackouts, triggering SPOFs, or disabling redundant backups.

The International Maritime Organization (IMO) defines cyber risk as: *"a measure of the extent to which Computer Based Systems (CBS) are threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised"* (International Maritime Organization, 2025). These risks are amplified by common vulnerabilities that can be found in shipboard systems, including:

- obsolete and unsupported operating systems, unpatched system software
- outdated or missing antivirus software and protection from malware
- inadequate security configurations and best practices, including ineffective network management, the use of default administrator accounts or passwords, and also ineffec-

tive network management which is not based on the principle of least privilege

- shipboard computer networks, which lack boundary protection measures and segmentation of networks
- safety critical equipment or systems always connected with the shore side
- inadequate access controls to cyber assets, networks etc. for third parties including contractors and service providers
- staff inadequately trained and/or skilled to manage cyber risks
- missing, inadequate or untested contingency plans and procedures. (Team, 2019; Shipping, 2017; Shipping, 2021.)

As further emphasized by GTMaritime (2022) many vessels continue to run outdated operating systems, leaving them exposed to known vulnerabilities because patches are no longer available. Ships often operate with a mix of old and new systems that were never designed to work together securely, and crew members may connect personal laptops, phones, or USB devices to onboard networks, bypassing security controls and introducing malware risks.

Even system updates, which should improve security, can create problems if poorly managed. Automatic updates may install incompatible patches or disrupt critical operations, especially when internet connections are limited or unstable. Without proper network segmentation, a flawed update on one system can also spread issues across multiple networks onboard.

Finally, the human factor remains central. Crew members are often the weakest link in cybersecurity, with risks that arise from weak passwords, careless handling of removable media, or falling victim to phishing attacks. At the same time, they are also the strongest line of defense. A well-trained and security-aware crew can identify suspicious activity early, enforce good practices, and follow emergency procedures when incidents occur. This is also stated by Loomis et al. (2021). Training and awareness therefore play a decisive role in reducing cyber risks and ensuring resilience at sea. (GTMaritime, 2022.)

2.2.2 Previous failures and their impact

The maritime industry has faced numerous failures that reveal the vulnerabilities of both mechanical and digital systems. Incidents involving machinery failures, software errors, and inadequate redundancy demonstrate how quickly safety and operations can be compromised at sea. Examining these previous failures provides valuable lessons for improving ship design, operational procedures, OT and IT systems. The following paragraphs highlight several notable cases that illustrate these risks in practice.

The first incident is a blackout involving the Viking Sky cruise ship, which occurred in Norway in March 2019. During this event, the vessel suffered a complete blackout, lost propulsion, and nearly ran aground during a storm (Ibrion, Paltrinieri & Nejad, 2021). The blackout was caused by insufficient lubricating oil in the diesel generators' sump tanks, a situation worsened by the ship's movement in turbulent seas. The investigation also identified a combination of operational, technical, and organizational safety deficiencies that contributed to the incident. According to the Norwegian Safety Investigation Authority (NSIA) report, the vessel should not have departed in the first place given these conditions (Norwegian Safety Investigation Authority (NSIA), 2024). According to the investigation, recovery from the blackout was time consuming and stressful due to limited crew training for such situations. Fortunately, no serious injuries or fatalities occurred.

While the Viking Sky blackout in 2019 is highlighted as a dramatic near-disaster and has been discussed separately, it was not the only incident of that year. Other cruise ships also faced blackout situations, such as the Coral Princess, which suffered a total power loss in Southeast Asia, leaving the vessel without propulsion or essential services for several hours before recovery. Similarly, Holland America's Nieuw Statendam experienced a blackout while departing Puerto Rico, delaying its voyage and alarming passengers. Unlike the Viking Sky case, these incidents did not escalate into full emergencies, but together they underline how even with redundancy, modern cruise ships remain vulnerable to sudden power failures. (Gardner, 2022a.)

Another power loss incident occurred in March 2024 with the Dali container vessel, which led to a collision with a primary support pier of a bridge. This collision resulted in the deaths of six workers and caused the partial collapse of the bridge (Marine Safety Consultants, 2024). The blackout was caused by a loose electrical cable that disrupted the vessel's critical systems. Further investigations indicated that the vessel's transformer and circuit breakers of the vessel were vulnerable to heavy vibrations, a known issue that had not been adequately addressed. In addition, there were concerns that the vessel departed port despite existing electrical and mechanical problems that had not been properly reported or resolved. (Group, 2024; Miller, 2024.)

The Carnival Triumph suffered a major incident in 2013 when a fire broke out in the aft engine room, leading to a total blackout. With power and propulsion lost, the ship was left adrift in the Gulf of Mexico. Essential services such as air conditioning, sewerage, and refrigeration quickly failed, creating extremely difficult conditions on board. Although backup systems were installed, they proved unable to restore critical functions, exposing weaknesses in redundancy and emergency preparedness. The event later became a stark example of how a single technical failure can escalate into a large-scale crisis (Authority & Guard, 2014).

It also showed that properly designed redundancy and well-practiced procedures could have eased recovery and limited the scale of disruption (Gardner, 2022a.)

These incidents highlight that blackouts and system failures remain a persistent risk in maritime operations. They show that even vessels equipped with redundant systems are not immune to accidents, particularly when redundancy is limited, misconfigured, or affected by unexpected conditions. Properly designed redundant systems, along with clear procedures, regular maintenance, and well-trained crews, are essential to reduce the impact of failures and improve ship safety. The Dali collision exemplifies the severe consequences of mechanical failures in congested shipping lanes, highlighting how a single failure can cascade and affect critical infrastructure, such as the fracture-critical Key Bridge. This incident underscores the importance of redundancy, real-time monitoring, and close coordination with port authorities (Marine Safety Consultants, 2024.)

While the examples discussed are significant, they represent only a fraction of accidents related to power loss or redundancy failures. This emphasizes the ongoing need for robust engineering and continuous improvement of safety practices throughout the maritime industry.

2.3 Decision Support and Stability Software

Like described by Bohanec (2003), decision support can be understood differently depending on the context and the people involved. In this work, a Decision Support System (DSS) refers to a computer-based information system that helps organizations make informed decisions by analyzing large amounts of data and providing interactive tools for evaluation and problem solving (Sauter, 2010). These systems are designed to support managerial decision making, allowing decision makers to explore different scenarios and evaluate alternative courses of action without replacing human judgment (Power, 1997). By providing structured support, DSS can improve decision quality, consistency, and speed, particularly in complex or semi-structured situations where human judgment alone may not suffice (Sauter, 2010.)

The key components of a DSS include a data management subsystem to integrate internal and external data, a model management subsystem to perform analyses or simulations, and an interactive user interface that allows managers to manipulate data and evaluate outcomes (Corporate Finance Institute team, n.d.). DSS can be classified into several types, data-driven, model-driven, knowledge-driven, document-driven and communication-driven, each tailored to specific decision-making environments and organizational needs (Vicky Sauter, 2002; Troy Segal, 2025.)

Recent research highlights the integration of DSS with modern business intelligence and real-time analytics, showing how these systems can improve operational efficiency, strategic planning, and overall decision making (Takkinen, 2016). In general, DSSs are crucial tools that combine computational analysis with human judgment, enabling faster, better informed decisions across multiple levels of management and diverse business functions (Sauter, 2010; Troy Segal, 2025.)

In the maritime sector, several specialized DSSs have been developed to improve safety and operational decision-making. Many of these systems were initially designed for naval vessels, where survivability and combat readiness are critical, but their underlying models and technologies are also applicable to passenger ships, as both types share similar structural characteristics (Takkinen, 2016). According to Takkinen (2016), examples of maritime DSS include the Bridge Officer Support System, Battle Damage Control System, Knowledge-Based Decision Support System, and NAPA Emergency Computer (NAPA EC). In addition, new systems are being developed, such as the hybrid DSS for Offshore Operations, which aims to optimize offshore operations, improve safety, and reduce environmental impact (Bakouchi, Dubois & Kerkeni, 2023.)

Overall, these examples illustrate the vital role of DSS in maritime operations, supporting timely and informed decision-making by combining real-time data, predictive modeling, and human judgment. As these systems continue to advance, their primary purpose remains to improve safety, efficiency, and situational awareness in complex and uncertain conditions. Building on this foundation, the next chapter focuses on specialized maritime software, including the NAPA Emergency Computer (NAPA EC), which demonstrates how DSS can be applied specifically for ship stability, damage assessment, and operational support in critical scenarios.

2.3.1 NAPA Emergency Computer

The NAPA Emergency Computer (NAPA EC) is a decision support system designed for cruise ships to monitor vessel vulnerability under normal conditions and provide survivability predictions in flooding emergencies. It is designed to continuously assess the vulnerability of the ship by integrating with the vessel automation system, monitoring tank and dry space sensors, watertight doors (WTD), sea conditions, and current loading condition through NAPA Stability. The system uses Vessel-TRIAGE categorization to visualize the overall vulnerability, providing the crew with clear indicators of the condition of the vessel.

Vessel-TRIAGE is the rapid assessment of a ship's condition after an incident, such as flooding, fire, or structural damage, with the aim of prioritizing actions that ensure safety and

stability. It focuses on things like stability, watertight integrity, and how serious the damage is. The process helps the crew decide whether to stabilize the vessel, contain the damage, or prepare for evacuation. Vessel-TRIAGE is divided into four levels (green, yellow, red, black) which are explained in more detail in Figure 4 (Nordström et al., 2016.)

GREEN	YELLOW	RED	BLACK
Vessel is safe and can be assumed to remain so	Vessel is currently safe, but there is a risk that the situation will get worse	Level of safety has significantly worsened or will worsen and external actions are required to ensure the safety of the people aboard	Vessel is no longer safe and has been lost
GENERAL SITUATION - The situation aboard is stable. Although the vessel may have been damaged by the accident, this damage does not threaten its seaworthiness or the people aboard. - The damage to the vessel has been assessed. It is highly unlikely that the damage will spread or get worse. - The vessel still protects the people aboard against the prevailing conditions.	**GENERAL SITUATION** - Damage to the vessel might affect its seaworthiness or the full extent of the damage has not as yet been determined. - Internal damage control measures and rescue operations have not been completed. Damage control is possible with reasonable resources available to carry out the proper measures. - Damage to the vessel may pose a direct or indirect threat to the people aboard.	**GENERAL SITUATION** - The vessel is significantly damaged, affecting its seaworthiness, and there is a threat to the people aboard. - A fire, leak or other damages to the vessel are not under control and escalation is highly likely. - The vessel no longer protects the people aboard against the prevailing conditions. - Major external resources are required.	**GENERAL SITUATION** - The vessel is capsized, broken, sunk, burnt or otherwise damaged so badly that it no longer provides protection to the people aboard against the prevailing conditions (that is, the vessel has totally lost its seaworthiness). - Even if the vessel is still completely or partly afloat, it is no longer safe to work aboard, even to save human lives.

Figure 4: Vessel-TRIAGE (Nordström et al., 2016).

In emergency situations, such as flooding detected by sensors or manually defined breaches, NAPA EC activates an emergency mode and predicts the progression of flooding, estimating the survivability of the vessel over the next hours. Although the system does not give specific instructions, such as counter-flooding measures, it provides advisory cards containing a general checklist for flood emergencies.

The NAPA EC interface presents the current vulnerability of the vessel, the flooded compartments, the predicted breaches, the floating position, the total flooded volume, and a sur-

vivability meter. A timeline of critical events and heel prediction graphs further support situational awareness, helping the crew monitor the vessel's status and anticipate potential risks during normal operations and emergencies. (NAPA, 2025.)

2.3.2 NAPA Stability

NAPA Stability is a widely used and trusted stability and safety management solution, recognized as a global standard in the maritime industry. It is a certified loading instrument onboard, compliant with the requirements of the relevant classification society. NAPA Stability is specifically designed for passenger vessels to ensure compliance with international regulations, such as Safe Return to Port (SRtP), while maintaining a user-friendly interface.

NAPA Stability provides accurate 3D calculations for a wide range of stability management functions, including intact and damage stability analysis, loading condition evaluation, floating position, trim optimization, and compliance with statutory stability criteria. The NAPA Emergency Computer (NAPA EC) relies on NAPA Stability for these calculations, illustrated in Figure 5, using its advanced 3D stability and safety management capabilities to assess vessel condition and support real-time decision-making. The system also features clear visual indicators and warnings that highlight the current condition of the vessel. (NAPA, 2025.)

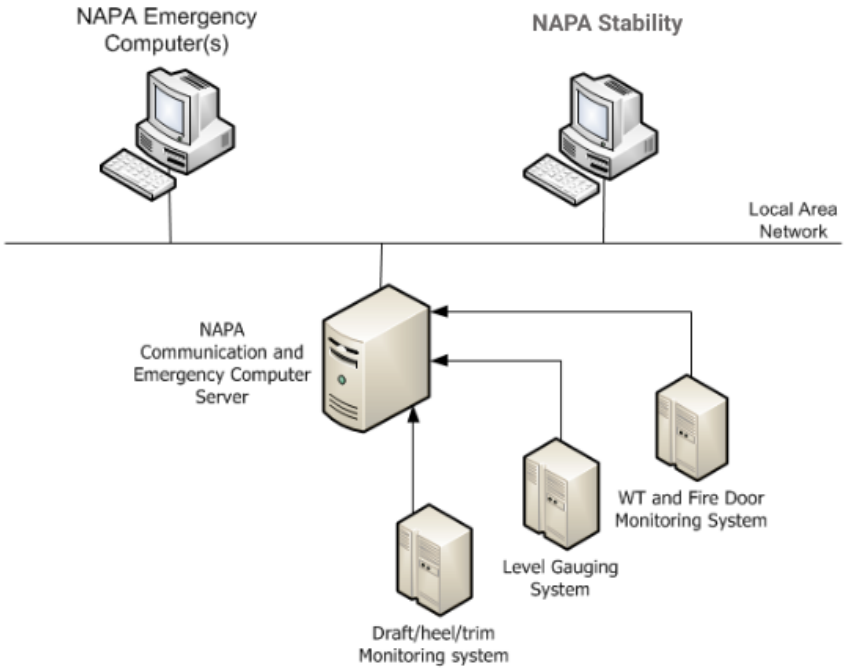

Figure 5: The Architecture between NAPA Emergency Computer (NAPA EC) and NAPA Stability (NAPA, 2025).

3 Methodology of the Case Study

The methodology of this case study is structured to evaluate the performance of NAPA services and NAPA software within a redundant environment. The aim is to determine how effectively systems function under simulated failure conditions and whether redundancy mechanisms ensure continuous operability during emergencies. To achieve this, the methodology is divided into three key parts: an explanation of the NAPA services involved in the study, a description of the setup of the test environment, and the definition of the test scenarios used to replicate real-life failures.

3.1 NAPA Services

NAPA services are background components that manage communication and data exchange between different software modules and ship systems. They are essential for the reliable operation of both the NAPA Emergency Computer and the NAPA Stability. In this context, the services are referred to as server, communication service and data broker, while their detailed roles are not elaborated upon as they are not essential to the work.

3.2 Test Environment

In order to conduct realistic testing, it is essential to have access to detailed information about the vessel and its specific ship 3D model. This ensures that the simulated scenarios would closely reflect the actual operational conditions.

3.2.1 Setting up redundant environment

To establish a secure and controlled testing environment, two separate virtual machines were created to represent the primary and secondary systems. The primary system works under normal conditions, and the secondary system gets activated if and when at least one of the NAPA services shuts down.

Server is a critical component required for both NAPA EC and NAPA Stability to function. In the default configuration, the primary server exclusively communicates with the user interfaces, NAPA EC Client and NAPA Stability Client. If the primary server loses connection to either client, the system automatically triggers the secondary server to take over after a short delay.

Before starting the testing process, each server was checked to confirm proper operation. This was achieved by installing and configuring one server at a time. When the second server was installed, the first server was shut down and restarted to validate the switchover

process. In addition, server priority settings were reviewed to ensure that both systems were active participants in the network and that the secondary server could reliably take over the role of the primary server when required.

3.2.2 Installations

Each virtual machine (VM) was equipped with installations of both NAPA EC and NAPA Stability. Following successful installation, all necessary NAPA services, including server, communication service, and data broker, were activated to enable full system functionality.

Once the server components were operational, NAPA EC Client and NAPA Stability Client, were launched and verified to be functioning correctly. At this stage, the environment was fully configured and ready to proceed with the planned test scenarios.

To modify the vessel conditions during the tests, scenarios could be created directly in NAPA EC or in NAPA Stability. For example, watertight doors could be opened, breaches could be simulated through NAPA EC, and the floating position of the vessel could be adjusted via NAPA Stability. Any changes made in NAPA Stability are automatically transferred to NAPA EC, however, the process does not work in reverse: modifications made in NAPA EC do not affect NAPA Stability, since NAPA EC operates as a decision support tool that relies on the information provided by NAPA Stability.

A diagnostic tool was also available as an additional option, and in many cases it simplified the testing process by providing a single interface with fewer manual steps compared to the standard client applications. In this setup, as with direct use of NAPA EC, no changes made in the diagnostic tool affected NAPA Stability. For these reasons, all tests were performed using the diagnostic tool, and after each modification, the results were verified in NAPA EC to ensure that the updates were correctly applied and displayed.

After the test environment was established as described, a clear distinction between the primary and secondary virtual machines was created. This was done by applying a small modification to the configuration of the secondary machine, making it easily identifiable during testing. In this case, WTDs were set to open on the secondary machine, triggering warning messages on the NAPA EC, while the primary machine operated without any modifications to the vessel's integrity, as illustrated in Figure 6 and Figure 7 below. This provided a clear visual difference between the two systems.

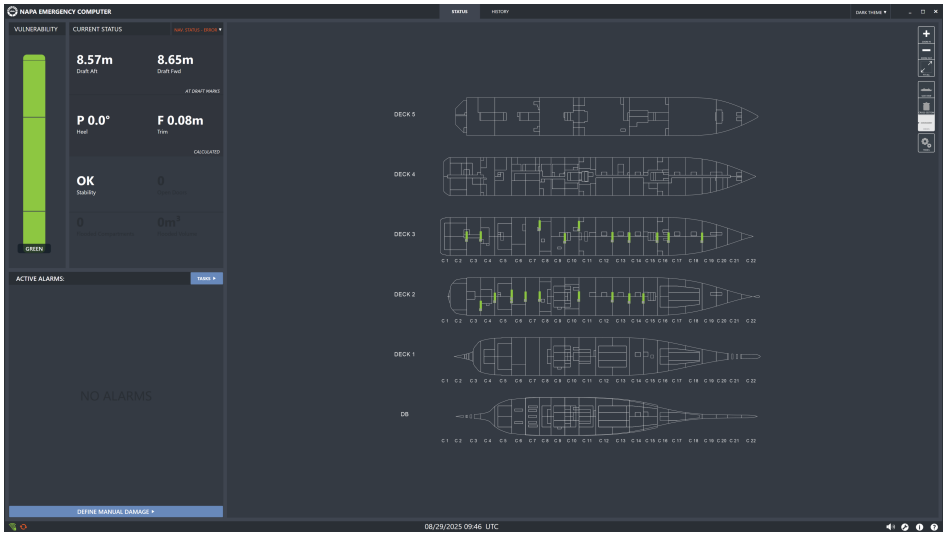

Figure 6: Primary virtual machine view under redundancy.

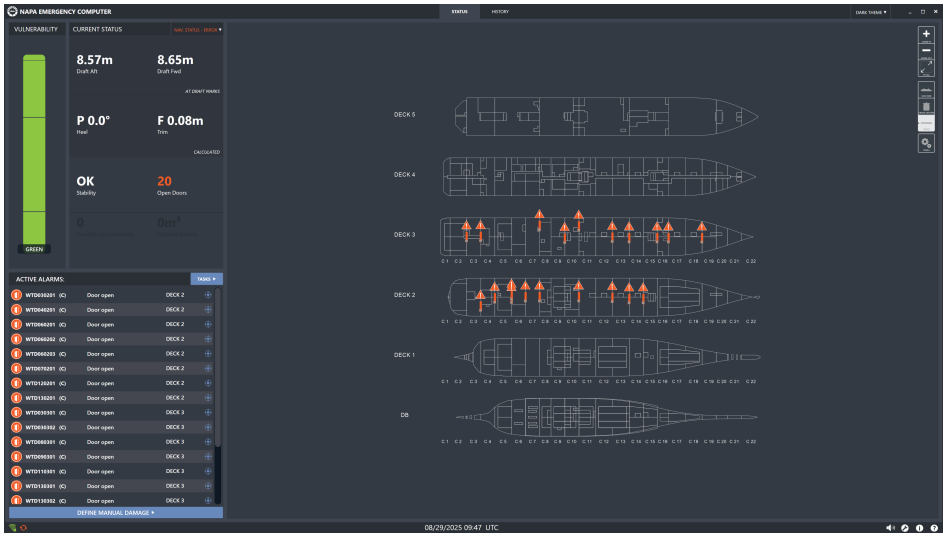

Figure 7: Secondary virtual machine view under redundancy.

3.3 Test Scenarios

The testing is classified into two categories: normal conditions and failure conditions. In this thesis, normal conditions refer to situations where all primary services are connected, whereas failure conditions occur when one or more services are disconnected. The main objective is to confirm that the NAPA services operate correctly under both circumstances.

Testing begins under normal conditions, with all NAPA services running and connected to the primary computer. In this state, both virtual machines are expected to receive data from the primary system and display vessel information consistently, without warnings or errors. The system configuration is then gradually adjusted to simulate different scenarios, ensuring that all changes are accurately reflected on both machines. These adjustments include modifying

the floating position of the vessel, opening and closing different combinations of WTDs, creating breaches, and altering the flood volume.

Changes in floating position include adjusting the draft, which determines how deep the vessel sits in the water. This can be simulated by adding or removing weight from the vessel. Another option is to adjust the trim, which refers to the vessel's longitudinal balance, meaning the vessel tilts forward or backward. The heel can also be modified, representing a sideways tilt instead of a longitudinal one. These adjustments are typically achieved by changing the amounts in the liquid tanks or simulating flooding on one side of the vessel. Such changes trigger warnings in the stability system if they fall outside the acceptable range for the specific vessel, triggering the vulnerability in the NAPA EC.

With WTDs, different scenarios can be created by varying both the number of doors that are open and their specific locations within the vessel. Breaches and flood events can also be simulated by assigning attributes such as breach size and flood volume, to represent the severity and extent of the situation. When WTDs are open, NAPA EC generates a warning list identifying each problem as seen in Figure 7. In addition, the visualization of the vessel model highlights the location of each WTD and displays a warning message next to every open door. However, creating a breach and modifying the flood volume activates the prediction calculation, which estimates how flooding will spread throughout the vessel and how it will affect the vessel's integrity, including heel and trim. The system also indicates whether evacuation may become difficult or impossible and whether the vessel is at risk of capsizing.

With all changes applied, NAPA EC should update the parameters identically on both virtual machines while maintaining their connection to the primary system. Since the secondary virtual machine is not connected, any local modifications to it should have no effect. Under these conditions, no warnings or errors are expected, and all updates from the primary system should be consistently reflected on both machines, demonstrating accurate and reliable data synchronization in normal operation.

To achieve the test objectives, multiple scenarios are created by running all possible combinations of NAPA services on the primary machine. These combinations are illustrated in Table 1 below. Testing begins with all services active, after which each service is shut down individually while adjustments to the vessel's parameters are carried out, which are presented in Table 2. In the first scenario, only the primary server is disconnected, and all modifications, such as changes to WTDs, floating position, and other vessel parameters, are performed under this condition. Once the server is reconnected, the process continues by shutting down communication service, followed by data broker, with the same set of simulations repeated for each case. Additional scenarios involve shutting down multiple services

simultaneously, including: server and communication service, server and data broker, communication service and data broker, and finally all services at once. In total, eight scenarios are executed to observe the system's behavior under different service configurations.

Table 1: Simulated test combinations.

Scenario	**Primary Server**	**Primary communication service**	**Primary data broker**
1	on	on	on
2	off	on	on
3	on	off	on
4	on	on	off
5	off	off	on
6	off	on	off
7	on	off	off
8	off	off	off

Table 2: Test scenarios.

Test ID	Parameter	Description / Action
L-001	Floating position	Adjusting draft, heel and trim by adding and removing liquids in ballast and heeling water tanks in the vessel
L-002	Breach	Creating breaches to different parts of the vessel and adjusting their size
L-003	WTD	One or more watertight doors are opened/closed
T-001	Server	primary server off
T-002	Server	Secondary server off
T-003	Server	Secondary server on
T-004	Server + L-001 to L-003	Vessel parameter changes made while primary Server off
T-005	Communication service	Primary communication service off
T-006	Communication service	Secondary communication service off
T-007	Communication service	Secondary communication service on
T-008	Communication service + L-001 to L-003	Vessel parameter changes made while primary communication service off
T-009	Data broker	Primary data broker off
T-010	Data broker	Secondary data broker off
T-011	Data broker	Secondary data broker on
T-012	Data broker + L-001 to L-003	Vessel parameter changes made while primary data broker off
T-013	Server + Communication service	Primary server + communication service off
T-014	Server + Communication service	Secondary server off
T-015	Server + Communication service	Secondary server on
T-016	Server + Communication service + L-001 to L-003	Vessel parameter changes made while primary server and communication service off
T-017	Server + Data broker	Primary server + data broker off
T-018	Server + Data broker	Secondary server off
T-019	Server + Data broker	Secondary server on
T-020	Server + Data broker + L-001 to L-003	Vessel parameter changes made while primary server and data broker off
T-021	Communication service + Data broker	Primary communication service + data broker off
T-022	Communication service + Data broker	Secondary data broker off
T-023	Communication service + Data broker	Secondary data broker on
T-024	Communication service + Data broker + L-001 to L-003	Vessel parameter changes made while primary communication service and data broker off
T-025	Server + Communication service + Data broker	Primary server + communication service + data broker off
T-026	Server + Communication service + Data broker	Secondary server off
T-027	Server + Communication service + Data broker	Secondary server on
T-028	Server + Communication service + Data broker + L-001 to L-003	Vessel parameter changes made while primary server, communication service and data broker off

4 Results

This chapter presents the performance of each test case described in the previous chapter under the defined circumstances. The scenarios are categorized into two conditions that are subject to review, normal condition, and simulated failure.

4.1 Performance in normal conditions

Testing of the redundant environment began under normal conditions. In this state, both virtual machines ran identical simulations, no warnings or error messages were generated, and all vessel parameters remained stable and consistent.

The second scenario for testing redundancy under normal conditions involved actively modifying vessel parameters. These modifications included adjusting the floating position by altering the draft, trim, or heel; opening and closing WTDs; creating breaches; and varying the flood volume.

Similarly to the first scenario, all modifications were automatically transmitted to both virtual machines. Changes in parameters such as floating position and flood volume were updated immediately after saving the attributes in the diagnostic tool, with real-time updates visualized in the client applications as they occurred. Breaches, corresponding flood volumes, and changes in the WTDs appeared after a short delay of around three seconds. In particular, the secondary machine consistently displayed the updated information with the same delay compared to the primary machine.

Finally, modifications were performed on the secondary virtual machine to verify that the changes made there would not affect the primary system or cause any parameter conflicts. None of the adjustments executed on the secondary machine appeared in the primary system. The service connections and vessel parameters remained properly isolated and the redundant environment maintained integrity under these conditions.

4.2 Performance under simulated failures

The test results for the simulated failure are divided into four categories to simplify the different test scenarios. These categories are individual server failure, communication service failure, data broker failure, and lastly combinations of different service failures.

4.2.1 Simulated Server failure

When the primary server was disconnected, the secondary server took over. In this situation, no visual changes occur in NAPA EC or NAPA Stability and information continues to flow through the primary virtual machine without interruption. Additionally, this transition did not trigger any server-related warnings in NAPA EC user interface, as the secondary server assumed control after a brief delay of approximately 30 seconds.

NAPA also has an additional application to monitor any warnings related to service communications (see Figure 10). However in this research the focus is on the NAPA EC user interface and because no server error indications were observed, the secondary server was shut down to verify whether the primary server would disconnect. When both servers were turned off, a warning bar appeared stating “Connection to server is lost” (see Figure 11). After reconnecting the secondary server, the connection to the system was restored and the error message disappeared.

Even when the vessel parameters are modified in the same manner as under normal conditions, both virtual machines update, with the secondary machine reflecting the changes after a short delay. Similarly, breaches, flood modifications, and changes in WTDs appear after a few seconds, and no new irregularities or unexpected behaviors were observed.

4.2.2 Simulated Communication Service failure

Similarly to the scenario where the primary server was disconnected, when the primary communication service went offline, the secondary communication service automatically took over. In contrast to the previous server test, both virtual machines then reflected the secondary as active, and as a result, the open WTD warnings became visible (Figure 7). However, when the secondary communication service was disconnected, the message “Server error, information is out of date” appeared. Once the communication service was reconnected, the connection was restored and the error message disappeared.

Since the secondary communication service functioned as the primary, changes in the vessel parameters were applied on the secondary virtual machine. All modifications were updated and in contrast, the changes made in the primary virtual machine had no effect on the current environment.

4.2.3 Simulated Data Broker failure

When the primary data broker disconnects, the secondary takes over. Here, a coupled switchover was observed. At this point, the open WTD errors are displayed as Figure 7 on page 24 shows, consistent with the modifications previously observed in the communication

service system.

The environment continued to operate without errors or connection issues. The NAPA EC Client also confirms that the required connections are working, displaying both the primary and secondary addresses, as well as the address currently in use, which corresponds to the secondary system. This is illustrated in Figure 8 below.

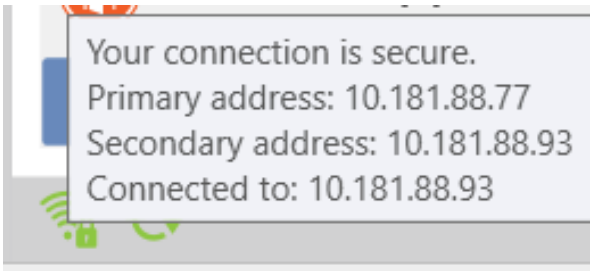

Figure 8: Connections on secondary address.

Even though the system confirmed the connection switch to the secondary address, the secondary was also disconnected as a precaution. In this case, the error "Connection to server is lost" appeared, but after reconnecting the data broker, the error message disappeared and the connection was restored. All modifications to the vessel parameters on the secondary virtual machine were updated, while changes made on the primary, had no effect.

4.2.4 Simultaneous service failures

As described in the test scenario section, all service combinations were tested, which included four additional test scenarios.

The first scenario involved disconnecting the server and communication service simultaneously. Both servers were initially shut down to confirm the disconnection, which resulted in the "Connection to server is lost" error message. The secondary server was then reconnected, clearing the error message. The primary communication service was then disconnected, causing the system to switch to the secondary communication service, displaying warnings for the open WTDs. Changes made to the status of the vessel on the secondary virtual machine were updated identically on both machines. No additional observations were made in this scenario.

The second scenario involved disconnecting the server and the data broker. The test again began by disconnecting and reconnecting the server, which produced the same results as before, including the "Connection to server is lost" message. The data broker was then disconnected, with each virtual machine displaying which data broker was connected in NAPA EC. Both machines showed a connection to the secondary. The communication service also switched

in the same manner as in the single-service disconnection tests. Then both virtual machines displayed the secondary communication service, showing warnings for the open WTDs. All vessel status modifications made on the secondary machine were updated identically on both virtual machines, though again with a short delay on the primary machine. Additionally, any changes made on the primary virtual machine had no effect on the parameters.

In the third scenario, the data broker and the communication service connections were disconnected one by one. The test began by disconnecting the communication service connection and confirming the switch from the primary to the secondary system, as indicated by all open WTD warnings. The primary data broker was then shut down, after which both virtual machines in NAPA EC showed that the connection was maintained through the secondary data broker. When the secondary data broker was also disconnected, the error "Connection to server is lost" appeared, and it disappeared once the secondary data broker was reconnected. All changes made on the secondary virtual machine were successfully updated on both virtual machines, with a short delay on the primary machine. In contrast, any changes made on the primary machine were not reflected on either virtual machine.

The final scenario involved disconnecting all services simultaneously. The test proceeded in the usual order, starting with the servers, followed by the communication service, and finally with the data broker. Shutting down all primary services resulted in no server errors, a connection to the secondary data broker and communication service, and the secondary system being displayed on each virtual machine, with warnings for the open WTDs. The test results were consistent with those of the previously run scenarios: all vessel status changes updated identically on both machines, with updates originating from the secondary machine, and the primary virtual machine reflecting the changes with a short delay.

5 Discussion

This chapter presents a detailed comparison between the expected results and the actual results of the tests conducted, highlighting any deviations and their potential impact on the case study. It examines how the system performed under various scenarios, including normal operation and service failures, and evaluates the reliability and consistency of data across redundant virtual machines. In addition, the chapter discusses lessons learned from the testing process and explores potential strategies to improve future testing, including more comprehensive scenario coverage, stress testing, and validation of automation and manual override procedures.

5.1 Data transfer reliability

After performing all the test scenarios defined earlier and comparing the outcomes with the expected results, 29/31 test scenarios passed with total success and the remaining 2/31 with partial success as seen in Table 3. This confirmed that the redundant environment generally performed as intended, with seamless transitions between primary and secondary systems and consistent data across both virtual machines.

The observed exceptions occurred with the data broker. In these scenarios, the expected outcome was that the system would continue to operate normally with only the data broker switching, while all other services remained unaffected. Instead, the communication service was also triggered, resulting in a transition from the primary system to the secondary communication service system. This unexpected switch was visible through the open WTD warnings, which indicated that the system had moved to the secondary environment (Figure 7).

Despite this deviation, the overall functionality of the system was not compromised. Data transfer continued smoothly without interruptions, both virtual machines remained synchronized, and EC shows the connection to the secondary data broker address as expected. For this reason the test results are shown as “Partial success” in Table 3. However, this outcome highlights the robustness of the redundant setup while also underlining the importance of validating individual service behaviors, to ensure predictable and reliable system responses under all conditions.

Across all test scenarios, the data transfer was stable and reliable. Updates were propagated identically across both systems. The only minor difference was a short delay in the inactive virtual machine, after which the data aligned fully with the active system. Also the delay when switching the server from primary to secondary is justified and has no practical im-

pact, as the system attempts to reconnect to the primary server without causing unnecessary switchovers or error notifications, which would otherwise appear in the system monitor, as illustrated in Figure 10.

Although NAPA has an additional system monitoring tool for tracking all warnings, it would be beneficial, at least from a testing perspective, for NAPA EC to display a notification during extended service interruptions. This would allow the user to see at all times which address each service is connected to, similarly to Figure 8, which would also reduce the number of steps required for this type of testing. Furthermore, the error messages could be formulated more clearly so that the user can immediately identify which service is experiencing connection issues directly from the NAPA EC Client.

5.2 Future research

For future research, it would be valuable to continue testing with multiple redundant systems, simulating configurations with several machines. Continuing these tests would allow for the assessment of cascading failures, in which the primary system fails, followed by the secondary system, with the tertiary system taking over. Furthermore, extending the testing to include all possible combinations of service failures, whether simultaneous or staggered, could provide a more comprehensive understanding of system behavior under extreme operational conditions.

Integrating tests with the automation and control system would be beneficial for improving reliability and performance. This should include scenarios involving high data volumes, as well as stress and load testing. Such testing helps detect interoperability issues, measure precision and responsiveness during failures, and verify that systems react appropriately under unexpected conditions.

Moreover, maximizing automation in future testing would facilitate systematic repetition of test scenarios. This would minimize reliance on manual execution while ensuring comprehensive validation of the system across a wide range of operational conditions.

Table 3: Test results.

Test ID	**Expected Outcome**	**Success rate**
L-001 to L-003	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM : no effect	Success
T-001	Switch to secondary server, no visual changes	Success
T-002	No connection to server -error	Success
T-003	Server -error disappears and connection returns	Success
T-004	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success
T-005	Switch to secondary communication service and secondary virtual view appears on both virtual machines	Success
T-006	Server error, information is out of date -error	Success
T-007	Server -error disappears and connection returns	Success
T-008	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success
T-009	Switch to secondary data broker, no visual changes, EC shows connection to secondary data broker address	Partial success
T-010	Connection to server is lost -error	Success
T-011	Server -error disappears and connection returns	Success
T-012	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success
T-013	Switch to secondary server and communication service, secondary virtual view appears on both virtual machines, no server error	Success
T-014	No connection to server -error	Success
T-015	Server -error disappears and connection returns	Success
T-016	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success
T-017	Switch to secondary server and data broker, no visual changes, EC shows connection to secondary data broker address, no server error	Partial success
T-018	No connection to server -error	Success
T-019	Server -error disappears and connection returns	Success
T-020	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success
T-021	Switch to secondary services, secondary virtual view appears on both virtual machines, EC shows connection to secondary data broker address	Success
T-022	Connection to server is lost -error	Success
T-023	Server -error disappears and connection returns	Success
T-024	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success
T-025	Switch to secondary services, secondary virtual view appears on both virtual machines, EC shows connection to secondary data broker address, no server error	Success
T-026	No connection to server -error	Success
T-027	Server -error disappears and connection returns	Success
T-028	Changes made in active VM: reflects on both virtual machines identically, Changes made in inactive VM: no effect	Success

6 Conclusion

This thesis focused on a case where a redundant system failed to maintain smooth operation and continuous data flow, resulting in a system blackout and delayed vessel departure. The objective was to test all possible combinations of NAPA service disconnections using NAPA software, including the NAPA Emergency Computer (NAPA EC) and NAPA Stability, to ensure the reliability of NAPA systems and their ability to maintain vessel safety and continuous operation under all conditions.

Despite extensive standard testing procedures, previous research on NAPA software redundancy was performed internally, primarily utilizing NAPA Stability, which requires only the server to operate. Although three redundant systems were tested instead of two, no errors were detected in the redundant setup. This highlights the importance of including the NAPA EC in the testing project, as it relies on multiple NAPA services working together. Furthermore, the case studied in this thesis involved redundancy issues specifically related to NAPA EC, which made its inclusion essential for a comprehensive evaluation.

The testing was carried out by evaluating all combinations of NAPA services along with various modifications to the vessel parameters, such as adjusting the floating position, opening and closing different combinations of watertight doors (WTDs), creating breaches, and changing the flood volume. Most of the results aligned with expectations, with the only notable finding being that some of the services reacted to each other's state changes. Specifically, when the data broker switched from the primary to the secondary system, it also caused the communication service to switch. Despite this unexpected interaction, data transfer remained reliable, and no software errors occurred.

It can be concluded that NAPA operates reliably under redundant configurations and that the tests did not reproduce a NAPA software fault in the studied scenarios. Although such incidents may occur, it remains crucial to investigate their root causes and to expand or adjust the focus of future testing. In general, based on this evaluation, the study demonstrated the efficiency and reliability of NAPA software and its services under redundant conditions.

References

Aksoy, I. (2025). *Software Integration Hell in the Maritime Industry*. Cited: 2025-08-25. URL: https://www.vibylabs.com/software-integration-hell-in-the-maritime-industry/.

American Bureau of Shipping (2024). *Blackout awareness and prevention on ships: technical and operational advisory*. Advisory. American Bureau of Shipping.

Association, C. L. I. (2025). *State of the Cruise Industry Report 2025*. Cited: 2025-10-07. URL: https://cruising.org/sites/default/files/2025-07/State%20of%20the%20Cruise%20Industry%20Report%202025.pdf.

Authority, B. M. & Guard, U. S. C. (2014). *The commonwealth of the Bahamas and The United States of America*. Investigation report. London, UK: Bahamas Maritime Authority.

Bakouchi, O. E., Dubois, H. & Kerkeni, S. (2023). Hybrid Decision Support System for Improved Offshore Operation Planning. In: *Proceedings of the 2023 MTS Dynamic Positioning Conference*. Houston, TX, USA: Marine Technology Society. URL: https://dynamic-positioning.com/proceedings/dp2023/2023%20MTS%20DP%20Conference%201.3_KERKENI_Paper_Hybrid%20Decision%20Support%20System%20for%20Improved%20Offshore%20Operation%20Planning.pdf.

Bambach, R. (2018). Proper DP System Configuration Ensures Redundancy Concept Succeeds. *Offshore Magazine*. URL: https://www.offshore-mag.com/vessels/article/16762084/proper-dp-system-configuration-ensures-redundancy-concept-succeeds.

Bohanec, M. (2003). Decision Support. In: *Data Mining and Decision Support*. Ed. by D. Mladenic, N. Lavrac, M. Bohanec & S. Moyle. Vol. 745. The Springer International Series in Engineering and Computer Science. Boston: Springer Science + Business Media, LLc, pp. 23–35. ISBN: 978-1-4615-0286-9.

CLIA, C. L. I. A. (2025). *2025 CLIA Cruise Industry Report: Strong Growth, Rising Demand & Sustainable Innovation*. Cited: 2025-09-16. URL: https://www.cruisetotravel.com/2025/05/24/2025-clia-cruise-industry-report-strong-growth-rising-demand-sustainable-innovation/#:~:text=37.7%20million%20cruise%20passengers%20expected%20worldwide%20in%202025%2C,of%20international%20travelers%20are%20considering%20their%20first%20cruise..

Corporate Finance Institute team (n.d.). *Decision Support System (DSS)*. Cited: 2025-09-8. URL: https://corporatefinanceinstitute.com/resources/management/decision-support-system-dss/.

Downer, J. (2009). *When Failure is an Option:Redundancy, reliability and regulation in complex technical systems*. Disscussion paper. London: London School of Economics and Political Science (LSE).

Eriksen, S. & Lützen, M. (2022). The impact of redundancy on reliability in machinery systems on unmanned ships. *WMU Journal of Maritime Affairs* 21, pp. 161–177. DOI: 10.1007/s13437-021-00259-7.

Gardner, N. (2022a). System redundancy on cruise ships and DP vessels. *Seaways: The International Journal of The Nautical Institute*, pp. 10–13. URL: https://www.nautinst.org/resources-page/system-redundancy-on-cruise-ships-and-dp-vessels.html.

Gardner, N. (2022b). System redundancy on cruise ships and DP vessels. *Seaways: The International Journal of The Nautical Institute*, pp. 10–13. URL: https://www.nautinst.org/static/8d412d11-6999-4ba5-a82891b207f1ac72/Free-Article-SeawaysJuly22.pdf.

Giddings, I. C. (2013). IMO Guidelines for Vessels with Dynamic Positioning Systems. In: *Proceedings of the Dynamic Positioning Conference*. Houston, TX, USA, Oct. 15-16, 2013: International Marine Contractors Association (IMCA). URL: https://dynamic-positioning.com/proceedings/dp2013/quality_giddings_pp.pdf.

Group, N. T. S. B. E. (2024). *Dali Shipboard Machinery Examination and Record of Electrical Testing*. Technical report. National Transportation Safety Board.

GTMaritime (2022). *Chinks in the Armour: Software and Communication Vulnerabilities on Ships*. GTMaritime. URL: https://www.gtmaritime.com/app/uploads/2022/12/security.pdf.

Ibrion, M., Paltrinieri, N. & Nejad, A. R. (2021). Learning from failures in cruise ship industry: The blackout of Viking Sky in Hustadvika, Norway. *Engineering Failure Analysis* 125, p. 105355. DOI: 10.1016/j.engfailanal.2021.105355.

International Maritime Organization (1974). *International Convention for the Safety of Life at Sea (SOLAS), 1974*. Cited: 2025-08-20. URL: https://www.imo.org/en/about/conventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx.

International Maritime Organization (2025). *Guidelines on Maritime Cyber Risk Management*. International Maritime Organization. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf.

International Maritime Organization (n.d.). *Passenger Ships*. Cited: 2025-08-21. URL: https://www.imo.org/en/ourwork/safety/pages/passengerships.aspx.

Lerus (2024). *Common Mode Failure: A Critical Challenge in Redundant Systems*. Cited: 2025-08-25. URL: https://www.lerus.com/articles/common-mode-failure-a-critical-challenge-in-redundant-systems.html.

Loomis, W., Singh, V. V., Kessler, D. G. C. & Bellekens, D. X. (2021). *A System of Systems: Cooperation on Maritime Cybersecurity*. report. Atlantic Council.

Marine Safety Consultants (2024). *Power Loss at Sea: The Dali Incident and the Hidden Risks of Maritime Engineering Failures*. Cited: 2025-09-8. URL: https://marinesafetyconsultants.

com / power - loss - at - sea - the - dali - incident - and - the - hidden - risks - of - maritime - engineering-failures/.

Miller, G. (2024). US alleges 'entirely avoidable' Dali disaster was caused by negligence. *Lloyd's List*. URL: https : / / www . lloydslist . com / LL1150696 / US - alleges - entirely - avoidable-Dali-disaster-was-caused-by-negligence.

NAPA (2025). *NAPA*. Cited: 2025-08-18. URL: https://www.napa.fi/.

Nintex (n.d.). *Running a Parallel Standby Environment*. Nintex. URL: https://help.nintex.com/en-US/nintexautomation/icg/5.8/Content/Plan/BCP-DisasterRestorEnv.htm.

Nordström, J., Goerlandt, F., Sarsama, J., Leppänen, P., Nissilä, M., Ruponen, P., Lübcke, T. & Sonninen, S. (2016). Vessel TRIAGE: A method for assessing and communicating the safety status of vessels in maritime distress situations. *Safety Science* 85, pp. 117–129. DOI: 10.1016/j.ssci.2016.01.003.

Norwegian Safety Investigation Authority (NSIA) (2024). *Report on loss of propulsion and near grounding of Viking Sky, Hustadvika, Norway 23 March 2019*. Technical report. Oslo, Norway: Norwegian Safety Investigation Authority (NSIA).

Oil Companies International Marine Forum (OCIMF) (2018). *Safety Critical Equipment and Spare Parts Guidance*. Oil Companies International Marine Forum (OCIMF). London, UK. URL: https://www.ocimf.org/document-libary/93-safety-critical-equipment-and-spare-parts-guidance/file.

Phillips, D. F. (1998). *Classic Single Point Failures of Redundant DP Systems*. Tech. rep. San Diego, California, USA: Nautronix Inc.

Power, D. J. (Oct. 1997). What is a DSS? *DSstar, The On-Line Executive Journal for Data-Intensive Decision Support* 1(3). URL: https : / / www . dssresources . com / subscriber / password/papers/whatisadss.pdf.

Red Ensign Group (n.d.). *Safe Return to Port: Instructions for the Guidance of Surveyors on the implementation of SOLAS regulations ll-1/8-1, ll-2/21 and ll-2/22*. Red Ensign Group. URL: https://www.redensigngroup.org/media/1282/safe-return-to-port_oct-2019.pdf.

Sauter, V. L. (2010). *Decision Support Systems for Business Intelligence*. Hoboken, New Jersey: John Wiley Sons. ISBN: 978-0-470-43374-4.

Shipping, I. C. of (2017). *The Guidelines on Cyber Security Onboard Ships*. version 2. International Chamber of Shipping. URL: https://www.maritimeglobalsecurity.org/media/1014/c-users-jpl-onedrive-bimco-desktop-guidelines_on_cyber_security_onboard_ships_version_2-0_july2017.pdf.

Shipping, I. C. of (2021). *The Guidelines on Cyber Security Onboard Ships*. version 4. International Chamber of Shipping. URL: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf.

Takkinen, E. (2016). Effect of Flooding Sensor Arrangement on Automatic Breach Assessment for Damaged Passenger Ship. Master's thesis. Helsinki, Finland: Aalto University.

URL: https://aaltodoc.aalto.fi/server/api/core/bitstreams/b1df669d-a47c-4d56-893e-2c8bf8bb66e1/content.

Team, S. E. (2019). *6 Common Cyber Risks Affecting the Maritime Industry*. Cited: 2025-08-25. URL: https://safety4sea.com/cm-6-common-cyber-risks-affecting-maritime-industry/.

The Switch (n.d.). *Redundant power - a lifesaver for ships*. Accessed: 2025-08-20. URL: https://theswitch.com/2018/08/28/redundant-power-a-lifesaver-for-ships/.

Troy Segal (2025). *Decision Support System (DSS): What It Is and How Businesses Use Them*. Cited: 2025-09-8. URL: https://www.investopedia.com/terms/d/decision-support-system.asp.

Vicky Sauter (2002). *Decision Support Systems*. Cited: 2025-09-8. URL: https://www.umsl.edu/~sauterv/analysis/488_f02_papers/dss.html.

Wärtsilä (n.d.). *Redundancy*. Cited: 2025-08-20. URL: https://www.wartsila.com/encyclopedia/term/redundancy.

Yang, D.-Y. & Wu, C.-H. (2021). Evaluation of the availability and reliability of a standby system with warm standby components and switching failures. *Reliability Engineering System Safety* 207, p. 107366. DOI: 10.1016/j.ress.2020.107366.

Appendix 1 Figures

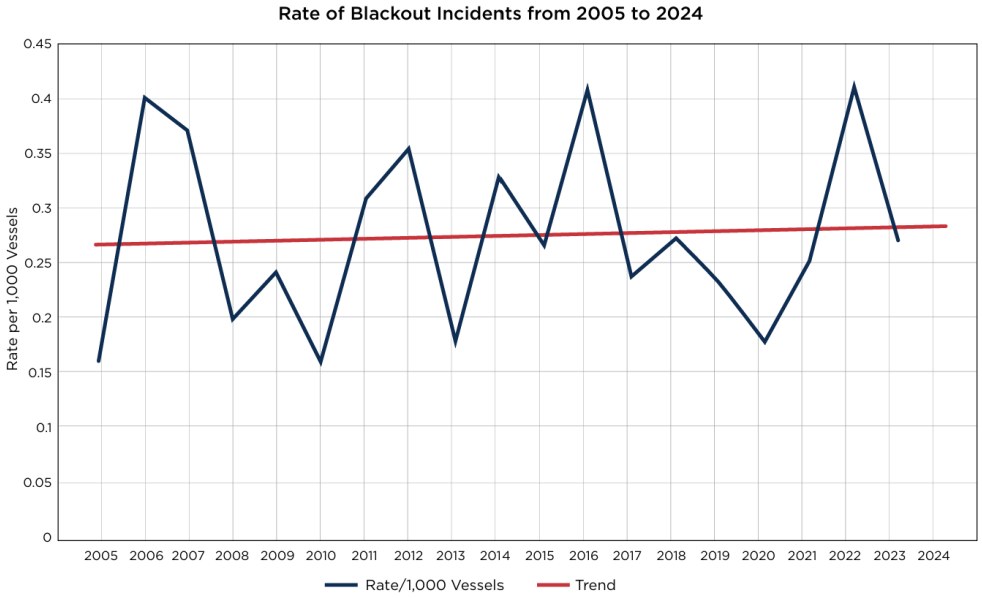

Figure 9: Rate of reported blackout incidents from 2005 – 2024 (American Bureau of Shipping, 2024).

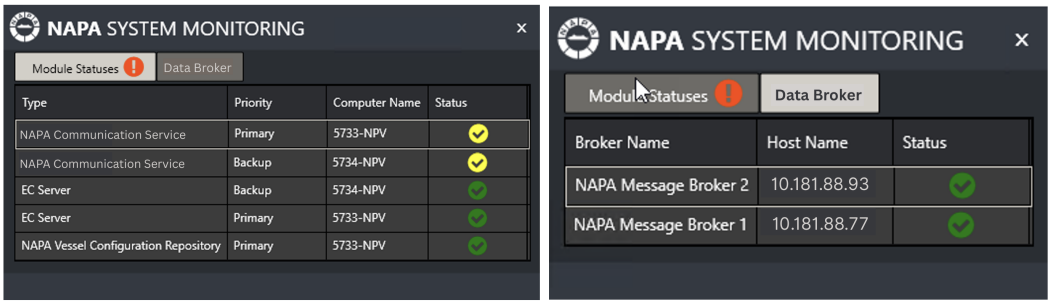

Figure 10: NAPA System monitor application, with all services connected.

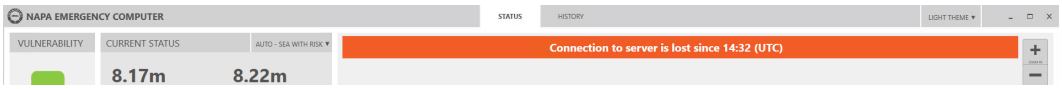

Figure 11: Example of an error when services are disconnected.