UNIVERSITY OF TURKU

Compliance analysis for cyber security marine standards

Evaluation of compliance using application lifecycle management tools

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Amir Trent

Supervisors:

Title Heidi-Maria Kallio (Wärtsilä)

Tahir Mohammed (University of Turku)

Seppo Virtanen (University of Turku)

June 2023

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Amir Trent
Title: Compliance analysis for cyber security marine standards
Number of pages: 75 pages, 1 appendix page
Date: June 2023

The aim of this thesis is to analyse cyber security requirements and notations from marine classification societies and other entities to understand how to meet compliance in current cyber security requirements from maritime class societies and other maritime organizations. The methods used in this research involved a desk review of cyber security requirements from IACS members, IACS UR E 27 and IEC 62443, a survey questionnaire of relevant cyber security standards pertinent to maritime product development, and Polarion, an application lifecycle management solution used to synthesize the cyber security requirements from the maritime class societies and determine their correlations to IEC 62443 as a baseline. Results indicate that IEC 62443 correlates to the standards from DNV and IACS (UR E 27) and majority of the requirements were deemed compliant in compliance gap assessments of a maritime product. The conclusion is that IEC 62443 can be utilised as a baseline cyber requirement with a requirements management tool like Polarion to analyse and satisfy compliance requirements from maritime class societies and maritime organizations that base their cyber security requirements according to IACS UR E27 and IEC 62443-3-3 and should be adopted in addressing future compliance analysis of cyber requirements focusing on autonomous shipping.

Keywords: Compliance Analysis, Maritime Cyber Security, Maritime Regulations, Cyber Security Marine Standards, IEC 62443

Table of contents

List of Figures

List of Tables

List of Abbreviations

AIS	Automatic Identification System
ABS	American Bureau Service
ALM	Application LifeCycle Management
BIMCO	Baltic and International Maritime Council
BV	Bureau Veritas
CBS	Computer Based Systems
CCS	Chinese Classification Society
CRS	Croatian Register of Shipping
DNV	Det Norske Veritas
DOS	Denial of Service
DDOS	Distributed Denial of Service
DP	Dynamic Positioning
ECDIS	Electronic Chart Display and Information System
ENISA	European Union Agency for Cybersecurity
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
LR	Lloyd's Register
IACS	International Association of Classification Societies
ICS	Industry Control Systems
IEC	International Electronic Commission
IMO	International Maritime Organization
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
ISM	International Safety Management
ISPS	International Ship and Port Facility Security Code
OEM	Original Equipment Manufacturer
OT	Operational Technology

MSC	Maritime Safety Committee
CLASS NK	Nippon Kaiji Kyokai
NIST	National Institute of Standards and Technology
PRS	Polish Register of Shipping
RINA	Registro Italiano Navale
SDL	Secure Development Lifecycle
SOLAS	Safety of Life at Sea
SuC	Systems Under Consideration
UR	United Requirements
VSAT	Very Small Aperture Terminal

1 Introduction

Industry 4.0 has revolutionized the world by changing the way industries manufacture and distribute products. This precedence has manifested itself in the shape of smart connected devices and processes that have been utilized to push the boundaries of digital technology, such as automation, Artificial Intelligence, Deep Learning, cyber security, the Internet of Things (IoT), and more [1]. This digital transformation has led to the development of smart cities, smart hospitals, smart factories, and more from different industries. The maritime industry is one sector that has been significantly affected by the effects of digital technology. With the integration of digitalization and IoT devices on the horizon, shipyard owners, manufacturers, and other entities are developing ways to leverage the technology to improve the efficiency of maritime shipping operations. This opportunity has manifested in the endeavours of smart shipping, which covers developing on-board systems and constructing ships with semi to fully autonomous capabilities [2]. Such automated shipping has now become a popular venture due to the various potential it has in terms of optimizing efficiency, such as reducing operational costs, human error, and time resources [3]. Inversely, with the integration of smart based-Computer Based Systems (CBS) connected to these ships has introduced attack vectors that can be exploited by attackers looking to cause significant damage to the ship. These types of cybersecurity challenges can bring exponential threats that impact the safety of the passengers and personnel on the ship. Classification societies and Maritime organizations have produced standards and guidelines with the objective of ensuring their cyber-enabled ships are resilient against these cyber attackers. With the increase of sophisticated cyber threats as a result of being connected, cyber-attacks being inflicted upon vessels and offshore facilities, such as the malware attack on International Maritime Organisation (IMO) with devastating implications, has prompted Maritime governance to be more active in increasing the cyber security functionality in maritime vessels and environments [4].

1.1 Background

Due to the nature of digitalization in the maritime industry, vessels, ports, and other environments have information and operation technology (IT/OT), Industry Control Services (ICS), and assets that are now connected to their onboard systems [5]. With the support of these connected systems, data can show pivotal information related to the vessel, such as fuel consumption, route positioning, system performance, and other functions, which has greatly improved operation efficiency, reduced human error, and increased navigational safety [6]. Under the utilization of these systems, shipping operations are now more cyber enabled through the adoption of IoT, automation (Autonomous ships), and Artificial Learning (AI) [7]. Due to the onboard systems on the vessels being heavily connected with the aforementioned technologies, the vessels are susceptible to cyber threats by hackers that can potentially compromise the integrity of the vessel and the safety of the passengers. As a result, there has been reported a high number of cyber orchestrated attacks to cyber-enabled ships, with attacks increasing up to 31% in 2020 according to a survey produced by The Baltic and International Maritime Council (BIMCO) and Safety at Sea [8]. Other reports have included a 900% increase in attacks over the span of three years, with record-breaking numbers of cyber incidents continuing to take place [9]. In additional even maritime organizations like International Maritime Organization (IMO) have been breached due to a cyber-attack [5]. In increasing the efforts of addressing these cyber security challenges that place a threat on maritime security and safety, governance bodies have produced compliance regulations on building cyber security resilience for ships. These regulations have been applied to ship owners, shipyards, and manufacturers in the hopes of placing urgency on maintaining a cyber security presence regarding critical assets on vessels. These standards come in the form of requirements developed by classification societies, International Electrotechnical Commission (IEC), BIMCO and other entities [10]. Because these several requirements are mandated by maritime law under provisions from IMO and different bodies, maritime industries need to meet and fulfil these requirements in order to be approved under the specified standard. These procedures come in the form of type approvals or certifications to illustrate compliance.

1.2 Key Concepts

1.2.1 Maritime cyber security

Maritime cyber security involves the protection of maritime environments, vessels, organizations, and assets using an assortment of cyber security utilities, guidelines, procedures, policies, risk evaluation, assessments, recommended practices/standards, security controls, training, governance, and other factors that contribute to cyber security in the Maritime industry [5]. Under the current progression of digitalization, systems both IT (Information technology) and OT (operational technology) use technologies including automation and IoT to improve maritime operations and are connected to the Internet, which makes them susceptible to hacker attacks resulting in compromising the safety of operational systems, vessels, and crews onboard [11]. Such attacks include Ransomware, Denial of Service (DOS), GPS spoofing, and many others that significantly threaten maritime safety and operations. In order to thwart these cybersecurity threats and risks, organizations need to establish a cybersecurity infrastructure to protect the safety of their assets, environments, and personnel. The strength of the organization's cyber security capabilities in mitigating these cyber-attacks depend on the maturity of the organization's cyber security practices. These practices, according to huoltovarmuukeskus [5], entail the support of senior management in adopting cyber security throughout the company, promoting awareness training, cyber security guidelines, Risk management, Risk assessment, cybersecurity infrastructure, cyber security frameworks, and collaboration with third parties.

1.2.2 Cyber security requirements:

Cyber security requirements involve the implementation of cyber security controls or features as safeguards to protect the systems of OT/IT systems of the organization. These requirements come in the form of industry standards or frameworks like IEC 62443, ISO 27001 (National Institute of Standards and Technology), NIST 800-82 and others. As for the maritime Industry, prominent cyber security requirements that are implemented in organizations entail guidelines from regulating organizations such as the International Maritime Organization (IMO) or BIMCO or from the International Association of Classification Societies (IACS) like Lloyd's Register (LR), Bureau Veritas (BV), and more. These cyber security requirements aim to address the security of these connected IT/OT systems and assess how it impacts the criticality

of maritime operations and safety for personnel, whether onboard ships or in other essential environments [12]. In doing so, these standards identify requirements critical to protecting all aspects of the lifecycle system in maritime shipping, whether it is for providing criteria for product developers in getting products certified and manufacturer compliance in their processes or establishing guidelines for security engineers in protecting cyber systems, or for ship integrators and shipowners to understand how their ship designs are cyber resilient against cyber-attacks [13]. The requirements also act as a metric in determining an organization's cyber hygiene regarding protecting their assets and gauging the strength of its cybersecurity infrastructure.

1.2.3 Compliance tracking

Compliance tracking entails the iterative process of monitoring, evaluating, and reporting compliance-related activities in business functions to ensure that these activities meet regulatory compliance [14]. In regard to maritime shipping, Maritime Organizations have issued regulations pertaining to cyber security capabilities in vessel onboard systems. These regulations are in response to the increasing threats to maritime security and safety by attackers. Such regulations include IMO, Maritime Safety Committee (MSC), International Ship and Port Security (ISPS) Code, International Safety Management (ISM) CODE and others [5], as well as regulations from classification societies in determining the cyber resilience of onboard systems equipment on vessels distributed through regulations such as IACS UR E 27 [15]. In ensuring that the regulations are fulfilled by classification societies or other maritime governing bodies, these processes and requirements can be monitored thoroughly with application lifecycle management (ALM) tools like Polarion ALM. These types of tools help support compliance tracking in finding gaps regarding compliance fulfilment of cyber security requirements, which in turn will improve how these organizations implement such requirements in their business activities, whether its lifecycle management, cyber security risk management, product development, and other cyber security practices [16].

1.2.4 Class Notations

Class Notations represent the details of certain class society rule requirements that have been fulfilled for maritime operations in the onboard, offshore, and newly constructed vessels.

Regarding cyber security, these notations address requirements pertaining to the functions of a vessel and other operational features from the ship owner across several security levels [17]. DNV's Cyber Secure class notation is an example of how class notations are utilized to address the security controls of a vessel from different security levels [18].

1.2.5 Classification Societies

Societies that establish and implement regulations and guidelines for the vessel's survey, construction, and design in addition to conducting inspections, surveys, and classification services on board ships. These activities aim to verify the integrity and foundation of a vessel's main functions. By meeting those standards, ships can demonstrate compliance with the rules mandated by the class societies toward maritime safety [17]. There are more than 50 classification societies globally, but the ones that are recognized as the leading societies from the European Union are members of the International Association of Classification Societies (IACS). Currently, there are 11 members recognized as part of the IACS, such as Det Norske Veritas (DNV), American Bureau of Shipping (ABS), Lloyd's Register (LR), Bureau Veritas (BV), China Classification Society (CCS), Nippon Kaiji Kyokai (ClassNK), (Croatian Register of Shipping (CRS), Polish Register of Shipping (PRS), Registro Italiano Navale (RINA), and Indian Register of Shipping (IRS) [19].

1.2.6 International Maritime Organization (IMO)

The International Maritime Organization is a division of the United Nations whose primary efforts involve improving the maritime safety and security of international shipping alongside preventing pollution from ships. It does this through the Maritime Safety Committee (MSC), which establishes codes, conventions, and guidelines covering every facet of maritime safety with examples such as managing fatigue, life-saving equipment, and more [20].

1.2.7 Polarion

It is an application used for managing system requirements throughout project lifecycles. Its main functionality is traceability in supporting compliance, audits, and other inspections.

Complementary features used for demonstrating traceability include dashboards for metrics/reports, tools for requirements and change management, and extensions that are compatible with Polarion [21].

1.3 Problem Statement

Currently, there are several cyber security standards, and guidelines that have been examined and utilized towards building cyber resilience in maritime vessels, most notably NIST 800-53, IEC 62443 series, IEC 27001, (IMO) Resolution MSC428(98) along with others from the classification societies [12]. With the latest developments in Maritime 4.0, vessels are becoming more connected, digitalized, and automatized, which creates more vulnerabilities and opportunities for cyber attackers to exploit. Under the regulations of IMO, the classification societies, and customers, suppliers must satisfy certain security requirements that ensure onboard vessels are cyber-resilient against cyber-attacks [15]. This process is audited by maritime governance bodies to verify that these onboard systems are cyber secure and meet security compliance resulting in certification of said product. In order to understand how to meet cyber security compliance in several of these standards for marine solutions, these requirements and the derived class notations have to be monitored, assessed, and documented against the onboard systems.

1.4 Objective and Research Questions

The goal of this thesis is specified in the following steps:

1. To identify cyber security requirements and notations from marine classification societies and other entities involved in maritime cyber security.
2. To analyse how to establish compliance with these cyber security requirements.
3. To propose a framework using an application management lifecycle to synthesise the cyber requirements for compliance analysis. This includes identifying, gathering, tracking security requirements from different standards, and finding correlations between them that can be used to determine a maritime solution's compliance against a specific cyber security standard in the form of a compliance gap assessment. As a result,

the framework can be applied in addressing compliance towards security requirements for automated vessels when they become more prevalent in the future.

By completing these objectives, the following research questions can be answered:

Research question 1: What are the relevant cyber security standards and class notations for products used in compliance tracking?

Research question 2: How do internationally recognized standards such as IEC 62443 compare to other cyber security requirements for marine solutions products?

Wartsila can use the outcome from the analysis as an approach to massage these additional standards into its market tracking development process towards automated shipping compliancy in the future.

1.5 Scope

To answer the research questions, the scope of this thesis is limited to reviewing marine cyber security requirements from the IACS classification society (BV, ABS, LR, CCS, DNV), IACS UR E 27 and non-marine standards such as IEC 62443. In addressing the relevancy of these cyber security standards from their compliance requirements, participants from cyber security and product development volunteered in a survey in which 11 only responded due to conflicting time restraints that prevented any interviews from being included. In addition, the analysis will involve the usage of one simulated product, which was assessed as part of a demonstration in using Polarion to assess marine products compliance against cyber security standards.

1.6 Company Client: Wärtsilä

Wärtsilä is a leading international powerhouse in manufacturing lifecycle solutions and developing cutting-edge technologies and services for marine and energy industries. Wartsila's focus is developing technologies and solutions that are environmentally sustainable, efficient, adaptive, and reliable that can provide value to customers. Wartsila's core objective is enabling sustainable societies through strategic collaboration/ecosystems, which allows us to find innovative approaches in advancing its technology, products, and services that have environmental, societal, and economic impacts on our clients, partners, and society [22].

1.7 Thesis Structure

The structure for this thesis is presented in the following process: Chapter 2 will describe the theoretical body, including the background review on maritime cyber security, maritime regulations, the marine classification societies of IACS, industry standards, cyber security requirements/notations, and lastly tracking compliance of these security requirements. Chapter 3 will discuss the methodology behind the research of the thesis. This will entail investigating the way the data will be formulated, collected, and analysed through qualitative data methodology that will involve desk review, case study, and survey on the relevancy of cyber security standards in maritime products. The analysis of the research will be highlighted in Chapter 4, demonstrating how the cyber security standards are gathered and tracked for cyber security compliance of maritime products. Chapter 5 details the outcome of the data analysis from Section 4 and provides future compliance recommendations. Lastly, Chapter 6 will present the conclusion in addition to future implications for how compliance against requirements for automated shipping could be met.

2 Theoretical Framework

This chapter explores the different elements of cyber security pertaining to maritime shipping. We will begin by discussing the existing literature on analysing cyber security standards requirements in maritime cyber security compliance. Next, the surrounding factors that impact maritime cyber security will be addressed, including describing the security control categories, the onboard system equipment and their cyber security challenges, the maritime bodies that regulate maritime cyber security, and the cyber security requirements that need to be complied with under these organizations.

2.1 Literature Review

Maritime cyber security has been gaining momentum due to the wide array of sophisticated cyber-attacks affecting cyber-enabled vessels such as autonomous vessels. To focus on efforts in mitigating these frequent cyber-attacks, maritime regulators have incorporated mandates on maritime companies to establish risk management frameworks that identify these cyber threats while implementing security controls to strengthen cyber resilience on vessels and onboard systems. The research on addressing cyber-risks involved with maritime cyber security has not been emphasised in the past due to the physical risks being prioritised over the implications of cyber risks within the maritime sector, as mentioned by Tam and Jones [23]. Understanding the necessity for protecting system assets and vessels against cyber-attacks whilst complying with maritime regulations on risk management and cyber resilience has encouraged organizations to leverage the standards of NIST CSF and IEC 62443 3-3 within their cybersecurity frameworks to accomplish this [24]. Research has been developing in this area regarding building frameworks using IEC 62443 as a baseline standard to assess compliance with cyber security requirements as proposed by Gorski, Wardzinki, and Nopanen [25], [26].

Hautamaki [27] implemented the usage of Polarion, an application management tool in which requirements can be documented, managed, and manipulated into traceable items. Using the tool, Hautamaki proved that cyber security compliance requirements can be processed and tracked but also addressed that the development of Polarion usability in regard to addressing compliance analysis was still in its infancy. Erich [28] expanded on this concept by introducing a framework that analyses compliance requirements from maritime regulators using a combination of different standards and regulations, including NIST 800/CSF, IEC 62443, and ISO 27001. In the study, Erich was able to determine the correspondence between NIST

800/CSF and IEC 62443 and apply them in establishing compliance with several of the cyber security requirements issued by Classification Societies. Although the NIST CSF, IEC 62443, and ISO 27001 standards do complement each other in most of their requirements, as Erich tested in his framework, not all of the requirements are aligned with some of the compliance requirements from the classification societies as their requirements continue to develop overtime. This is more evident as all of the IACS classification societies are now updating their requirements to match IEC 62443 in order to accommodate the new mandatory compliance of IACS UR E27 for vessels that are certified by IACS maritime classification members. This presents a challenge as UR E27 requirements are based on IEC 62443 3-3 and 62443-4-1 for secure product development processes, so that would mean maritime organizations would need to begin aligning more of their requirements toward IEC 62443 in order to satisfy compliance for IACS UR E27.

Huuskonen [29] have expanded on this research by incorporating security controls from NIST CSF and 62443 3-3 and CIS in a verification and validation framework to assess cyber risks in automated vessels. Her results indicated that with the inclusion of security tools, security requirements can be verified and validated, which is useful for ensuring compliance with maritime regulators in the future. In her assessments, the knowledge of IEC 62443 was less familiar, thus impacting the overall practicality of its application in verifying and validation the analysis of the IEC 62443 3-3.

This literature review details the challenges in conducting compliance analysis of cyber security standards for maritime regulation bodies. The reasons are due to maritime companies keeping up with constant developments in maritime regulations, unfamiliarity with different cyber security standards, and a lack of developing a framework to identify and assess cyber compliance requirements. This research addresses these concerns with the implementation using Polarion and building around its traceability features using IEC 62443 3-3 as a baseline in order to comply with maritime regulations that align with IEC 62443-3-3.

2.2 Maritime Cyber Security

Maritime cyber security involves the protection of maritime environments, vessels, organizations, and assets using an assortment of cyber security utilities, guidelines, procedures, policies, risk evaluation, assessments, recommended practices/standards, security controls,

training, governance, and other factors that contribute to cyber security in the Maritime industry. These activities are now regulated under several codifications, such as the SOLAS convention, ISM code, ISPS Code, EC Regulation 725/2004, IMO MSC.428(98) Cyber Risk Management in Safety Management Systems [8]. This is done to address the rise of cyber-attacks on onboard systems that have affected personnel, cargo, vessels, equipment, and facilities by cyber attackers due to Covid-19 and the development of digitalized systems [30]. These cyber-attacks include jamming, spoofing, and Denial of Service (DOS) to critical vessel systems. Because these systems are interconnected, it is essential for maritime cyber security to address protections for both IT systems, which may include routers, switches, laptops, mobile devices, internet services, as well as OT systems (navigational sensors, propulsion systems, cargo management systems, automated systems). Because of the threats to maritime safety and security, maritime organizations are mandated to establish security controls to protect these systems. These mandates based on IMO resolution MSC.428(98) are published in different guidelines prevalent in the maritime industry, namely, guidelines of BIMCO, IACS recommendation on Cyber Resilience, DSCA Cyber Security Guide, and guidelines from DNV-GL-RP-0496, and DNV-GL-CP-0231, which references prominent cyber security standards such as NIST CSF, IEC 62443 and IEC 27001 [31]. These frameworks have been heavily integrated into several cyber security requirements from IACS societies, maritime organizations, and other entities. Therefore, established as the benchmark of security controls for implementing cyber security for ships and satisfying compliance with maritime regulations.

2.3 Maritime Cyber Security Compliance

Cyber security was not considered a priority in maritime operations in the past but now has been considered a necessity due to the implications of digitalisation in the maritime sector. With more onboard systems on vessels becoming interconnected, the threats of cyber security attacks increase. With cases such as the Hellman ransomware attack, Danaos supply chain attack, Swire pacific offshore breach, and others [32] affecting the security of vessels, ports, and offshore facilities, Maritime government bodies like IMO has published regulations ensuring maritime operators, owners, and suppliers implement cybersecurity risks into their Safety Management Systems (SMS) to help strengthen maritime cyber security within the sector.

Because IMO regulations of MSC-FAL.1/Cir.3 and Resolution MSC.428(98) are a part of maritime law under cyber security, it is necessary for ship vendors, ship owners, ship

integrators, and ship operators to meet cyber security compliance with these regulations [33]. Meeting cyber security compliance entails having frameworks that involve a cyber risk management program centred around five focal points, such as risk identification/detection/response, asset protection, and recovery of assets, which delves further into asset mapping, threat analysis, policies, and security controls. These frameworks are incorporated into standards such as NIST CSF, IEC 62443 series, and more which are extended into other standards from IACS classification societies [34]. Failure to comply with maritime cyber security regulations will result in ships being detained in port, and failed entry into international harbours, which will impact the global economy dependent on maritime shipping [35]. The benefits of ensuring maritime cyber security compliance with different standards include credibility of cyber security resilience through certification and internal/external systems audits and improved cyber security hygiene from vessel and offshore personnel [36].

2.4 Security Control Categories

In producing onboard systems for vessels for cyber resiliency, there are essential controls that need to be implemented as part of the cyber risk management under IMO MSC.428(98) resolution. These security controls are interchangeable and overlap with other standards, such as the 62443 series, NIST CSF framework, and frameworks from IACS classification societies. The implementation of these security controls is based on securing and hardening IT and OT systems. The protection of IT technology involves the CIA priority of confidentiality, integrity, and availability, whilst the security of OT technology entails the priority of availability, integrity, and confidentiality. Because OT assets are tied into critical infrastructures of Industry Control Systems (ICS), such as the functionality of vessel with the inclusion of IT technology, adequate security controls need to be enforced and secure for both IT/OT assets to reduce the potential for a cyber-attack. The security controls are implemented around these main topics in some iterations, including Risk Assessment, Network segmentation, Firewall configuration, Remote Access, Malware Protection, Logging and Monitoring, system update maintenance, system hardening, backup, and recovery [5].

2.4.1 Risk Assessment

Classifies functions and services critical for vessel operation, such as navigation and propulsion. Categorizes assess (IT/OT) assets that support vessel operations. Assesses risk and impact on critical assets and functions. Establishes a plan of action that will mitigate or reduce risks to assets. Update inventory of assets and risk assessment.

2.4.2 Network Segmentation

Segmentation between assets and critical systems in other networks to reduce breaches by hackers. Segmentation goes into establishing and isolating networks for different essentials systems (wi-fi networks, controls to communication, engine, cargo, bridge systems)

2.4.3 Firewall Configuration

Configuring firewall policies in accordance with how systems are segmented to allow authorized traffic within the systems. This entails protecting networks and critical systems, filtering traffic communication between networks, and configuring default-deny controls to prohibit non-authorized traffic.

2.4.4 Remote Access

Identify external suppliers and internal users that have remote access to essential vessel systems. Document network ports, IP addresses, and systems that are required for remote access to critical systems. Document every remote access connection and ensure non-disclosure agreements for remote access usage are established.

2.4.5 Malware Protection

EDR solutions are used for protecting systems against malware attacks. EDR components include monitoring and response features (IDS/ IPS systems). Involve configuring malware protection solutions on critical systems. Ensure that all malware protection solutions are automatically updated at frequent intervals. They provide systems that lack malware protection

capability with alternative solutions to safeguard against malware. They protect external portable devices such as USB drives and are analysed for malware contamination before inserting them into critical systems inside the vessel.

2.4.6 Logging and Monitoring

Monitoring and logging events in order to detect potential attacks on critical systems and assets. Enable monitoring and logging solutions such as Event Management features for auditing OT and IT systems in the vessel by establishing a centralised solution for logging all activities from IT and OT systems. The logging solution allows continuous monitoring features to identify indicators of cyber-attacks. Set up logging features for firewalls and other essential networked systems.

2.4.7 System Update Maintenance

Involves updating systems regularly in order to prevent attackers from exploiting vulnerabilities that grant access to critical systems and networks. Provide documentation of patching/update activities and role responsibilities, and ensure systems are updated in an organized manner. Ensure systems that are exposed to untrusted systems, such as systems with remote access, are updated frequently. Monitor and check vulnerabilities published by vendors for all systems and applications used on the vessel.

2.4.8 System Hardening

This entails ensuring that all assets IT/OT are securely hardened and configured according to industry recommendations. It involves securing networks and security configurations such as firewalls, switches, and Wi-Fi networks with robust/complex passwords and protocols. Provide guidelines on changing default administrative user passwords, securing USB ports, firewalls, and other essential features. Centralising configurations that secure critical systems on the vessel, such as ECDIS, GPS, etc, along with other essential systems and applications that are utilised.

2.4.9 Onboard system Components

Nowadays, a vessel is comprised of multiple automated systems that are integral to the vessel not only for autonomous functionality but also for navigational safety, positioning, and manoeuvrability. These systems include Electronic Chart Display Information System (ECDIS), Global Navigation Satellite System (GNSS), Global Positioning System (GPS), Automatic Identification System (AIS), Radar, Very Small Aperture Terminal (VSAT), Dynamic Positioning (DP), Propulsion/Power control systems, Industrial Control Systems and IT network systems as depicted in Figure 1 [36], Kevin Jones. The following systems will highlight their significance to the vessel's operability.

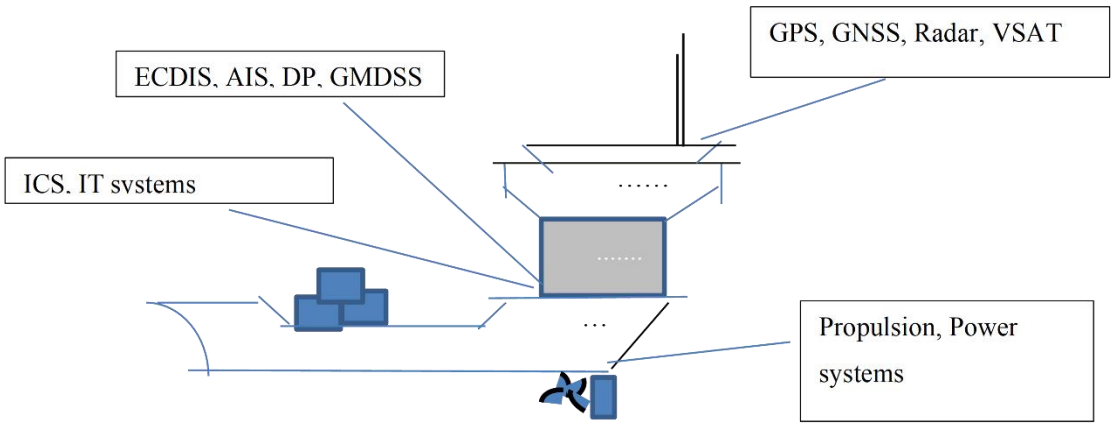


Figure 1. Automation Systems on the vessel that are connected digitally.

ECDIS: The Electronic Chart Display Information System is a navigational device that utilizes electronic charts to display the positioning of the vessel and proximal surroundings. The electronic charts are collected from data from navigational sensors like AIS, GPS etc. and displayed on LCD multi-view monitors giving seafarers an accurate viewing of the ship in real timer, enhancing navigation safety and efficiency.

GNSS: The Global Navigation Satellite System relies on a network of satellites to provide signals that indicate the positioning of the vessel and information on other surrounding ways

that can support route navigation in the sea, around the port, or docking in a harbour resulting in efficient route selection and navigational awareness.

GPS: Global Position System has the same functionalities as the GNSS and works in conjunction with each other. The fundamental difference between the two systems is that GPS technology pertains to the satellite system, while the GNSS is able to utilize a network of satellites outside of North America. By utilizing other navigation satellites from around the world, the range of sensors increases which would enhance the accuracy and reliability of the positioning of the vessel.

Automatic Identification System: AIS systems provide pertinent information to other vessels and port stations automatically, which includes its identity, vessel type, ship position, vessel speed, route, and navigational status. This allows the ships with AIS systems to be tracked and monitored, which allows the support of vessel traffic monitoring, collision avoidance, accident investigation and search/rescue operations.

Radar: Navigation instruments that utilize an antenna that transmits microwaves around the vessel surrounding environments. The microwave from the antenna is reflected from other vessels and objects, thus creating a generated image of the view the microwaves were able to detect. This enables seafarers to navigate safely and avoid collisions with ships and other objects and for shore stations to monitor and regulate vessel traffic efficiently. Radar components are used simultaneously with GPS and GNSS systems to optimize the navigational positioning of the ship and to provide a detailed view of its surroundings.

VSAT: VSAT provides high data communication with the usage of a satellite, ensuring stability in high waters while exchanging data to and from its satellite network. Such communication features include high broadband Internet and video connectivity.

GMDSS: Automates transmitting and receiving distress signals from other ships and from the vessel to the harbour. This ensures support for search and rescue operations, receiving bridge-to-bridge communications, receiving signals for the location of the vessel and other general communications.

Dynamic Positioning: A system that automatically maintains the position of the vessel and heading. Using the propulsion system as a basis, the vessel can regulate itself from deviating from its course, which helps it avoid potential collisions with other ships and other environments.

ICS and IT systems: Industrial Control Systems and Information Systems work in conjunction regarding the operations of the vessel. ICS or OT technology entails the control processes of the infrastructure of the ICS system or, in this case, the vessel. The Vessel's ICS systems monitor and regulate the different functions of the ship, such as pressure, flow, speed, equipment status, fuel consumption, control, levels, and other attributes. The IT systems are used in sending and transmitting data for the control processes in addition to providing data protection for the ICS systems through cyber security.

Propulsion and machinery management and power systems: These systems involve monitoring/controlling steering, propulsion functionality, and machine equipment onboard. The functionality of propulsion/machinery/power systems helps provide navigation efficiency and safety.

2.5 Maritime Cyber challenges

Leveraging digitization and automation technology for onboard systems has the potential to leave vessels susceptible to cyber-attacks from threat actors. The implications behind attacking these vessels can have devastating repercussions resulting in major incidents or impacting navigation safety for seafarers, the vessel, and other vessels. The most prominent cases in relation to these types of attacks including the NotPetya incident on Maersk in 2017, the Naantali port attack in 2019, the Hurtigruten attack in 2020, the IMO attack in 2020 and several others [32]. The motivations behind such attacks include financial gain, disruption of ship operations, commercial and industrial espionage, disruption of infrastructure and more and depend on the threat actor performing these attacks (Hacktivists, Cyber criminals, State-sponsored actors, Terrorists, and thrill seekers). The attacks deployed during these cases are more relevant to autonomous systems and include ransomware, GPS spoofing, DDOS attacks, Jamming attacks, and Signal compromise attacks. The components that are critical to maritime shipping due to being connected networks also find themselves at risk of several of these attacks [37]. The following will discuss ways these systems are vulnerable.

Vulnerabilities on Automatic Identification System: The primary vulnerability that can be exploited for AIS systems is that it is easily accessible to the public. By having sites such as vessel finder that can easily identify such vessels, AIS systems open themselves up to exploitation. In addition, because AIS also have the capability to transmit communication in the air without authentication, this leaves them exposed to actors as well. Such repercussions from these vulnerabilities can make AIS systems susceptible to signal interferences, spoofing the location of the vessel, and misleading info shared about the identity of the system. Impact includes commandeering of the vessel and stealing sensitive data.

Vulnerabilities of ECDIS: In regard to ECDIS charts, old system updates and the usage of charts transmitted via Universal Serial Bus (USB) can present numerous vulnerabilities, such as being able to inject malicious malware into OT systems, corrupting files or stealing valuable data. Even worse, data from the charts can be modified, thus impacting route selections that could affect the safety of other ships.

Vulnerabilities of GPS and GNSS: Due to heavy reliance on satellite networks to provide sensor data for vessel positioning and optimizing route navigation, and provide communication to other vessels, GPS GNSS are high valuable targets for threat agents. Various attacks employed to exploit the systems involve spoofing and jamming of GPS/GNSS signals, DOS attacks, modification of packages or man-in-the-middle attacks (MITM). The cause of these vulnerabilities can be due to issues such as usage of unsecured protocols, default factory configuration of the accounts. Such attacks can result in disruption of ship operations, deceiving GPS coordinates, and service delays.

Vulnerabilities in Radar detection: Radar signals can be vulnerable to DDOS attacks from cyber criminals, jamming, and spoofing attacks. Such vulnerable can result in collision incidents affecting damage to the vessel and loss of life, along with disruption to cargo delays.

Vulnerabilities in VSAT: Because its transmission capabilities from network interfaces are transparent and accessible, that leaves VSAT systems susceptible to attacks of modification of GPS coordinates, spoofing, or malware attack. In addition, VSAT sensitive information is available online regarding the identification of ships, brand names, as well as manufacturer websites that use default factory logons to access the system. Attacks can exploit this

vulnerability, allowing them to steal sensitive data and spoofing the GPS positions that can affect navigational safety.

Vulnerabilities in OT and IT systems: Because Onboard IT and OT systems are connected to onshore facilities, suppliers run the risk of having these systems exposed to attacks if they are not authenticated and protected with strong encryption mechanisms, weak remote-control policies, or proper network protection. In addition, human errors, when it comes to inefficient cyber training or cyber awareness, are just as critical a vulnerability compared to the others mentioned. Such Vulnerabilities can lead to disruption of IT/OT systems, disclosure of sensitive data, damage to equipment, hijacking controls of the vessels which can have devasting consequences to the impact of personnel, environments, and other vessels.

Vulnerabilities in Propulsion /power control systems: Systems that are unauthenticated or have default/weak user account credentials open themselves up to cyber-attacks such as DDOS, modification, or other related malware attacks. These are the attacks that, if Propulsion/power systems that are not adequately protected, can potentially suffer damages to their propulsion systems, the vessel of the ship, information of services revealed, and other devastating consequences.

2.5.1 Maritime Countermeasures and Mitigations of Equipment

As explained in the previous sections, vulnerabilities exposed on digital systems on the vessel can lead to risk that can be exploited in cyber-attacks by attackers, which can greatly impact the safety of the vessel, equipment, and the personnel on board. The following are mitigations that can help prevent the digital systems addressed from becoming targeted in a cyber-attack [38].

2.5.2 Mitigations for VSAT Risks

Table 1. Mitigations for VSAT

Outdated VSAT software:
Updated software versions of installed inside the VSAT terminals
Software updates are inspected in regular intervals to fix vulnerabilities
All software updates must be logged
Eavesdropping attacks:
VSAT admin web interface should be capable of supporting secure protocols like Hyper Text Transfer Protocol Secure (HTTPS) and Secure Shell version 2 (SSHv2)
Cross-site scripting (XXS) attack:
VSAT interface should have security controls in place such as implementing input sanitisation, output encoding, content security policy (CSP) to secure against script attacks such as XXS.
Unauthorized access of vessel network (Administrator, File Transfer Protocol (FTP), and Command-line access):
Configure Firewalls to allow solely whitelisted IP addresses within a subnet.
Initiate Multi-Factor Authentication (MFA)
Changed default username and password for administrator account.
Update regularly OS, antivirus, and other software components.
Increase complexity of passwords, and implement password reset policy.

2.5.3 Mitigations for Wireless Local Area Network (WLAN)

Table 2. Mitigations for WLAN Systems

Denial of Service (DoS) attack:
Configure Firewall to permit connections for whitelisted IP addresses now.
Eavesdropping/Session hijacking attack:
Use secure encryption standards for wireless standards. (Wireless Equivalent Privacy) WEP as a minimum level of security must be utilized, whilst more secure stronger standards like Wi-Fi Protected Access 3 (WPA3) is recommended.

2.5.4 Mitigations for ECDIS

Table 3. Mitigations for ECDIS systems

Malware attack (through Universal Serial Bus (USB) ports):
ECDIS system must have antivirus software installed to scan external media before inserting it into the system.
ECDIS charts that are updated must be logged.
Enable usb ports in admin login and disable in other logins.
DOS attack:
Networks should be monitored continuously for unusual traffic with Intrusion detection systems (IDS).
Firewalls should be installed in the ECDIS system to restrict unauthorised IP addresses from infiltrating the vessel's network.
Spoofing attack:
Software must be updated routinely.
Default username/password to Serial-to-IP converters web interfaces must be changed.

2.5.5 Mitigations for RADAR

Table 4. Mitigations for RADAR systems

Malware intrusion attack:
Train personnel to recognize phishing emails.
Install antivirus solution on in the system that contains ECDIS chart updates to prevent spread of malware from reaching to the RADAR system from ECDIS system.
Man-in-the-middle (MITM) attack:
Enforce server message block (SMB) signing to prevent MITM attacks and alteration of SMB communications.

2.5.6 Mitigations for AIS

Table 5. Mitigations for AIS systems

Spoofing attack:
Authenticate AIS messages.
Use RFeye software to discern between real and spoofed transmission signals.
Replay (DOS) attack:
AIS messages must be monitored with Timestamps to prevent recorded messages being resent and eavesdropped by attackers.
Frequency hopping attack:
Assure Integrity and authenticity of AIS messages:
PKI infrastructure can be implemented for RF communications.

2.5.7 Mitigation for GPS

Table 6. Mitigations for GPS systems

GPS Spoofing attack:
Anti-spoofing techniques such as absolute power monitoring should be used in order to identify spoofed signals in GPS receiver
GPS Jamming:
Utilize anti-jamming methods like spectrum monitoring to detect GPS jammers

2.5.8 Mitigation for DP Systems

Table 7. Mitigations for Dynamic Position (DP) systems

DOS attack:
DP system software should be updated.
Networks should be monitored for abnormal traffic with IDS systems
System should be able to Allow and Deny certain IP addresses and installing firewalls that will only permit known IP addresses in the network.
Spoofing attack:
Anti-spoofing techniques such as absolute power monitoring should be used in order to identify spoofed signals in GPS receiver.
Backdoor attack:
Implement advanced antivirus software that can prevent and detect malicious malware attacks such as malware that enables backdoor access into systems.

2.5.9 Mitigations for GMDSS

Table 8. Mitigations for GMDSS systems

Spoofing attack:
Authenticate messages between vessels and port authorities.
Authentication of exchanged messages can be ensured with an implemented PKI schema.
Eavesdropping attack:
Software within the GMDSS system must be updated to prevent attackers from downloading malware into the system in which they can eavesdrop and commit other malicious cyber-attacks.
DOS attack:
DOS attacks can be prevented by only permitting known IP addresses with firewalls configured in the GMDSS system.

2.6 Maritime regulations

The rise of automation and digitalized networks have changed the landscape of maritime shipping but have also introduced cyber challenges that pose a threat to vessels, facilities, and other maritime environments. The inclusion of IT and OT technologies connecting to onboard ships have further increased the attack range that criminals have exploiting these systems. As mentioned in the previous section regarding how impactful these threats are, along with highly publicized incidents such as the NotPetya malware on Maersk, the risk of maritime safety and security due to the cyber-attacks warrants the integration of cyber security in maritime operations [39]. Following the current development of autonomous ships, cyber security needs to be prioritized as the many vulnerabilities tied to automated systems onboard (i.e., ECDIS, GNSS) greatly threaten safety if exploited [40]. The following regulations are discussed in regard to their significance to maritime security.

2.6.1 BIMCO

BIMCO (Baltic and International Maritime Council) is one of the premier international organisations of ship owners globally. Their objectives stem from providing expertise (maritime clause/contract administration) and other services (market insight, training, expert advice etc.) to promote security and value to its members of the maritime shipping industry. In addition, they also support global maritime frameworks such as IMO that help establish transparency and harmony in regulating maritime shipping.

To address the cyber security challenges in maritime shipping, BIMCO and other leading shipping organizations have collectively produced a publication called Guidelines on Cyber Security onboard Ships, which acts as a reference to navigate assessing cyber risk management in the vessel. The main themes of the guidelines focus on Identifying threats, identifying vulnerabilities, assessing risk exposure, establishing response plans, and Response/Recovery from cyber security incidents. These themes help establish the foundation to further strengthen cyber security for vessels [11].

2.6.2 IMO

IMO (International Maritime Organization) is a particular branch of the United Nations whose primary function is regulating the security and safety of maritime shipping as well as impeding the pollution of ships that impact the environment. Part of this function is establishing a universally implemented and adopted regulatory framework which involves all facets of maritime shipping, thus ensuring that shipping operations are done securely, safely, efficiently, and facilitated in an environmental manner internationally. In addressing the challenges that threaten the safety and security of cyber-enabled vessels due to the frequent number of cyber threats performed by attackers, IMO has issued several publications to manage cyber risks that help support safe and secure shipping operations [41].

The guidelines highlighted under IMO's MSC-FAL.1/Cir.3 that address recommendations towards cyber risk management are Guidelines on Cyber Security on boards, IEC 27001, NIST Framework, alongside IACS Recommendation on cyber resilience [4].

2.6.3 ENISA

ENISA is a specialized division of the European Union that is dedicated to obtaining and fostering a high level of cybersecurity throughout Europe. ENISA facilitates this objective by supporting EU cyber security policy, endorsing cyber security schemes certifications that help promote credibility to various ICT products, processes, and services, along with collaborating with other EU entities and member states, thus creating a more robust cyber security infrastructure for Europe and its citizens.

In response to the current cyber security threats and digital transformation that has presented a challenge to maritime security, ENISA has proposed guidelines for cyber risk for port operators to build effective cyber security practices that will improve cyber security infrastructure. Such practices include cyber risk assessment, implementing a plan that addresses cybersecurity awareness, training, improving cyber security maturity and more [42].

2.6.4 IACS

IACS (International Association of Classification Societies) is a non-profit organisation that supports maritime regulation and safety by establishing standards and requirements pertaining

to the design and construction, and equipment placed on the vessels. The IACS, in conjunction with establishing regulation and standards, also involves classification and statutory certification of regulating bodies to ensure transparency, interpretation, and compliance of these regulations are understood, adopted, and implemented in order to establish security and safety in maritime shipping. The classification and certification process are performed by the 12 members of the IACS whose responsibility is to review, mandate, and ensure compliance with IACS requirements related to the security of maritime vessels and environments. IACS, as a collective, have its own guidelines and recommendations regarding implementing cyber security processes onboard vessels, such as Rec 166-Recommendation on cyber resilience and UR E26 and E27 [43].

Rec166 delves into the delivery of cyber resilience OT/IT systems on board and implementing a framework for these systems. UR E26 and E27, respectively, focus on requirements pertaining to cyber resiliency for vessels and onboard equipment and systems, which will be further examined in the later chapter, **cyber requirements and notation**.

Each of the 12 classification members of IACS have their own requirements and guidelines towards cyber resiliency in vessels. Under recommendation 166 as a reference, the rules and regulations of each of the societies are specified according to its own classification criteria. Some of these members will be discussed with their own cyber security requirements in scope in the **cyber requirements and notations section.**

2.7 Marine classification societies

The Marine classification societies are members within the regulatory body of IACS. The members participation with IACS involves implementing, adopting, and enforcing minimum requirements that mirror the current direction of technology and other developments within the maritime industry. Each member, as mentioned, has their own requirements in this regard that focus on the cyber resiliency of vessels [44]. The following will discuss some of the prevalent members of the IACS.

2.7.1 ABS

ABS is an American regulatory body of the IACS founded in 1862, whose focus is providing classification services to marine solutions and promoting the protection of marine environments and facilities. These efforts come in the form of many different services such as compliance services, audits, surveys of ship constructions, development of standards and more. Regarding cyber security, ABS has standards and rules involving the cyber resilience of marine vessels called The ABS Guide for Implementation for Marine and Offshore Assets as well as an added section based on IACS UR E26 and UR E27 [45].

Within the Implementation for Marine and Offshore Assets, the notations that are discussed are CS-Ready, CS-System, CS-1, and CS-2 [46].

2.7.2 DNV

DNV is viewed as the world's leading class society and the primary member of the IACS society. Originated as Det Norske Veritas in Norway in 1864, it joined forces with Germanischer Lloyd (GL) from Germany and was fused as DNV GL but reverted back to DNV in 2021. DNV's classification services are centred around vessels and offshore facilities and certification services on materials, components, management systems, and competency. DNV's standards on cyber security for vessels have been developed to examine the cyber security needs of the operations within the ship and protect the integrity of functions offshore and newly constructed ships [47].

DNV's cybersecurity guidelines for vessels are implemented around three notations Cyber Essentials, Cyber Secure and Cyber Secure+. These three notations are aligned with IEC 62443 series, specifically 62443 3-3, which modelled IACS UR E26/E27. The notations match the security level of what threats the attacks are derived from [48].

2.7.3 LR

Lloyd's Registry is the British representative member of the IACS and the world's first maritime classification society. Founded in 1760, working in over 70 locations, and providing

services to customers from 182 countries, LR's work pertains to classification, compliance, and consultancy services in offshore facilities and marine environments [49]. LR's involvement in cyber security standards for marine environments have documents dedicated to the integrity of cyber security for vessels called LR CS ShipRight procedure for owners, operators, and third-party vendors [50].

2.7.4 BV

Bureau Veritas is an IACS member based in France that was founded in 1828 and is one of the founding members of the IACS society, along with being one of the largest classification societies. Bureau Veritas responsibilities outside classification services is to provide verification compliance services and develop standards toward cyber security to marine and offshore businesses that will ensure their safety and security with a presence of 1,600 offices within 140 countries [51].

BV's contribution to cyber security regulation on vessels comes in the form of NR 695 rules [52]. These Rules adhere to IACS compliance and IMO that provides shipowners and suppliers a guideline to meet compliance with testing and hardening onboard systems before vessels are constructed. NR 695 has several notations in regard to the security level of cyber security robustness, which are Cyber Secure, Cyber Managed, and Cyber Resilient.

2.7.5 CCS

Chinese Classification Society is a classification member of the IACS society based in China, with Beijing as its main headquarters. The CCS was established in 1956 and is acknowledged as the government authority of 60 big international shipping countries and houses more than 120 offices worldwide. The CCS's function involves providing services such as classification, certification, and surveys, in addition to establishing regulatory standards [53]. Involving addressing cyber security, CCS has produced two regulatory documents named Guidelines for Requirement and Security Assessment of Ship Cyber System and Guidelines on Maritime Cyber Risk Assessment and Cyber Safety Management System [54].

2.8 Industry Standards

Thanks to the effects of Industry 4.0, maritime operations are now connected to digital systems involving IT and OT technology to maximise navigation and transportation capabilities. As a common challenge with systems connected digitally, it leaves vulnerabilities that can exploit, causing further damage to the systems and compromising the safety of the ship, equipment, and personnel onboard the vessel. To help reduce these issues, cyber security is implemented as part of maritime operations, from the construction, design, and commission of the vessel along with the systems integrated onboard. Different Industry standard frameworks of cyber security are used that are designed to protect the OT/IT assets that control and support IACS and ICS processes. The following subsections will highlight the more prominent frameworks used in maritime shipping.

2.8.1 IEC 62443 series

The 62443 series is a framework developed by the IEC comprised of security controls enforced to ensure the protection of IACS processes. Because IACS is integral to critical infrastructure such as shipping, the framework encapsulates all the components involved within the lifecycle of IACS, such as the processes, the security controls, and the competence of personnel. These components are disassembled into nine standards categorized into four themes: General, Policies and procedures, System, and Components and requirements, as shown in Table 9. The General theme covers the first standard, 62443-1-1, which delves into the terminology, context, and frameworks of the 62443 body. Policies and procedures cover the next three standards, 62443-2-1, 62443-2-3, and 2-4. The System topics break down the next three standards 62443 3-1, 62443-3-2, and 62443-3-3. Lastly, the subject Components and requirements highlight the last two standards, 62443-4-1 and 62443-4-2 [55].

Table 9. IEC 62443 Framework

IEC 62443 Framework

General	Policies	System	Component
62443-1-1 Terminology, Concepts and Models	**62443-1-2** Establishing an Industrial Automation and Control System Security Program	**62443-3-1** Security Technologies for IACS	**62443-4-1** Product Development Requirements
62443-1-2 Master Glossary of Teams and Abbreviations	**62443-2-2** IACS Protection Levels	**62443-3-2** Security Risk Assessment and System Design	**62443-4-2** Technical Security Requirements for IACS Components
62443-1-3 System Security Conformance Metrics	**62443-2-3** Patch Management in the IACS Environment	**62443-3-3** System Security Requirements and Security Levels	
62443-1-4 IACS Security Lifecycle and Use-Cases	**62443-2-4** Requirement for IACS Service Providers		
	62443-2-5 Implementation Guidance for IACS Asset Owners		

2.8.2 NIST Cybersecurity Framework

NIST cybersecurity framework is a standard developed by the National Institute of Standards and Technology (NIST) and is based on other common cybersecurity standards, recommendations, and functions for organizations to manage their cybersecurity risk. It was developed to provide a comprehensive language for managing and expressing amongst internal

and external stakeholders regarding risk and cybersecurity management. The framework is centred around five functions named Protect, Detect, Identify, Respond, and Recover, and within each function is a category pertaining to the specified pillar, such as Asset Management under Identify or Data Security under Protect, as shown in Figure 1. Under the category are subcategories or requirements that describe the activity or guideline based on the specified category [56]. These subcategories are referenced from other standards, including IEC 62443, that can also be used for integrating security controls in maritime systems.

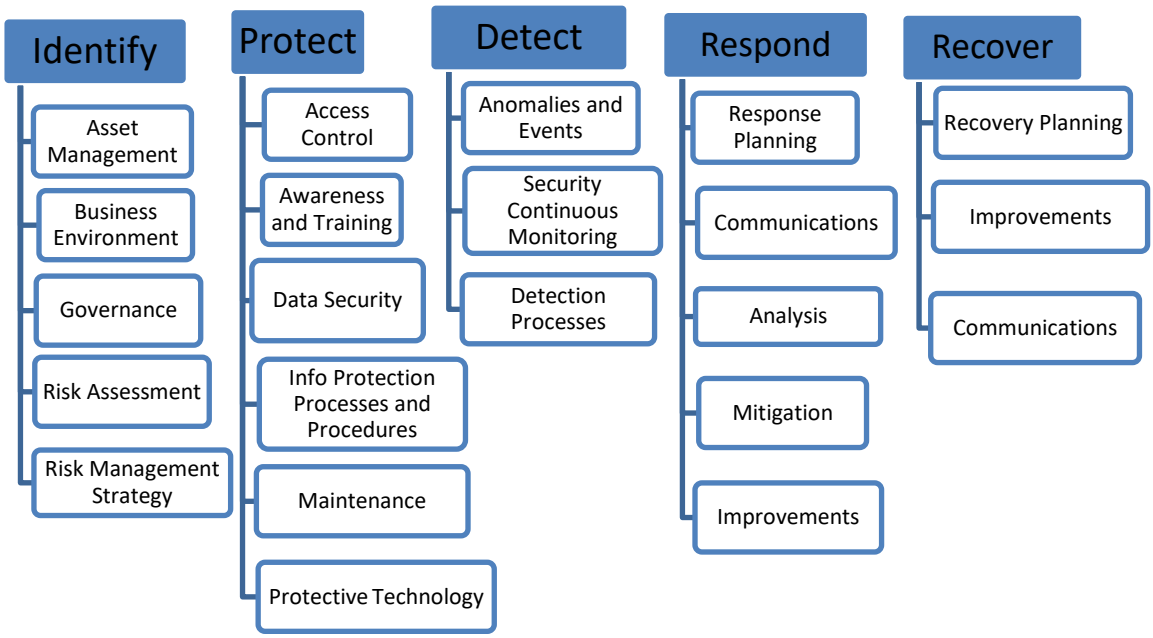


Figure 2. Diagram of NIST Cyber Security Framework (CSF)

2.9 Cyber security requirements of maritime standards and class societies with class notations

This section will delineate common cyber security standards involved with maritime shipping and highlight the different notations within the standards that will differentiate the various levels of security impacted by the requirement.

2.9.1 IEC 62443-3-3

IEC 62433-3-3 is a prominent cyber security standard applied towards IACS (Industry Automated Control Systems) systems. 62443 3-3 is relevant in regard to being used as a basis for creating requirements centred around the resiliency of ship systems since 62443-3-3 is correlated with some of the classification societies (i.e., DNV, BV) in their cybersecurity frameworks. 62443-3-3 comprises seven Foundation requirements (FR) (Identification and authentication control, Use control, System integrity, Data confidentiality, Restricted data flow, Timely response to events and Resource availability) that describe the main topics that cover the specific requirements. In addition to the FRs, there are Requirement Enhancements (RE) that strengthen the security for the given requirement. Security Levels (SL 1-4) measure the capacity of which the systems are protected from vulnerabilities that can be exploited [57]. An example of a few requirements is indicated in Tables 10-12.

Table 10. SR 1.1 Human User Identification and Authentication

Requirement from Identification and authentication control category regarding identifying all human users.

5.3 SR 1.1 – Human user identification and Authentication
5.3.1 Requirement The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

Table 11. RE of SR 1.1-Human user and authentication

Requirement enhancements based on the current security level (SL) for strengthening the security of the security control.

Requirement 5.3.3 enhancements
5.3.3.1 SR 1.1 RE 1 – Unique identification and authentication The control system shall provide the capability to uniquely identify and authenticate all human users. **5.3.3.2 SR 1.1 RE 2 – Multifactor authentication for untrusted networks** The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks). NOTE See 5.7.3.5.7.3.1, SR 1.5 – Authenticator management, RE 5.7.3.1 for enhanced authenticator management for software processes. **5.3.3.3 SR 1.1 RE 3 – Multifactor authentication for all networks** The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.

Table 12. Security Levels for Requirement SR 1.1

Security levels 1-4 assigned to requirement SR 1.1. based on the measure of confidence that the security control is free from vulnerabilities.

5.3.4 Security levels
The requirements for the four SL levels that relate to SR 1.1 – Human user identification and authentication are: • SL-C (IAC, control system) 1: SR 1.1 • SL-C (IAC, control system) 2: SR 1.1 (1) • SL-C (IAC, control system) 3: SR 1.1 (1) (2) • SL-C (IAC, control system) 4: SR 1.1 (1) (2) (3)

2.9.2 DNV GL-SHIP RULE

The CYBER SECURE notation series is part of a three-series class notation that establishes an adaptable and organized foundation for the construction and implementation of controls to identify, detect, respond, and, lastly, recover from cyber security incidents [58] (Chapter 5 Section 21). The different levels that are messaged within DNV are **Cyber Secure, Cyber Secure(essential), and Cyber Secure (Advanced).**

- **Cyber Secure:** Identifies the default level for cyber risk reduction and acts as the common baseline for all the requirements. The default notation covers the most impactful vulnerabilities to a system and is established as security profile 0 for the Systems Under Considerations (SuC).

- **Cyber Secure (Essential):** Considers ships that have fulfilled an essential level in implementing security control. It covers the existing underliers of the first notation but focuses on the control systems, mainly that it satisfies the capabilities of security level 1 under IEC 62443.

- **Cyber Secure (Advanced):** The last notation, Cyber secure (Advanced), addresses the same range of Cyber secure (Essential), but the security level has been upped to 3 (security profile 3 to address how to protect systems against more sophisticated (advanced) attacks. Figure 3 shows the layout of how the notations are assigned according to the Security level that is highlighted.

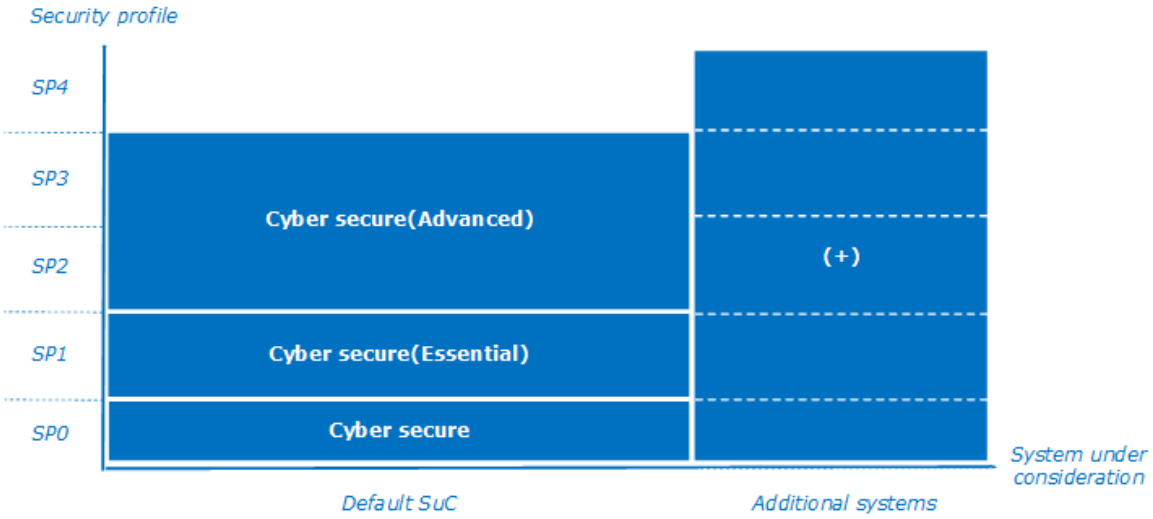


Figure 3. DNV Cyber Secure Notations. Ranges from SP0 being bare minimum to SP1 (Essential) equivalent to IEC 62443 3-3 SL1 and SP3/SP4 (Advanced) equivalent to SL 3 of IEC 62443 3-3

An example of a requirement from DNV-GL SHIP RULE under identification and authentication is Identifier management. This requirement details the capability of identifying and authenticating human users. In addition, it enforces identification and authentication on all interfaces that provide human user access to control systems that support segregation of duties and least privilege. Table 13 showcases more information about Identifier management including its summary, Security Level, and compliance parameters.

Table 13. Description of Requirement Identifier Management

Description of Requirement Identifier Management which is equivalent to SR 1.4 Identification management from IEC 62433 3-3.

Requirement summary and amendments	*SL*	Compliance
See IEC-62443-3-3 SR 1.4 It shall be possible to manage identifiers in the system. The intention is to allow for segregation of duties and least privilege by assignment of different privileges depending on user, role, group or interface.	*SP0* *SP1* *SP2* *SP3* *SP4*	N/A YES YES YES YES

2.9.3 LR Cyber ShipRight

The LR Cyber ShipRight framework has two notations used toward fulfilling cyber resiliency goals within the cyber security framework in LR. The two notations are **Cyber Security ShipRight (Design & Build) and Cyber Security ShipRight (Operational**). The one that will be observed is LR Cyber ShipRight (Design & Build)

LR Cyber ShipRight (Design & Build)

This ShipRight notation focuses on security controls pertaining to network architecture, configuration, design and build of new systems. The target audience for this notation is tailored for the ship integrators and suppliers of systems. Furthermore, the ShipRight notation is mapped to both mandatory IACS E27 controls and 62443-3-3 security requirements.

The areas covered under ShipRight (Design & Build) includes Asset Management, Authentication & Authorization, Secure Networks & Systems, Risk Management & Assurance, Handover & Delivery.

In addition, there are four descriptive notes (DN) that coincide with the Security Levels of 62443 3-3 and there are **Established, Enhanced, Accomplished,** and **Optimised**.

- **Established** levels represent the baseline requirements required to meet compliance from organizations like BIMCO, IMO, and TSMA and equivalent to the SL1 from 62443.

- **Enhanced** levels indicate a higher level above the basic level of cyber maturity for organisations and equals the Security level 2 of 62443-3-3
- **Accomplished** levels would indicate more advanced capabilities to deal with higher levels of cyber risk and associates with the Security Level 3 of 62443-3-3.
- **Optimised** levels detail capabilities from a mature cyber security model that have been assured regarding processes in detecting and responding to cyber threats [59].

The following table depicts one of the requirements from the Asset & Data Management Pillar and the descriptive notes that are associated with it.

Table 14. LR CS ShipRight requirement: Asset/Data Mgmt.

Description of Asset and Data Management requirement from Asset Management Category

Sub-Domain	**Build/Design Controls Description**	**Level 1(Established) Outcomes**	**Level 2(Enhanced) Outcomes**	**Level 3 (Accomplished) Outcomes**	**Level 4 (Optimised) Outcomes**
Identification of critical assets	The shipyard must ensure an inventory of critical assets is produced and handed over to ship operator. Note: Critical assets are defined as those computer-based systems that are directly used to monitor, and control ship systems.	There is a list of inventories for computer based systems that are directly used to control, alarm and monitor ship systems. The list is updated during the life of the ship. The list will include both hardware and software for these systems that is essential for its operation.	Any changes to the software or hardware assets in the inventory list is tracked to ensure new vulnerabilities and dependencies are assessed. There is a network diagram to illustrate communication between vessel systems, their physical location, system categorisations, VLAN and IP details, network technology and topology used, cable type,	A design philosophy document should be produced for identified assets to introduce asset purpose. A system diagram should be produced for identified assets to show communication channels and dependent systems. For software inventory, name and publisher, installation date, version number and motivations, maintenance type (local/remote),	

			details of external connections	accounts type (generic/dedicated),	

2.9.4 ABS CyberSecurity Implementation For The Marine and Offshore Industries

ABS CS Notations

The notations behind ABS are applied when conducting cybersecurity reviews and surveys of OT and IT systems on vessels and offshore equipment. These notations are **CS-System, CS-Ready, CS-1, and CS-2** described as follows:

- **CS-System:** Applies to the supplier or Original Equipment Manufacturer (OEM) equipment built onto a specific vessel. This notation also verifies that the systems in place is issued an ABS CyberSafety PDA Certificate. In addition, the CS-System notation can be used to satisfy the later CS-1 and CS-2 security requirements.
- **CS-Ready:** Applies to the shipyard integrator for specific ships and documents that cybersecurity procedures and controls are implemented into essential OT/IT systems during vessel construction. In addition, this notation is utilized by the organization to satisfy both CS-1 and CS-2 requirements.
- **CS-1/CS-2:** Applies to an Organization, shipowner, or vessel manager for specific ship and documents that the ship has fulfilled the necessary requirements for a cyber security program [60].

Here lie some of the requirements for the CS-System notation from Table 15. This pertains to suppliers such as Wärtsilä.

Table 15. ABS CS-system requirements

Describes CS-system requirements pertaining to suppliers once they have acquired their PDA certificate from ABS class.

#	ABS CS-System Requirements	References
1	Person or persons responsible for cybersecurity of the OEM enterprise and products is documented.	ABS CyberSafety Vol-7, Subsection 2/5 **1 – CS Representative**
2	Foundational cybersecurity guidance applied by the OEM to the enterprise and products are to be submitted to ABS.	
3	Copies of quality or cybersecurity certificates held by the OEM are to be submitted to ABS.	
4	OEM cybersecurity policies and procedures are documented that govern: ● Cybersecurity training in cyber hygiene and specialized cybersecurity functions. ● Physical access security. ● Digital access authorization of OEM personnel and contractors, including enrolment and unenrolment. ● Digital access authorization of OEM installed and portable digital devices.	ABS CyberSafety Vol-7, Subsection 2/5 **2 – Policies & Procedures**
5	The composition, responsibilities, capabilities, and staffing of the OEM cybersecurity Incident Response Team are documented.	ABS CyberSafety Vol-7, Subsection 2/5 **3 – Incident Response**

2.9.5 CCS- Guidelines for Ship Security 2023

The new recent edition of CCS Guidelines for Ship Security 2023 is now more correlated with IEC62443 3-3, and so the notations of CCS M/P/S reflect that 62443 3-3 security levels 1-4. CCS has three notations **Class M**, **Class P**, and **Class S** described as follows:

- **Class M:** Class M is the lowest notation and signifies that the cyber risk management requirements are fulfilled.

- **Class P:** Class P is the standard notation for CCS cyber security and indicates that basic network security requirements for the vessel are met. Essentially this notation is equivalent to the minimum-security level (SL 0) of 62443-3-3.

- **Class S:** Class S is the higher notation for CCS cyber security and pertains to the higher cyber security requirements for the vessel that must be met. This notation equates to SL 1-4 of 62443 3-3 [61].

The following Tables 16-18 show how some of the requirements (SR1.1) are formulated and show how identical they are to 62433 3-3.

Table 16. SR 1.1 Requirement User Identification and Authentication / Requirement Enhancements (RE)

SR 1.1User identification and authentication requirements extracted from IEC 62443 3-3

SR Number	Requirement	Security Level 0	Security Level 1	Security Level 2	Security Level 3	Security Level 4
SR 1.1	CBS It shall be possible to identify and authenticate all persons accessing the system.	✓	✓	✓	✓	✓
SR 1.1 RE 1	CBS it shall be possible to uniquely identify and authenticate all persons			✓	✓	✓
SR 1.1 RE 2	CBS Multi-factor authentication should be used for people accessing through untrusted networks	✓	✓	✓	✓	✓
SR 1.1 RE 3	CBS-Multi-factor authentication should be adopted for all personnel					✓

Table 17.SR 1.2 Requirement Software and device identification and authentication

SR 1.2 Software and Device Identification and Authentication Requirements extracted from IEC 62443 3-3

SR Number	Requirement	Security Level 0	Security Level 1	Security Level 2	Security Level 3	Security Level 4
SR 1.2	CBS shall be possible to identify and authenticate all processes and devices accessed through the interface	✓	✓	✓	✓	✓
SR 1.2 RE 1	CBS shall be able to uniquely identify and authenticate all software processes and devices				✓	✓

Table 18. SR 1.3 Requirements Account Management

SR 1.3 Account Management requirements extracted from IEC 62443 3-3

SR 1.3	CBS shall provide the ability to support authorized users to manage all accounts, including adding, activating, modifying, deactivating and deleting	✓	✓	✓	✓	✓

2.9.6 BV-NR 659

BV-NR 659 has three notations pertaining to the cyber security of vessels that are outfitted with onboard equipment and networks that may be assigned to new ships or currently built ships depending on the specifications of the notation. These notations are **CYBER MANAGED, CYBER SECURE, AND CYBER RESILIENT**.

- **CYBER MANAGED –** This notation equates to the first security level for newly constructed and current vessels. The notation essentially covers categories of personnel training, remote access, critical equipment, and cyber and change management.

- **CYBER SECURE-** The CYBER SECURE notation pertains to newly constructed ships secured by design. This notation addresses requirements involving equipment hardening and vessel secure by design.

- **CYBER RESILIENT-** This is a new notation established by BV to conform to the mandatory compliance of IACS UR E26/E27 requirements focused on cyber resilience of new vessels when confronting cyber threats. This notation covers the cyber resilience of ships that is applied under UR IACS UR E26 for shipowners/integrators and the cyber resilience of onboard equipment and systems under IACS UR E27 that applies to suppliers [62].

Table 19 shows depict some of the requirements for Cyber Resilient Notation (onboard systems and equipment /IACS UR E27).

Table 19. Cyber Resilient Notation Requirements

Requirements Si No. 1-4 are extracted from IACS UR E 27, which is based on the IEC 62443-3-3 requirements.

Si No.	Objectives	Requirements
1	Human user identification and authentication	The CBS is to identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS is to provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS is to provide the capability to support the management of identifiers by user, group and role (IEC 62443-3-3/SR 1.4)
4	Authenticator management	The CBS is to provide the capability to: • Initialize authenticator content • Change all default authenticators upon control system installation • Change/refresh all authenticators • Protect all authenticators from unauthorized disclosure and modification when stored and transmitted. (IEC 62443-3-3/SR 1.5)

3 Methodology

Research by Sekaran [63] is defined as the systematic and coordinated process of investigating a specific problem in order to find a solution. This process is conducted through systematically analyzing, gathering, evaluating, interpreting, and reporting data, with the aim of identifying patterns that provides the answer to the problem. The purpose of conducting the research is either to add to the existing body of knowledge by developing new theories or improving the existing ones in that field. Depending on the study, several methodologies can be explored to conduct the research, such as qualitative research, quantitative research, applied research, analytical research, descriptive research, fundamental research, empirical research, conceptual research, and others.

The research methodology in this thesis will be performed via qualitative research. Qualitative research, as defined by Aspers and Corte [64], describes the multi-method approach of interpreting empirical data, whether it is through the means of personal experience, case studies, interviews, visuals, texts and more, in order to delineate a deeper understanding of human phenomena in its natural setting. Afterwards, the researcher can use the conclusion from the research to answer the question of "why" rather "what" is not observed in solving the dilemma to the problem. Doing so can expand the current theory with new insights and knowledge or evolve into unfamiliar territory with new challenging concepts that enrich the theoretical framework of the subject matter.

3.1 Case Study

Wärtsilä is an Original Equipment Manufacturer (OEM) and service provider of lifecycle solutions. A part of their activities involves providing services that pertain to maintaining cyber resilience to onboard systems/vessels and mitigating risk as enforced under the ISM Code supported by the IMO's MSC Resolution 428(98). This compliance is implemented in several maritime cyber security frameworks, including IEC 62443, IACS classes (e.g., ABS, DNV) and other standards [56]. The cyber security measures that entail product development for Wartsila's lifecycle solutions in fulfilling this compliance are applied in our Secure Development Lifecycle (SDL) model, which is based on the IEC 62443 standard. The part of the SDL model that will be focused on is Product Security Development, most specifically the

review of security requirements as it pertains to the central theme of the thesis regarding compliance [65].

Wärtsilä's approach towards cyber security compliance for their maritime product development entails tracking several security requirements from different cyber security standards (IACS classification societies, IEC standards, and customer requirements). In addition, these cyber security standards are later assessed against Wartsila's maritime products to see if these products meet compliance requirements for certification under specified maritime regulation bodies (IACS classes, IEC). These compliance requirements might either be requested by the customer or deemed mandatory by maritime regulation (IACS) from implementing new regulations toward improving maritime cyber security within the industry (IACS UR 27). Because of the ever-changing landscape of cyber security in maritime operations, certain regulations are put into effect in order to improve maritime security. Such regulations are IACS UR requirements E26 and E27, implemented for new vessels for January 1, 2023 [66]. Because E27 emphasizes the supplier's responsibility to ensure cyber resilience with onboard equipment in ships, there is a necessity for fulfilling compliance under E27. Monitoring market cyber security standards and analyzing them against their products provides assurance that Wartsila's as a supplier when it comes to meeting compliance requirements by maritime bodies and is trustworthy as a service providing upon providing adequate cyber security services for external customers looking to address compliance gaps within their assets. As there are many standards in the maritime industry, there are challenges in managing the maintenance of simultaneously tracking relevant standards for product security and assessing products against different cyber security requirements for class certification and sales. Polarion, an application lifecycle management (ALM) tool, has been utilized to optimise certification and compliance analysis activities for our products by synthesizing all the cyber security requirements from different standards and documenting them under Polarion.

3.2 Polarion Software

Polarion, a software founded in 2004, and purchased by Siemens, a Germany Manufacturer company, is a unified solution utilized for requirements management in relation to software and product development lifecycle. Its deep functionality in change and configuration management, metrics and audit reports, reuse management, test management, issue management and many

more allows for flexibility in collaboration, traceability, workflow, optimized productivity, and automation towards demonstrating evidence of compliance as described in Figure 4 [21].

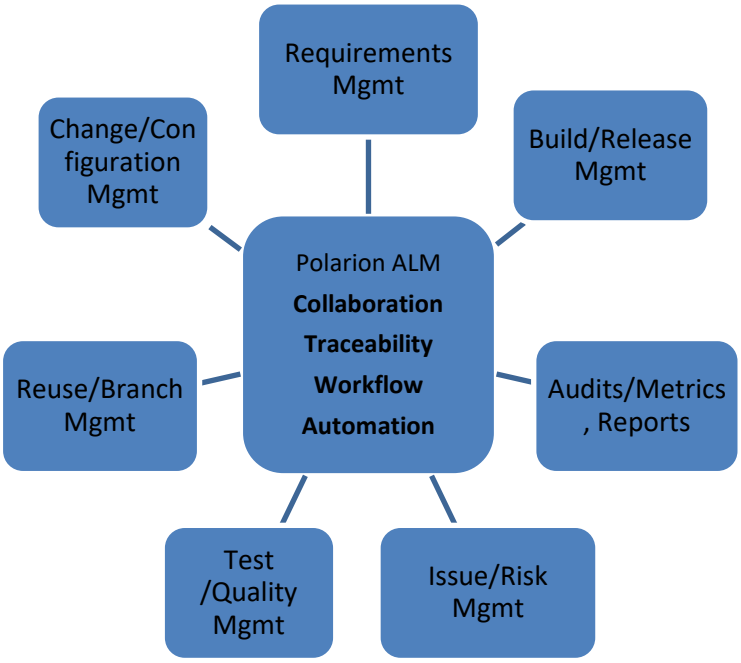


Figure 4. Features of Polarion ALM Software

3.2.1 Polarion functionality in tooling for compliance analysis in Wärtsilä

The motive for utilizing Polarion in Wärtsilä is using an interface that efficiently tracks and gathers requirements from several cyber security standards to be used for documentation and conducting Compliance Gap Assessments toward fulling compliance regulations for external customers and classification societies. This involves a streamlined process for creating repositories for storing the documents/creating tasks, importing the requirements, and converting them into work items that can be used for establishing gap assessments, correlation between different requirements, issuing tickets on JIRA platform, and updating the document metadata to for more functionality.

3.2.2 Repositories for Cyber Security Compliance Tracking

Within the main repository, there are several projects pertaining to the compliance tracking of cyber security requirements for Wärtsilä. The main projects that are covered within the repository are Product Security Requirements, Assessments (Marine, Energy), and Security Engineering & Architecture. Each of these projects have their own spaces pertaining to the components within that service, such as Cyber security standard documents for Product Security Requirements, Requirement Assessment templates for Marine and Energy Cyber Assessment, and tasks for compliance tickets for Security Engineering & Architecture. Figure 5 displays the layout for the mentioned projects. In addition, the next subsection describes what is contained in the projects.

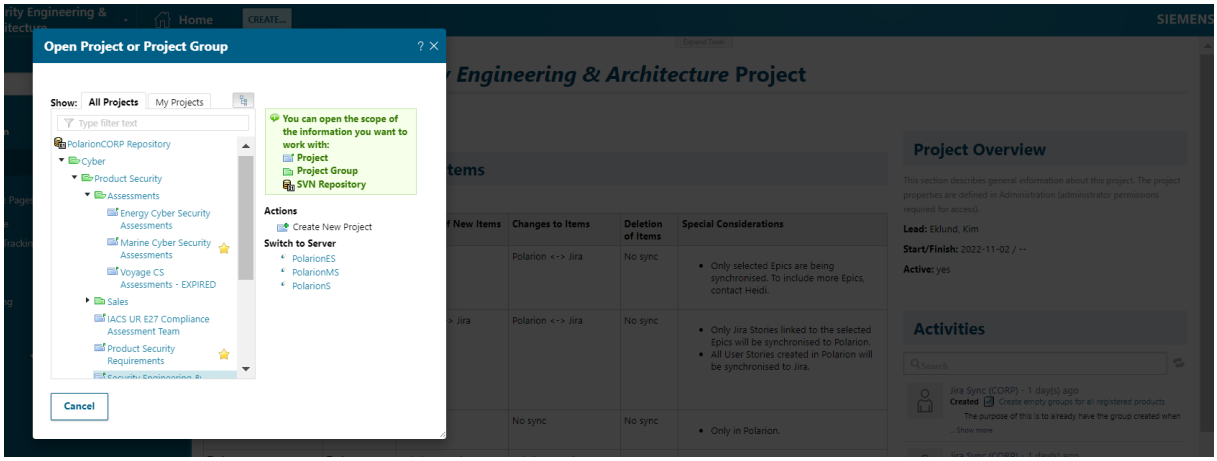


Figure 5. Wartsila Polarion CS Compliance Projects pertaining to compliance assessments of market products.

3.2.3 Product Security Requirements

The project is a depository for all the cyber security documents imported into Polarion. The cyber security documents contained in the space are derived from classification societies requirements (i.e., IACS, ABS, DNV, CCS, BV, LR, CLASS NK), standard (IEC 62443, 61162, 63154), external customers, and Wärtsilä's baseline requirements as shown in Figure 6.

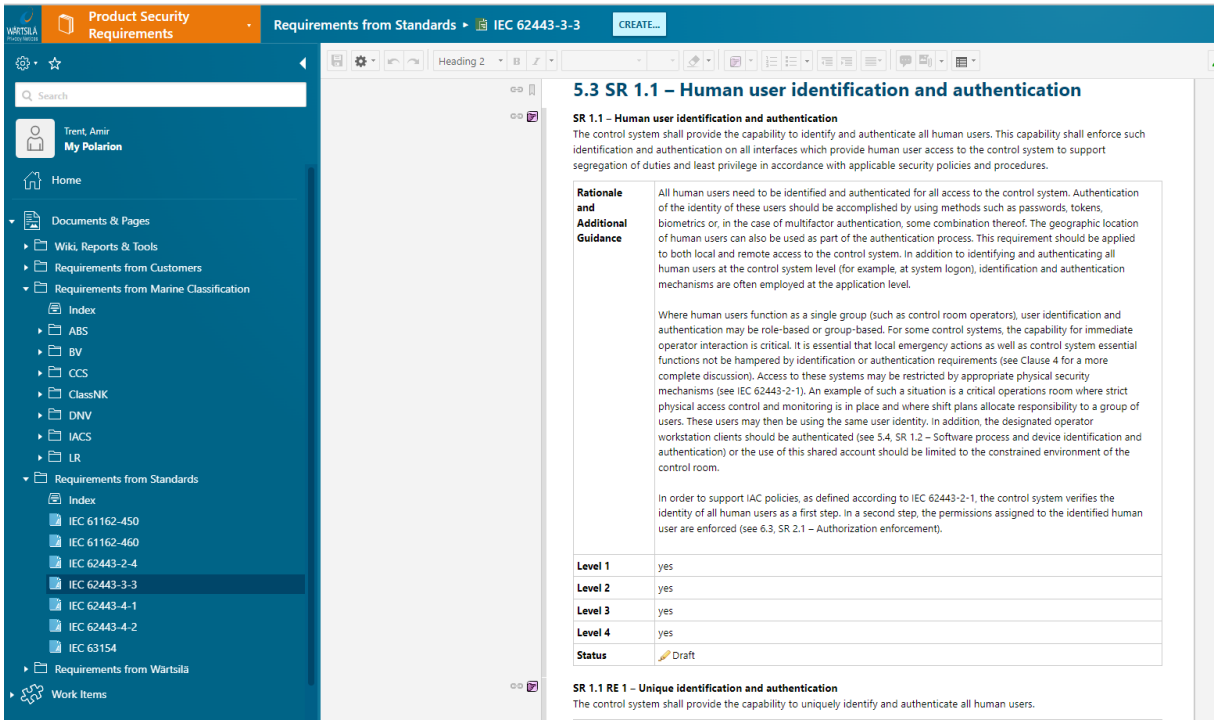


Figure 6. Display of SR 1.1 Human user identification and authentication requirement in IEC 62443 3-3 configured as a work item requirement in Polarion from our Product Security Requirements Project

In addition, each of the requirements within the documents is converted into work items such as SR 1.1-Human user identification and authentication from the IEC 62443-3-3 document, as shown in Figure 6. This will be further discussed regarding the nuances of the construction of work items later.

The other documents within the Product Security Requirement Project, in addition, have reports, tools, and wiki that support the usage of how the requirements as work items will be utilized, including correlation between requirements from different standards, new releases of cyber security requirement documents from the maritime classes, creating a template for compliance assessment of a product as depicted in Figure 7.

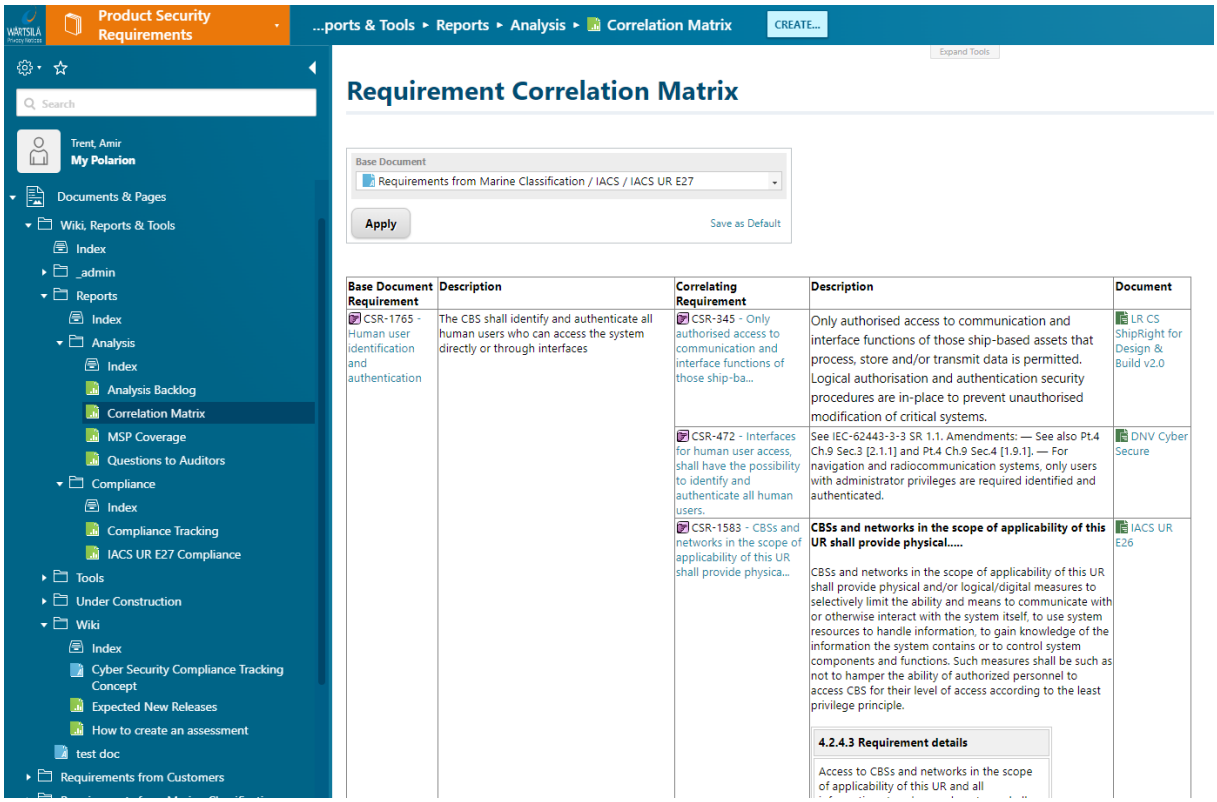


Figure 7. Configuring work items from requirements in original documents (i.e., IEC 62443, DNV, IACS UR E 27) to indicate correlation between other requirements.

3.2.4 Marine Cyber Security Assessments

The Marine Cyber Security Assessments project consists of templates derived from the original cyber security requirement documents in the Product Security Requirements project. The derived templates are used to conduct gap assessments of the maritime products against specific cyber security requirements in question. This assessment of the product will be used as a reference for auditing purposes towards meeting compliance for certifications from a class society or demonstrating compliance with various standards for external customers. In addition, there are other tools used to support the analysis of a product's assessment, such as monitoring the current status of an assessment with Assessment Backlog, the results of an assessment with Assessment Report, and comparison between two assessments with Assessment Compare to identify disparities of compliance from the two. The main page of Marine Cyber Security Assessment, as depicted in Figure 8, shows some of the products from different business units, such as Marine Power, where the assessments are maintained, and the aforementioned features (e.g., Assessment Backlog, Report, and Comparison).

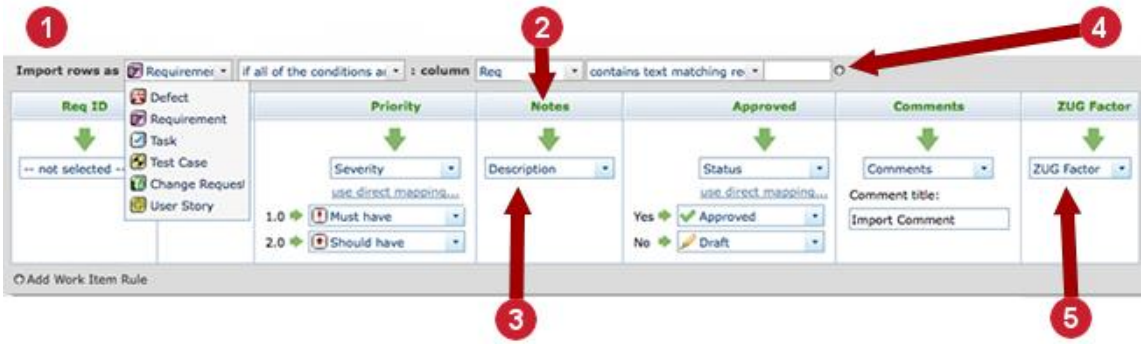
Figure 8. Collection of Maritime Products selected for Cyber Security compliance assessments.

3.2.5 Requirement Work Items

Once the requirements are imported into Polarion via Manual or through Excel worksheet as illustrated in Figures 9 and 10, the requirements can be converted into work items based upon the work items type that are configured. Once these requirements are converted into work items, then the work items can be further customized with default or customized metadata fields [58].

3.2.6 Requirement Fields

As mentioned in the previous section, fields are properties used to enhance the functionality of the work items. The work items can be categorized and modified for tracking, reporting, and conducting test cases which will be displayed in the analysis section [67]. In the administration page, as pictured in Figure 11, the custom fields can be customized into several types (e.g., Boolean, Enumeration, String text) to further improve the categorization of the work items for tasks such as the correlation of several requirements. The primary fields that were created for the Product Security Requirements Project to be used for the cyber security requirements alongside the marine assessments are depicted in Figures 12 and 13 how they appear in the work item properties sidebar after being created, such as field 62443 references.



1-Work Item import rule
2-Excel Column
3-Setup of Fields
4-Conditional rule
5-Custom field configuration

Figure 9. Example of automatic import of cyber security requirements extracted from excel worksheet.

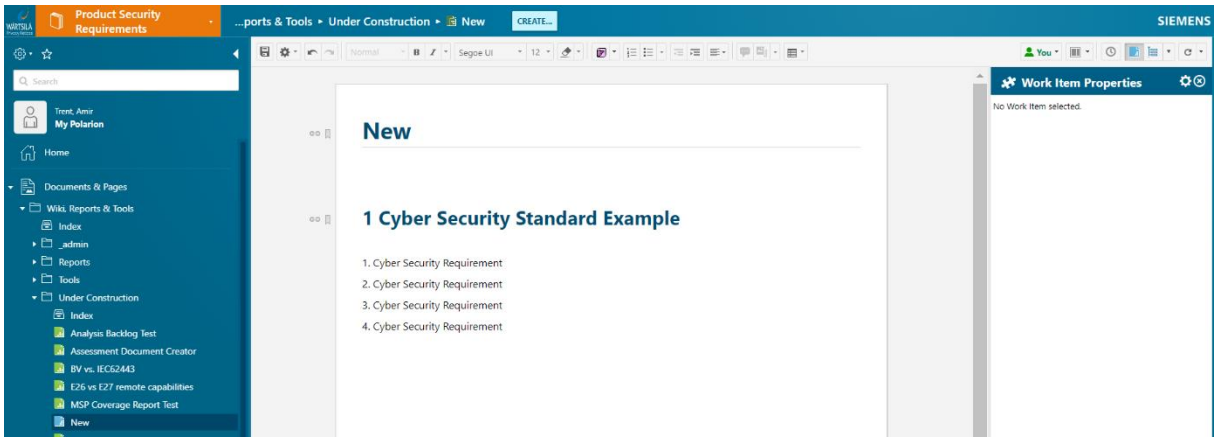


Figure 10. Example of manual import of cyber security requirements via copy/paste from original documents.

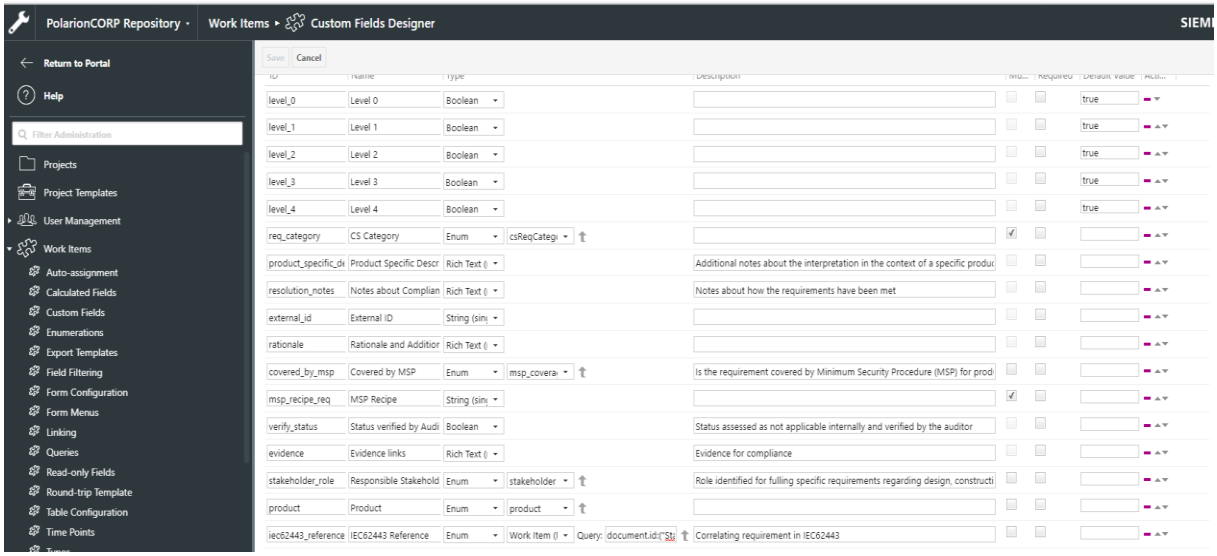


Figure 11. Configuration of default custom fields via administration configuration page.

Attribute	Description / Purpose
Title	Short summary of the requirement
Description	Longer description of the requirement
External ID	ID of the requirement in the original document, if available
CS Category	Category of the requirement
Level 0/1/2/3/4	Security levels in which the requirement is applicable in the original document
Responsible Stakeholder	Stakeholder identified to be responsible of the implementation of the requirement
IEC62443 Reference	IEC62443-3-3 or IEC62443-4-1 requirement that the requirement correlates with
Covered my MSP	If the requirement can be fulfilled by complying with the Wärtsilä's Minimum Security Procedure or not
Rationale and Additional Guidance	Rationale and Additional Guidance related to the requirement from the original document

Table 2 Additional attributes to be filled in during the assessments

Attribute	Description / Purpose
Product Specific Description	This field can be used to add a context specific description for the requirement in the assessed product context
Status verified by Auditor	This field can be used to mark that the assessment result has been verified by an auditor, i.e. it is not only an internal assessment
Notes about Compliance	Use this field to describe how the compliance has been achieved or why the requirement is not applicable for the product
Evidence Links	Add links and description of the evidence that can be used to prove compliance with the requirement
Status	In the assessment, the status is the compliance status.
Resolution	

Figure 12. Example of Custom fields created from configuration page to trace requirements and use for compliance assessments.

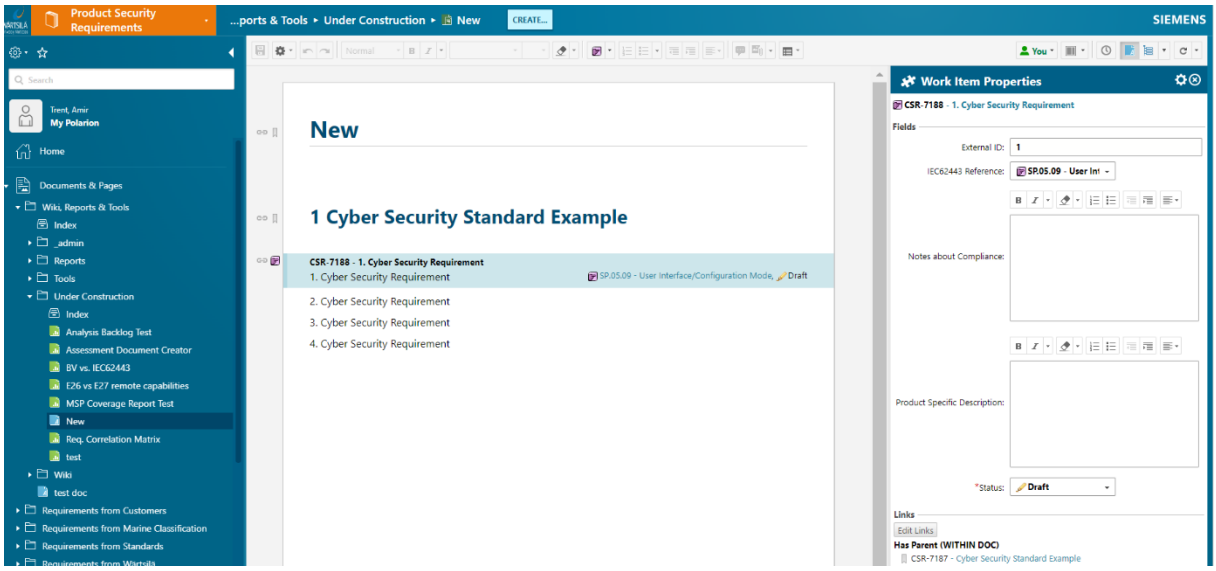


Figure 13. Example of how fields are displayed from the sidebar of work item requirements when selected. Field IEC 62443 3-3 as shown from the sidebar is configured to align its specific requirement to the work item.

3.3 Data Collection

The data collection from qualitative research for this thesis will be conducted through desk review, survey, and case study of Wartsila's activities on compliance analysis of cyber security standards and requirements for maritime product development.

3.4 Desk Review

Bowen [68] defines the desk review methodology as an organized process that analyses and studies pertinent documents for a particular study or research. The cause behind this qualitative research methodology is to interpret and examine data that correlate with existing evidence of information and can yield credibility to the prevalent body of theoretical knowledge. Desk reviews have five important functions which it is used in qualitative research such as: providing insight on background information pertaining to the context of the study, secondly to produce questions that expand upon the current arguments of a particular field, third to support research data using other sources of data (e.g., surveys, interviews), fourthly it is used to compare previous documents and identify new developments, and lastly it can be used as a means to corroborate evidence between other materials.

In this desk review, the materials that were analyzed pertained to cyber security standards from IACS classification standards, NIST website, IEC-62443, and guidelines from maritime regulation bodies such as BIMCO, IMO, and ENISA. The significance behind these cyber security standards is that they are based or loosely correlate around 62443 as it involves automatic controls and other systems that are now implemented in onboard systems, so the cyber security requirements from ship suppliers, shipowners, and integrators reflect that. Table 20 details the documents of the cyber security standards that were obtained. The reasoning behind obtaining these documents is because they pertain to the current landscape of maritime cyber security, in which these requirements are implemented toward protecting onboard equipment on vessels.

Table 20. Cyber Security Standards/Frameworks

Prevalent Cyber security Standards that are used in assessing the compliance of cyber security in ships and onboard equipment/products.

Maritime Regulation	**Standard/Guideline**
BIMCO	Guidelines on Cyber Security Onboard Ships
IMO	Recommendation 166
IEC	62443 series
NIST	CSF/800-82/
IACS	UR E 27 Cyber Resilience of Onboard Systems and Equipment
LR(IACS)	LR Cyber ShipRight for Design and Build
DNV(IACS)	DNV-RU-SHIP Pt.6 Ch.5 Sec.21
ABS(IACS)	ABS CyberSafety for Equipment Manufacturers
CCS(IACS)	CCS Guidelines for Requirement and Security Assessment of Ship Cyber System 2020
BV(IACS)	BV-NR659 Rules on Cyber Security For The Classification of Marine Units

3.5 Survey

Surveys are utilized as a part of qualitative research to obtain information from participants that indicate opinions, ideas, narratives, patterns, and experiences on a particular topic [69]. This would be administered through answering a series of open-ended questions that will help generate rich data on the given subject. With multiple people from various backgrounds and

experiences answering the questions, surveys can help produce data from several perspectives, adding flexibility and variety to the research. Surveys can be distributed in 3 main methods such as person to person contact surveys, telephone surveys, or online surveys. The latter was performed for this thesis.

The advantage of conducting online surveys is that they are relatively easier to obtain responses from participants and less time-consuming compared to the telephone and contact survey method, can be distributed across a wide range of people that may not respond or receive the survey simultaneously, and responses are easier to be interpreted with pre-typed answers. Inversely, with online surveys, questions can be misleading, which may consequently evoke answers that are not pertinent to the main topic in the survey. In addition, having a narrow sample can distort the results of the survey.

3.5.1 Survey Questionnaire

The survey was conducted with 11 employees from Wärtsilä, of which seven members belong to Maritime product development, and 4 participants are members of Maritime Cyber Security involved in security architecture and cyber security compliance and certification review. In regard to their work experience with maritime products, 5 participants have worked within 3-6 years, three members have 7-10 years, and three have worked longer than 11 years, as indicated in Figure 14.

The main question of the survey pertained to what the most relevant cyber security maritime requirements are observed for compliance within maritime product development according to the participants from a scale of not at all to very relevant. Based on that metric with eight cyber security standards from class societies and IEC (e.g., IEC 62443, 61162-460, BV, DNV, LR, CCS, ABS, and IACS UR E27), the results are as shown in Table 21 and Figure 15.

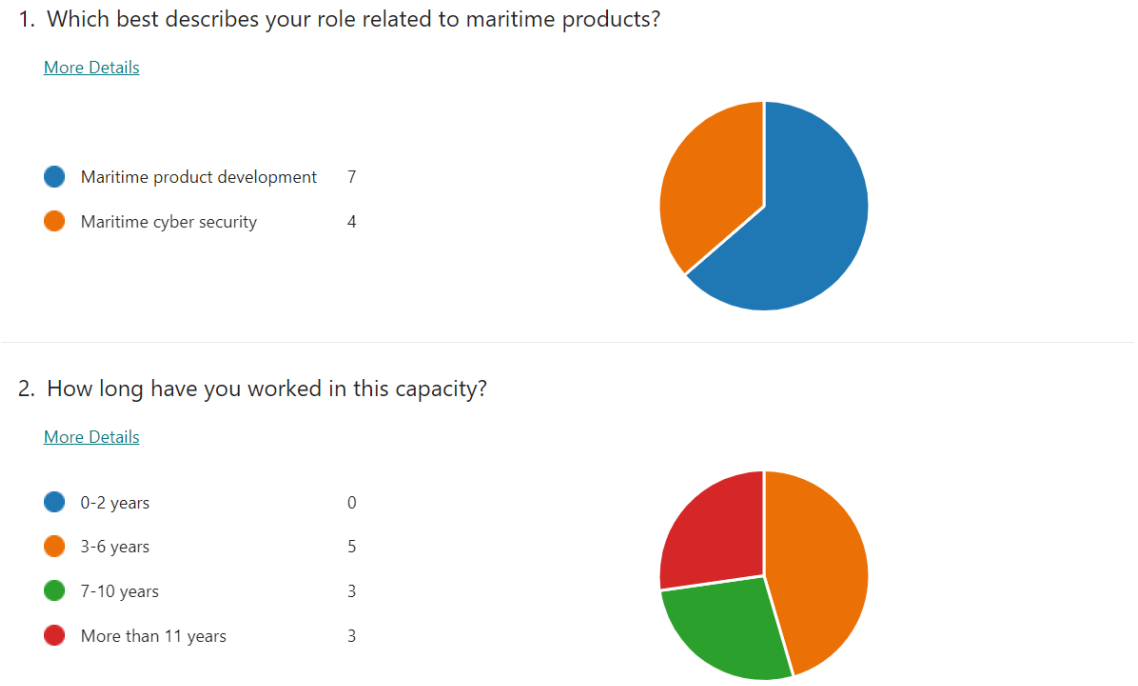


Figure 14. Data on participants roles and years of occupancy

Table 21.Cyber Security Compliance Survey Results

The results for the relevant cyber security standards in terms of compliance for maritime products.

Cyber Security Standards/Frameworks	Not at all Relevant	Neither Relevant	Neither Relevant nor Relevant	Relevant	Very Relevant
IEC 62443		18.2%		18.2%	63.6%
IEC 61162-460	9.1%	27.3%		18.2%	45.5%
BV	9.1%		18.2%	45.5%	27.3%
DNV				54.5%	45.5%
LR	9.1%	9.1%	27.3%	18.2%	36.4%
CCS	9.1%		27.3%	36.4%	27.3%
ABS	9.1%	27.3%		36.4%	27.3%
IACS UR E27	11.1%	22.2%			66.7%

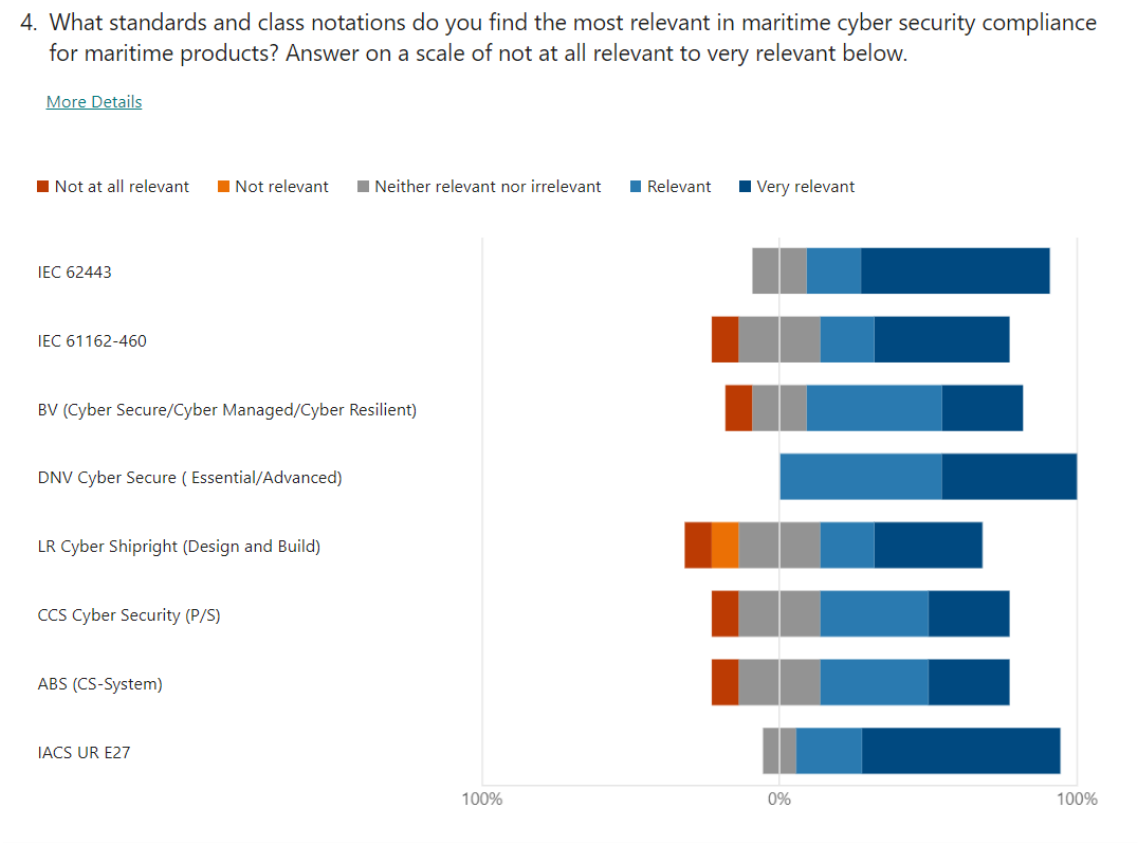


Figure 15. Results from selected standards in terms of relevancy in maritime cyber security compliance.

Based on the survey results, the standards deemed Relevant or More relevant compared to the rest of the standards were DNV, IEC 62443, and IACS UR E27. The reason for this is because a majority of the maritime products that are being assessed for certification and compliance against the different cyber security standards are through DNV, as it is the biggest classification society stated by [70], IEC 62443 3-3 as it is part of our product cyber security development activities and is internationally recognized regarding cyber security of industrial automation and control systems and for IACS UR E 27 as suppliers such as Wartsila must meet its security requirements under IACS. As a result of the compliance requirements of UR E 27, classification societies such as DNV, BV, LR, and CCS have started to modify their cyber security requirements to align better with IACS UR E 27 requirements using 62443 3-3, 62443 4-1 as references. Because IACS UR E 27 is based on IEC 62443 standards, it is easier for suppliers who are trying to be certified under maritime classes like DNV to meet their class requirements and obligatory requirements like IACS UR E27. Considering IEC 62443 and IACS UR E27 are the most relevant standards from the survey, it is important to see how maritime products can

meet these requirements under compliance regulations. This is where Polarion will be used in analysing how the products can be tested for compliance in the Analysis section.

4 Implementation of Polarion Software for Compliance Analysis

From the data gathered from the survey and desk review, The analysis portion was conducted through the tracking of the relevant requirements (62443, DNV, IACS UR E 27) that was imported into Polarion, upon which a correlation matrix of requirements vs 62443 was analyzed, and then concluded with an assessment of a simulated product against two requirements to verify the compliance and correlation with other the other standards using IEC 62443 as a baseline.

4.1 Tracking relevant cyber security standards for compliance

Based on the survey, these are currently the prevalent requirements that are tracked for compliance in Wartsila's maritime products whether, upon request by external customers, looking for certification from maritime classes, or using baseline standards such as IEC 62443 to develop other sub-standards in product security development. Polarion can be used for gathering, managing, and documenting the specific standards for eventual assessments of products against the specific standard. As shown in Figure 16, the compliance tracking delineates how the requirements will be stored. Starting with the main container Product Security Requirements is where all the requirements categorized as Class requirements (e.g., ABS, BV, CCS, DNV), Standard requirements (IEC 62443 series, 61162-460, 63531), Customer Requirements (e.g., Rolls Royce, Carnival), and baseline requirements (derivative of IEC 62443 3-3). Figure 17 shows IEC 62443 3-3 security requirements as it looks when documented, and Figure 18 outlines configuring the metadata properties of the requirements as work items. These metadata fields can be configured accordingly to how the requirements are going to be managed regarding traceability, workflow, reporting etc.

The next section within the same Polarion Repository, as shown in Figure 16, is the Product Security Assessments container containing Maritime Cyber Security Assessments pertaining to compliance assessments of maritime products and Energy Assessments pertaining to energy-based products. Inside the assessments, multiple products from our Marine business function can be selected and analyzed during internal audits to see address compliance gaps and discern how they measure up against standards used for certification or sales.

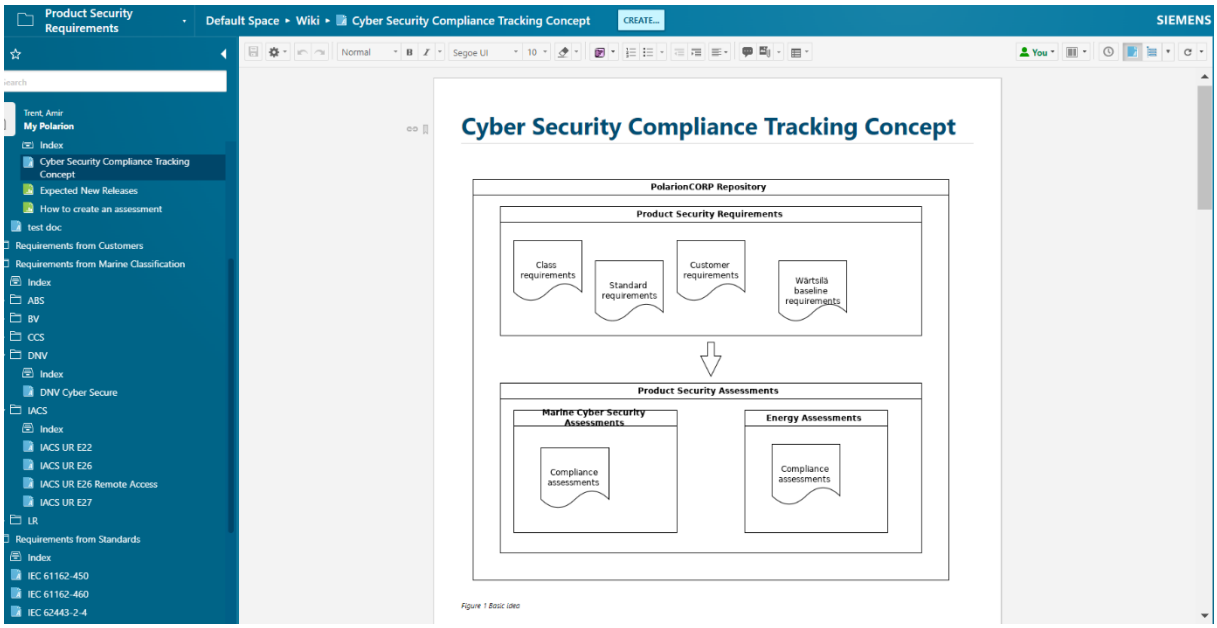


Figure 16. Compliance Tracking Concept for maritime requirements

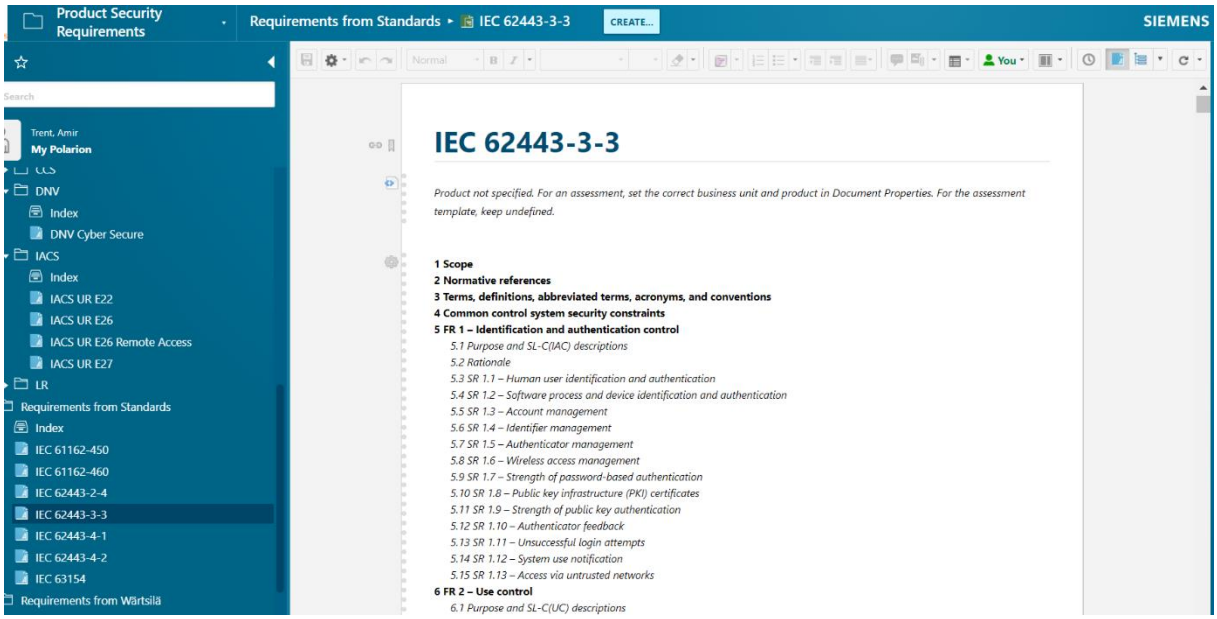


Figure 17. IEC 62443-3-3 imported into Polarion as work items.

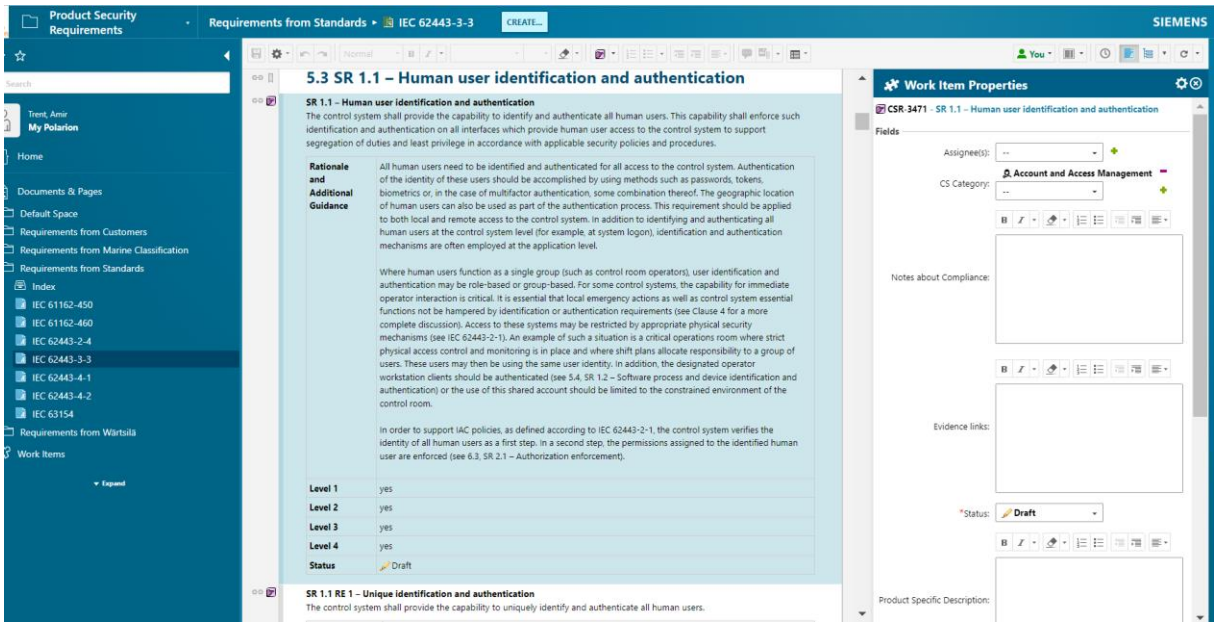


Figure 18. Requirements from 62443 3-3 as work items being modified with the custom fields.

4.2 Current gap of other classifications of requirements vs 62443 requirements

In compliance analysis of products against cyber security standards, tracking gaps of requirements against other requirements such as our baseline 62443, helps address compliance requirement gaps that are needed for protecting our products and assuring the fulfilment of those compliance requirements from different maritime classes.

Using Polarion under Product Security Requirements, a Correlation matrix was created to assess which requirements are mapped depending on how they correlate with each other from the description of the requirement. Taking several of the standards and class notations from the survey, such as DNV cyber secure, we can see how much some of its requirements are aligned between IEC 62443 3-3 and IACS UR E27 as shown in Figure 19. Because DNV requirements with Cyber Secure notation are based on IEC 62443 3-3 along with IACS UR E27, the majority of the DNV requirements, if not all, correlate with both 62443 3-3 and IACS UR E 27. Another requirement, such as LR (Cyber ShipRight) Design and Build, may not be completely aligned with IEC 62443 requirements regarding the vulnerability management process, as shown in Figure 20. By showing how these requirements correlate or differ, you can identify gaps within the requirements that allow for easy traceability for compliance audits and discern missing security controls needed for onboard products delivered to external customers.

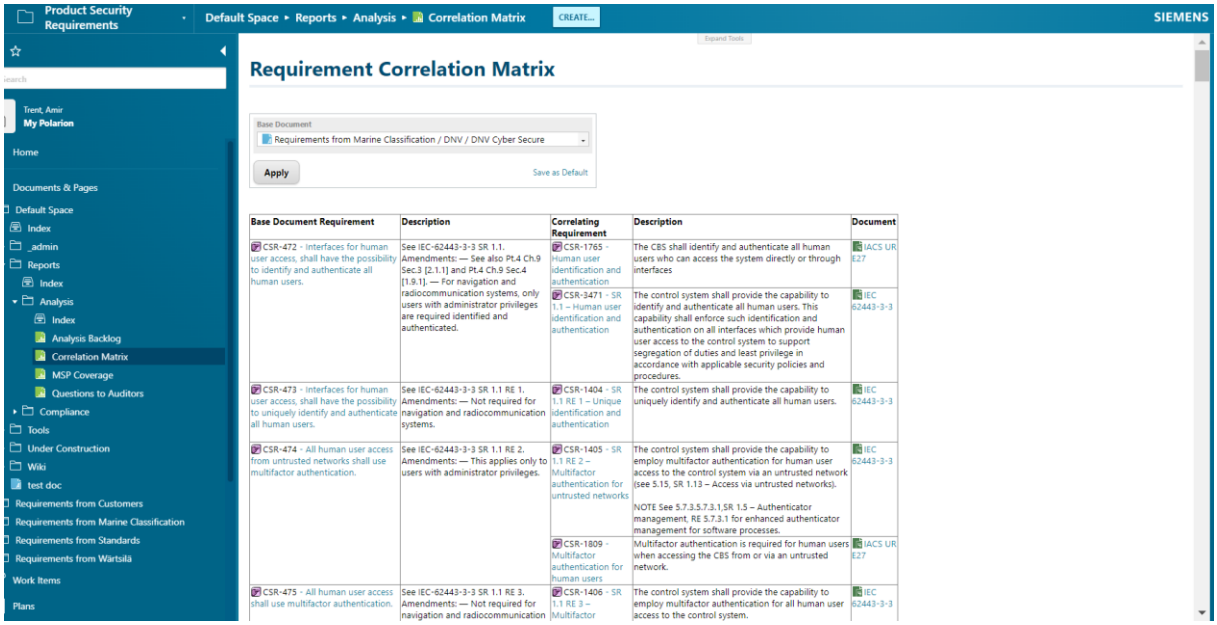


Figure 19. Correlation from some of the requirements of DNV, 62443 3-3, and IACS UR E 27

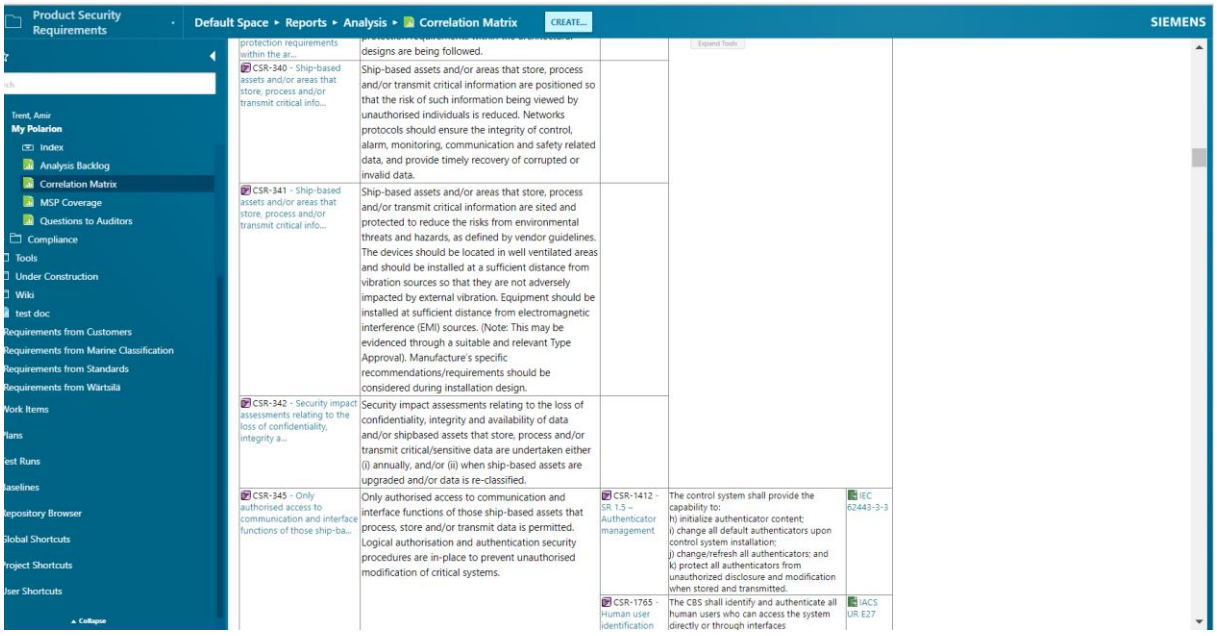


Figure 20. Some of the requirements from LR CS ShipRight that correlate with IEC 62443 3-3 and IACS UR E 27

4.3 Polarion analysis of compliance

Regarding maritime product assessments, the analysis is performed by reviewing the cyber security standard under which a maritime product is being examined for compliance and addressing any requirement gaps that have not been satisfied. An assessment starts with a created template derived from a document with the original maritime cyber security standard requirements. The following step is inserting the metadata fields (id, 62443 reference, evidence links, notes of configuration, compliance status, description) that will be used to mark the compliance status and trace the evidence links for compliance. Figure 21 shows the setup for creating an assessment template and the result indicated in Figure 22, which will showcase the assessed product (WCM) title along with the derived fields ready for assessment.

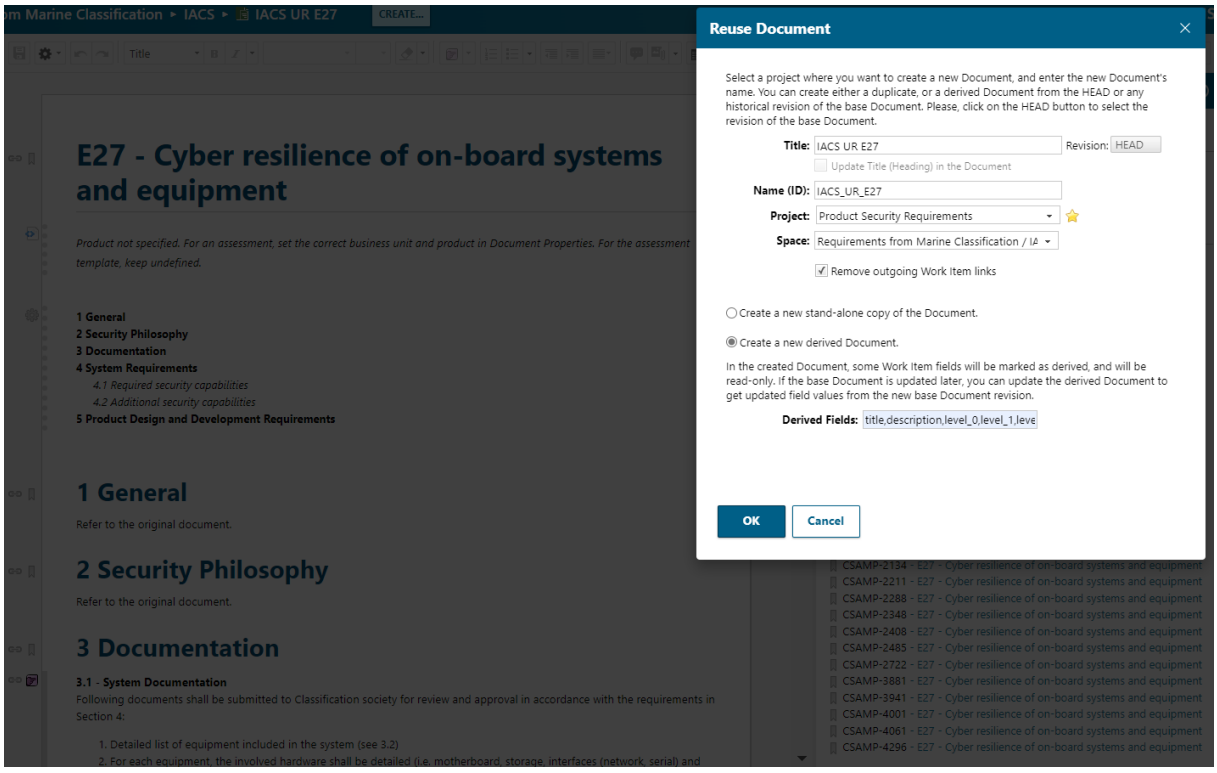


Figure 21. Configuration for Product Compliance Assessment of IACS UR E 27 template.

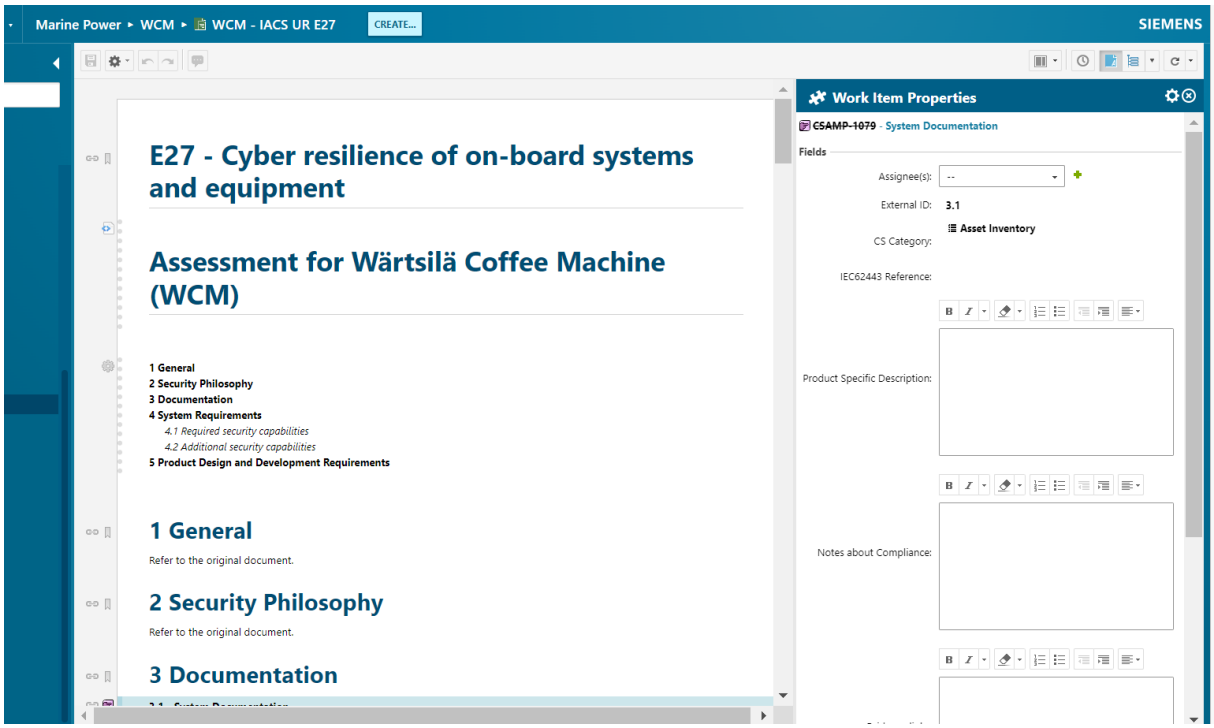


Figure 22. Created Compliance Assessment for product (WCM) against IACS UR E 27.

Now that the template is created with the necessary fields, all the requirements are then reviewed between a cyber security expert and product member against the WCM product and marked for being compliant or not in the status, along with inputting relevant notes in the fields related to the highlighted requirement as indicated in Figure 23.

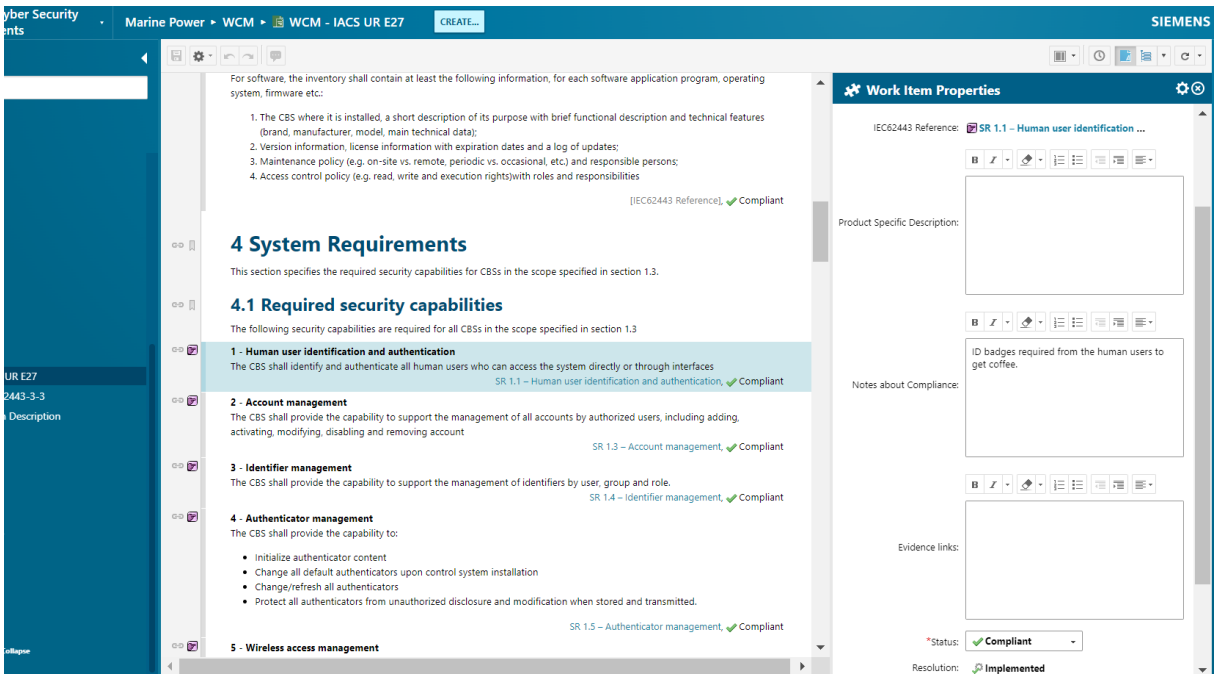


Figure 23. Illustration of how work items and custom fields created from requirements IACS UR E27 are used for assessing the compliancy of product WCM.

5 Compliance Assessment Results and Discussion

A gap assessment was used from the configured work items and metadata fields derived from the IEC 62443 3-3 document in Polarion to determine the compliance of maritime product against IACS E27. Based on this assessment using an Assessment Report and Assessment Compare and a more readable format for interpretation, the gap of compliance can be measured along with an indicator of compliance from any cyber security requirement that hasn't been assessed yet by comparing their correlation.

5.1 Assessment Report

The Assessment Report is a dashboard used to examine the results of an assessment of a product against a cyber security standard. The categories that make up the assessment report are seperated into Non Compliant Items, Mitigated Items, Compliant, Unclear and Not Applicable.

- **Non-Compliant Items**- Requirements marked as non-compliant against the product
- **Mitigated Items**- Requirement Items that have been compliant but with mitigations.
- **Compliant Items**- Requirement items that meet compliancy.
- **Unclear Items**- requirements that are uncertain for declaring (compliancy/non-compliant, N/A..etc)
- **Not Applicable**-Requirement items not applicable for compliance.

5.1.1 Assessment Report Results

The results for the WCM for IACS UR E27 displayed in Figure 25 were largely compliant from 40 out of 52 Compliant requirements, with 1 deemed as unclear, and 10 assessed as N/A or out of scope due to not being connected to a network. Based on this result, WCM is able to satisfy cybersecurity requirements mandated by IACS when undergoing an external audit. This gives customers an idea as far as how close or how far the product is towards meeting compliance with cyber security standards, in this case, IACS UR E27. A more readable format of the assessment can be submitted to interpret the compliance gap of the requirements, as shown in Figure 24

The results for the WCM for 62443 3-3, as depicted in Figure 26, were not compliant with only 3 items out of 52 requirements that satisfied compliance, 86 items that were Not Assessed and 10 items that were tested as Non Applicable and 1 item being unclear. This signifies to the customer that the current assessment is non-compliant because there is a high compliance gap based on the number of assessed requirement items. Although there is a low number of compliance items due to a lot of unassessed requirements, the product does meet compliance with the same requirements that were examined in the WCM/IACS UR 27 assessment, based on IACS UR E27 being aligned with IEC 624433-3.

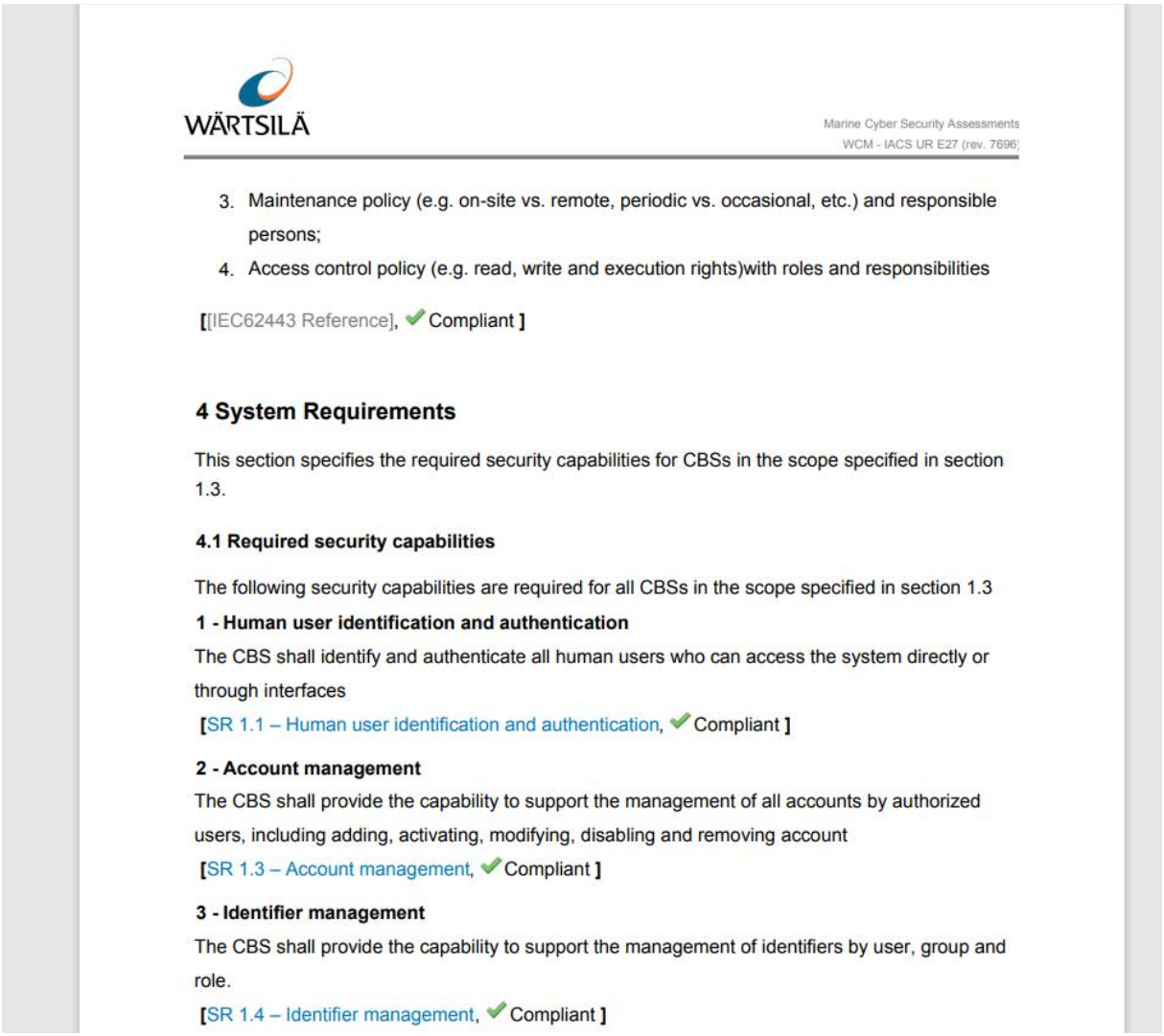


Figure 24. PDF format of Compliance Assessment of WCM without fields configuration.

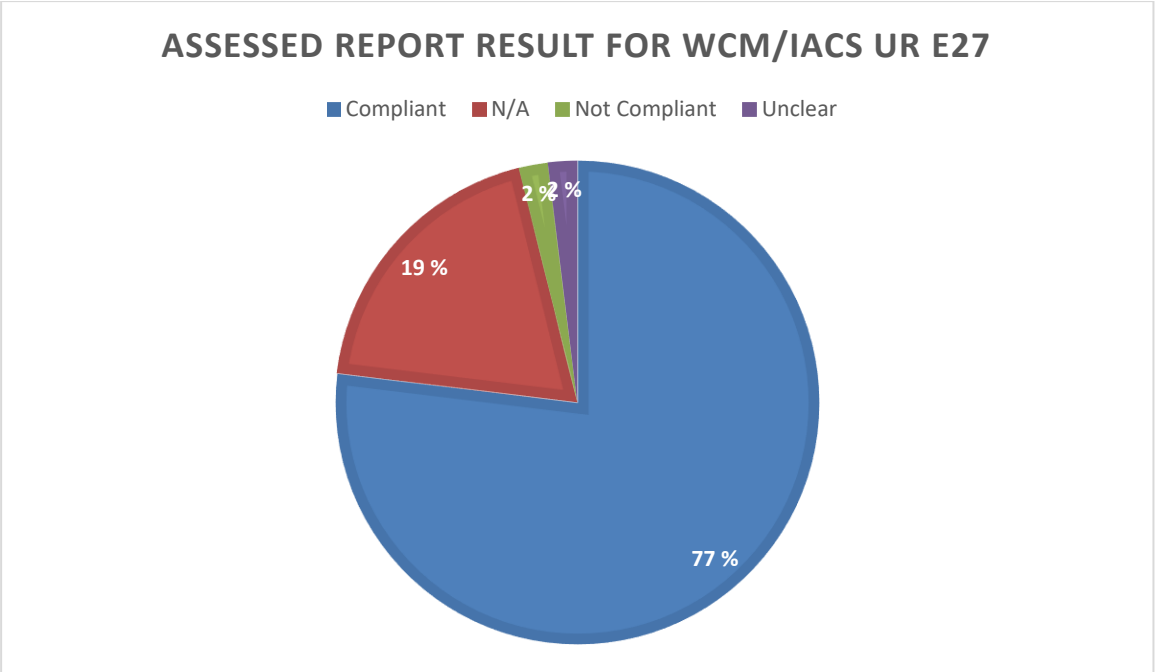


Figure 25. Assessment report results for WCM product compliance with IACS UR E27 cyber security requirements.

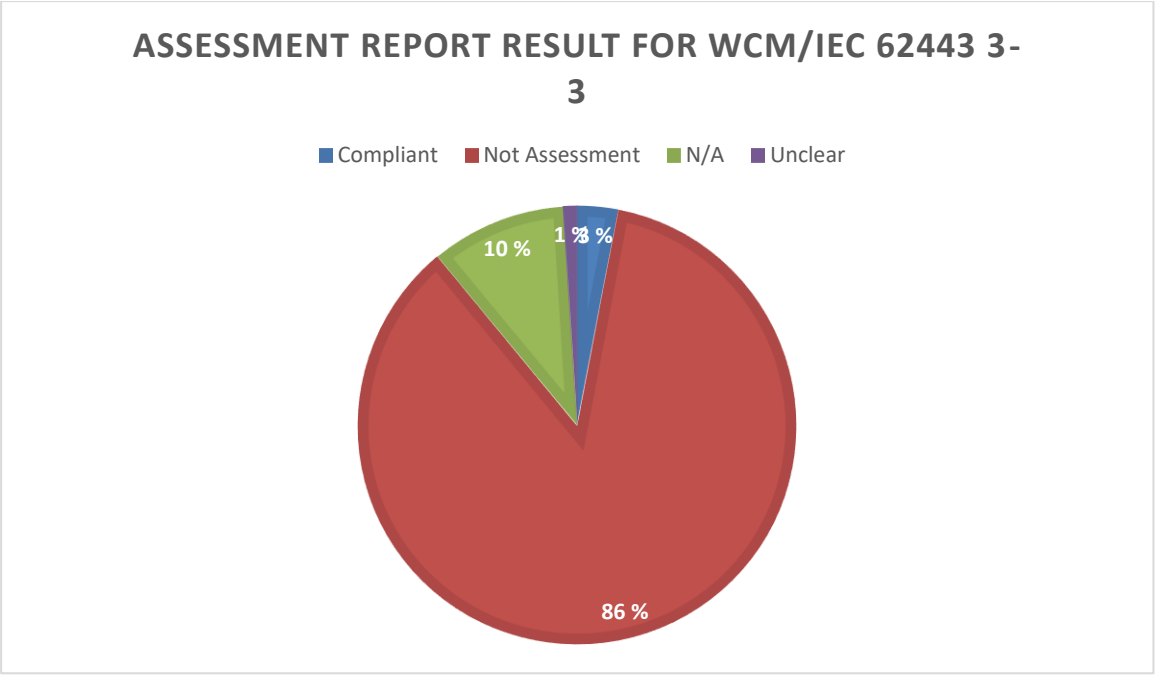


Figure 26.Compliance Report result for WCM product against IEC 62443 3-3 cyber security requirements.

5.1.2 Assessment Comparison

The Assessment Comparison report is used to compare two assessments against each other. In addition, this report also allows the user to derive an assessment for a set of requirements based on another assessment that has been completed. Using IEC 62443 3-3 as a reference baseline, the report will assess if the 1st assessment is correlated with an IEC 62443 3-3 reference against another assessment with IEC 62443 3-3 references from a derived document. If there is a correlation, the result will produce the assessment results from the requirements of the derived document against the requirements of the first document based on how many requirements that are assessed. In addition, the assessment comparison report can also show the probability of compliance from a set of requirements that haven't been assessed against a product yet versus an already assessed document.

5.1.3 Assessment Comparison Result

Based on comparing the documents from WCM (IACS UR E27) and WCM (IEC 62443 3-3), the results were rendered as 41 out of 100 requirements matching (41.0%) with 30 requirements under Compliant, one requirement under Unclear, 10 requirements under N/A and 38 requirements as Not Assessed as shown in Figure 27. Given the fact that IACS UR E27 requirements are based on IEC 62443 3-3 requirements, the rate of correlation between the two assessed documents would be higher if the remaining 38 non-assessed requirements were analysed.

In regard to comparing the document from WCM (IACS UR E27) with DNV Cyber Secure requirements that have not been assessed yet, the results are 41 out of 100 requirements (41.0%) matching with 30 requirements deemed Compliant, 59 requirements deemed Not Assessed, 10 requirements that were tested as N/A and 1 requirement for Unclear. This signifies that the same WCM product that was assessed with IACS UR E27 cyber security requirements can also meet the same level of compliance with DNV Cyber Secure requirements if the 59 requirements that were Not Assessed are assessed as compliant.

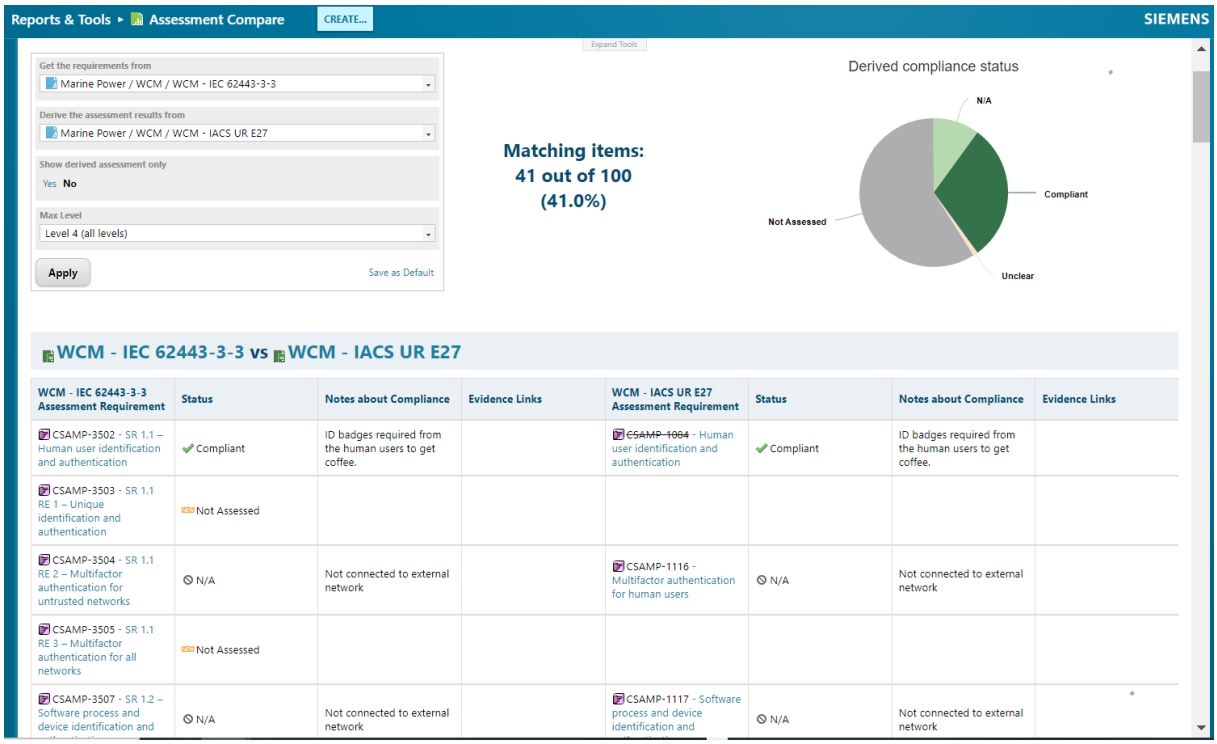


Figure 27. Results from correlation of compliancy between both IACS UR E27 and IEC 62443 3-3 for product WCM

5.1.4 Interpretation of Results

The results compiled from the Assessment Report and Assessment Comparison indicate that any product that is assessed with requirements that are mapped with IEC 62443 3-3 can meet compliance with other cyber security requirements that correlate with IEC 62443 such as IACS UR E27 or DNV Cyber Secure.

5.2 Discussion

Due to the impact cyber threats have on the current status of maritime safety and security, maritime bodies such as IMO and IACS class societies have implemented security requirements towards how onboard equipment needs to be integrated into vessels to increase cyber resilience. To fulfil compliance towards these requirements that are relevant for maritime products, Wartsila is utilizing Polarion for capturing the necessary requirements and assessing them against our products. The results gathered displayed how compliant the product was against mandatory standards like IACS UR E27 and prevalent ones like 62443.

The results indicated that IACS UR E27 and 62443 3-3 have correlations with each other when analysing them against maritime products for cyber security compliance. This will support class

standards and other standards that have a linkage between the requirements of 62443 3-3, making the compliance assessments easier for products that require certification from standards that are aligned under 624433 3-3 and IACS UR E27, such as DNV Cyber Secure standard or LR Cyber ShipRight. For the standards whose requirements that do not correlate with 62443 3-3, Polarion helps track the relevancy of those requirements to further improve our baseline requirements within 62443 in our secure product development phase.

The generalizability of the results can be impacted by the low sample size of the participants from the survey. Furthermore, the survey participants being from Wärtsilä could open up the possibility for interpretations of biases, thus affecting the credibility of the survey and the analysis results. Despite these concerns, the results and the survey are valid due to all IACS classification societies basing their cyber security requirements on IEC 62443 3-3 to support meeting mandatory compliance from IMO and IACS (UR E 27). In addition, all vessels that are classified are required to comply with IACS UR E 27, which is based on 62443 3-3, so by complying with IEC 62443 requirements, the majority of mandatory IACS UR E27 requirements are satisfied. To dismiss any indicator of biasness, some companies are being certified under IEC 62443 due to the support its security controls provide in protecting automated ICS systems, including ABB, Kongsberg, KONE Marine, Velmet, and Siemens.

6 Conclusion and Future research directions

The thesis focused on analysing cyber security requirements and notations from marine classification societies and other entities to understand how to comply with cyber security requirements.

The primary questions for this were as followed:

1.What are the relevant cyber security standards and class notations for products used in compliance tracking?

2. How do internationally recognized standards such as IEC 62443 compare to other cyber security requirements for marine solutions products?

The first question is answered with the current compliance of IACS UR E 27. UR E 27 is deemed mandatory by IACS issued upon class vessels looking to maintain their compliance of maritime cyber security with onboard equipment to improve its cyber resilience against current maritime cyber attacks. To facilitate the compliance of IACS UR E27 requirements, other IACS class societies have revised their cyber security requirements to be mapped with 62443-3-3. The research from the survey indicated that cyber security standards DNV, IEC 62443, and IACS UR E27 were relevant towards compliance tracking of maritime product based on the mandatory requirements of IACS UR E 27 for class-certified ships that need to be met along with how other maritime class societies and external customers are developing their requirements to align with IACS UR E27 and IEC 62443-3-3. The second research question was resolved with the implementation of Polarion to further discern IEC 62443-3-3 comparability with the relevant cyber security requirements identified from the survey. The analysis of the cyber security requirements from IEC 62443-3-3, DNV, and IACS UR E27, determined that all three standards' security requirements correlate with each other from which out of the two (IEC 62443-3-3 and IACS UR E 27) that were assessed in the compliant gap assessment for maritime product WCM matched almost equally as compliant. As an outcome, this research has indicated that IEC 62443 can be established as a baseline in meeting compliance with cyber security requirements from maritime class societies and external customers and other standards that are aligned or overlap with IEC 62443 and IACS UR E27, such as frameworks from ISO 27001 and NIST CSF. IEC 62443 enables flexibility in engaging and developing security development lifecycle (SDL) support for maritime products like what

Wärtsilä has implemented in their SDL activities while being able to fulfil mandatory requirements set by maritime regulation bodies such as IMO and IACS and other entities.

Based on these conclusions, Future research can be focused on implementing IEC 62443 3-3 as a baseline for maritime cyber security compliance with the usage of requirement management tooling such as Polarion in assessing current cyber security requirements that have been revised to incorporate new notations by maritime class societies (e.g., BV, ABS) and used to identify correlating requirements in other cyber security standards that are requested by external customers. This can an opportunity in addressing future compliance analysis of cyber security requirements focused on the cyber resilience of autonomous ships.

References

[1] G. Kavallieratos, V. Diamantopoulou, and S. Katsikas, “Shipping 4.0: Security requirements for the cyber-enabled ship: Semantic scholar,” IEEE Transactions on Industrial Informatics, 2022. Doi: 10.1109/TII.2020.2976840.

[2] Ministerie van Algemene Zaken, “Smart shipping: Comprehensive automation in the maritime sector,” Maritime transport and seaports | Government.nl, https://www.government.nl/topics/maritime-transport-and-seaports/smart-shipping-comprehensive-automation-in-the-maritime-sector (accessed Jun. 2, 2023).

[3] “Digitalization in maritime transport: Ensuring Opportunities for Development,” UNCTAD, https://unctad.org/publication/digitalization-maritime-transport-ensuring-opportunities-development (accessed Jun. 6, 2023).

[4] “Maritime Cyber Risk,” International Maritime Organization, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (accessed Jun. 6, 2023).

[5] Maritime cybersecurity – best practices for vessels - huoltovarmuuskeskus, https://www.huoltovarmuuskeskus.fi/files/a9cb864dbec0780649661775ea66b6f1db076efb/cybersecurity-best-practices-for-vessels.pdf (accessed Jun. 6, 2023).

[6] Nozomi Networks, “Improving maritime cybersecurity,” Nozomi Networks, https://www.nozominetworks.com/blog/improving-maritime-cybersecurity-and-operational-resiliency/ (accessed Jun. 6, 2023).

[7] Y. Ichimura, D. Dalaklis, M. Kitada, and A. Christodoulou, “Shipping in the era of digitalization: Mapping the future strategic plans of Major Maritime Commercial Actors,” Digital Business, 2022. Doi: 10.1016/j.digbus.2022.100022.

[8] Maritime cybersecurity – best practices for vessels - huoltovarmuuskeskus, https://www.huoltovarmuuskeskus.fi/files/a9cb864dbec0780649661775ea66b6f1db076efb/cybersecurity-best-practices-for-vessels.pdf (accessed Jun. 6, 2023).

[9] A. S. Review, “Maritime cyber-attacks increase by 900% in three years,” Maritime cyber-attacks increase by 900% in three years – Cyber Security Review, https://www.cybersecurity-review.com/news-july-2020/maritime-cyber-attacks-increase-by-900-in-three-years/ (accessed Jun. 6, 2023).

[10] “Maritime Cyber Risk,” International Maritime Organization, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (accessed Jun. 6, 2023).

[11] I. Ashraf et al., “A survey on cyber security threats in IOT-enabled maritime industry,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–14, 2022. Doi: 10.1109/tits.2022.3164678.

[12] “The Guidelines on Cyber Security onboard ships,” BIMCO Home, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed Jun. 6, 2023).

[13] “ISA/IEC 62443 series of standards - ISA,” isa.org, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed Jun. 6, 2023).

[14] S. G. Team, “What is compliance tracking?,” Strike Graph: Cybersecurity Compliance SaaS, https://www.strikegraph.com/blog/what-is-compliance-tracking (accessed Jun. 6, 2023).

[15] “IACS adopts New Requirements on Cyber Safety,” IACS, https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/ (accessed Jun. 6, 2023).

[16] “Best practices for compliance monitoring in cybersecurity,” SecurityScorecard, https://securityscorecard.com/blog/best-practices-for-compliance-monitoring-in-cybersecurity/ (accessed Jun. 6, 2023).

[17] Classification societies – what, why and how? - IACS, https://iacs.org.uk/media/8871/classification-what-why-how.pdf (accessed Jun. 6, 2023).

[18] “Cyber secure class notation,” DNV, https://www.dnv.com/services/cyber-secure-class-notation-124600 (accessed Jun. 6, 2023).

[19] Webmaster, “Inspections of recognised organisations,” EMSA, https://www.emsa.europa.eu/inspections/assessment-of-classification-societies.html (accessed Jun. 6, 2023).

[20] “Frequently asked questions,” International Maritime Organization, https://www.imo.org/en/About/Pages/FAQs.aspx (accessed Jun. 6, 2023).

[21] Requirements management, requirements gathering ... - polarion, https://polarion.plm.automation.siemens.com/products/polarion-requirements (accessed Jun. 6, 2023).

[22] “About Wärtsilä: Learn more about the company,” Wartsila.com, https://www.wartsila.com/about (accessed Jun. 6, 2023).

[23] K. Tam and K. D. Jones, “Maritime cybersecurity policy: The scope and impact of evolving technology on International Shipping,” Journal of Cyber Policy, vol. 3, no. 2, pp. 147–164, 2018. Doi: 10.1080/23738871.2018.1513053.

[24] Progoulakis, I., Rohmeyer, P. and Nikitakos, N. (2021) 'Cyber Physical Systems Security for maritime assets', Journal of Marine Science and Engineering, 9(12), p. 1384. Doi: 10.3390/jmse9121384.

[25] Górski, J., Wardziński, A. (2019). Supporting Cybersecurity Compliance Assessment of Industrial Automation and Control System Components. In: Flammini, F. (eds) Resilience of Cyber-Physical Systems. Advanced Sciences and Technologies for Security Applications. Springer, Cham. Doi: 10.1007/978-3-319-95597-1_4.

[26] V. Nopanen, "Unifying cybersecurity requirements in Automation Projects," Trepo, https://trepo.tuni.fi/handle/10024/146144 (accessed Jun. 27, 2023).

[27] S. Hautamäki, "Managing Requirements of Standards and Regulations for Engine Control System: Case Study of Storing System Requirements from DNV in Polarion," Theseus, https://www.theseus.fi/bitstream/handle/10024/94092 (accessed Jun.27, (2023)

[28] S. Erich, "Cyber Security Framework for Napa onboard products," Theseus, https://www.theseus.fi/handle/10024/496718 (accessed Jun. 27, 2023).

[29] K. Huuskonen, Cybersecurity validation and verification for automated vessels - theseus, https://www.theseus.fi/bitstream/handle/10024/509882/Huuskonen_Katja.pdf?sequence=4 (accessed Jun. 6, 2023).

[30] K. Kuhn, S. Bicakci, and S. A. Shaikh, "Covid-19 digitization in maritime: Understanding cyber risks," WMU Journal of Maritime Affairs, 2022. Doi: 10.1007/s13437-021-00235-1.

[31] The Guidelines on Cyber Security onboard ships - ics-shipping.org, https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf (accessed Jun. 6, 2023).

[32] "How bad was maritime cyber security in 2021? consider these 8 incidents," Cyberstar, https://www.zkcyberstar.com/2022/03/15/how-bad-was-maritime-cyber-security-in-2021-consider-these-8-incidents/ (accessed Jun. 6, 2023).

[33] K. Kanwal, W. Shi, C. Kontovas, Z. Yang, and C.-H. Chang, "Maritime cybersecurity: Are onboard systems ready?," Maritime Policy & Management, pp. 1–19, 2022. Doi: 10.1080/03088839.2022.2124464.

[34] "Maritime Cyber Security: A comprehensive approach," placeholder_200x200, https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach (accessed Jun. 6, 2023).

[35] “Frequently asked questions on maritime security,” International Maritime Organization, https://www.imo.org/en/OurWork/Security/Pages/FAQ.aspx (accessed Jun. 6, 2023).

[36] M. Olney, “What are the benefits of cyber security compliance and the consequences of non-compliance?,” Insights, https://insights.integrity360.com/what-are-the-benefits-of-cyber-security-compliance-and-the-consequences-of-non-compliance (accessed Jun. 9, 2023).

[37] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, “Cybersecurity challenges in the Maritime Sector,” MDPI, 2022. Doi: 10.3390/network2010009.

[38] P. Rajaram, M. Goh, and J. Zhou, “Guidelines for cyber risk management in Shipboard Operational Technology Systems,” arXiv.org, 2022. Doi: 10.1088/1742-6596/2311/1/012002.

[39] C.-H. Chang, S. Wenming, Z. Wei, P. Changki, and C. Kontovas, “Welcome to LJMU research online,” Evaluating cybersecurity risks in the maritime industry: a literature review | LJMU Research Online, 2019.

[40] N. Ayalon, “Cybersecurity and automation in shipping,” Seatrade Maritime, https://www.seatrade-maritime.com/opinions-analysis/cybersecurity-and-automation-shipping (accessed Jun. 6, 2023).

[41] “Brief history of imo,” International Maritime Organization, https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx (accessed Jun. 6, 2023).

[42] “Cybersecurity in the maritime sector: Enisa releases new guidelines for navigating cyber risk,” ENISA, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk (accessed Jun. 6, 2023).

[43] “About Iacs,” IACS, https://iacs.org.uk/about/ (accessed Jun. 6, 2023).

[44] “IACS Vision and mission statement,” IACS, https://www.iacs.org.uk/about/iacs-vision-and-mission/ (accessed Jun. 6, 2023).

[45] “Home,” American Bureau of Shipping (ABS) Eagle.org, https://ww2.eagle.org/en/about-us/who-we-are.html (accessed Jun. 6, 2023).

[46] “Home,” American Bureau of Shipping (ABS) Eagle.org, https://ww2.eagle.org/en/Products-and-Services/cyber/abs-cybersafety.html (accessed Jun. 6, 2023).

[47] “About DNV,” DNV, https://www.dnv.com/about/index.html (accessed Jun. 6, 2023).

[48] “Cyber secure class notation,” DNV, https://www.dnv.com/services/cyber-secure-class notation-124600 (accessed Jun. 6, 2023).

[49] “LR is a leader in professional services for Engineering and Technology,” Lloyd’s Register, https://www.lr.org/en/who-we-are/ (accessed Jun. 6, 2023).

[50] “LR Shipright procedures,” Lloyd’s Register, https://www.lr.org/en/shipright-procedures/ (accessed Jun. 6, 2023).

[51] “A business to business to society company,” Bureau Veritas, https://group.bureauveritas.com/group (accessed Jun. 6, 2023).

[52] “NR659 rules on cyber security for the classification of Marine units,” Marine & Offshore, https://marine-offshore.bureauveritas.com/nr659-rules-cyber-security-classification-marine-units (accessed Jun. 6, 2023).

[53] Hanneng, About CCS, https://www.ccs.org.cn/ccswzen/about?columnid=201912240228526379 (accessed Jun. 6, 2023).

[54] Hanneng, China Classification Society, https://www.ccs.org.cn/ccswzen/ (accessed Jun. 6, 2023).

[55] Security of Industrial Automation and Control Systems, https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf (accessed Jun. 6, 2023).

[56] “Questions and answers,” NIST, https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics (accessed Jun. 6, 2023).

[57] Edition 1.0 2013-08 international standard, https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf (accessed Jun. 6, 2023).

[58] “Rules and standards,” DNV, https://www.dnv.com/rules-standards/index.html (accessed Jun. 6, 2023).

[59] “LR Shipright procedures,” Lloyd’s Register, https://www.lr.org/en/shipright-procedures/ (accessed Jun. 6, 2023).

[60] ABS cybersafety for equipment manufacturers - eagle.org, https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/256_cybersafetyV7/cybersafety-V7-equipment-manufacturers-guide-oct19.pdf (accessed Jun. 6, 2023).

[61] Hanneng, Guidelines for ship Cyber Security 2023, https://www.ccs.org.cn/ccswzen/articleDetail?id=20230523102991147 1&columnId=202007171176731956 (accessed Jun. 6, 2023).

[62] "NR659 rules on cyber security for the classification of Marine units," Marine & Offshore, https://marine-offshore.bureauveritas.com/nr659-rules-cyber-security-classification-marine-units (accessed Jun. 6, 2023).

[63] R. Bougie and U. Sekaran, "Research methods for business: A skill building approach, 8th edition," Wiley.com, https://www.wiley.com/en-us/Research+Methods+For+Business%3A+A+Skill+Building+Approach%2C+8th+Edition-p-9781119561248 (accessed Jun. 6, 2023).

[64] P. Aspers and U. Corte, "What is qualitative in qualitative research," Qualitative sociology, 2019. Doi: 10.1007/s11133-019-9413-7.

[65] "Cyber security at Wärtsilä," Wartsila.com, https://www.wartsila.com/about/cyber-security (accessed Jun. 6, 2023).

[66] Wärtsilä, "Who do you entrust your business-critical assets to?," Wartsila.com, https://www.wartsila.com/insights/article/who-do-you-entrust-your-business-critical-assets-to (accessed Jun. 6, 2023).

[67] Siemens, "Getting started", Siemens.com https://docs.plm.automation.siemens.com/content/polarion/19.1/help/en_US/user_and_administration_help/getting_started.html (accessed Jun. 6, 2023).

[68] G. A. Bowen, "Document analysis as a qualitative research method," Qualitative Research Journal,2019. Doi: 10.3316/QRJ0902027.

[69] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy, "The online survey as a qualitative research tool," International Journal of Social Research Methodology, 2021. Doi: 10.1080/13645579.2020.1805550.

[70] I. Mraković and R. Vojinović, "Maritime Cyber Security analysis – how to reduce threats?," Transactions on Maritime Science, vol. 8, no. 1, pp. 132–139, 2019. Doi: 10.7225/toms.v08.n01.013.

Appendices

The main heading of the appendices is not numbered. The same styles are used in the appendices as in the text chapters.

Appendix 1: Survey Questions

1. Which best describes your role related to maritime products?
2. How long have you worked in this capacity?
3. Which country do you work in?
4. What standards and class notations do you find the most relevant in maritime cyber security compliance for maritime products? Answer on a scale of not at all relevant to very relevant below.
5. What other cyber security standards are relevant for you that are not listed in Question 4? Please skip this question if you have nothing else to add.
6. Are you available for a 30–40-minute interview? If so, please write your email address for contact.