Bolbot, Victor; Xiang, La; Brunou, Päivi; Kiviharju, Mikko; Ding, Yu; Valdez Banda, Osiris

Cybersecurity risk assessment of a marine Dual-Fuel engine on inland waterways ship

Published in:
Proceedings of the Institution of Mechanical Engineers. Part M: Journal of Engineering for the Maritime Environment

DOI:
10.1177/14750902241265173

Published: 01/02/2025

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Bolbot, V., Xiang, L., Brunou, P., Kiviharju, M., Ding, Y., & Valdez Banda, O. (2025). Cybersecurity risk assessment of a marine Dual-Fuel engine on inland waterways ship. *Proceedings of the Institution of Mechanical Engineers. Part M: Journal of Engineering for the Maritime Environment*, *239*(1), 67-91. https://doi.org/10.1177/14750902241265173

Cybersecurity risk assessment of a marine Dual-Fuel engine on inland waterways ship

Victor Bolbot[1,2*][0000-0002-1883-3604], La Xiang[3], Päivi Brunou[4], Mikko Kiviharju[5,2], Yu Ding[3] [0000-0002-9989-4723], Osiris Valdez Banda[1,2] [0000-0002-7805-8144]

[1]*Marine Technology, Department of Mechanical Engineering, Aalto University, 02150, Espoo, Finland*

[2]*Kotka Maritime Research Centre, 48100 Kotka, Finland*

[3]*College of Power and Energy Engineering, Harbin Engineering University, Harbin, China*

[4]*Novia University of Applied Sciences, Turku, Finland*

[5]*Department of Computer Science Aalto University, 02150, Espoo, Finland*

*victor.bolbot@aalto.fi

ABSTRACT: Increased connectivity renders the ships more cost-effective but also vulnerable to cyberattacks. Since ships are assets of significant value and importance, they constitute a lucrative object for cyber-attacks. The power and propulsion functions are among the most safety critical and essential for ship operations. Simultaneously, the use of Dual-Fuel (DF) engines for power generation and propulsion has become very popular in the recent years. The aim of this research is the risk identification and analysis of potential cybersecurity attack scenarios in a DF engine on inland waterways ship. For this purpose, we employ an adapted version of Failure Modes, Vulnerabilities and Effects Analysis (FMVEA). In our approach we demonstrate how the implementation of FMVEA can be interconnected with the existing assurance processes for maritime engines and novel developments in the field of risk theory. We also provide insights in the riskiest cybersecurity attacks on DF engine and how to reduce their risks.

Abbreviations Table

Abbreviation	**Definition**
CAN	Control Area Network
DF	Dual Fuel
DoS	Denial of Service
ECU	Electronic Control Unit
FME(C)A	Failure Modes and Effects (Criticality) And Effects
FMVEA	Failure Mode, Vulnerabilities and Effects Analysis
HAZID	Hazard Identification
IACS	International Association of Classification of Societies
ICS	International Chamber of Shipping
IT	Information Technology
LI	Likelihood Index
NOx	Nitrogen oxides
OT	Operational Technology
SI	Severity Index
SOx	Sulphur oxides
STPA	System-Theoretic Process Analysis
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
VSAT	Very Small Aperture Terminal (a satellite link)

1 INTRODUCTION

Marine engines constitute the heart of any power and propulsion plant on ships [1, 2]. However, a natural output of combustion process in marine engines includes harmful environmental emissions such as nitrogen oxides (NO_x), sulphur oxides (SO_x), as well as greenhouse gaseous emissions [3, 4]. For these reasons and due to the novel stringent regulations, the use of marine Dual Fuel (DF) engines on ships has become popular[5-9]. Multiple researchers demonstrated that the use of DF engines is a cost-efficient way to comply with the currently enforced environmental regulations [10-12].

These new developments are accompanied with the increased ships interconnectivity[13]. In marine engines specifically interconnectivity is on the rise to enable remote monitoring and control of the engines and support implementation of condition-based maintenance [14-16]. This interconnection is coming at the cost of increased maritime systems vulnerability to cyberattacks [17-19]. Ships constitute of Information Technology (IT) and Operational Technology (OT) systems[20] and can be targeted by attackers due to their significant value and their importance for the global supply chain[21]. Several cyber incidents have been already reported in the maritime industry where significant financial losses were reported [22], whilst many of the successful cyberattacks remain undisclosed to avoid negative public coverage[18]. It is anticipated that the intensity and number of cyberattacks in the maritime will only increase[23-25].

A cyber-attack on the ship engines can cause serious safety implications similar to one caused by component failure in the engines such as propulsion loss, blackouts, temporal or permanent engine damage, threaten the ship safety or result in severe disruption in ship operations [26-28]. Therefore, due to its' importance to the ship safety, ensuring that the engines remain protected against cyberattacks should be one of the top priorities as also reported in [20, 29].

Considering the arising cybersecurity issues, the aim of this study is to implement a risk assessment of cyber-attack scenarios in a DF engine tailored to relevant procedures followed by the engine manufacturers, to identify potential vulnerabilities and damages that can be incurred on the engine, to propose control measures for cyber-attack scenarios and provide recommendations for the cyber risk assessment of engines in view of the currently implemented assurance procedures. Consequently, the study concentrates on the DF engine and related networks and not the ship as a whole, albeit a reference ship network from inland waterway ship is used as input to the analysis.

This article is structured as follows. First review of the related research in connection to DF engines risk assessment and cybersecurity risk assessment is provided. Afterwards, the investigated engine characteristics, and study scope are provided along with the analysis assumptions and the involved team of experts. Then the methodology and the methodology steps' rationale are presented. The results of applying the methodology to the selected DF engine and implications for research and practice are discussed in section five. Lastly, the main findings of the study are being summarised in the conclusions section.

2 RELATED RESEARCH AND GUIDELINES

The safety of the ship is a heavily regulated domain. The most influential standardisation body in maritime safety is the UN International Maritime Organization (IMO), whose guidelines are ratified by most of the UN nations. IMO Maritime Safety Committee (MSC) has published guidelines (Circulars) on maritime cyber risk management[20], which reference different International Association of Classification of Societies (IACS) guidelines, such as Rec.166, UR E22 and others and highlight the propulsion and power systems as vulnerable systems.

Unlike the automotive industry e.g.[30], there are less applicable domain-specific threat modelling frameworks for maritime. There are existing general-purpose information security risk management guidance (e.g. NIST SP800-30 [31]), but they always need to be adapted for the actual domain and system in any case, and full applicability cannot be expected. The work by Lamba et al.[32] claims that most existing general-purpose risk management standards are not specific enough for a single domain, and domain-specific standards from other domains (e.g. aviation) are not applicable, and application of the "closest candidate" is needed nevertheless.

ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss, in turn, reverted with their own guidelines addressing cyber risks[29, 33-35] on risk matrixes. Same criticism can be directed against other guidelines for cyber risk management as in [36] where multiplicatory risk matrixes were used. At the same time, the cybersecurity guidelines for inland waterway ships involve the one addressing ports[37], yet they do not explicitly address the inland water ship systems. PIANC instead has reverted with some risk mitigation measures for navigation systems used in inland waterway ships in their awareness paper [38] , yet not addressing the engines to great detail.

The main regulatory guidelines used by the marine engine manufacturers are the guidelines issued by IACS such as UR E26 [39] and UR E27 [40] (mandatory for classed ships and offshore

installations contracted for construction after 1st of July 2024 [41]). These guidelines include several requirements related both to the procedures and goals that shall be satisfied by the investigated systems, the required data for analysis and assignment of responsibilities among stakeholders for engines cybersecurity assurance. As per customer request, specific class societies guidelines can be incorporated by the engine manufacturers during design. The use of IEC 62443[42] is frequently considered as a prerequisite when performing risk assessment and selection of cybersecurity controls in marine engines[43]. These guidelines and IEC 62443 standards do not prescribe any method for risk assessment, leaving the selection of the method to the engine manufacturer, subject to some generic constraints on the risk assessment procedures. These regulatory guidelines can be viewed as aligned to the high-level requirements specified in [20]

The implementation of Failure Modes and Effects (Criticality) And Effects (FME(C)A) is considered a pre-requisite for the type approval of marine engines control as set by IACS in Recommendation N138[44], and therefore, FME(C)A is employed for these engines safety assessment [45]. The FME(C)A has been applied in several studies to the engines for the purposes of development of intelligent diagnosis techniques [46], to support the application of preventative maintenance [47], for engine cylinder safety analysis [48], for crankcase explosions investigation [49], turbocharger fouling risk assessment[50], for criticality analysis [51], for safety analysis in combination with simulations [27]. FMEA has been also applied to multiple other maritime systems[52-56].

However, FMEA is primarily oriented via goals in safety rather than security. Thus, factoring security-related goals, such as cybersecurity, in the results requires additional approaches. No surprise, FMEA in combination with Bayesian Networks[56, 57] was applied to cyber risk assessment to maritime systems as well. Yet, these approaches did not consider any specific threat modelling technique. FMECA was used in conjunction with MITRE ATT&CK framework for cyber risk assessment in autonomous ships [58], without delving into characteristics relevant to the engines. A security-oriented extension on FMEA was presented in[59], called Failure Modes, Vulnerabilities and Effects Analysis (FMVEA). It was used to identify potential cyber-attack scenarios on a marine DF in [26], but without implementing the risk analysis and uncertainty assessment.

System-Theoretic Process Analysis (STPA) was used together with other cybersecurity methods for analysis of cyber risks in autonomous ships [60-64]. Hazard Identification (HAZID) based cyber risk assessment of autonomous ships was used in [65-67]. STRIDE (Spoofing,

Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) was also used for cyber risk assessment in autonomous and maritime systems [68-70]. MITRE ATT&CK framework was also employed in [70-73] for cybersecurity in autonomous and advanced maritime systems.

As it can be observed, none of these studies implemented risk assessment using FMVEA in DF engines subject to the limitations described in UR E26 [39], UR E27 [40] , IEC 62443 [42]. The incorporation of FMVEA in the cyber risk assessment and regulatory update process would have several advantages. First, it is similar to FMECA already required by the class societies in Recommendation N138[44] from the engine manufacturers, which would facilitate its application, as adapting the FMECA results to the FMVEA format would be obviously easy. This is strong advantage of FMVEA in comparison to STPA and HAZID and any customized method as for instance in [21, 74, 75]. FMVEA has also been compared as a method to other ones such as STPA[76] and CHASSIS[77] in a software fault setting and, in the case where systems are evaluated via decomposition, found to be superior.

Furthermore, FMVEA is incorporating STRIDE for cybersecurity risk assessment[59] and for guiding the cybersecurity analyst in identifying attack scenarios. STRIDE was recognised as the most popular threat model in software application security[78] which facilitates its application for the cybersecurity practitioners. Although STRIDE was developed originally for software applications' security, it has found uses for more general cybersecurity especially in the transport sector[68, 79-82], computer networks[83], supply chain[84] even DNA sequencing related technologies[85]. STRIDE was also suggested to be used as input to other safety analysis techniques, which is done in FMVEA, recognizing its strength in identifying the threat scenarios[80, 86].

The STRIDE threat categorisation was applauded with respect to identification of high level attacks in [32, 70, 80, 87] and there is evidence that maritime community is experimenting with this methodology[36, 68-70] so it will not be completely unfamiliar to the maritime experts. Some researchers have criticised STRIDE for being unable to find scenarios related to sending false signals or privacy violation[88] and proposed additional categorisations to be included. However, we reckon that these attack scenarios can be accommodated easily under the umbrella of broad categories of Tampering and Information disclosure attacks respectively.

The concerns about the suitability of threat modes for the analysis have pushed some of the researchers to promote application of methods like MITRE ATT&CK[58]. However, MITRE

ATT&CK has over 600 attack techniques[58], which poses direct question of effectiveness and easiness of application for the considered case study, which is a DF engine. In an integrative study[70], it was concluded that STRIDE and MITRE ATT&CK should not be viewed as antagonistic methods, as they have different granularity of attack scenarios, as STRIDE can be used to identify high-level attack scenarios and MITRE ATT&CK more elaborate one, contributing to the high level one identified by STRIDE. Similar conclusions can be derived from findings in [79, 80], where it was demonstrated that STRIDE attack scenarios can be elaborated further by employing extra, more detailed attack analysis techniques. Furthermore, whilst some of the novel attack types might not be directly mentioned in STRIDE keywords, like social engineering, physical attacks or zero-day exploits, they can be and are referred during the identification of vulnerabilities leading to STRIDE types of threat modes in FMVEA[59].

Therefore, by including STRIDE, FMVEA can support the identification of potential impact of cyber-attacks on the engine performance, the safety and environment by considering the various threat modes and their effects with relative easiness without overloading the practitioner as if MITRE ATT&CK or other detailed technique were used. Other advantages include incorporation of the vulnerabilities that can be exploited and the direct link between the threat modes and the failure modes and effects [59]. Furthermore it is both scenario and component-based approach in line with requirements from IEC 62443 [42]. Last, but not least the FMVEA can be used to develop some design recommendations for the engine manufacturers by incorporating risk control measures in similar manner as FME(C)A.

For the reasons above, we decided to employ an altered version of Security Application of FME(C)A which is currently referred as a Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) [59] by rendering it compliant with UR E26[39], UR E27 [40], IEC 62443 [42] and also NIST SP 800-30. To ensure the compliance, we expanded the types of consequences in section 4.4, altered the ranking process and the ranking scales for likelihood and severity as elaborated in 4.6. Furthermore we provided some novel criteria for risk assessment in line with the new findings in the risk science with respect to uncertainty[89, 90]. Thanks to this risk assessment we can estimate the security zones levels in line with UR E26[39], and IEC 62443 [42]. The proposed risk control measures were also crosschecked with the recommendations UR E26[39], UR E27 [40] for conformity, at least some of them.

The novelty of this article stems from the implementation of marine DF engine control system cyber risk assessment. Another contribution stems from the adaptation of FMVEA to the needs

of the cyber risk assessment in marine engines considering the recommendations from IACS[39, 40] and IEC 62443[42], used by the engine manufacturers, which has resulted in multiple deviations from the classical FMVEA approach. Furthermore, we employ novel risk matrix incorporating uncertainty in our risk assessment and decision-making. Such a consideration is novel, as the incorporation of epistemic uncertainty has been reported only for security purposes so far (for instance herein[91, 92]), but very limited applications exist for cybersecurity at master thesis level as in [93].

3 MATERIALS

3.1 Investigated engine description

The previous section proposed methodology was applied to a small DF engine (Figure 1). We decided to use this engine, since it has been used in previous studies [11, 94, 95] and several of the authors have very good knowledge of the particular engine. The engine is located in the power laboratory of Harbin Engineering University, Harbin, China. The investigated DF engine was converted from conventional diesel engine. The DF engine characteristics are shown in

Table 1 and the layout of the DF engine is presented in Figure 2. The main considered components of the engine are provided in Table 2.

The engine was rendered DF through a retrofit, where a natural gas supply system was added, and the Electronic Control Unit (ECU) was updated for engine in figure. This DF engine as other DF engines can operate in the diesel mode and DF mode. The DF mode operation is reliant on the injection of diesel fuel, which has lower auto-ignition temperature and works as an ignition source for the natural gas combustion. As such, the ignition diesel fuel is typically responsible for around 10% and the natural gas for around 90% of the total energy release in DF mode. The low-level control includes control over the process of natural gas injection (timing, duration, mass), pilot diesel injection (timing, duration, and mass), engine speed keeping, opening of waste gate valve based on desired engine output and operating mode (DF or diesel). The ECU is responsible for monitoring that the critical parameters (provided in Table 2 and Figure 2) are in acceptable ranges. In case abnormal values are observed for the monitored parameters, a shut-down command is issued by the ECU and the fuel supply is slowly cut.

This engine power output is relatively small and its type is similar to the one that can act as a main engine on small inland waterways ships as presented in [96] and small short sea-shipping

vessels. For the sake of the study (this is an assumption), we consider the engine to be interconnected to the ship network as presented in Figure 3 and Figure 4, which is a common communication network in this type of ships as we know from literature[65, 97]. In the same figures also the potential attack entry points, attack surface and data flow diagrams are presented. It is also considered that only captain is available on the ship, which is typical for this type of vessels[96].

The below represent now realistic assumptions for the engine communication network[65, 97] since the actual engine is located in a test bed. The ECU is integrated in the engine room Control Area Network (CAN) alongside other engine room controllers running on Ethernet communication protocol and is receiving high level control commands from the captain on the bridge. The captain sets the desired engine speed, whilst ECU is responsible for low level control (tertiary control). The ECU is also assumed to be responsible for controlling the timings of the inlet/exhaust gas valves. This is only assumption with respect to engine functions, the actual engine does not do that. This was included to assess the performance of some advanced functions.

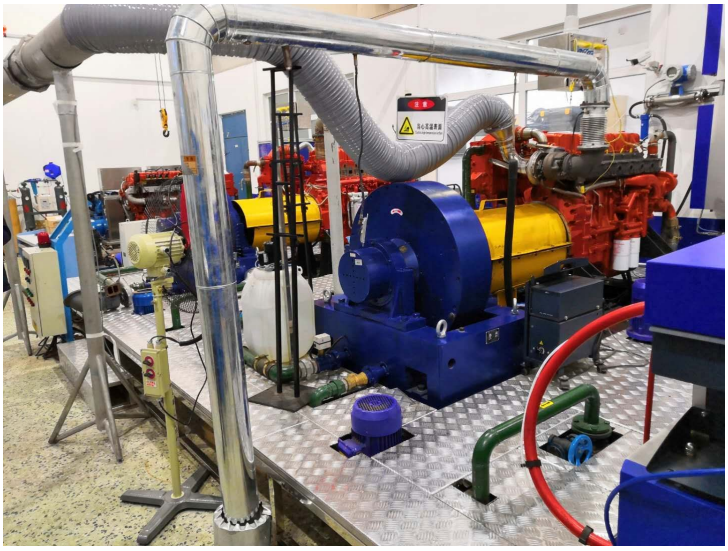

Figure 1 YC6K dual fuel engine testbed

Table 1 Main characteristics of investigated DF engine.

Parameter	Unit	
Cylinder number	-	6
Bore	mm	129
Stroke	mm	155
Type	-	4S
Compression Ratio	-	16.5:1
Displacement per cylinder	L	2.03

Nominal Engine Speed	rpm	1800
Nominal power	kW	300
Pilot injection timing	°CA	-5

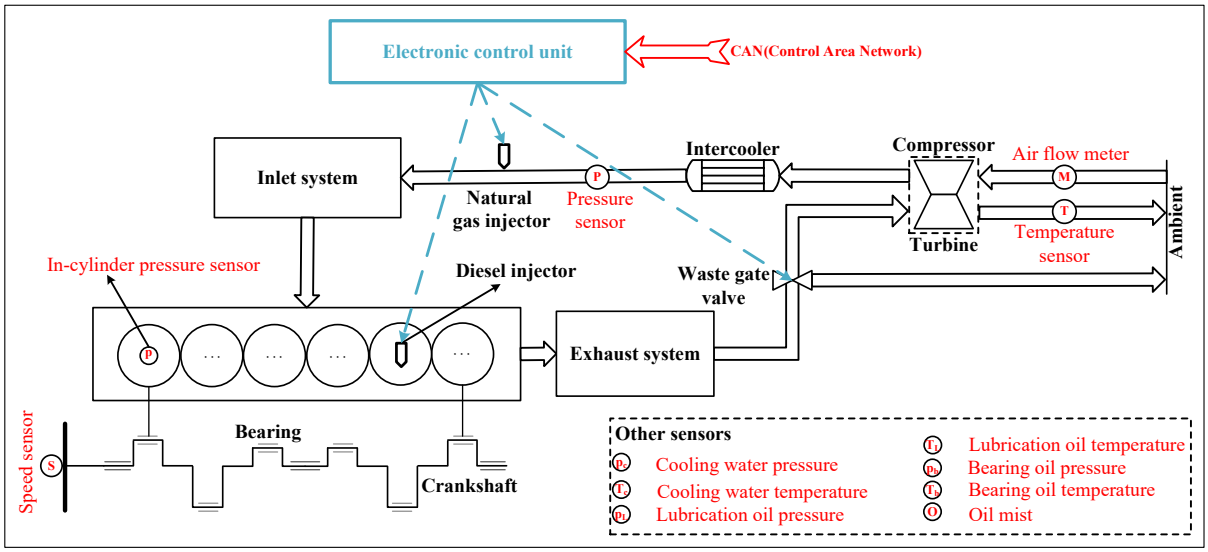

Figure 2 Investigated DF engine layout.

Table 2 Investigated DF engine components description.

N°	Component	Function
1	ECU	It is integrated to the local control area and mainly controls the natural gas injection (timing, duration and mass), pilot diesel injection (timing, duration and mass), exhaust gas and waste gate opening. It also receives the engine operating signals, including air flow, inlet pressure, in-cylinder pressure, engine rotational speed, exhaust temperature after turbine, cooling water pressure and temperature, lubrication oil pressure and temperature, bearing oil temperature and pressure, and oil mist concentration inside the crankcase. It also shut down the engine in case of emergency.
2	Inlet pressure sensor	A low-pressure sensor is installed after intercooler for monitoring the inlet pressure, which is an input for controlling waste gate valve.
3	In-cylinder pressure sensor	A piezoelectric in cylinder-pressure sensor is installed on the cylinder head to obtain the in-cylinder pressure diagram, which is then transferred to the ECU for monitoring maximum pressure.
4	Engine speed sensor	It is installed on crankshaft for safety analysis and power control.
5	Exhaust temperature sensor	It is used to measure the temperature at the exhaust gas manifold downstream turbine for monitoring the engine thermal load.
6	Cooling water pressure and temperature sensors	These are used for monitoring the working condition of cooling water system.
7	Lubrication oil pressure and	These are used for monitoring the working condition of lubrication oil system.

	temperature sensors	
8	Bearing oil pressure and temperature sensors	These are used for monitoring the working condition of bearing oil system.
9	Oil mist sensor	It is used for detecting the oil mist concentration inside the crankcase for preventing explosion.

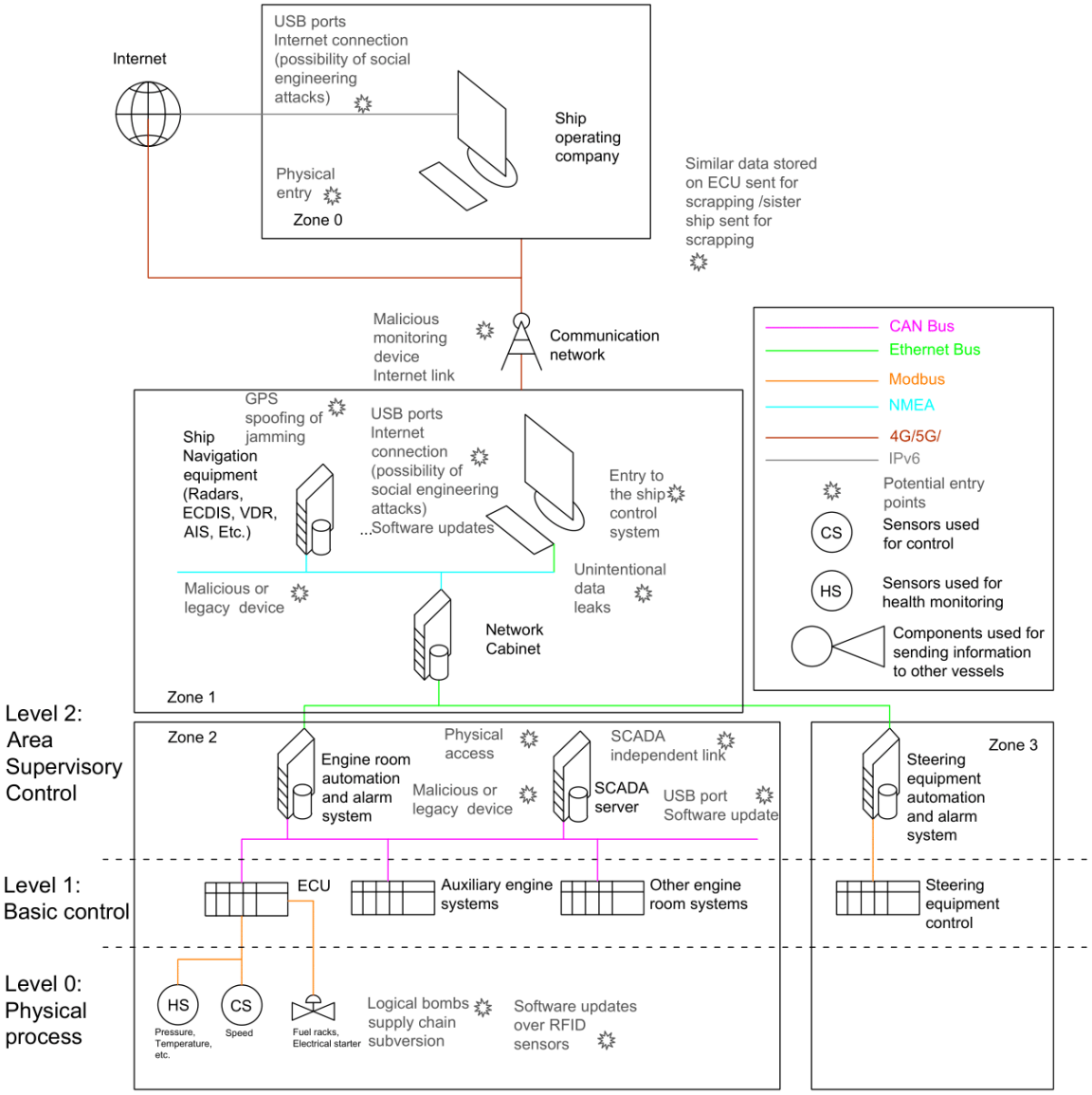

Figure 3 Investigated ship communication network and attack surface.

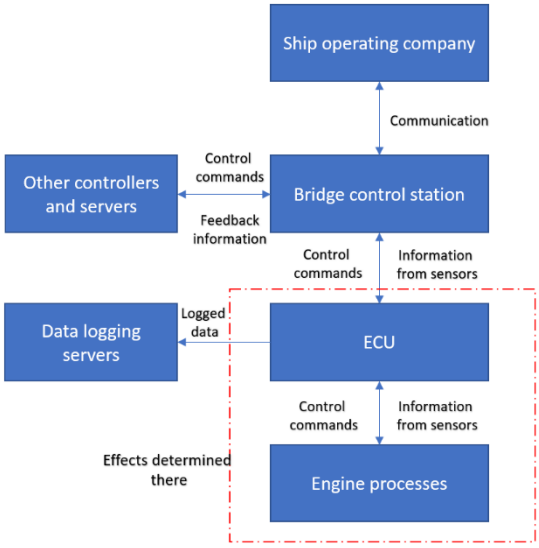

Figure 4 Simplified data flow diagram

3.2 Analysis assumptions and scope

- The analysis focused on the elements which we consider to be primarily affected by the cyberattacks and they are highlighted in Figure 2 with red colour and blue colour.
- Identification of random mechanical, hardware and software failures and their impact on cybersecurity is outside the scope as this is part of FME(C)A.
- It is also assumed that there is a constant, reliable, and unobscured supply of electrical power to ECU, fuel (pilot and natural gas), air and cooling water to the engine from auxiliary systems. The potential cyberattacks on the systems supplying electrical power to ECU, fuel (pilot and natural gas), air and cooling water to the engine are outside analysis scope.
- It is acknowledged that the cyberattacks impact on the engine is different in different operational area and mode. For instance, a power loss during manoeuvring is more hazardous than during sailing in open ocean or away from shore and other ships. However, in our analysis any engine loss is already considered as highest severity consequence irrespectively of whether it is occurring in sailing or manoeuvring, so we follow a conservative approximation with justification provided in section 4.6. In this way the analysis can concentrate the effects on the engine level.
- Engine manufacturers perspectives are mostly adopted for the design of risk assessment process and interpretation of the results.
- The engine is interconnected to the network similar to the one on inland waterway ships

and short sea going ships, which influences the attack vectors identified.

3.3 The associated expert group

The method steps are initially implemented by the first author in this publication to generate the preliminary list of scenarios. Then during the brainstorming session involving several of the authors of the publication, the preliminary list is further refined, elaborated and ranked by following the methodology steps. The experts background and educational level is provided in the Table 3.

Table 3 All the experts involved in the identification and ranking of cybersecurity scenarios

a/a	Expert educational level	Related expertise	Years of experience	Role in their organisation
1	PhD	Knowledge of cybersecurity methods, maritime systems vulnerabilities, marine engines safety aspects	8	Post-doctoral researcher on safety and cybersecurity in maritime systems
2	PhD	Knowledge of marine engines and marine engines safety, design and performance aspects	9	Assistant professor on marine engines
3	B.Sc M.Sc (Ongoing)	Knowledge of maritime cybersecurity, security engineering, non-functional requirements, cybersecurity and quality standards, quality assurance, risk management and cybersecurity awareness	21	Managing director, Expert on ENISA ad hoc working group

4*	M.Sc.	Knowledge of marine engines from operational perspective	12	Chief Engineer
5	PhD	Knowledge of cybersecurity standards and frameworks and risk analysis	21	Professor of Practice in cybersecurity

* Involved only during scenarios development, not the risk assessment in section 4.6.

4 METHODOLOGY

4.1 Methodology overview

The methodology overview is provided in Figure 5. The preparatory step includes analysis scope definition, identification of under investigation systems components and functions, and the development of the attack surface, which is already described in section 3. Then methodology steps are applied in iterative manner. First, for each of the components, a threat mode is identified using STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) by Kohnfelder and Garg [98]. Then for each threat mode the main potential effects are specified during step two. Third step includes the identification of potential exploitable vulnerabilities in the system components leading to the threat mode based on the attack surface and potential attack types that the experts are aware of. Then in the fourth step the likelihood and severity of the identified scenario are estimated and compared to the acceptance criteria. During the fifth step, the cybersecurity scenarios control measures are identified, and the final are suggested in step six. Lastly, we aggregate the generated results in a tabular format as required by FMVEA to better communicate the generated results.

Through the whole analysis we consider the following categories of attackers based on the literature [21, 29, 65, 99-102] as in Table 4. The consideration of attack groups influenced the threat modes, the effects and the finally provided rankings in the study.

Table 4 Identified attack/system penetration groups.

a/a	Attack group	Goal
1	Generic hackers	Spreading their malware around the web network to get ransom

2	Amateur hackers	Improving and training their hackings skills
3	Ethical hackers	Finding vulnerabilities in system with the goal to improve the system
4	Former/current malicious employees	Taking revenge on the ship operating company
5	External providers	Stealing the machinery/condition-based data
6	Activists (Hacktivists)	Delay or cancel the introduction of autonomous vessels or of specific vessels
7	Criminal hackers	Stealing the ship, her cargo, components or seeking for a monetary reward
8	Competitors	Stealing valuable data or sabotaging and damaging the ship
9	Terrorists	Damaging the ship and/or causing fatalities
10	Criminals	Transferring illegal cargo or people
11	Nation states	Damaging or taking control over the ship Developing non access / zero GPS zones

Comparing the methodology to a general-purpose information security NIST SP800-30 risk assessment methodology, we can state that it follows the principles very closely, although this is not intended to be a full risk management framework (RMF):

- Risk assessment occurs on the Information System Tier (Tier 3, which is the most detailed level according to the NIST SP800-30 Ch.2.4.3). However, Tier 1 and 2 assessments are implicitly present when considering the impacts.
- The risk assessment here follows the NIST SP800-30 guidelines process steps 1 through 2 from preparation to conducting the assessment. Results Communication (Step 3) is the purpose of the study and Assessment Maintenance (Step 4) will require the deployment of the target system as well as the risk management framework itself.

The Table 5 below shows the correspondence of NIST SP800-30 different steps to this analysis steps:

Table 5 The compliance to NIST SP800-30 risk assessment guidelines.

NIST SP800-30 Task	Function in this study	Ref. in NIST
Task 1-1: Identify Purpose, Task 1.2: Identify Scope	Cybersecurity of DF engines	Chapters 1.1-1.2
Task 1-3: Identify	STRIDE and expert opinion, uncertainties	Chapter 2, Fig.1,

Constraints	also considered indirectly	Table 3
Task 1-4: Identify Information Sources	The DF engine information system	Figs 2 and 3
Task 1-5: Identify Approach	STRIDE and FMVEA	Chapter 2, Fig.1.
Task 2-1: Identify Threat Sources	Attacker groups, STRIDE, expert opinion	Tables 3-4, and 10,
Task 2-2: Identify Threat Events	By a combination of STRIDE threat modes and target components	Chapter 5.2, Table 10
Task 2-3: Identify Vulnerabilities	Based on expert opinion	Chapter 5.3, Tables 3 and 10
Task 2-4: Determine likelihood	Based on expert group opinion, uncertainties also considered indirectly	Tables 3 and 10
Task 2-5: Determine Impact	Based on expert group opinion	Tables 3 and 10
Task 2-6: Determine risk	Based on domain specific safety standards[1]	Chapter 4.6 and Table 7

The main deviations from a generic information security RMF (in this context and scope) are thus:

- The use of additive (/logarithmic) risk calculus instead of multiplicative (/linear). This is justified since the goals are safety-oriented, even though the threat sources are security-oriented.
- Omitting the explicit uncertainties from the consideration. In the NIST recommendation, these concern Tasks 1-3 and 2-4. Since the likelihood is based on

[1] NIST deems the exact method of risk calculation to be out of scope. However, the example table (SP800-30 Table I-2) is more linear/multiplicative than logarithmic/additive, or different from this study.

expert opinion and the risk levels have coarse granularity, the uncertainties are implicitly factored in. It is left for a future study to make the analysis more analytical with an explicit view of the uncertainties.

Comparing the approach in this study to actual maritime domain specific cybersecurity regulation, such as IMO MSC-FAL.1/Circ.3, the level of detail used here is significantly deeper than in Circular-level regulation or guidance. Also, the focus here is more on risk identification and assessment rather than security program creation (which is what the Circular is recommending). For example, the whole methodology used in this text can fit into the MSC-FAL.1/Circ.3 first Functional Element (from Ch.3): Identify. The Identify-element in the Circular is an asset-based approach that "identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations".

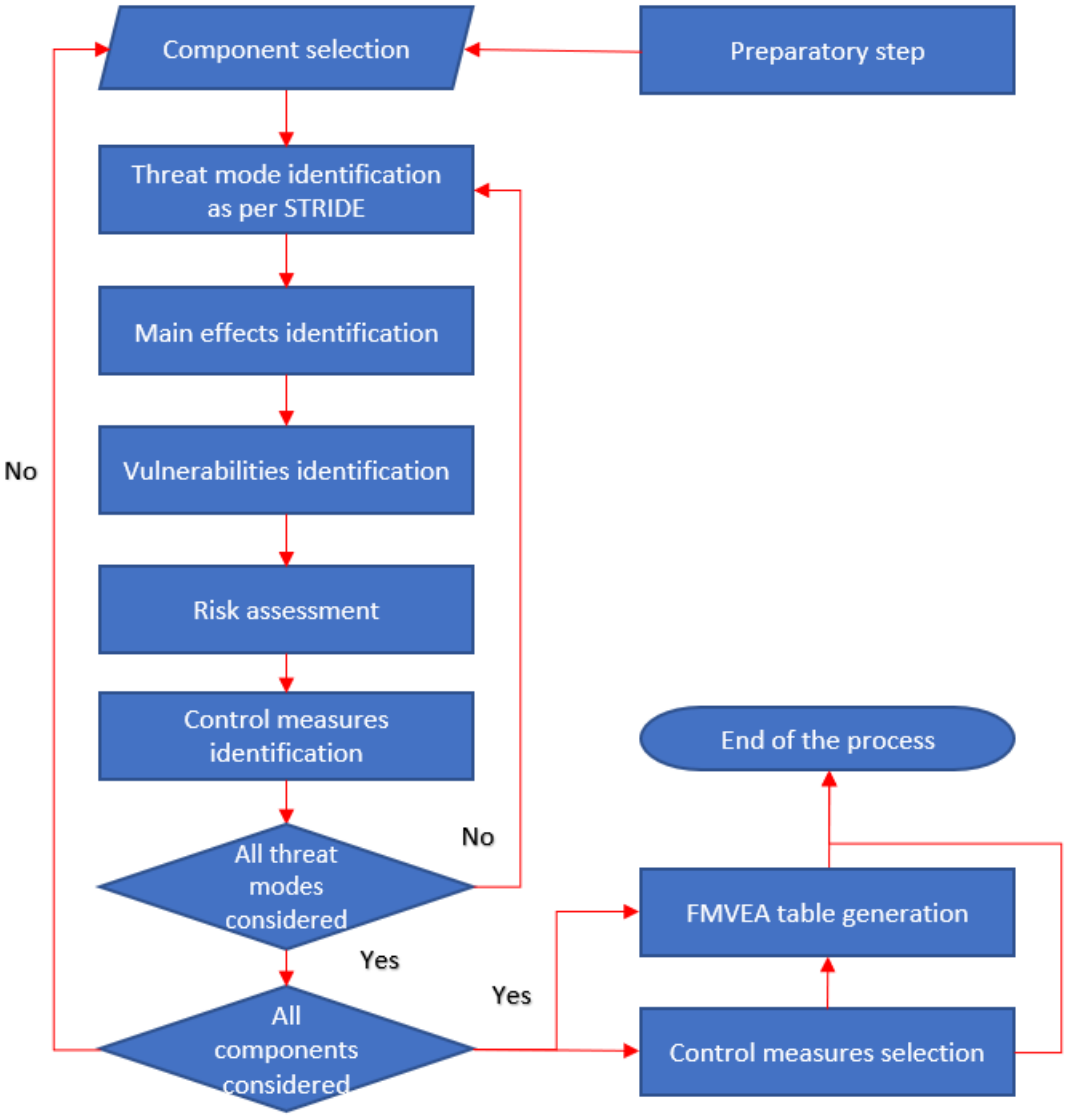

Figure 5 The methodology flowchart.

4.2 Preparatory step – Gathering the necessary information

During this preparatory step, the investigated system boundaries, components, and functions are identified. Processes such as functional and structural breakdown are employed. The breakdown focus is on the components responsible for the system parameters monitoring, control, and communication such as sensors, programming logic controllers, communication networks protocols, as they are the one most vulnerable to cyber-attacks [101]. Based on that information an attack surface is developed, depicting the possible access points for the investigated system in line with the requirements from IACS [39], as presented in Figure 3.

4.3 Step 1 – Threat modes identification

The identification of the threats modes in FMVEA is supported with STRIDE method as originally suggested in FMVEA [59]. STRIDE is a method developed by Kohnfelder and Garg [98] and includes the identification of the following threat modes:

- Spoofing, which refers to the attack where the person/controller successfully identifies himself as another entity.
- Tampering, which refers to the intentional modification of software program, communication signals and measured parameters leading to modification of function or reduction in functions' performance.
- Repudiation, which refers to the control of responsibility and reputability.
- Information disclosure, which refers to the information breach and confidentiality loss.
- Denial of service (DoS), which refers to the function loss due to denial-of-service attack.
- Elevation of privilege, which refers to obtaining elevated access to the resources.

During the identification of various threat modes we discuss the intentions of various attack groups from Table 4 in connection with the threat modes.

4.4 Step 2 – Main effects identification

The previously identified threat modes are used to determine their main effects. First, we consider the cyberattacks impact on component level and then on engine level. The main threat modes effects are identified by considering the engine characteristics, components interactions, potential attack groups intentions (Table 4). The analysis of potential effects is implemented on the system level (i.e. engine level, not ship level) in terms of safety (human injuries/death), environmental pollution (e.g. NOx, hydrocarbons emissions), the investigated system safety (e.g. equipment damages), operational consequences (engine not being operational or having reduced performance/output), reputational consequences and confidentiality breaches. These constitute the different facets of the consequences for cyber risks. Such considerations are aligned to the requirements specified in IACS guidelines [39]. In this way we differentiate from the originally proposed FMVEA.

4.5 Step 3 – Vulnerabilities identification

During this step we reflect on the existing and potential vulnerabilities in the under-investigation system that can be exploited to result in threat modes. This step is implemented

by exploiting the technical expertise of the study participants, previous reported cyber incidents [18], the known vulnerabilities reported in the literature e.g. [103] and databases [104] and considering the attack surface. In this way, the link between the threat modes and vulnerabilities is established. The knowledge of the existing and the potential vulnerabilities is used as input for the likelihood of attacks estimation and for the identification of potential control measures. This is also implemented to remedy for the limited number of threat modes in the STRIDE, since STRIDE is not considering in much detail the social engineering attacks.

4.6 Step 4 – Risk assessment

The risk assessment is implemented semi-quantitatively using risk matrix. In our analysis, severity, likelihood, uncertainty and finally risk assessment significantly deviate from the initial recommendations for FMVEA [59] as we adopt procedures based on the IACS guidelines and IEC 62443 standards considering the engines specifics and uncertainty analysis is deeply integrated into the risk assessment. The risk assessment is linked to the various threat actor groups that can exist either on the ship or outside the ship's networks during the discussions related to risk ranking (Table 4).

On overall we decided to use the logarithmic scale for severity and likelihood scales in Table 6 and Table 7 in line with the Formal Safety Assessment risk matrix, which is state-of-the-art risk matrix in the maritime[105]. This is also similar to Recommendation N138[44] and IEC 62443-2-1 tables [42]. As has been elaborated by multiple researchers, the use of linear scales as in [21, 33, 58] will result in a series of inconsistencies [34, 35]. This naturally led us to use rather coarse ranking scales. Considering the uncertainties that are involved in every risk assessment[106-108] and especcially in the cyber risk assesment[42], or risk assessment of novel systems[96, 105, 109, 110], our aim was to capture the level the risk, rather than its precise value. For this also reason we opted not to use more precise ranking schemes as in [21, 58, 65, 75], since we have a good team of experts supporting the claims and discussions and for simplicity reasons, albeit this could be also possible. We also considered the most expected likelihood and severity. Uncertainty analysis is used though to determine the scenarios where we need to consider the worst case likelihood and severity as explained more thorougly in the paragraphs concerning risk matrix.

For the same reasons we also decided not to expand the likelihood scale to lower levels, as we reckon that claiming a likelihood of one event per 1000 ship-years might not have support from relevant evidence, due to the need for extensive data[111]. We also reckoned that providing likelihood of a threat realisation on a monthly basis for an engine would indicate unrealistically

bad design and management. Furthermore the highest frequency specified in the confidential FMECA results and the Recommendation N138[44] was set at 1 event per ship year. This resulted in only three index values for the likelihood. This similar to previous research study on the autonomous ships' cybersecurity, where similarly three indexes were used[68, 80], with the difference in the description for the index values.

For the severity the main effects are estimated based on the identified effects of step 2 and ranked using Table 6. The Table 6 is adopted based on the existing guidance for the risk assessment in IACS for engine control systems [44] and consequence scale in IEC 62443-2-1 [42] and previous research on risk matrixes[21, 36, 96, 112]. We expanded the initial list of consequences in [44] by considering additionally the impact of cyber-attacks in terms of environmental pollution, engine failures, critical information stealing and reputational impact. We consider all the severity types (safety, environmental, financial, reputational) referred in Table 6 during assessment and for the ranking the highest severity is used.

This classification of the severity, where the engine failure or loss is considered the top severity event (and consequently in the risk matrix of Table 9 frequently occurring as critical) renders it very useful from the manufacturer perspective, as it is independent from the operational mode (manoeuvring, sailing, etc.). This is also conservative, as irrespectively of the ship size and operational mode the frequent engine failure or loss is unacceptable in Table 9. This severity classification is well aligned with the top severity ranking in Recommendation N138[44] and with some confidential engine FMECA reports top severity rankings for DF engines some of the authors are aware of. Similarly the lowest classification is aligned to the confidential FMECA report and Recommendation N138[44], which resulted in only three severity index values as in Recommendation N138[44]. This is similar to previous research study on the autonomous ships cybersecurity, where similarly three indexes were used[68, 80], albeit with different description for the index values.

Generally, the likelihood estimation is challenging, as it is difficult to predict how easy a vulnerability will be exploitable by potential attackers once it is become known, even if historical data on cyber incidents becomes available [42]. Therefore, for the likelihood estimation as per recommendations expressed in IEC 62443-2-1 [42] and IACS [39] the following factors are used:

- The exposure of the considered system
- Easiness of threat mode exploitation due to vulnerability

- The threat motivation and capabilities in executing a cyber-attack

These factors have been repeatedly recognised as important for the likelihood estimation in academic publications [21, 65] and class society guidelines [99]. The relevance of these factors for each scenario is discussed during our risk assessment workshops, and a Low, Medium or High likelihood is assigned to a potential scenario.

The description of likelihood scales in Table 7 is similar to the one provided in IACS guidelines for engine control systems [44] which has logarithmic scale for likelihood (High is equivalent to one year of operation, Medium to 1 to 10 years and so on), but the definition is altered to depict the evolution of likelihood for the cyber-attacks in line with example provided in IEC 62443-2-1 [42] (Table A1). The use of 1, 10 years is also in line with Formal Safety Assessment Risk matrix[105] and such a logarithmic scale can be considered as state of the art approach in the maritime.

In line with the developments in risk science, we have adopted an additional uncertainty evaluation from [96, 106, 107, 113] considering some modern definitions of risk[114-116] relying on uncertainty. The relevant scales are provided in Table 8, which have been retrieved from the relevant literature. In this way the epistemic uncertainties are also captured in our analysis and our study seems to be one of the first one using this type of uncertainty classification as a part of dedicated cyber risk assessment (some applications to security can be found herein[91, 92]). The inclusion of such metrics can be justified by the fact that the ship lifetime can be significant varying from 25 to 50 years in some cases[17], so asking question related to how the cybersecurity picture can change in the upcoming years is also important. The discussions we had concentrated on how uncertainty can influence both likelihood and severity of the considered scenarios.

Table 6 The Severity Index (SI) table.

SI	Rating	Definition
3	High	Serious impact on safety, e.g. fatality/ies and/or Serious impact on engine performance e.g. engine stop Critical engine damage Significant and undetected air pollution exceeding prescribed levels Critical engine design data leakage Loss of brand image
2	Medium	Medium impact on safety, e.g. injury and/or Medium impact on engine performance e.g. engine de-rated Accelerated engine degradation / quickly repairable engine damage Significant degradation in engine consumption performance Significant but detectable air pollution / mediocre air pollution not exceeding the prescribed levels Some important design parameters leakage Loss of customer confidence
1	Low	Negligible to low impact on safety and/or (First aid or recoverable injury) Negligible to low impact on engine output Slightly inefficient engine operation / increased fuel consumption Negligible engine degradation Negligible (non-detectable) air pollution Widely known engine data leakage No impact on the reputation

Table 7 Likelihood table (LI)

L	Rating	Definition
3	High	A threat/vulnerability whose occurrence is likely in the next year of operation or more frequently
2	Medium	A threat/vulnerability whose occurrence is likely in the next 10 years of operation
1	Low	A threat/vulnerability for which the likelihood of occurrence is deemed possible in a fleet of ships (10 ships) in the next ten years or lower

Table 8 Uncertainty rating tables[96, 106, 107, 113]

U	Rating	Definition
1	Low uncertainty	Most of the following conditions are met: The assumptions made are seen as very reasonable and are not anticipated to change during lifecycle - Low potential for novel attacks arise Much reliable data are available There is broad agreement/consensus among experts The phenomena involved are well understood; models used are known to give predictions with the required accuracy
2	Medium uncertainty	Conditions between those characterizing low and high uncertainty e.g.: The phenomena involved are well understood, but the models used are considered simple/crude and have the potential to change in the future - Medium potential for novel attacks arise Some reliable data are available. Various views exist among the experts
3	High uncertainty	Most of the following conditions are met: The assumptions made represent strong simplifications and can easily change in the future - Attackers might learn/find new ways of attack Data are not available, or are unreliable

		There is lack of agreement/consensus among experts The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions

For the evaluation of identified scenarios risk, the risk matrix as in Table 9 is provided. As a basic scenario, for the SI+LI=2, the level of risk is considered as Low, for SI+LI=4 or SI+LI=3 and high level of uncertainty the risk level is equal to Medium, for SI+LI=4 and high level of uncertainty the risk level is considered as high and for SI+LI=5 or 6 the risk level is considered as high, irrespectively of the knowledge and uncertainty level. This SI+LI consideration is in line with the risk matrix and risk level provided in IEC 62443-2-1 (Table A.3) [42]. The incorporation of uncertainty is aligned to precautionary principle presented in [117] according to which high severity consequences with high uncertainty should be provided due regard, so scenarios with SI=3 and U=2 are also considered as having high risk. Such incorporation of uncertainty in the analysis is also in line with previous publications on the risk assessment in autonomous ships[96, 113] and some recent developments in oil and gas industry with respect to risk assessment [118, 119]. This classification of the scenarios is also used to determine the actual risk level of the security zone and conduit that the engine of the case study belongs.

Table 9 Risk matrix for risk evaluation.

	SI	1		2		3	
LI		Low (L)		Medium (M)		High (H)	
3	High (H)	U=1,2	U=3	U=1,2		U=1,2	
2	Medium (M)	U=1,2	U=3	U=1,2	U=3	U=1,2	
1	Low (L)	U=1,2,3		U=1,2	U=3	U=1	U=2,3

4.7 Step 5 – Control measures identification

During this step we specify the control measures for the identified scenarios. The focus is on the measures that can be used to prevent the threat modes from occurring (preventative control measures), the measures to mitigate the threat modes by reducing the consequences of attacks (mitigative control measures) and measures that can be used to detect the failure and threat modes (detective control measures). For that we also refer to the UR E26[39], UR E27 [40]. The presentation of the identified measures in the FMVEA table is implemented based on the easiness (cost) of their implementation, starting with the simplest and cheapest measures and ending with the most expensive. The easiness of application of various control measures was determined during the discussion with experts at the workshops without using any numerical references, to simplify the approach.

4.8 Step 6 – Control measures selection

During that step we select some specific control measures. We investigate the effect of the identified control measures on the risky scenarios' likelihood and severity, the easiness and cost of their application and how frequently the control measures appear in the relevant scenarios. The selection of the control measures is supported by the identified risk level of various scenarios and zone to which the engine belongs, as recommended in IEC 62443-2-1 [42]. For the risks that were in the medium zone we discuss the uncertainty and also suggest safety recommendations in lines with the precautionary principle[117].

Based on these considerations, we select the final control measures as recommended options for the engine. For the control measures selection, we consider the reduction of identified scenarios with high and medium risk to medium or low risk. However, control measures tackling low level risk are also proposed if they are deemed easy to apply. This risk management is implemented to reduce the potential of surprises stemming from those scenarios which were considered as unlikely. A conformity to the UR E26[39], UR E27 [40] is verified.

4.9 Step 7 – FMVEA results aggregation

Lastly, the results are aggregated in tabular format as per requirements of FMVEA. This is implemented to support the communication of the results to the ultimate decision-makers and for reporting purposes. Sample table is provided in Table 10.

Table 10 The FMVEA results.

a/a	Component	Threat mode	Main Effects	Potential vulnerabilities	LI	SI	Control measures

5 RESULTS & DISCUSSION

5.1 Step 1 – Threat modes identification results

Out of the 15 identified threat scenarios in Table 11, ten or two thirds are related to the ECU. The ECU is responsible for the control and monitoring of the DF engine, implementing multiple functions (see Table 2), so it is no surprise that it has more potential threat modes and scenarios than the sensors. For the identified scenarios in the ECU, two of them were related to spoofing threat mode, with systems representing itself either as ECU or as bridge control console. Five of them were related to the tampering threat mode resulting in the modification of various ECU control settings, yet only one was related to the DoS, repudiation, and elevation of privilege attacks respectively. For the tampering threat mode, we considered grouping some

of the potential attacks (e.g. tampering resulting in change of timing of inlet or exhaust valves), as their effects (step 2) were similar. There is no critical information stored on the ECU but still the attacker might be interested in identifying the engine operational settings to be able to alter them. We assume that attackers interested in stealing critical engine information such as operational settings and fuel consumption would concentrate on the O&E manufacturers on shore data centres and design offices, ECU from scrapped ships freely available on market, class society data or other easily accessible ship systems. Our conclusion herein is very similar to the one provided in BIMCO guidelines [29] with respect to OT technologies.

We considered three types of attack scenarios on sensors, namely tampering, DoS and spoofing type. The attack on control sensors (speed sensors and air pressure sensor) were grouped, as the effects of cyber-attack on them are similar. Similarly, the attack scenarios on safety sensors (cylinder cooling water temperature sensors, lubrication oil temperature and pressure sensors, turbocharger speed sensors, exhaust temperature sensors, oil mist sensors) were grouped. In both safety and control sensors the DoS and tampering threat modes were considered. DoS and tampering are similar to the complete failure and offset/non-responsive/delayed sensor measurements failure modes which can appear under normal conditions as elaborated in [27]. However, we reckon that during cyberattacks the range and the value in offset/non-responsive/delayed sensor measurement can be much greater than observed during physical failures.

5.2 Step 2 – Main effects identification results

As described in the methodology section, we consider the effect first on component level (ECU and sensors) and then on engine level. Such a two-fold consideration of effects supports the identification of the different threat modes effects on the engine.

For the spoofing threat modes in ECU the main effects involve disrupted and degraded communication, which can result in the engine control loss and degraded performance, especially during the transient operations. This might also result in the crew losing awareness of the actual engine condition.

Tampering threat modes are more severe in their effects, as they can alter the engine performance significantly causing engine damages. Typical potential damage scenarios include knocking, misfiring, turbocharger surging and overspeed conditions. They can be caused by altering the timing of natural gas/pilot fuel injection, timing/setting of the waste gate valve opening or through altering PI (Proportional-Integral) controller settings. The engine will react

erratically, and it will be impossible to connect it to the electric network in the power plant. If such attacks are disclosed, they might affect the reputation of the ship operating company.

The DoS attack on ECU will result in the engine loss or engine controllability loss. Elevation of privilege attack can result into control transfer to other location, whilst repudiation can be used to hide the attacker identity and as supportive to other attacks on the engine.

The tampering and spoofing attacks on control sensors can have similar effects with the tampering attacks on the ECU. The DoS on control sensors instead will lead to the engine shutdown due the critically of these sensors and interlinks to ECU safety shutdown function. The attacks on safety sensors will contribute to the engine damage or render the engine inoperable.

5.3 Step 3 – Vulnerabilities identification results

The attack surface as depicted in Figure 3 is quite extensive. However multiple vulnerabilities needs to be exploited to reach the engine as it is located deep in the ship network (Zone 2) indirectly communicating with the rest of the world.

For the ECU spoofing attacks, unauthorised hardware or obsolete hardware in Zone 1 and 2 could be potentially exploited. Alternatively, software vulnerabilities and weak passwords on the whitelisted systems could be used. Malware could be installed on these systems to render this type of attack feasible through open USB ports, VSAT vulnerabilities [120] or remote patching options. For the tampering attacks on ECU, the potential attack paths requires penetration into Zone 2 and also altering the settings of ECU [121], but otherwise the attack path is similar as for ECU spoofing. For the elevation of privilege and repudiation attacks additional software and access management vulnerabilities needs to be exploited. For the DoS on ECU, CAN network vulnerabilities can be exploited as has been demonstrated by some researchers on cars cybersecurity [122, 123]. The high-power electromagnetic pulses can be also considered as a potential attack medium for DoS [124]. Despite they can affect multiple electronics at the same time, they are very sophisticated type of attack [124] and go significantly outside our analysis scope since they refer to the electromagnetic warfare.

It is instructive to observe situations, where the actual networks are different than the planned and different systems than described in the drawings are installed. The legacy systems can overcomplicate the analysis and lead to attack paths, which were completely unexpected and render the control measures identified and selected later in section 5 and 6 less efficient.

Relatively few known vulnerabilities can be exploited for attacks on sensors. Logic bombs, supply chain subversion and physical attacks are the considered options [125, 126]. But potentially more vulnerabilities can be found in the future.

5.4 Step 4 – Risk assessment results

The results of the risk assessment are provided schematically in Figure 6 and in more detail in Table 11. The uncertainty has been depicted using circles of various size in line with recommendations from[107]. As it can be observed, most of the considered scenarios were assigned low likelihood (14/16 or 88%), even without considering the control measures and only 2/16 medium likelihood. This can be attributed to the fact that the ECU is located deeply in the ship network, and therefore it is not so easy to reach and access. This does not exclude though that actors with significant resources such as states and terrorists with potential interests in damaging the engine on a commercial vessel as in our case, might turn their attention to the engine. Only the spoofing attack on ECU was assigned a higher likelihood, due to its relative easiness of implementation, proximity to external communication networks and potential significant consequences for the ship network on overall, if other systems in addition to engine are considered. DoS on ECU likelihood was ranked higher, considering that it is much easier to shut down the engine than to implement the tampering attacks, especially for an inland waterway or short sea going vessels.

Attacks on sensors for a specific commercial ship are even more intricate and less effective if we consider the motivations and goals for different actors. We reckon that it is more likely that a physical failure occurs on sensors than a cyberattack. This resulted in low level likelihood for sensor attacks, even for DoS.

In terms of severity no scenario was assigned a low severity, as engine is a safety critical system on a ship, with tight interactions among the components and any alteration in its control functions might lead to significant degradation or damage of the engine or litigation costs. Also, we reckon the attackers would not be interested in attack scenarios with low severity considering the resources required for these attacks.

In terms of uncertainty though, several scenarios related to ECU tampering attacks were ranked as highly uncertain. Most of the uncertainty judgement in these cases stemmed from uncertainty related to likelihood, whilst there were generally greater confidence in relation to the severity and impact. As mentioned in the methodology section, likelihood estimations are generally challenging. Yet, we considered higher uncertainty, since many of the critical

information related to the ship systems access can be accidentally leaked[127] or found on system components inappropriate scrapped/purged for information on ship sister vessels. Furthermore, it is known from the previous experience on cyber-attacks, that the more attackers become acquainted with the system they attack, the more elaborate attacks they implement and more frequently they do so[128]. The attackers might even install the relevant malware and wait for a suitable moment to activate it. Another source of uncertainty stems from unintentional or attacks aiming at another system. So, it is anticipated that more elaborate attacks can easily intentionally/unintentionally arise. In this situation, historical data is of little help and relevant lack of incidents on OT[29] can be misleading. Such a consideration is in line with discussions from [25, 29], where generally attacks on OT are anticipated to increase.

Consequently, the risk assessment results indicate that there are mostly low likelihood and high severity scenarios, located in the yellow or green area, with only scenario in the red area. Yet, with uncertainties considered, more scenarios are upgraded to the red area. So the risk level of the zone 2 could be considered as medium, if the only high risk scenarios are addressed, following the precautionary principle[117]. The identified and considered control measures are discussed in more detail in the next sections.

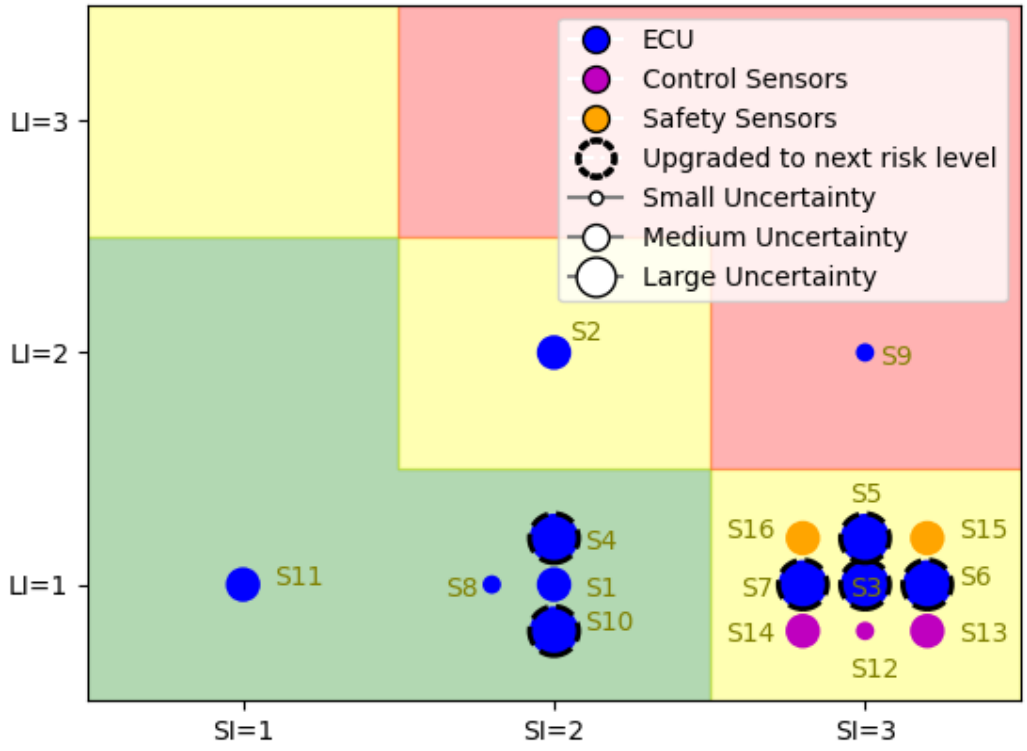

Figure 6 Risk matrix results for different scenarios considering uncertainty.

5.5 Step 5 – Control measures identification

The minimum set or control measures is provided in Table 1 and additional in Table 2 of UR E27[40]. Here we discuss some of the most relevant to our case study based on the risk assessment results. The identified control measures are also presented in the last column of Table 11 based on their easiness of application, starting with the simplest and ending with the most complex one.

Reducing the potential of entrance to the system for malicious actors by blocking USB ports, using strong passwords, physical checks and physical monitoring can be considered as easy to implement but also strong in effectiveness operational cybersecurity measures. More advanced measures include the whitelisting of components, virus- and intrusion detection systems, use of kernels security zones, sophisticated and multiple access verification software update processes, ECU robustness (fault tolerance) increase. Some identified design measures include micro segmentation and demilitarisation, use of mechanical control instead of electronic control, advanced alarm and monitoring system, redundancy in sensors. Their detailed selection for our use case is discussed in the next section.

5.6 Step 6 – Control measures selection

Some of the measures constantly repeat in the considered scenarios such as strong passwords and multifactor authentication on VSAT and 4G/5G, physical checks, closing the USB ports on SCADA server, regular checks and vigilant monitoring. They are easy to implement, and their application is generally recommended as a part of sound cybersecurity practices recommended by standards in line with the defence in depth approach [39, 40, 42] on conventional ships. It should be noted that the old VSAT systems might not be capable of implementing strong passwords, so it might be prudent to consider hardware updates. Antivirus-systems on the computers connected to the internet are required [39] even if their implementation contributes to complexity and increased vulnerability. Antivirus-software act typically as a blacklisting function which needs to be constantly updated, so the increased connectivity due to antivirus updates should be subject to careful trade-off. As per IACS requirements[39], control such as firewall between zone 1 and 2 shall be established or the computers connected to the internet and used for communication to the shore segregated from the rest of the network. Segmentation is also important in the view of unintentional connections to the OT systems by the crew, which can lead to cybersecurity breach.

Upgrading the hardware, for instance installing more up-to-date computers will also significantly reduce the attack vector. However, it is hard to determine, which systems can be replaced at all without losing critical functionality. Version dependency from applications to operating system, drivers and hardware is a big problem. It can be also costly.

Whitelisting principle can be considered as an easy fix to be applied to the systems to avoid hazards from the legacy systems or other systems pretending as ECU/bridge control system and can be used as a mean of access control[39]. Some of the mechanical protections as mechanical overspeed protection are already required by the regulations for safety reasons [129], so they need to be included also for cybersecurity reasons. Communication kill switch and remotely operated manual override can be also considered as easy mitigative control measures [39]. Stringent requirements and impedance to ECU software update might reduce the likelihood for many of the tampering scenarios. Additionally, the increased robustness of ECU can be used as a barrier not only to cyber-attacks but also to sensors failures. Robustness is especially important, considering the high uncertainties. Manual reboot shall be provided as well [39].

The reduction in electronically controlled functions and processes is not a way to go as it will reduce the engine efficiency. Furthermore, it does not seem necessary to have intrusion

detection systems, be cautious about the trustworthiness of sensors/ECU suppliers or increase the sensors number because of cybersecurity concerns (unless they are RFID). The use of intrusion detection systems might increase the complexity and result in unnecessary false alarms due to the deviations in the operational systems parameters as the error management in old and legacy systems might not be optimised. There is no need for additional alarm monitoring system for engine, as the existing alarm system but also visual and audio observation can make aware the crew of potential issues.

This might not be the case for an unmanned or partially autonomous ship, as there will be a need for a replacement of the visual and audio observation, so additional controls should be in place [130, 131]. For a military vessel of similar size extra measures shall be considered, as the likelihood of attacks is increased (instead of Low should be considered Medium or High) in many cases.

On overall the suggested control measures for the commercial vessel, except ensuring the ECU robustness might not reduce the severity of the considered scenarios, but they will bring the zone risk level at medium level by reducing the potential of surprise as they will render it even less possible for a successful cyberattack to occur on the considered case.

5.7 Step 7 – FMVEA results aggregation

The aggregated results are presented in FMVEA table as in Table 11.

.

Table 11 FMVEA analysis for the DF engine

a/a S	Component		Threat mode	Main effects		Potential vulnerabilities	LI	SI	RI	U	Identified potential control measures (presented in priority of easiness)
				Effect on component	Effect on engine						
1	Electronic control unit	Spoofing	Spoofing attack in Zone 2 (Other controller representing itself as the ECU to Zone 1)	-Disrupted communication between the ECU and other controllers such as the bridge control console	-Adequate power not provided when required -Excessive power generated by engine -Crew awareness of actual health and power state of marine engine(s) reduced	-Unauthorised hardware installed or remained (legacy systems) on the ship + defective maintenance and inspections + malware installation through VSAT vulnerabilities or malware installed through USB port or during software update or using social engineering attacks as first entry point to system -SCADA having independent internet link -Another computer e.g. SCADA server mimicking the ECU (malware installation) -Exploitation of logic bombs and backdoors -Outdated software -Unintentional data leaks e.g. inappropriate sister ship scrapping, crew sending data to wrong actors	1	2	3	2	-Strong passwords on VSAT and multifactor access on SCADA -Physical Checks -Closing the USB ports on SCADA server -Whitelisting -Antivirus on computers -Stringent requirements for software update (multiple verification system) -Zone 1 segmentation - Demilitarised zones in Zone 1

2			Spoofing attack in Zone 1 or Zone 2 (Other controller representing itself as the bridge control console) (Can be considered as combination of spoofing and tampering attack)	-ECU receiving control commands from fake controller(s)	-Power output not following the power demand	-Unauthorised hardware installed (legacy systems) on the ship + defective maintenance and inspections + malware installation or malware installed through USB port/VSAT or during software update or using social engineering attacks -SCADA having independent internet link -Malware installed on e.g. SCADA mimicking the bridge control console -Exploitation of logic bombs and backdoors -Outdated/Obsolete software such as Windows 7 -Unintentional data leaks e.g. inappropriate sister ship scrapping, crew sending data to wrong actors	2	2	4	2	-Strong passwords on VSAT and multifactor access on SCADA -Physical Checks -Closing the USB ports on SCADA server -Antivirus on computers -Whitelisting for systems in Zone 1 -Zone 1 segmentation -Hardware update for obsolete software (like Windows 7)
3		Tampering	Tampering attack resulting in changing the PI settings of speed governor function implemented by ECU or resulting in changing the injection timing and mass for dual-fuel mode	-Inappropriate control commands sent by ECU	-Engine providing too slow/ too fast response, engine overspeed, engine speed/load reduction -Knocking, misfiring, torsional vibrations, improper emissions (NOx, HC), turbocharger surging effects. -In high knocking case engine shutdown might not be feasible which might result in damage -Decrease in engine efficiency -Load sharing, network instability, connection problems	-Settings in systems allowing remote modification of controller settings -Open USB port on other controllers/systems + malware - Malware transferred though VSAT vulnerabilities or legacy systems or SCADA having independent internet link -Unintentional data leaks e.g. inappropriate sister ship scrapping, crew sending data to wrong actors	1	3	4	3	-Strong passwords on VSAT and multifactor access on SCADA -Closing the USB ports on SCADA server -No remote modifications allowed -Crew monitoring the operational conditions and capable of rebooting/restoring system -Alarm monitoring system -Type approval processes -Use of mechanical overspeed protection

4			Tampering attack resulting in closure or opening or different opening of waste gate valve in diesel or dual-fuel mode		-Little effect on diesel mode -Incomplete combustion process, vibrations, misfiring, knocking, turbocharger surging in natural gas mode	As above	1	2	3	3	Same as for 3 -Mechanically-based control opening of waste gate valve
5			Tampering attack resulting in closure or opening or different opening of exhaust gas valve or inlet valve		-Gas-exchange process failure, turbocharger surging and choke -Incomplete combustion process, misfiring due to the lack of oxygen - Engine shutdown due to high-temperature exhaust gas alarming -Power and propulsion loss	As above	1	3	4	3	Same as for 3 -Mechanically-based control opening of exhaust gas valve
6			Tampering attack resulting in turning off some safety and monitoring functions	-ECU not sending or sending fake safety information to the alarm system	-Can be combined with other attacks to cause considerable damage to engine	As above	1	3	4	3	Same as for 3 -Use of independent safety monitoring controller (other hardware)

7			Tampering attack resulting in ECU perceiving wrongly the received information from sensors	ECU perceiving the pressure measurement as speed or vice versa and giving control commands as in scenarios 3-6	-Engine unstable behaviour resulting in shutdown -Misfiring, knocking, power loss, or even severe structure damage due to wrong PI control	As above	1	3	4	3	Same as for 3
8		Repudiation	Repudiation attack by assigning the software modification to other entity	Altered patch history	-Legal implications, no direct implications for the engine -Can be combined with other attacks to cause damage to engine without being assigned responsibility	-Buffer overflow and command injection vulnerabilities	1	2	3	1	- Digital signature appended to the software package and check results sent to the actual users
9		DoS	Denial of service attack on ECU	-No functions implemented by ECU	-Engine control loss	-CAN vulnerabilities exploitation -Malware installation (as previously) -SCADA having independent internet link	2	3	5	1	-Same as for 3 -Possibilities for rebooting of software -Alarm monitoring system -CAN protection systems
10		Elevation	Elevation of privileges to remote operator/ operator/ another operator	Control over engine transferred to remote location	-Loss of engine control in other attacks	-Logic bombs -Weak passwords -Inappropriate access control management	1	2	3	3	-Communication kill-switch -Multiple verification system -Use of reliable equipment provider
11		Informatio	Stealing the engine critical operational information	Critical engine parameters know to the attacker	-Can be used for other attacks	-Logic bombs -Weak passwords -Inappropriate access control management	1	1	2	2	More advanced access control management

12	Control sensors (engine speed sensor, air pressure sensor for	Spoofing	Spoofing resulting in sensors confusion	Altering the communication address of sensor	-Engine overspeed/unstable performance, misfiring, knocking, power loss, or even substantial structure damage due to wrong PI control -Engine shutdown	-Logic bombs -Inappropriate connections -Supply chain subversion	1	3	4	1	-Crosscheck of sensor measurements -Use of mechanical overspeed protection -Independent safety systems shutting down the engine
13		Tampering	Tampering of sensors	Freezing sensors value	-Inappropriate power and propulsion generation -Engine overspeed / unstable performance resulting in substantial damage	-Logic bombs -Physical attack -Zero vulnerabilities -Supply chain subversion -Software update if RFID sensors used	1	3	4	2	-Use of different/advanced sensors for control and monitoring -ECU robustness increase -Use of reliable equipment supplier -Advanced alarm monitoring system -Use of mechanical overspeed protection
14		DoS	Denial of service attack e.g., causing sensor give zero value	Wrong input to ECU	-Engine shutdown -Problems with engine starting	-Logic bombs -Physical attack -Zero vulnerabilities -Supply chain subversion -Communication flooding	1	3	4	2	-Redundancy in sensors -Use of reliable equipment supplier
15	Safety and monitoring sensors	Tampering	Tampering resulting in sensor measurement modification	Sensors giving wrong value	-Engine shutdown -Problems with engine starting -Engine damage or wear	-Logic bombs -Physical attack -Zero vulnerabilities -Supply chain subversion -Software update if RFID sensors used	1	3	4	2	-Redundancy in sensors -Operator visual and audio monitoring -Use of reliable equipment supplier
16		DoS	Denial of service attack on sensors	Sensors giving no output	-Engine shutdown	-Logic bombs -Physical attack -Zero vulnerabilities -Supply chain subversion -Communication flooding	1	3	4	2	-Redundancy in sensors -Operator visual and audio monitoring -Use of reliable equipment supplier

5.8 Demonstrated methodological advantages

The presented enhanced FMVEA is both component and scenario based cyber risk assessment methodology. It starts with components and finishes with scenarios. In this way it captures the physical and the functional facets of the system and cyberattacks. As it is aligned to the maritime regulatory framework and the known standards, and well-routed in the scientific research, it can constitute a useful tool in the hands of maritime practitioners, especially the engine manufacturers.

The ranking is rather simple and wide (on a logarithmic level), and the selection of the control measures does not follow any complex mathematical ranking procedure as in [21, 58, 65, 75]. However, simplicity might be treated as a strength, since not all the parameters are easy to quantify, and the generated resulted in such approaches still suffer from uncertainty. It means that less effort is needed to derive some useful conclusions. Furthermore, the approach does not exclude potential more advanced ranking procedures incorporation. However, this is left for consideration in future research.

The main FMVEA strength is in the identification of potential effects and consequences of the cyberattacks on a mechanical system due to the use of FMEA format. This would be challenging to be identified in graph theory methods, which would still rely on some of reasoning as in FMVEA. Also, we consider in FMVEA the potential of the attack through legacy systems, which might skip the attention of the cyber risk analysis relying solely on the ship drawings and communications. Furthermore, the FMVEA application does not exclude its combination with other methods as already mentioned.

5.9 Results and methodology limitations

The attack scenarios are presented to be independent in Table 11. However, a very advanced and interested attacker or investigator can combine the scenarios to implement a more elaborate successful attack. This emergent attack scenarios were not assessed as a part of the process, but this can be easily done using attack trees, graph models or adding a combinatory scenario, since these identified scenarios can used for construction of more complicated attack scenarios, similarly with FMEA providing input to Fault Tree development. Furthermore, as we treated the underlying scenarios of the complex attack, this complex attack is already indirectly addressed in FMVEA. So more sophisticated approaches based on graph theory and formal ship network models could consider them in much greater detail [132] based on our results.

The rankings that we considered in the analysis are based on expert feedback and the current state of the art knowledge. We also considered uncertainties in our rankings. However, the area of maritime cybersecurity is rapidly evolving and thus such assessment should be treated with caution and updated based on the developments in the area[39]. Attackers are constantly looking for the loopholes in the systems, and it is similar to the hunting or competition process. To capture this attack scenarios risk evolution more elaborate risk assessment methods based on game theory, immune response system or prey-predator algorithms should be considered [17, 133].

The rankings for the DF engine were derived considering the specific engine function as main engine and inland waterway ship / small short sea going ship network. If the engine was used a small diesel generator together with other multiple generators on another ship, this would result in different ECU functions and network interconnections and functions, additional power management system functions and novel emergent hazards leading to power generation loss [134-136], which would require identifying additional scenarios and additional rankings implementation on a different system level. Yet the results could be used as input to the identification of potential pathways to blackouts and power loss on ships involving complex processes for power generation and management, which can be addressed in future research as another dedicated case study. Furthermore, treating the engine loss conservatively in the risk management, we partially also addressed the cases where the engine loss due to cyber-attack leads to blackout.

Also, as mentioned some control measures applicability and rankings would have altered if the ship was considered for military or autonomous operations, as this would alter the profile of interested attackers and ship networks, and this was briefly discussed in the paper. Yet, exactly the same methodology could be applied for these cases as well. The results are also still applicable to the diesel engines used in similar context as DF engines can be viewed having greater functionalities and risks than diesel engines.

5.10 Implications for research and practice

From research perspective, the conducted results validate the widely perceived conclusion that attacks on OT systems can lead to significant safety implications, even if the likelihood is low[29, 65]. However, in addition to that it demonstrates that not all of the STRIDE attacks scenarios hold the same relevance to the OT systems, since repudiation, elevation of privilege and information disclosure appear much less frequently and have lower risk than denial of service, tampering and spoofing attacks. This finding is similar to the one provided in[26, 70, 80] but slightly

different from the results in [68, 69], where the same number of STRIDE threat modes was considered but the risk level was generally higher for denial of service, tampering and spoofing attacks. This means that STRIDE and consequently FMVEA applications can be further optimised and improved by focusing on those scenarios that hold the highest relevance to the attack scenarios on OT systems, such as denial of service, tampering and spoofing attacks.

Focusing on the engine and not the whole ship also turned an effective way to support the analysis of the relevant engine related safety implications, which can be useful for the engine manufacturers and for ship owner if he/she becomes more interested in the relevant failure modes. This result constitutes another argument in favour of cybersecurity and safety management in line with "divide and conquer" approach[137, 138] in parallel to the heavily promoted systemic approaches[139, 140], addressing emergent risks and coarse ship-level risk assessment approaches such as already used in aviation on (Functional Hazard Analysis on high, aircraft level and subsequent FMEA and/or Fault Tree Analysis for critical scenarios on system level)[141] and now suggested for autonomous ships[96, 142] (initially coarse ship level risk assessment and then more detailed ship system risk assessment level).

The incorporation of uncertainty supported identification of some aspects related to our intrinsic assumptions on cyber-attacks during risk assessment and justifying better why some some scenarios require more effective treatment/should be considered more risky. In this way the demonstrated risk assessment approach constitute an attempt to bridge the gap between the industry and academia [89], when it comes to incorporation of novel risk definition relying on uncertainty[116], supporting industrial stakeholders in using novel risk science concepts in their daily practices.

The uncertainty related to some of the scenarios, demonstrate the need for increased cyber robustness and cyber resilience with respect to the marine engines. This involves developing novel approaches which would test in a virtual environment the effect of cyberattacks, similarly to the approaches already proposed for safety[25, 27]. Engines needs to be designed in such a way, that even if an attack happens, harm/damage to the personnel/engine is minimised, since we cannot fully eradicate the likelihood of attack.

From practical perspective, it can be observed, that there are multiple potential ways in which attacks on engine, can lead to engine loss or damage, even if it is located inside the ship network. These results highlight the importance of better understanding of interactions between the cyber, physical parts in the advanced maritime systems and also impact on humans, with

respect to the potential cyber risk and the need to update and incorporate methods in the industrial processes such as FMVEA in addition to the classical FMECA and model-based approaches to attacks assessment on networks currently used by industry.

The results also demonstrated an elevated risk on the control components, compared to sensors, which translates in the relevant increased management effort for them compared to sensors at the current stage of knowledge. Furthermore, the same results demonstrate, that in addition to the state-of-the art cybersecurity solutions, the risk of cyberattacks can be also mitigated using mechanical barriers. This holds a special relevance in the applications with high risk or interest for attackers such as autonomous ships. Also, not necessary the expensive control measures are effective, as they simultaneously can become additional entry points as this happens with antiviruses or add complexity as it happens with intrusion detection systems. However, in some cases such obsolete computers, employing expensive mitigations might be inevitable.

As it been shown in the related research and guidelines section, the cybersecurity regulatory framework for inland waterway ships systems seems to be covering limited aspects. The demonstrated approach, routed in the relevant IACSs guidelines, safety and cybersecurity assessment methods could constitute a basis for more systematic development of relevant and adapted guidelines and requirements in inland water ways ships. The findings related the engines could be also used as input for these more specific requirements.

6 CONCLUSIONS

In this paper a risk assessment of a ship DF engine on inland waterway vessel based on FMVEA adapted to maritime employed standards and guidelines, considering uncertainties has been presented.

The main findings of this study are as follows:

- Tampering, Spoofing and DoS attacks scenarios can be considered as important threat modes for the investigated DF engine from severity perspective.
- Tampering attacks on the ECU can cause significant damage to the engine, but simultaneously they have low likelihood. Yet, with uncertainties considered, they still require treatment. DoS attack on the engine, if not addressed, has a higher risk. Attacks on sensors are deemed less likely.
- Multiple vulnerabilities can be employed to conduct the attacks on the engine in

commercial ship, but they can be relatively easy addressed. However additional control measures might need to be considered on military or autonomous ships.

- The FMVEA method constitute an effective method for identification and management of cyber risk in maritime systems with its greatest strength in identifying effects of cyberattacks on the maritime systems. FMVEA can be also used in conjunction with other cybersecurity methods for better cyber risk management.
- Achieving robustness and resilience in marine engines in view of cyberattacks and associated uncertainties becomes more important.

We believe that the conducted study presents a useful adaptation of FMVEA which can become a practical tool for the maritime practitioners. Future research could concentrate on investigating in greater detail the cyberattacks propagation paths and their effect on combined likelihood in the maritime systems, methods integration and enhancement or applying FMVEA to other maritime systems.

7 DISCLAIMER

The opinions expressed herein are those of the authors and should not be construed to reflect the views of Aalto University, Harbin Engineering University, Wärtsilä Voyage, Royal Carribean, CTN or any referred or acknowledged organisations and individuals.

8 ACKNOWLEDGMENTS

The authors affiliated with Aalto university acknowledge the funding that they have received for conducting and presenting the research from Merenkulun säätiö under application number 20220087 and from AutoMare project funded by Finnish Ministry of Education and Culture under application number 117784. The authors also kindly acknowledge the support they received from Matti Suominen, Ross Bailey and Tero Vänskä from Wärtsilä, Oussama Methlouthi from CTN and from Christopher Stein from Royal Caribbean.

9 REFERENCES

1. Papanikolaou A. *Ship design: methodologies of preliminary design*. Springer, 2014.
2. Abaei MM, Hekkenberg R and BahooToroody A. A multinomial process tree for reliability assessment of machinery in autonomous ships. *Reliability Engineering & System Safety* 2021; 210: 107484. DOI: https://doi.org/10.1016/j.ress.2021.107484.
3. Deng J, Wang X, Wei Z, et al. A review of NOx and SOx emission reduction technologies for marine diesel engines and the potential evaluation of liquefied natural gas fuelled vessels. *Science of the Total Environment* 2021; 766: 144319.
4. Joung T-H, Kang S-G, Lee J-K and Ahn J. The IMO initial strategy for reducing Greenhouse Gas (GHG) emissions, and its follow-up actions towards 2050. *Journal of International Maritime Safety, Environmental Affairs, and Shipping* 2020; 4: 1-7.
5. ABS. *Ship Energy Efficiency Measures - Status and Guidance*. 2013.
6. Wärtsilä. WÄRTSILÄ 50DF engine technology. 2009.
7. MAN. ME-GI Dual Fuel MAN B&W Engines. MAN B&W Engines, 2014.
8. Yang R, Theotokatos G and Vassalos D. Parametric investigation of a large two-stroke marine high-pressure direct injection engine by using computational fluid dynamics method. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2020; 234: 699-711. DOI: 10.1177/1475090219895639.
9. Murat Durmaz and Ergin S. A Numerical Study on the Performance and Emission Characteristics of Dual-Fuel LNG Diesel Engine. *TEAM 2019*. Tainan, Taiwan2019.
10. Bolbot V, Trivyza NL, Theotokatos G, et al. Cruise ships power plant optimisation and comparative analysis. *Energy* 2020; 196: 117061. DOI: https://doi.org/10.1016/j.energy.2020.117061.
11. Xiang L, Theotokatos G and Ding Y. Parametric investigation on the performance-emissions trade-off and knocking occurrence of dual fuel engines using CFD. *Fuel* 2023; 340: 127535.
12. Palmén M, Lotrič A, Laakso A, et al. Selecting Appropriate Energy Source Options for an Arctic Research Ship. *Journal of Marine Science and Engineering* 2023; 11: 2337.
13. Jo SW and Shim WS. LTE-Maritime: High-Speed Maritime Wireless Communication Based on LTE Technology. *IEEE Access* 2019; 7: 53172-53181. DOI: 10.1109/ACCESS.2019.2912392.
14. Katsikas S, Dimas D, Defigos A, et al. Wireless modular system for vessel engines monitoring, condition based maintenance and vessel's performance analysis. In: *PHM Society European Conference* 2014.
15. Trivyza NL, Rentizelas A and Theotokatos G. A novel multi-objective decision support method for ship energy systems synthesis to enhance sustainability. *Energy Conversion and Management* 2018; 168: 128-149. DOI: https://doi.org/10.1016/j.enconman.2018.04.020.
16. Tsitsilonis K-M and Theotokatos G. A novel method for in-cylinder pressure prediction using the engine instantaneous crankshaft torque. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2022; 236: 131-149. DOI: 10.1177/14750902211028419.
17. Bolbot V, Kulkarni K, Brunou P, et al. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection* 2022; 39: 100571. DOI: https://doi.org/10.1016/j.ijcip.2022.100571.
18. Meland P, Bernsmed K, Wille E, et al. A retrospective analysis of maritime cyber security incidents. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 2021; 15.
19. Orhan M and Celik M. A literature review and future research agenda on fault detection and diagnosis studies in marine machinery systems. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment*; 0: 14750902221149291. DOI: 10.1177/14750902221149291.
20. IMO. Guidelines on Maritime Cyber Risk Management. *MSC-FAL1/Circ3/Rev1*. 2021.

21. Tam K and Jones K. MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs* 2019; 18: 129-163. DOI: 10.1007/s13437-019-00162-2.
22. Nate L. The cost of a malware infection? For Maersk, $300 million. *Digital guardian* 2020.
23. Brew L, Drazovich L and Wetzel S. The Impact of COVID-19 on the Security and Resilience of the Maritime Transportation System. In: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* 2021, pp.510-517. IEEE.
24. Bicen S and Celik M. A bibliometric review on maritime inspection analysis: Current and future insights. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2023; 237: 275-292. DOI: 10.1177/14750902221119341.
25. DNV. Maritime cyber priority 2023. 2023.
26. Bolbot V, Methlouthi O, Banda O, et al. Identification of cyber-attack scenarios in a marine Dual-Fuel engine. *Trends in Maritime Technology and Engineering Volume 1* 2022: 503-510.
27. Stoumpos S, Bolbot V, Theotokatos G and Boulougouris E. Safety performance assessment of a marine dual fuel engine by integrating failure mode, effects and criticality analysis with simulation tools. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2022; 236: 376-393. DOI: https://doi.org/10.1177/14750902211043423.
28. Dugan SA and Utne IB. Statistical analysis of vessel loss of command frequency. *Maritime Transport Research* 2024; 6: 100104.
29. BIMCO. The Guidelines on Cyber Security Onboard Ships Version 4.0. 2021.
30. AUTOSAR. Standards - AUTOSAR Documents, https://www.autosar.org/search?security (2023).
31. NIST. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. 2012.
32. Lamba A, Singh S, Balvinder S and Rela S. To Classify Cyber-Security Threats in Automotive Doming Using Different Assessment Methodologies. *International Journal For Technological Research In Engineering* 2015; 3.
33. Anthony Cox Jr L. What's wrong with risk matrices? *Risk Analysis: An International Journal* 2008; 28: 497-512.
34. Duijm NJ. Recommendations on the use and design of risk matrices. *Safety Science* 2015; 76: 21-31.
35. Levine E. Improving risk matrices: the advantages of logarithmically scaled axes. *Journal of Risk Research* 2012; 15: 209-222.
36. iTrust. *Cyber Risk Management in Shipboard Operational Technology Systems* 2022. Centre for research in cyber security.
37. CESNI. Good practice guide: Cybersecurity in inland navigation - Especially for ports. 2023.
38. PIANC. Awareness paper on cybersecurity in inland navigation. 2019.
39. IACS. E26 Cyber resilience of ships. 2022.
40. IACS. E27 Cyber resilience of on-board systems and equipment. 2022.
41. DNV. IACS Unified Requirements for Cyber Security Mandatory from 1 January 2024, https://www.dnv.com/news/iacs-unified-requirements-for-cyber-security-mandatory-from-1-january-2024-227429 (2022).
42. IEC. *Security for industrial automation and control systems - IEC 62443*. 2018 2018.
43. Wärtsilä. Who do you entrust your business-critical assets to?, https://www.wartsila.com/insights/article/who-do-you-entrust-your-business-critical-assets-to (2024, accessed 24/4/2024 2024).
44. IACS. Recommendation for the FMEA process for diesel engine control systems. In: Machinery, (ed.). International Association of Classification Societies (IACS), 2014.
45. Ahmed S and Gu X-C. Accident-based FMECA study of Marine boiler for risk prioritization using Fuzzy expert system. *Results in Engineering* 2020: 100123. DOI: https://doi.org/10.1016/j.rineng.2020.100123.
46. Banks J, Hines J, Lebold M, et al. *Failure modes and predictive diagnostics considerations for diesel engines*. 2001. Pennsylvania State Uvin University Park Applied Research lab.

47. Cicek K, Turan HH, Topcu YI and Searslan MN. Risk-based preventive maintenance planning using Failure Mode and Effect Analysis (FMEA) for marine engine systems. In: *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on* 2010, pp.1-6. IEEE.
48. Ling D, Huang H-Z, Song W, et al. Design FMEA for a diesel engine using two risk priority numbers. In: *Reliability and Maintainability Symposium (RAMS)* 2012, pp.1-5. IEEE.
49. Cicek K and Celik M. Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship. *Safety Science* 2013; 51: 6-10.
50. Ceylan BO. Marine diesel engine turbocharger fouling phenomenon risk assessment application by using fuzzy FMEA method. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2023: 14750902231208848.
51. Lazakis I, Raptodimos Y and Varelas T. Predicting ship machinery system condition through analytical reliability tools and artificial neural networks. *Ocean Engineering* 2018; 152: 404-415. DOI: https://doi.org/10.1016/j.oceaneng.2017.11.017.
52. Milioulis K, Bolbot V and Theotokatos G. Model-based safety analysis and design enhancement of a marine LNG fuel feeding system. *Journal of Marine Science and Engineering* 2021; 9: 69.
53. Milioulis K, Bolbot V, Theotokatos G, et al. Safety analysis of a high-pressure fuel gas supply system for LNG fuelled vessels. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2022; 236: 1025-1046. DOI: 10.1177/14750902221078426.
54. Dionysiou K, Bolbot V and Theotokatos G. A functional model-based approach for ship systems safety and reliability analysis: Application to a cruise ship lubricating oil system. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 2021: 14750902211004204. DOI: 10.1177/14750902211004204.
55. Karatuğ Ç, Ceylan BO and Arslanoğlu Y. A risk assessment of scrubber use for marine transport by rule-based fuzzy FMEA. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment*; 0: 14750902231166030. DOI: 10.1177/14750902231166030.
56. Uflaz E, Sezer SI, Tunçel AL, et al. Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. *Reliability Engineering & System Safety* 2024; 243: 109825.
57. Park C, Kontovas C, Yang Z and Chang C-H. A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management* 2023; 235: 106480.
58. Amro A, Gkioulos V and Katsikas S. Assessing cyber risk in cyber-physical systems using the ATT&CK framework. *ACM Transactions on Privacy and Security* 2023; 26: 1-33. DOI: https://doi.org/10.1145/3571733.
59. Schmittner C, Gruber T, Puschner P and Schoitsch E. Security application of failure mode and effect analysis (FMEA). In: *International Conference on Computer Safety, Reliability, and Security* 2014, pp.310-325. Springer.
60. Dghaym D, Hoang T, Turnock S, et al. An STPA-based formal composition framework for trustworthy autonomous maritime systems. *Safety science* 2021; 136: 105139.
61. Zhou X, Liu Z, Wang F and Wu Z. A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Engineering* 2021; 222: 108569.
62. Glomsrud J, Xie J, Michael B and Enrico Z. A Structured STPA Safety and Security Co-analysis Framework for Autonomous Ships. *European Safety and Reliability conference*. Germany, Hannover2019.
63. Omitola T, Downes J, Wills G, et al. Securing navigation of unmanned maritime systems. 2018.
64. Cardellicchio D. Naval Automation Cyber Defence Guidelines. *Technology and Science for the Ships of the Future*. IOS Press, 2018, pp.943-949.

65. Bolbot V, Theotokatos G, Boulougouris E and Vassalos D. A novel cyber-risk assessment method for ship systems. *Safety Science* 2020; 131: 104908. DOI: https://doi.org/10.1016/j.ssci.2020.104908.
66. Bolbot V, Theotokatos G, Wennersberg L, et al. A novel risk assessment process: Application to an autonomous inland waterways ship. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 2021; 0: 1748006X211051829. DOI: 10.1177/1748006x211051829.
67. Bolbot V, Theotokatos G, Boulougouris E and Vassalos D. Safety related cyber-attacks identification and assessment for autonomous inland ships. *Internation Seminar on Safety and Security of Autonomous Vessels*. Helsinki, Finland2019.
68. Kavallieratos G, Katsikas S and Gkioulos V. Cyber-Attacks Against the Autonomous Ship. In: *Computer Security* (eds Katsikas SK, Cuppens F, Cuppens N, et al.), 2019// 2019, pp.20-36. Springer International Publishing.
69. Kavallieratos G, Spathoulas G and Katsikas S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. *Sensors* 2021; 21: 1691.
70. Bolbot V, Basnet S, Zhao H, et al. Investigating a novel approach for cybersecurity risk analysis with application to remote pilotage operations. In: *European Workshop on Maritime Systems Resilience and Security* 2022.
71. Jo Y, Choi O, You J, et al. Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors* 2022; 22: 1860.
72. de Peralta F. Cybersecurity Resiliency of Marine Renewable Energy Systems‐Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk. *Marine Technology Society Journal* 2020; 54: 97-107.
73. de Peralta F, Watson M, Bays R, et al. Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management. *Marine Technology Society Journal* 2021; 55: 104-116.
74. Kavallieratos G, Katsikas S and Gkioulos V. SafeSec Tropos: Joint security and safety requirements elicitation. *Computer Standards & Interfaces* 2020; 70: 103429. DOI: https://doi.org/10.1016/j.csi.2020.103429.
75. Meland P, Nesheim D, Bernsmed K and Sindre G. Assessing cyber threats for storyless systems. *Journal of Information Security and Applications* 2022; 64: 103050. DOI: https://doi.org/10.1016/j.jisa.2021.103050.
76. Sulaman SM, Beer A, Felderer M and Höst M. Comparison of the FMEA and STPA safety analysis methods–a case study. *Software Quality Journal* 2017: 1-39.
77. Schmittner C, Ma Z, Schoitsch E and Gruber T. A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive Cyber-Physical Systems. *1st ACM Workshop on Cyber-Physical System Security*. Singapore, Republic of Singapore2015.
78. Hussain S, Kamal A, Ahmad S, et al. Threat modelling methodologies: a survey. *Sci Int(Lahore)* 2014; 26: 1607-1609.
79. Abuabed Z, Alsadeh A and Taweel A. STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles. *Computers & Security* 2023; 133: 103391.
80. Sahay R, Estay DS, Meng W, et al. A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. *Computers & Security* 2023; 128: 103179.
81. Madan BB, Banik M and Bein D. Securing unmanned autonomous systems from cyber threats. *The Journal of Defense Modeling and Simulation* 2019; 16: 119-136.
82. Tamimi A, Hahn A and Roy S. Cyber threat impact analysis to air traffic flows through Dynamic Queue Networks. *ACM Transactions on Cyber-Physical Systems* 2020; 4: 1-22.
83. Chang J-S, Jeon Y-H, Sim S and Kang AN. Information security modeling for the operation of a novel highly trusted network in a virtualization environment. *International Journal of Distributed Sensor Networks* 2015; 11: 359170.

84. Wong AY, Chekole EG, Ochoa M and Zhou J. On the security of containers: Threat modeling, attack analysis, and mitigation strategies. *Computers & Security* 2023; 128: 103140.
85. Ali SS, Ibrahim M, Sinanoglu O, et al. Security assessment of cyberphysical digital microfluidic biochips. *IEEE/ACM transactions on computational biology and Bioinformatics* 2015; 13: 445-458.
86. Kaneko T, Takahashi Y, Okubo T and Sasaki R. Threat analysis using STRIDE with STAMP/STPA. In: *The international workshop on evidence-based security and privacy in the wild* 2018, pp.10-17.
87. Fatimah Sidi, A. Jabar Marzanah, Lilly Suriani Affendey, et al. A Comparative Analysis Study on Information Security Threat Models: A Propose for Threat Factor Profiling. *Journal of Engineering and Applied Sciences* 2017; 12: 548-554. DOI: 10.36478/jeasci.2017.548.554.
88. Monteuuis J-P, Boudguiga A, Zhang J, et al. Sara: Security automotive risk analysis method. In: *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* 2018, pp.3-14.
89. Aven T. On the gap between theory and practice in defining and understanding risk. *Safety science* 2023; 168: 106325.
90. Aven T. Practical implications of the new risk perspectives. *Reliability Engineering & System Safety* 2013; 115: 136-145.
91. Askeland T, Flage R and Aven T. Moving beyond probabilities–Strength of knowledge characterisations applied to security. *Reliability Engineering & System Safety* 2017; 159: 196-205.
92. Askeland T, Flage R and Guikema SD. Assessing the risk reducing effect of measures against intelligent attacks: review and discussion of some common approaches. *International Journal of Business Continuity and Risk Management* 2021; 11: 25-51.
93. Araskalaei AH. *Evaluation of IT Security Risk Standards Relative to Risk Analysis and Management Science*. University of Stavanger, Norway, 2020.
94. Xiang L, Theotokatos G, Cui H, et al. Parametric knocking performance investigation of spark ignition natural gas engines and dual fuel engines. *Journal of Marine Science and Engineering* 2020; 8: 459.
95. Xiang L, Theotokatos G and Ding Y. Investigation on gaseous fuels interchangeability with an extended zero-dimensional engine model. *Energy conversion and management* 2019; 183: 500-514.
96. Bolbot V, Theotokatos G, Wennersberg LA, et al. A novel risk assessment process with application to autonomous inland waterways vessels. *Part O: Risk and Reliability* 2021.
97. Stefani A. *An introduction to ship automation and control systems*. United Kingdom, London: Institute of Marine Engineering, Science & Technology, 2013.
98. Kohnfelder L and Garg P. The threats to our products, https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx (1999, accessed 2.3.2022 2022).
99. BV. Rules on Cyber Security for the Classification of Marine Units. In: BV, (ed.). *NR 659 DT R00*. Paris, France2018.
100. Boyes H and Isbell R. Code of practice - cyber security for ships. In: Technology TIoEa, (ed.). London, United2017.
101. Flaus J-M. *Cybersecurity of industrial systems*. London, United Kingdom: ISTE Ltd, 2019.
102. IEC 27005 - Information technology - security techniques - Information security risk management.
103. Caprolu M, Di Pietro R, Raponi S, et al. Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Communications Magazine* 2020; 58: 90-96.
104. CISA. CISA - Industrial Control Systems, (2019).
105. IMO. *Revised guidelines for formal safety assessment (FSA) for use in the IMO rule-making process*. 2018 2018. London.
106. Flage R and Aven T. Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability: Theory & Applications* 2009; 4.
107. Goerlandt F and Reniers G. On the assessment of uncertainty in risk diagrams. *Safety Science* 2016; 84: 67-77.

108. Kaplan S and Garrick BJ. On the quantitative definition of risk. *Risk Analysis* 1981; 1: 11-27.
109. Fan C, Montewka J and Zhang D. A risk comparison framework for autonomous ships navigation. *Reliability Engineering & System Safety* 2022; 226: 108709. DOI: https://doi.org/10.1016/j.ress.2022.108709.
110. IMO. *MSC. 1/Circ 1455 Guidelines for the approval of alternatives and equivalents as provided for in various IMO instruments*. 2013 2013. United Kingdom, London.
111. Stamatelatos M, Dezfuli H, Apostolakis G, et al. *Probabilistic risk assessment procedures guide for NASA managers and practitioners*. 2nd ed. Washington DC, USA: NASA Center for AeroSpace Information, 2011.
112. Bolbot V, Theotokatos G, McCloskey J, et al. A methodology to define risk matrices–Application to inland water ways autonomous ships. *International Journal of Naval Architecture and Ocean Engineering* 2022; 14: 100457.
113. Wróbel K, Montewka J and Kujala P. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. *Reliability Engineering & System Safety* 2018; 178: 209-224. DOI: https://doi.org/10.1016/j.ress.2018.05.019.
114. Aven T. The risk concept—historical and recent development trends. *Reliability Engineering & System Safety* 2012; 99: 33-44.
115. ISO. Risk management - Guidelines - ISO 31000. British Standards Institution, 2018.
116. Society for Risk Analysis Glossary.
117. Aven T. A risk and safety science perspective on the precautionary principle. *Safety Science* 2023; 165: 106211.
118. Røyksund M and Engen OA. Making sense of a new risk concept in the Norwegian petroleum regulations. *Safety science* 2020; 124: 104612.
119. Norway PSA. Integrated and unified risk management in the petroleum industry. 2018.
120. Wingrove M. Secure VSAT to prevent cyber attacks, (2020).
121. Adepu S, Kandasamy NK, Zhou J and Mathur A. Attacks on smart grid: Power supply interruption and malicious power generation. *International Journal of Information Security* 2020; 19: 189-211.
122. Bozdal M, Samie M and Jennions I. A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions. In: *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* 2018 2018, pp.201-205. IEEE.
123. Kang TU, Song HM, Jeong S and Kim HK. Automated Reverse Engineering and Attack for CAN Using OBD-II. In: *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)* 2018 2018, pp.1-7. IEEE.
124. Arduinia F, van der Venb C, Lanzratha M and Suhrkea M. The threat of Intentional Electromagnetic Interference to Maritime Vessels. 2022.
125. Shinohara T and Namerikawa T. On the vulnerabilities due to manipulative zero-stealthy attacks in cyber-physical systems. *SICE Journal of Control, Measurement, and System Integration* 2017; 10: 563-570.
126. Oates R, Roberts J and Twomey B. Chains, links and lifetime: Robust security for autonomous maritime systems. *Marine Electrical and Control Systems Safety*. Glasgow, United Kingdom2017.
127. Baugher J and Qu Y. Create the Taxonomy for Unintentional Insider Threat via Text Mining and Hierarchical Clustering Analysis. *European Journal of Electrical Engineering and Computer Science* 2024; 8: 36-49.
128. Elgan M. How do some companies get compromised again and again?, https://securityintelligence.com/articles/how-do-some-companies-get-compromised-again-and-again/ (2023, accessed 2024/5/11 2024).
129. IMO. Safety Of Life At Sea. International Maritime Organisation, 2014.
130. Amro A and Gkioulos V. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security* 2023; 22: 249-288.

131. Yaacoub J-PA, Noura HN, Salman O and Chehab A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security* 2022: 1-44.
132. Akbarzadeh A and Katsikas SK. Dependency-based security risk assessment for cyber-physical systems. *International Journal of Information Security* 2022. DOI: 10.1007/s10207-022-00608-4.
133. Ventikos NP and Louzis K. Developing next generation marine risk analysis for ships: Bio-inspiration for building immunity. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 2023; 237: 405-424.
134. Bolbot V, Theotokatos G, Boulougouris E, et al. A Combinatorial Safety Analysis of Cruise Ship Diesel–Electric Propulsion Plant Blackout. *Safety* 2021; 7. DOI: 10.3390/safety7020038.
135. Rokseth B, Utne IB and Vinnem JE. A systems approach to risk analysis of maritime operations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 2017; 231: 53-68. DOI: doi:10.1177/1748006X16682606.
136. Reliability analysis of three-dimensional shipboard electrical power distribution systems. In: Dubey A, Santoso S, Arapostathis A and Dougal R, (eds.). *2015 IEEE Electric Ship Technologies Symposium (ESTS)*. Washington DC, USA2015.
137. Machiavelli N. *The art of war*. University of Chicago Press, 1521.
138. Bolbot V, Owen D, Chaal M, et al. Investigation of Statutory and Class society Based Requirements for Electronic Lookout. In: *European Conference on Safety and Reliability* 2023.
139. Hollnagel E. *Safety-I and safety-II: the past and future of safety management*. CRC press, 2018.
140. Leveson N. Safety III: A systems approach to safety and resilience. *MIT Eng Syst Lab* 2020; 16: 2021.
141. SAE. *ARP4761 - Guidance and methods for conducting the safety assessment process on civil ariborn systems and equipment*. 1996 1996.
142. EMSA. *Study of the risks and regulatory issues of specific cases of MASS*. 2020 2020.