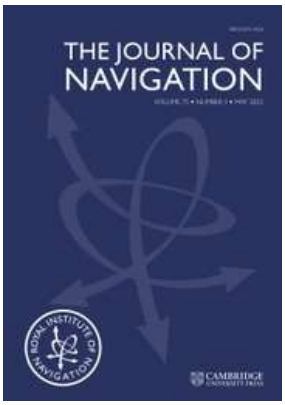
2023-01-31

Cybersecurity risk assessment of VDR

Soner, O

10.1017/s0373463322000595
Journal of Navigation
Cambridge University Press (CUP)



Published as: Söner, Ö, Kayisoglu, G., Bolat, P., & Tam, K. (2023). Cybersecurity risk assessment of VDR. The Journal of Navigation, 1-18. doi:10.1017/S0373463322000595

Ömer Söner *0000-0002-8100-7874*
Gizem Kayisoglu *0000-0003-2730-9780*
Pelin Bolat *0000-0003-4262-3612*
Kimberly Tam *0000-0003-2840-5715*

Acknowledgement. This study is supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) - 2214-A - International Research Fellowship Programme for PhD Students [REF: 53325897-115.02-152823]. This study is also supported by University of Plymouth, Cyber-SHIP Lab.

Cybersecurity risk assessment of VDR.

Ömer Söner*[1], Gizem Kayısoglu[2], Pelin Bolat[3], Kimberly Tam[4]

[1]Department of Maritime Transportation Management Engineering in Maritime Faculty, Van Yuzuncu Yıl University, Van, Turkey.
[2]Department of Maritime Transportation Management Engineering in Maritime Faculty, Istanbul Technical University, Istanbul, Turkey.
[3]Department of Basic Sciences in Maritime Faculty, Istanbul Technical University, Istanbul, Turkey.
[4]School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth, UK.

Abstract

VDR is a data recording system that aimed to provide all navigational, positional, communicational, sensor, control, and command information for data-driven investigation of accidents onboard ships. Due to the increasing dependence on interconnected networks, cybersecurity threats are one of the most severe issues and critical problems when it comes to safeguarding sensitive information and assets. Cyber-security issues are extremely important for the VDR, considering modern VDRs may have internet connections for data transfer, network links to the ship's critical systems, and the capacity to record potentially sensitive data. Thus, this research adopted Failure Modes and Effects Analysis (FMEA) to perform a cybersecurity risk assessment of VDR in order to identify cyber vulnerabilities and specific cyber-attacks that might be launched against the VDR. The findings of the study indicate certain cyber-attacks (false information, command injection, viruses) as well as specific VDR components (DAU, remote access, playback software) that required special attention. Accordingly, preventative and control measures to improve VDR's cybersecurity have been discussed in detail. This research makes a contribution significantly to the improvement of ship safety management systems, particularly in terms of cybersecurity.

Keywords: Maritime, Cyber-security, Risk Assessment, VDR, FMEA.

***Corresponding author: e-mail: soneromer023@gmail.com.

1. Introduction

The voyage data recorder (VDR) is one of the most critical systems onboard ships that aimed to preserve crucial information about a ship to enable a data-driven investigation to identify the cause(s) of ship accidents. Therefore, it is dangerous if access to its data is limited, or it is poorly recorded (OCIMF, 2020). VDR requirements have recently been revised due to new improvements in information and communications technology (ICT). This enables shipowners, operators, and accident investigators. With this amendment, new VDRs have to meet expanded requirements, such as recording data for longer periods of time, as well as providing additional data input sources (IMO, 2012). Moreover, new VDRs may provide remote connectivity to transfer large amounts of data.

Big Data and the Internet of Things (IoT) is being rapidly adopted by the shipping industry to transform many aspects of shipping operations, not only for safety-critical applications and data-driven decision making, but also real-time monitoring and reducing pollution. New VDR regulations may enhance safe navigation and optimization given the large range of ship operating data (Barkow et al., 2011; Danelec, 2021). While the VDR's main purpose is to store information, for compliance with the industry regulations, remote navigational assessments and audits can provide an effective way of navigational safety decision support, rapid analysis following an incident, and lower audit expenses, or, more significantly, increase audit frequency (OCIMF, 2020). Apart from forensic analysis, proactive use of VDR data can substantially reduce the number of accidents reported by the shipping industry (Piccinelli & Gubian, 2013). Since ships' performance optimization requires high-dimensional ship operating data, new VDR data would be particularly beneficial when used to improve ship energy efficiency and environmental performance (Perera & Mo, 2020).

ICT has introduced new advantages for the shipping industry, and also increased the vulnerability of shipboard Information Technology (IT) and Operational Technology (OT) infrastructure to cyberattacks (Heering et al., 2020). As modern ship’s systems connect to shoreside networks through the internet, new points of vulnerability emerge that cyber-attackers might use to get sensitive information, disable essential equipment, steal identities, help in smuggling commodities, and even hijack a ship, its crew, and its cargo (Danelec, 2016; Tam & Jones, 2019). In addition to network security, which can affect a VDR, data protection, and hardware security, cybersecurity is a concern with all of the dangers that an intentional and unintentional cyberthreats may pose to the information systems. Therefore, cybersecurity is of paramount importance for the shipping industry.

Regarding cybersecurity, shipping stakeholders have presented new standards, requirements, resolutions, guidelines, and recommendations to raise awareness of cyber risks and vulnerabilities in the shipping industry. The International Maritime Organization (IMO) has published the guideline on maritime cyber risk management (IMO, 2016), and the American Bureau of Shipping (ABS) has developed standards for marine and offshore cybersecurity (ABS, 2016). Numerous shipping organizations, such as BIMCO, CLIA, and ICS, have collaborated to develop a unique cybersecurity guideline onboard ships to assist in the implementation of a competent cyber risk management plan (BIMCO, 2020).

The number of studies on cybersecurity assessment research is also growing. One main themes is cyber-risk assessment for autonomous ships (Katsikas, 2017; Tam & Jones, 2018; Kim et al., 2020; Zhou et al., 2020; Zhou et al., 2021). Another popular area of research is the security assessment of ship control systems (Babineau et al., 2012; Shang et al., 2019; Svilicic et al., 2019; Kavallieratos & Katsikas, 2020; Bolbot et al., 2020). Complex methodological techniques have been introduced to perform cyber-security analysis (Omitola, 2018; Kavallieratos et al., 2018; Glomsrud & Xie, 2019; Guzman et al., 2019). Similarly, critical ship and port operational technology systems, such as ECDIS (Svilicic et al., 2019a; Svilicic et al., 2019b) and port infrastructure (Papastergiou et al., 2015; Tam et al., 2021; Gunes et al., 2021), have also been investigated. Cybersecurity risk has become a major concern for the shipping industry as a result of recent reported instances (Meland et al., 2021; Heering et al., 2021). Ships' IT and OT systems are particularly vulnerable as they were built with relatively low awareness of cybersecurity (King, 2005). Cyberattacks can have significant outcomes. For example, three fishermen died when the Singaporean ship Prabhu Daya collided with a fishing boat in 2012 (MD, 2022), but when officials boarded the ship, one of the members inserted a USB stick into the VDR, causing all data to be lost. Santamarta (2015) reported that the VDR data files on an Indian cargo ship were overwritten also using a USB stick.

Despite the considerable research and worldwide effort, cyber-attacks in the shipping industry are increasing at an alarming rate. Since modern VDRs may have internet connections for data transfer, network connections to the ship's critical systems (AIS, ECDIS, etc.), and the ability to record potentially sensitive information, cyber-security considerations are crucial (OCIMF, 2020). As the systematic literature review reveals, research that is specifically dedicated to investigating VDR cybersecurity risk is currently lacking. Therefore, it is critical to take the required steps to safeguard VDR from current and emerging cybersecurity threats. To fill this gap, the aim of this study is to apply a quantitative risk assessment to analyse cybersecurity risk, taking into consideration industry expectations, technical changes, and literature shortages, in order to remedy aforementioned gaps. The structure of the study is outlined as follows. The first section deals with the study motivation and a systematic literature review. The second section of this study presents the utilized model. In the next part, the case study is performed. The last section concludes the study and discusses future research.

2. Methodology

Failure modes and effects analysis (FMEA) is a systematic analysis approach that enables to identify, avoid, and remedy potential failure modes, failure causes, failure impacts, and problem areas in a system (Stamatis, 2003). As FMEA is an inductive technique, it has been utilized as a risk assessment tool to identify failure modes and prioritize them for proactive interventions (Liu, 2016). In the 1960s, the aerospace industry introduced FMEA as a formal design technique, and its application area has expanded to other sectors to improve the reliability and safety of goods and processes, designs, and services (Cicek & Celik, 2013; Liu et al., 2015). FMEA cybersecurity risk assessment are viable now as well (Ralston et al., 2007; Haseeb et al., 2021) as it an assess risks associated with cyber components by investigating components, modules, and subsystems to establish failure modes in a system, as well as their causes and implications (Akula & Salehfar, 2021).

Ratings	Occurrence (O)	Possible failure rate
10	Extremely high: failure almost inevitable	≥1 in 2
9	Very high	1 in 3
8	Repeated failures	1 in 8
7	High	1 in 20
6	Moderately high	1 in 80
5	Moderate	1 in 400
4	Relatively low	1 in 2000
3	Low	1 in 15,000
2	Remote	1 in 150,000
1	Nearly impossible	≤1 in 1,500,000

Table 1 Traditional failure mode occurrence ratings.

FMEA is performed in a series of successive steps: (1) each component of the process, system or subsystem is examined to identify potential failure modes (2) probable consequences (failure's effects) of each failure mode are surveyed (3) Occurrence, Severity, and Detection for each identified failure are evaluated. How frequently a certain failure cause is expected to occur is known as the Occurrence (O). The evaluated severity of the failure's impact on the process, system and its surroundings is Severity (S). The probability evaluation of the monitoring system(s) recognizing a cause/mode of failure prior to the component/system being damaged and shut down is referred to as Detection (D) (Pillay & Wang, 2003). According to Liu (2016), the traditional FMEA evaluates the O, S, and D features using a 10-point linguistic scale. The ranking systems for each risk factor shown in Table 1, Table 2, and Table 3 (Liu et al., 2012; Liu, 2016). Thereafter, for each failure mode, a risk priority number (RPN) is calculated to prioritize the failure modes. (Pillay & Wang (2003) defines the RPN, as given by Eq. (1).

$$RPN = O \; x \; S \; x \; D \qquad (1)$$

Ratings	Severity (S)	Severity of Effect
10	Hazardous without warning	Highest severity ranking of a failure mode, occurring without warning and the consequence is hazardous
9	Hazardous with warning	Higher severity ranking of a failure mode, occurring with warning and the consequence is hazardous
8	Very high	Operation of system or product is broken down without compromising safe
7	High	Operation of system or product may be continued, but performance of system or product is affected
6	Moderate	Operation of system or product is continued, and performance of system or product is degraded
5	Low	Performance of system or product is affected seriously, and the maintenance is needed
4	Very low	Performance of system or product is less affected, and themaintenance may not be needed
3	Minor	System performance and satisfaction with minor effect
2	Very minor	System performance and satisfaction with slight effect
1	None	No effect

Table 2: Traditional failure mode severity ratings.

Rating	Detection (D)	Criteria
10	Absolutely impossible	Design control does not detect a potential cause of failure or subsequent failure mode or there is no design control
9	Very remote	Very remote chance the design control will detect a potential cause of the failure or subsequent failure mode
8	Remote	Remote chance the design control will detect a potential cause of failure or subsequent failure mode
7	Very low	Meager chance the design control will detect a potential cause of failure or subsequent failure mode
6	Low	Low chance the design control will detect a potential cause of failure or subsequent failure mode
5	Moderate	Moderate chance the design control will detect a potential cause of failure or subsequent failure mode
4	Moderately high	Moderately high chance the design control will detect a Potential cause of the failure or subsequent failure mode
3	High	High chance the design control will detect a potential cause of failure or subsequent failure mode
2	Very high	Very high chance the design control will detect a potential cause of failure or subsequent failure mode
1	Almost certain	Design control will almost certainly detect a potential cause of failure or subsequent failure mode

Table 3: Traditional failure mode detection ratings.

Failure modes are prioritized to choose effective preventative measures and control plans that may prevent the occurrence or mitigation of potential failures (Cicek & Celik, 2013; Liu, 2016).

3. Application

3.1 Voyage Data Recorder

The VDR is made of many components (see Figure 1) (Gallagher, 2015). These are standard for almost all manufacturers, unless they have additional functionality like remote access.

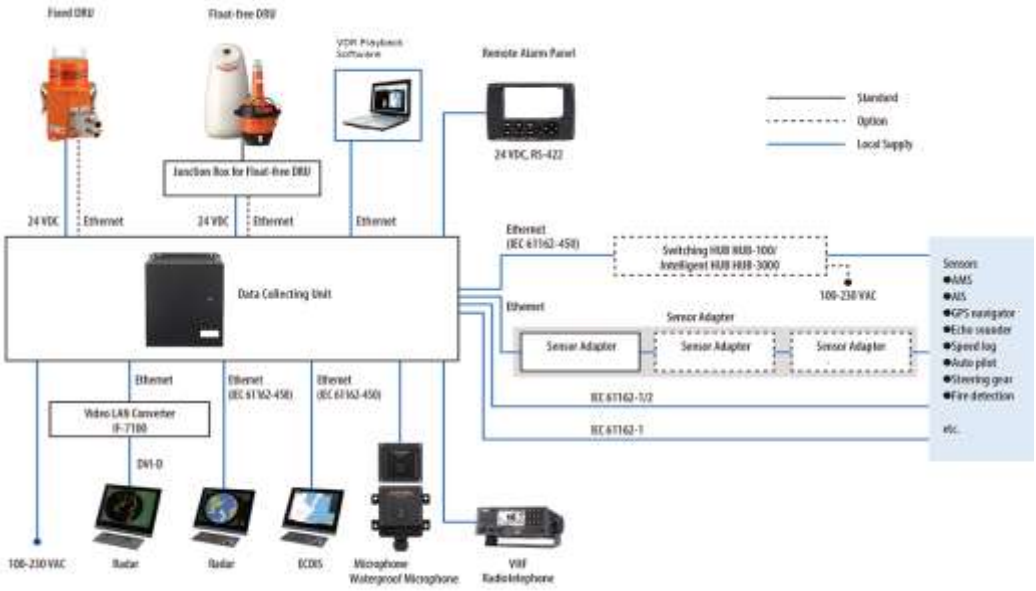


Figure 1. Configuration of VDR onboard (Gallagher, 2015).

These components have many physical and digital interfaces, using internationally recognized format such as Ethernet, USB, FireWire, and IEC 61162 (i.e. Marine radio) to communicate with signal sources, download the stored data and run the data on an external computer (BS EN IEC 61162-1, 1996; BS EN IEC 61162-2, 1999).

3.2 Case Study

The present study aims to uncover VDR cyber vulnerabilities, reveal which particular cyber-attacks it is vulnerable to, and use the robust FMEA risk assessment to rank those risks.

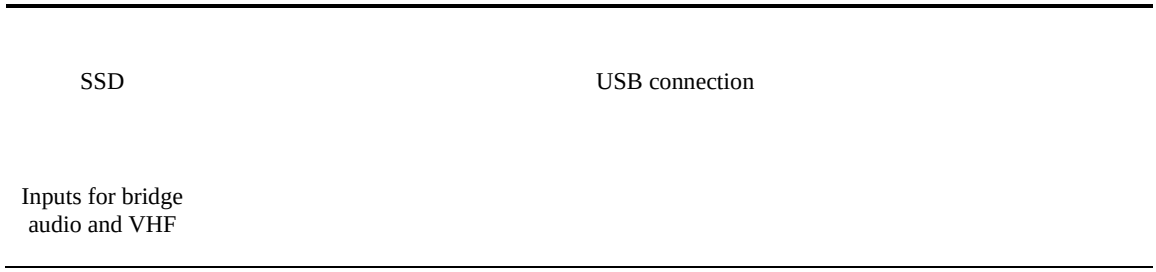
3.2.1 Identification of Cyber Vulnerabilities and Cyber-attacks for VDR

Since experts identify potential failure modes using FMEA methodology, participants with the right experience is essential. It should be noted, however, that reported cyber incidents for VDR are rare. Therefore, the initial data (cyber vulnerabilities and attacks) has been collected from research papers (Jo et al., 2022; Kaleem Awan & Ghamdi, 2019; Silverajan et al., 2018; Tam et al., 2022; Tam & Jones, 2019), accidents/incident reports (Kovacs, 2015; Santamarta, 2015).

According to the VDR components in Figure 1, Data Acquisition /Collection Unit (DAU) has numbers of inputs for serial data (IEC 61162-1, IEC 61162-2), Modbus, network data (IEC 61162-450, and for VHF and bridge audio data. It has also built-in UPS, and about 30 days of recording capacity on SSD. Some of sensors data such as heading, positioning, and speed information are collected directly via the serial NMEA interfaces (standard IEC 61162) into the DAU, other data (e.g. AIS, ECDIS, NAVTEX) are collected via Ethernet into the DAU for the serial NMEA sensors (Svilicic et al., 2019). Protective fixed capsule and float-free capsule have Ethernet (100BASE-TX) and powered from DAU with the Power over Ethernet (PoE). The bridge control panel has interface for operational performance test and powered from USB or DAU PoE. Indoor and outdoor microphones have built-in amplifier, filters, and buzzer for self-test and powered from DAU. VDR playback software (Windows-OS based application), provides real-time monitoring and data replay, extracts data from the VDR through a web browser via Web Extractor tool. The technical infrastructure is summarized in Table 4.

Table 4. The technical specification of VDR components.

DAU	Protective Fixed Capsule	Float-free Capsule	Bridge Control Panel	Bridge Microphone	VDR Playback Software
IEC 61162-1, IEC 61162-2 and Modbus for serial data	Ethernet interface	Ethernet interface	Ethernet interface	Powered from DAU (PoE	Windows based application
IEC 61162-450 for network data	Powered from DAU (PoE)	Powered from DAU (PoE)	Powered from DAU (PoE)		Extract VDR data from (web browser/Web Extractor tool)



The increase of usage of insecure network or serial data protocols (e.g., Modbus) in real-world systems dramatically increases risk. For this paper, this can introduce risks when devices (ECDIS, AIS, RADAR, sensors etc.) send information to VDR. Modbus is an open protocol and that supports RS232/422/485 and Ethernet protocols, allowing communication between industrial devices like Programmable Logic Controllers (PLCs), sensors and meters. Parian et al. (2020) stated that Modbus protocol has no confidentiality and data integrity, leaving it vulnerable to malware and man-in-the middle attacks. Bhatia et al (2014) and Queiroz et al (2009) showed that Modbus protocol has vulnerabilities against flooding-based attacks and Denial of Service (DoS) attacks. Huitsing et al. (2008) defined 20 separate attacks for Modbus Serial such as diagnostic register reset, remote start, and slave reconnaissance. They categorized the impacts of the attacks against Modbus Serial in four group as interception, interruption, fabrication, and modification of target control system assets. The impacts of these attacks are loss of confidentiality, loss of control, and loss of awareness.

The international standard series for application in marine navigation, radio communication and system integration (IEC 61162) can transmit serial and network data in the VDR, while more secure than Modbus, still has vulnerabilities. National Marine Electronics Association (NMEA) 0183 is a standard which supports one-way serial data transmission from a single talker to multiple listeners (NMEA, 2021). Tran et al. (2021) stated that NMEA 0183 does not include any encryption, authentication or validation. Therefore, data transmitted to VDRs (e.g. ship speed, position, depth) in printable ASCII characters (plainstext). Due to this, NMEA 0183 packets are vulnerable to DoS, spoofing and sniffing. Moreover, RS-232 of serial interface family, which supports baud rate 4800 for NMEA 0183 using in the VDR, has vulnerability against buffer overflow attacks (Malviya, 2020). Previous research has shown that NMEA 0183 High Speed is similarly vulnerable 0183 (Amro, 2021) .

NMEA 2000, which came after 0183, is a low-cost, moderate capacity, bi-directional, multi-transmitter/multi-receiver instrument network to interconnect marine electronic devices. It is based on CAN (Controller Area Network). Although this standard is 50 times faster than NMEA 0183, it is not intended to support high-bandwidth applications such as video (NMEA, 2021). NMEA 2000 shares vulnerabilities with its underlying CAN serial bus technology. Malicious code can be executed on sniffed packets in the broadcast and packets can be played back (replay attack), invalidate data, or inject revised traffic (Amro, 2021). The replay attacks can be performed especially on the audio-visual system because of the insecure communication line between the cameras or microphone and receiving systems such as VDR. Data can also be changed via replay attacks. This attack can be performed on a Bridge microphone connected to

a VDR, and is possible because of the lack of confidentiality and integrity security measures on CAN (Silverajan et al., 2018). These attacks, as well as DoS and Trojan Hourses, could potentially reveal confidential data, create malfunctions, force system resets, or even eliminate criminal evidence of industrial espionage and fraud (Kessler, 2021).

Ethernet (IEC 61162-450) is used for maritime systems like GPS, compass, and AIS sensors, to transmit data to the VDR (Hemminghaus, Bauer, & Padilla, 2021). This protocol works based on the UDP/IP-stack and uses IPv4 multicast with individual receiver groups according to the equipment type. On these networks, Person-on-the-side (PotS) and Person-in-the-Middle (PitM) attacks are often possible, meaning an attacker can passively listen, or actively tamper or replay messages (Hemminghaus, Bauer, & Wolsing, 2021). There is only option for authentication, which is the Message Digest 5 (MD5) hash algorithm. However, the key of the MD5 hash can be broken easily (Hemminghaus, Bauer, & Wolsing, 2021).

Web-based tools and software on a VDR can facilitate testing and servicing, retrieving stored data for playback and extracting data for safety and performance purposes. Commonly cyber-attacks used against web-based tool is SQL injection, XML injection, and insecure serialization. Attacks against VDR can use SQL keystroke injection, DDoS, ransomware, virus deployment, reverse shell access, obfuscation SSD corruption through USB drives on an integrated bridge system. Silverajan et al. (2018) also stated that some VDRs have been vulnerable to buffer overflows, flawed firmware update mechanisms, and common injection vulnerabilities. Malicious payloads and harmful code such as ransomware, malware, viruses and spyware, can be introduced with removable media, malicious firmware updates, or a compromised device (e.g. sensor) in the connected system. Santamarta (2015) stated that there are vulnerabilities for the VR-3000 VDR that give attackers unauthorized remote network access to affected devices and execute arbitrary commands with root privileges. In this case, attackers can access, change or delete all recorded information in VDR. According to the VDR firmware update process for VR-3000, an attacker-controlled string could be executed if not properly sanitized. However, as they are not often sanitized, arbitrary commands with root privileges can be executed by remote unauthenticated attackers due to this vulnerability.

3.2.2 FMEA Application and Results

Supplied with the literature data from above, an expert group carried out the key FMEA procedures outlined in Section 2. Initially, potential failure modes are determined by experts based on cyber vulnerabilities derived from available publications. Then, the effects and causes of each failure mode have been defined with the provided literature review. Next, experts consensually assign the occurrence, severity, and detectability ranking for each failure mode by using the scales presented in Table 1, Table 2, and Table 3, respectively. Lastly, Eq. (1) is used for the calculation of the RPN values and all performed actions displayed in Table 5 are referred to as the FMEA analysis worksheet. Four experts in maritime cyber-security participated; one electronic engineer, two computer engineers, and one maritime transportation engineer.

Table 5. FMEA analysis worksheet.

Failed Component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
Data Acquisition Unit	Man in the middle attack	•To be able to bypass IP address authentication •ARP spoofing tool to scan for the IP and MAC addresses of hosts in the target's subnet •Insecure communication protocols	•Eavesdrop or to impersonate one of the parties, gain full visibility any online data exchange, alter the packets, and steal data via IP spoofing, DNS spoofing (for Web-based VDR Connect and RAS), and ARP spoofing (for DAU and fixed and float capsules)	5	6	8	240
Protective Fixed and Float Free Capsules				2	4	10	80
Web-based VDR Connect and Remote Access Solution				5	9	5	225
Data Acquisition Unit	Arbitrary command injection with root privileges	•Insufficient input validation	•Remote access to the database, full control of data such as delete and modify data •Remote access to folders, directories, files etc.	5	10	9	450
Protective Fixed and Float Free Capsules				2	8	10	160
Bridge Control Panel				6	10	7	420
Web-based VDR Connect and Remote Access Solution	SQL injection	•Older functional interfaces and non-validated •input vulnerabilities in a database	•Unauthorized viewing of recorded data, delete, change, destroy of data within database (MySQL)	4	10	6	240
Web-based VDR Connect and Remote Access Solution	Insecure serialization	•Unsafe programming language high level languages such as python c# browser interface code (html java) and deserialization function	•Modifying the serialized object to obtain admin privileges and tamper with the data	10	10	9	900
Web-based VDR Connect and Remote Access Solution	XML external entity injection (XXE)	•A weakly configured XML parser	•Exposure of sensitive data, server-side request forgery (SSRF), or denial of service attacks	7	8	5	280
Data Acquisition Unit	Ransomware	•Clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website •Human factor by bridge control panel via USB stick or internet/Ethernet connection	•Lock the system without damaging any files by using a technique called crypto viral extortion. •Encrypting the victim's files and making them inaccessible	8	10	1	80
Protective Fixed and Float Free Capsules				2	9	3	54
Bridge Microphones				2	2	1	4
Bridge Control Panel				4	8	1	32
Data Acquisition Unit	Backdoor	•Default or weak passwords •Human factor by bridge control panel via USB stick or internet/Ethernet connection	•Record your keyboard input, •copy sensitive information from your drives, •spy on you using your microphone and webcam.	4	9	9	324
Protective Fixed and Float Free Capsules				3	3	8	72
Bridge Microphones				3	5	9	135
Bridge Control Panel				4	7	9	252
Data Acquisition Unit	Viruses	•Clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website •Human factor by bridge control panel via USB stick or internet/Ethernet connection	•Slow computer performance •Erratic computer behavior •Unexplained data loss •Frequent computer crashes •spread from device to device •damage a device or steal data	8	9	4	288
Protective Fixed and Float Free Capsules				5	8	8	320
Bridge Microphones				4	5	8	160
Bridge Control Panel				8	8	4	256
Data Acquisition Unit	Spyware	•Downloading bundle ware, or bundled software packages •Visiting a compromised website or opening a malicious attachment in an email.	•Data Theft and Identity Fraud •Computer Damages	4	7	5	140
Protective Fixed and Float Free Capsules				1	1	8	8
Bridge Microphones				6	7	9	378

Bridge Control Panel		•Human factor by bridge control panel via USB stick or internet/Ethernet connection		3	7	7	147
Data Acquisition Unit	Trojan Horse	•Malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. •Human factor by bridge control panel via USB stick or internet/Ethernet connection	•Deleting data, blocking data, modifying data, copying data •Disrupting the performance of computers or computer networks	4	7	7	196
Protective Fixed and Float Free Capsules				3	10	8	240
Bridge Microphones				2	5	10	100
Bridge Control Panel				5	8	7	280
Data Acquisition Unit	Tampering –Replay attack	•Malwares such as Trojan, ransomware, backdoor •ARP spoofing	•Deleting data, blocking data, modifying data, copying data	2	5	9	90
Protective Fixed and Float Free Capsules				3	10	8	240
Bridge Microphones				1	2	10	20
Bridge Control Panel				2	3	9	54
Data Acquisition Unit	Denial-of-Service (DoS)	•A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users.	•Unusually slow network performance (opening files or accessing websites), •Unavailability of a particular website, or •An inability to access any website.	5	8	1	40
Protective Fixed and Float Free Capsules				1	2	1	2
Bridge Microphones				7	8	3	168
Bridge Control Panel				7	9	1	63
Data Acquisition Unit	Reverse Shell Access	•A remote command execution vulnerability	•Remote access all the system	2	9	10	180
Data Acquisition Unit	Buffer overflows	•A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer	•Cause the execution of malicious code	6	8	9	432
Web-based VDR Connect and Remote Access Solution				7	10	8	560
Data Acquisition Unit	Feed false information into the VDR	•GPS, AIS spoofing, •Attacks to ECDIS, RADAR	•Saving inaccurate data to VDR •Misleading investigators during an accident investigation	6	10	9	540
Protective Fixed and Float Free Capsules				6	10	9	540
Bridge Microphones				2	5	9	90
Bridge Control Panel				6	10	7	420
Web-based VDR Connect and Remote Access Solution				8	10	7	560
Data Acquisition Unit	Attempt to access other ship systems through the connections to the VDR	•An attacker may try to send malware to the other systems by introducing it into the VDR so that it disseminates through the data links to the connected equipment.	•GPS, AIS spoofing, •Attacks to ECDIS, RADAR •Critical ship accidents such as grounding, collision, sinking •Saving inaccurate data to VDR •Misleading investigators during an accident investigation	2	8	10	160
Protective Fixed and Float Free Capsules				1	8	10	80
Bridge Microphones				1	8	9	72
Bridge Control Panel				2	8	10	160

The quantitative findings of FMEA application to cyber risk assessment are highlighted to clarify, prioritize, and develop the essential preventive measures. At this point, special attention should be paid to the RPN values of the cyber-attacks (failure mode) and VDR components (failed components) in order to reveal the significant cyber-attacks and vulnerabilities specifically to the VDR. Thus, the RPN values of cyber-attacks are shown in Figure 2 to highlight the most significant cyber-attacks on the VDR. Accordingly, the top three serious cyber-attacks for VDR are feeding false information, command injection, and viruses.

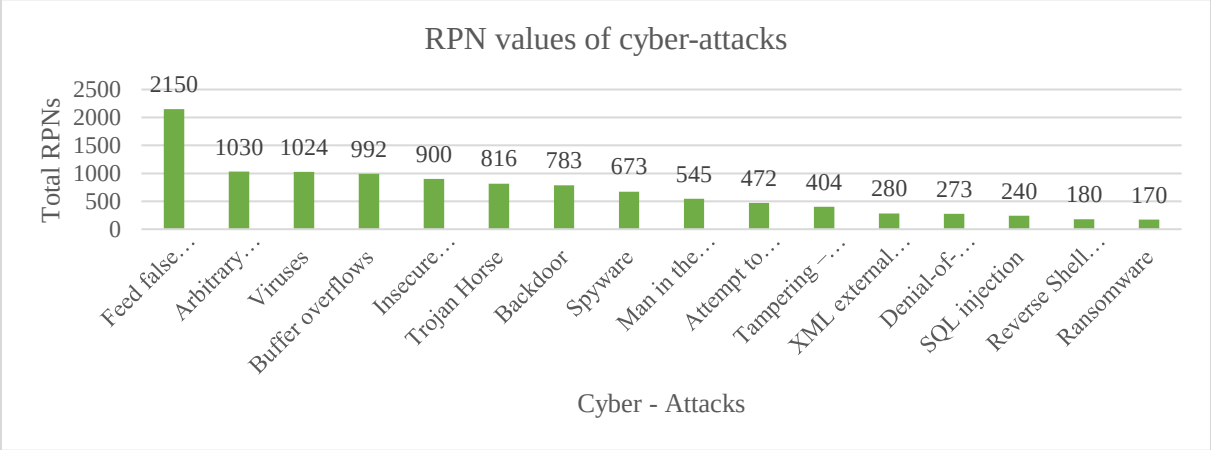


Figure 2. Cyber risk analysis for VDR.

On the other hand, Figure 3 demonstrates the RPN values of VDR components in order to expose the most critical failed components. According to the results, the most vulnerable VDR components are DAU, connect and remote access playback software, and bridge control panel, respectively.

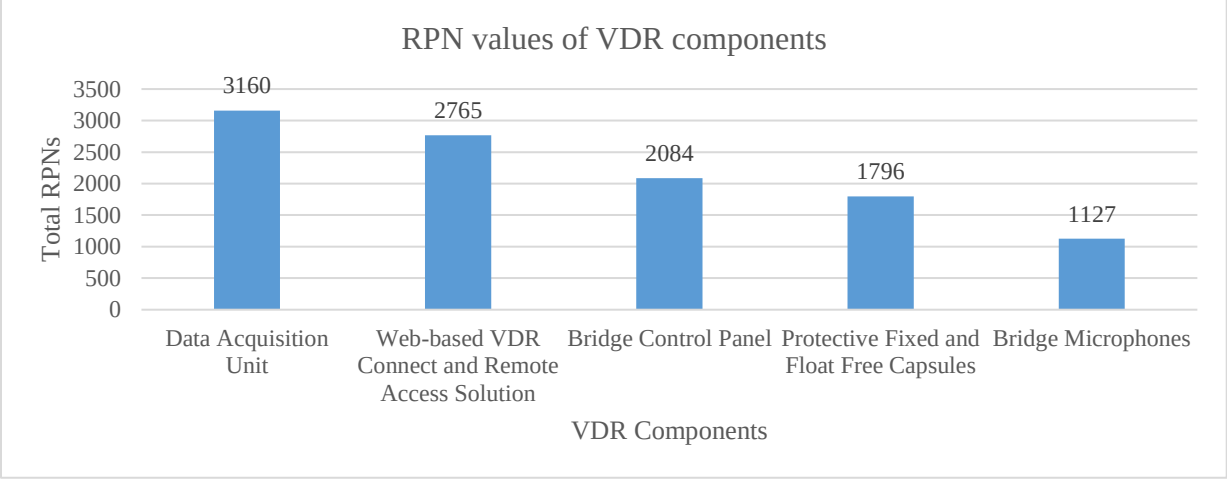


Figure 3. Cyber risk analysis for VDR components.

Beyond that, further in-depth analysis is also possible. For example, investigating cyber-attacks on each component may also assist to develop satisfactory precautions and improving VDR cybersecurity.

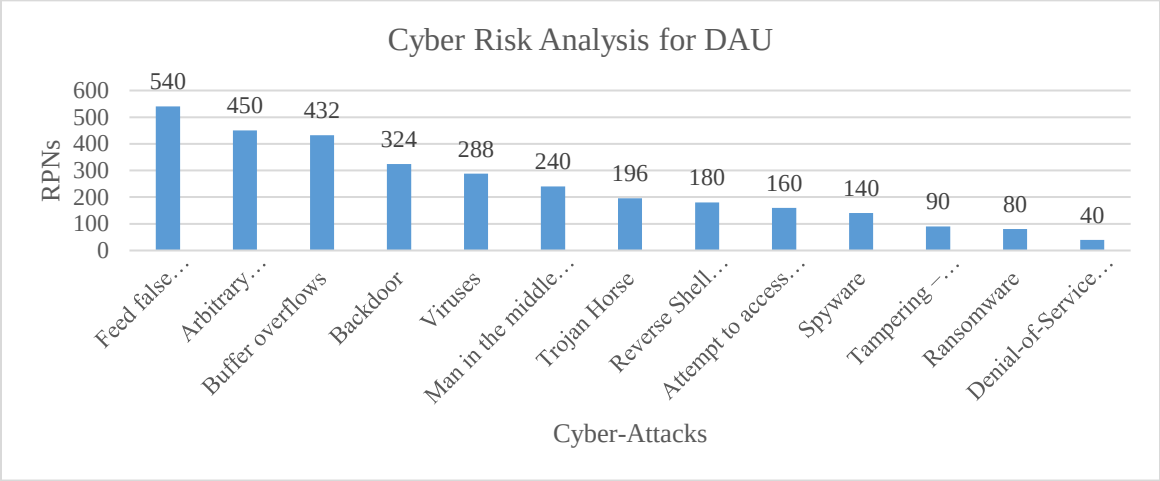


Figure 4. Cyber risk analysis for DAU.

Figure 4 depicts the RPN values of cyber-attacks that are especially relevant to the DAU. Accordingly, the most dangerous attack for DAU is to feed fake information into the VDR with 540 RPN values. Considering the average value of the RPN value of DAU (243), arbitrary command injection with root privileges, buffer overflows, backdoor, and viruses are among other crucial cyber-attacks that jeopardize the cybersecurity of DAU. Control measures for the prioritized failure modes is discussed in detail in the next subsection to clarify the implementation of the FMEA application results in cyber risk assessment on VDR.

3.2.3 Findings and Discussions

According to the overall results, feeding false information into the VDR is the most critical cyber-attacks for VDR, since it is able to carry out for every part of VDR and it has generally high-level occurrence, severity and low-level detectability for all VDR parts. Essentially, it is not directly a specific cyber-attack against VDR, it is indirect attack which caused by cyber-attacks targeted other bridge onboard system. False information can come into the VDR when any cyber-attacks against bridge integrated systems which sends the data to VDR occur such as unauthorized remote access to ECDIS, GPS spoofing, or AIS spoofing. These attacks vary according to the vulnerability of each vessel's own technical infrastructure and may result in the out-of-service of each device, changing the information it contains, and infiltration of other integrated systems. For instance, ECDIS charts and routes can be deleted or modified. If a VDR stores that false data, it would provide false information to accident investigators. Further research of attacks on other systems to feed false information the VDR, and mitigations, is out of scope for this paper.

On the other hand, arbitrary command injection attacks have the second highest RPN. It can be carried out as one of the most critical attacks on the DAU, as one of the medium level risks on the capsules, and as the riskiest attack on the bridge control panel. This arises from the weaknesses of an unprotected system which enables the execution of arbitrary commands.

During arbitrary command injections, an attacker could get full control of the host operating system or the server compromising the software and all its data, which is high impact.

Viruses, which have a relatively high RPN, are also regarded as serious cyber risks. There are several types of malwares that affect the DAU, protective fixed and float free capsules, bridge control panel, and bridge microphones. The riskiest ones are those that can delete and steal VDR data, to flood VDR networks, and slow down the system performance. Spyware, more specifically, is the riskiest for bridge microphone. This could inform the counterparty in the accident. Ways to prevent malware from tampering, stealing, and deleting VDR data is to set up secure backup systems for storage, and more secure networks for data transfers.

In case of buffer overflow attack, attackers can overwrite memory and change the execution path. For this reason, VDRs with remote access have a higher risk against this attack. Although insecure serialization is not risky for VDRs overall, it has the highest RPN value (900) when evaluated separately. Furthermore, it is the riskiest cyber-attacks for Web-based VDR Connect and Remote Access Solution and VDR playback software. If serialization of data goes wrong, information can be lost as objects are deconstructed. Conversely, if deserialization is not secure, unauthorized users can input malicious code, providing an entry point for the attacker, and increasing the attack surface. For instance, if a VDR data is deserialized by a website incorrectly, an attacker could manipulate serialized objects in order to pass harmful data into the VDR software application code. Digital signatures or other integrity control methods can be introduced to prevent this kind of malicious object creation or other data interference. User privileges can also follow least privilege principal.

Although this paper focuses on the attacks that have been ranked with higher-than-average risks using FMEA, it should not be forgotten that attacks below the average risk and but with high-level effects should also be taken into consideration. Furthermore, when the results of this study are evaluated from a different viewpoint, it is seen that the most vulnerable components of VDR is DAU. DAU is considered the most vulnerable components of the VDR, since it has a numerous protocols and standard interfaces for serial and network data, operating system, network and Ethernet connections. It has more integration of information and private industrial control system technologies. Therefore, it has more several vulnerable entrances point for the attackers as well as mentioned-in Section 4.2.1 in comparing with other parts of VDR. Moreover, DAU, which is the main and compulsory component of VDR, is the first and the most important place for collecting the VDR data and the data stay on it for the longest time. For this reason, when any one of the assessed attacks is actualized against DAU, the expected impact of it is also high.

The second more risky component of VDR is VDR connect and remote access solution and VDR playback software. It is a web-based solution and the VDR data playback on the VDR software in a PC in real time. VDR connect and remote access solution that is optional products for VDR onboard provides to transit the data from the VDR via satellite to the home office. In this context, it has information technologies and software functions instead of industrial control system technologies. Since the vulnerabilities for web-based networking or authorized access exist more and attackers are familiar to perform cyber-attacks against information technologies, especially against web-based applications, this part of VDR is resulted as critically risky.

Ranked three for critical risks according to this study is the bridge control panel. This is a console which has an interface with the VDR to carry out VDR operational performance test regularly, shows any kind of VDR system errors with alert functions, has button to stop or start VDR recording, has USB stick entrance, and powered by DAU. The possibilities and detectability of the cyber-attacks against bridge control panel are in the medium level due to the smaller number of entrances point such as having only Ethernet interface with DAU. The cyber-attacks exploited the Ethernet vulnerabilities, leaked from DAU, and caused by human operation on console intentionally or unintentionally can be performed.

The protective fixed and float free capsules and bridge microphones are in the last order in terms of cyber risk assessment for VDR. Because they are more physical equipment instead of being hardware, software, information or control systems. The protective fixed and float free capsules have Ethernet interface with DAU in such as bridge control panel. They are only used for reaching last 48 hours data in case of any accident. Basically, the possibilities cyber-attacks against capsules are less than bridge control panel due to the not having user function excluding Ethernet vulnerabilities and leakage from DAU. Bridge microphones have the least risk according to this study. They do not retain data, therefore, the most severe consequence of the cyber-attacks against bridge microphones can be denial of service, break of the bridge conversation and VHF communication instead of cyber-attacks targeting data.

4. Conclusion

Although great efforts have been made to improve cybersecurity onboard ships IT and OT systems, cyberattacks have yet to be entirely prevented for VDR. However, the effects of intentional or unintentional actions can be reduced by conducting a cyber risk assessment to develop effective control measures that enable safeguarding VDR from current and emerging cybersecurity threats. Therefore, a cybersecurity risk assessment of VDR has been conducted in order to identify failure components, cyber vulnerabilities, and potential cyberattacks to develop feasible measures. At this point, FMEA methodology is utilized since it is recognized as one of the most effective ways for assessing the risk associated with cyber components. According to the FMEA results, a serious level of preventive action is required especially for certain cyber-attacks such as feeding false information, command injection, and viruses and VDR components (DAU, remote access, playback software, etc.). These attacks vary depending on the vulnerabilities of each ship's specific technological architecture and can result in the device being taken out of service, the information it carries being changed, and other interconnected systems being infiltrated. Furthermore, as those attacks may lead the VDR to receive faulty data, which is then recorded in the VDR's body, it gives accident investigators misleading information. In addition, the data acquisition unit is the most critical component in terms of having several interfaces for serial and network data, an Ethernet connection, and collecting all-vital information in its own body for a long time. In this respect, VDR should be designed by taking into consideration especially built-in library functions instead of calling OS commands directly, a white list for inputs to ensure the system allows solely pre-approved inputs, secure Application Programming Interfaces, antivirus, and anti-spam programs in the OS used in DAU, principles of least privilege and network segmentation for all components of VDR, and network traffic monitoring connected to VDR. Given that these cyber-attacks against

VDR have impacted a large number of shareholders in the shipping industry (shipowners/operators, accident investigators, P&I Clubs, etc.) minimizing the cyber vulnerability and preventing the risk of cyber-attacks is crucial. Thus, preventive and control measures have been considered to improve the cybersecurity of VDR. Consequently, this study makes valuable contributions to improving ships' safety management systems, especially from a cybersecurity perspective through proposing mitigation, and recovery in the case of the identified attacks, and determining vulnerable components of the VDR.

Acknowledgement

This study is partially funded by The Scientific and Technological Research Council of Turkey (TÜBİTAK) - 2214-A - International Research Fellowship Programme for PhD Students [REF: 53325897-115.02-152823].

This study is also supported by University of Plymouth, Cyber-SHIP Lab.

Also, the authors would like to thank the experts for their assessment, comments, and efforts towards improving our manuscript.

References

Adams, P. (2021). *5 Things How VDR software prevent corporate data from cyberattacks*. MEGASIGNAL. https://megasignal.org/5-things-how-vdr-software-prevent-corporate-data-from-cyberattacks

Amro, A. (2021). Cyber-Physical Tracking of IoT devices : A maritime use case. *In Norsk IKT-Konferanse for Forskning Og Utdanning*, *3*.

Bhatia, S., Kush, N., Djamaludin, C., Akande, J., & Foo, E. (2014). Practical Modbus flooding attack and detection. *Conferences in Research and Practice in Information Technology Series*, *149*, 57–65.

Danelec. (2021). *DM100 VDR, Voyage Data Recorder*. VDR Manufacturer Brochure. https://denmark.xcontain.com/company/danelec-electronics-a-s/

Danelec Systems. (2016). *White Paper on Vdr Cybersecurity*.

Gallagher, S. (2015). *Hacked at sea: Researchers find ships' data recorders vulnerable to attack*. ArsTECHNICA. https://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/

Halfond, W. G. J., Viegas, J., & Orso, A. (2008). A Classification of SQL Injection Attacks and Countermeasures. *Preventing Sql Code Injection By Combining Static and Runtime Analysis*, 53.

Hemminghaus, C., Bauer, J., & Padilla, E. (2021). BRAT: A BRidge Attack Tool for Cybersecurity Assessments of Maritime Systems. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(1), 35–44. https://doi.org/10.12716/1001.15.01.02

Hemminghaus, C., Bauer, J., & Wolsing, K. (2021). SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures. *2021 International*

Symposium on Networks, Computers and Communications (ISNCC), 1–6. https://doi.org/10.1109/ISNCC52172.2021.9615738

Huitsing, P., Chandia, R., Papa, M., & Shenoi, S. (2008). Attack taxonomies for the Modbus protocols. *International Journal of Critical Infrastructure Protection*, *1*(C), 37–44. https://doi.org/10.1016/j.ijcip.2008.08.003

IMO. (2012). *ADOPTION OF REVISED PERFORMANCE STANDARDS FOR SHIPBORNE VOYAGE DATA RECORDERS (VDRs). IMO Resolution MSC 333(90)*.

IMO. (2017a). Guidelines on Cyber Risk Mangement. *Imo*, *MSC-FAL*(1/Circ.3), 1–6.

IMO. (2017b). *IMO Resolution MSC.428 (98)*. *428*(June 2017), 2017.

IMO. (2021). *IMO 2021 Cybersecurity Compliance for Maritime*. Information Center for the New IMO 2021 Regulation. https://imo-2021.com/imo2021

Imperva. (2022). *Command Injection*. https://www.imperva.com/learn/application-security/command-injection/

Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors*, *22*(5), 1860. https://doi.org/10.3390/s22051860

Kaleem Awan, M. S., & Ghamdi, M. A. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering*, *7*(10). https://doi.org/10.3390/jmse7100350

Kessler, G. C. (2021). The can bus in the maritime environment – technical overview and cybersecurity vulnerabilities. *TransNav*, *15*(3), 531–540. https://doi.org/10.12716/1001.15.03.05

Kovacs, E. (2015). *Ship Data Recorders Vulnerable to Hacker Attacks*. SecurityWeek. https://www.securityweek.com/ship-data-recorders-vulnerable-hacker-attacks

Kumar, A., Poonia, M. P., Pandel, U., & Jethoo, a. S. (2011). FMEA : Methodology , Design and Implementation in a Foundry. *International Journal of Engineering Science and Technology*, *3*(6), 5288–5297.

Malviya, N. (2020). *RS-232 and RS-485*. Infosec. https://resources.infosecinstitute.com/topic/rs-232-and-rs-485/

National Cybersecurity Centre. (2020). *Cyber Essentials: Requirements for IT Infrastructure*. *August*, 1–12.

NIST Cybersecurity Framework Team. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium*, *535*, 9–25.

NMEA. (2021). *NMEA Standards*. National Marine Electronics Association. https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard

Northrop Grumman. (2007). *A Practical Guide to Marine Voyage Data Recorders for Newbuilds and Retrofits*. Sperry Marine. https://www.yumpu.com/en/document/read/3454792/a-practical-guide-to-marine-voyage-data-recorders-for-newbuilds-

NTT. (2022). *OS Command Injection*. NTT Application Security. https://www.whitehatsec.com/glossary/content/os-command-injection

Parian, C., Guldimann, T., & Bhatia, S. (2020). Fooling the Master: Exploiting Weaknesses in the Modbus Protocol. *Procedia Computer Science*, *171*(2019), 2453–2458.

https://doi.org/10.1016/j.procs.2020.04.265

Queiroz, C., Mahmood, A., Hu, J., Tari, Z., & Yu, X. (2009). Building a SCADA security testbed. *NSS 2009 - Network and System Security*, 357–364. https://doi.org/10.1109/NSS.2009.82

Santamarta, R. (2015). *Maritime security: Hacking into a voyage data recorder (VDR).*

Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity Attacks and Defences for Unmanned Smart Ships. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, IThings/Gree*, 15–20. https://doi.org/10.1109/Cybermatics_2018.2018.00037

Svilicic, B., Rudan, I., Frančić, V., & Doričić, M. (2019). Shipboard ECDIS cybersecurity: Third-party component threats. *Pomorstvo*, *33*(2), 176–180. https://doi.org/10.31217/p.33.2.7

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., Giménez, P., Crichton, T., & Jones, K. (2022). Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. *Journal of Transportation Technologies*, *12*(01), 1–27. https://doi.org/10.4236/jtts.2022.121001

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

Tran, K., Keene, S., Fretheim, E., & Tsikerdekis, M. (2021). Marine Network Protocols and Security Risks. *Journal of Cybersecurity and Privacy*, *1*(2), 239–251. https://doi.org/10.3390/jcp1020013

Liu, H. C. (2016). FMEA using uncertainty theories and MCDM methods. In FMEA using uncertainty theories and MCDM methods. Springer, Singapore.

Scipioni, A., Saccarola, G., Centazzo, A., & Arena, F. (2002). FMEA methodology design, implementation and integration with HACCP system in a food company. Food control, 13(8), 495-501.

Cicek, K., & Celik, M. (2013). Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship. Safety science, 51(1), 6-10.

Liu, H. C., You, J. X., Ding, X. F., & Su, Q. (2015). Improving risk evaluation in FMEA with a hybrid multiple criteria decision-making method. International Journal of Quality & Reliability Management.

Akula, S. K., & Salehfar, H. (2021, November). Risk-based Classical Failure Mode and Effect Analysis (FMEA) of Microgrid Cyber-physical Energy Systems. In 2021 North American Power Symposium (NAPS) (pp. 1-6). IEEE.

Pillay, A., & Wang, J. (2003). Modified failure mode and effects analysis using approximate reasoning. Reliability Engineering & System Safety, 79(1), 69-85.

Liu, H. C. (2016). FMEA using uncertainty theories and MCDM methods. In FMEA using uncertainty theories and MCDM methods (pp. 13-27). Springer, Singapore.

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cybersecurity risk assessment for SCADA and DCS networks. ISA transactions, 46(4), 583-594.

Haseeb, J., Mansoori, M., & Welch, I. (2021, October). Failure Modes and Effects Analysis

(FMEA) of Honeypot-Based Cybersecurity Experiment for IoT. In 2021 IEEE 46th Conference on Local Computer Networks (LCN) (pp. 645-648). IEEE.

Stamatis, D. H. (2003). Failure mode and effect analysis: FMEA from theory to execution. Quality Press.

Liu, H. C. (2016). FMEA using uncertainty theories and MCDM methods. In FMEA using uncertainty theories and MCDM methods. Springer, Singapore.

Scipioni, A., Saccarola, G., Centazzo, A., & Arena, F. (2002). FMEA methodology design, implementation and integration with HACCP system in a food company. Food control, 13(8), 495-501.

Cicek, K., & Celik, M. (2013). Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship. Safety science, 51(1), 6-10.

Liu, H. C., You, J. X., Ding, X. F., & Su, Q. (2015). Improving risk evaluation in FMEA with a hybrid multiple criteria decision-making method. International Journal of Quality & Reliability Management.

Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships. In 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity) (pp. 1-8). IEEE.

Katsikas, S. K. (2017, April). Cybersecurity of the autonomous ship. In Proceedings of the 3rd ACM workshop on cyber-physical system security (pp. 55-56).

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2018). Cyber-attacks against the autonomous ship. In Computer security (pp. 20-36). Springer, Cham.

Kim, M., Joung, T. H., Jeong, B., & Park, H. S. (2020). Autonomous shipping and its impact on regulations, technologies, and industries. Journal of International Maritime Safety, Environmental Affairs, and Shipping, 4(2), 17-25.

Zhou, X. Y., Liu, Z. J., Wang, F. W., Wu, Z. L., & Cui, R. D. (2020). Towards applicability evaluation of hazard analysis methods for autonomous ships. Ocean Engineering, 214, 107773.

Zhou, X. Y., Liu, Z. J., Wang, F. W., & Wu, Z. L. (2021). A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Engineering, 222, 108569.

Shang, W., Gong, T., Chen, C., Hou, J., & Zeng, P. (2019). Information security risk assessment method for ship control system based on fuzzy sets and attack trees. Security and Communication Networks, 2019.

Kavallieratos, G., & Katsikas, S. (2020). Managing cybersecurity risks of the cyber-enabled ship. Journal of Marine Science and Engineering, 8(10), 768.

Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime cyber risk management: An experimental ship assessment. The Journal of Navigation, 72(5), 1108-1120.

Babineau, G. L., Jones, R. A., & Horowitz, B. (2012, November). A system-aware cybersecurity method for shipboard control systems with a method described to evaluate cybersecurity solutions. In 2012 IEEE Conference on Technologies for Homeland Security (HST) (pp. 99-104). IEEE.

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. Safety Science, 131, 104908.

Omitola, T., Downes, J., Wills, G., Zwolinski, M., & Butler, M. (2018). Securing navigation of unmanned maritime systems. Proceedings of the International Robotic Sailing Conference

2018, Southampton, United Kingdom, 31-08-2018.

Guzman, N. C., Kufoalor, D. K. M., Kozine, I., & Lundteigen, M. A. (2019, September). Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel. In Proceedings of the 29th European Safety and Reliability Conference, Lower Saxony, Germany (pp. 22-26).

Glomsrud, J. A., & Xie, J. (2019, September). A structured STPA safety and security co-analysis framework for autonomous ships. In European Safety and Reliability conference, Germany, Hannover.

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019-a). Assessing ship cyber risks: A framework and case study of ECDIS security. WMU Journal of Maritime Affairs, 18(3), 509-520.

Svilicic, B., Rudan, I., Frančić, V., & Doričić, M. (2019-b). Shipboard ECDIS cybersecurity: Third-party component threats. Pomorstvo, 33(2), 176-180.

Tam, K., Moara-Nkwe, K., & Jones, K. (2021). A Conceptual Cyber-Risk Assessment of Port Infastructure. 2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs. 28-29 January 2021, Virtual Conference, Parede, Portugal.

Papastergiou, S., Polemi, N., & Karantjias, A. (2015, August). CYSM: an innovative physical/cybersecurity management system for ports. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 219-230). Springer, Cham.

King, J. (2005). The security of merchant shipping. Marine Policy, 29(3), 235-245.

Santamarta, R. (2015). Maritime security: Hacking into a voyage data recorder (VDR). IOActive.

Heering, D., Maennel, O. M., & Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. In Developments in Maritime Technology and Engineering (pp. 49-61). CRC Press.

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cybersecurity incidents. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.

Liu, H. C., Liu, L., Liu, N., & Mao, L. X. (2012). Risk evaluation in failure mode and effects analysis with extended VIKOR method under fuzzy environment. Expert Systems with Applications, 39(17), 12926-12934.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cybersecurity risk assessment for seaports: A case study of a container port. Computers & Security, 103, 102196.