Cybersecurity Risk Assessment: the Ship Maintenance Databases' Case Study

Suzana LAMPREIA, Victor LOBO, and Valter VAIRINHOS

Abstract—**Nowadays, to reduce the crew, ships are being automated with complex systems. This fact has the objective of minimizing navigation costs, risks, and pollution. On-board equipment and systems operation is usually monitored and controlled using both on-board and shore management software. This may lead to an unsafe situation, from a cybersecurity point of view. A cyberattack aiming at the control and monitoring systems can put the crew and ship in danger. The objective of this paper is to make a cyber-attack risk evaluation matrix, considering maintenance data from a diesel engine propulsion system of a Portuguese Navy frigate and its implemented maintenance system. By defining these matrixes, the risk of a cyberattack to selected equipments are evaluated. To obtain that matrix, the occurrence probability, the impact, and the level of exposure to unsafe internal and external interventions were considered. From this matrix, the impact significance is computed. These article starts with an introduction of cybersecurity, then it is presented a cybersecurity state of art considering maritime environment, and the maintenance management system implemented in the Portuguese Navy, then the risk matrix is developed, applied, and finally there are presented the conclusions about the results of the research work.**

Index Terms—**Cybersecurity, Ship, Maintenance, Database.**

I. Introduction

At present, whether for information and people management, systems and equipment, everything is networked. Working in a network and through digital systems has gone from the need to modernize, automate and optimize work, share information, and increase security to an imposition that no state can ignore. When we talk about network and information systems connections, we are also talking about physical security and confidentiality of some data. While network systems have brought improvements in work and security, they have also given rise to a certain ease in accessing data from different geographical locations and by people outside the process. All this development, availability, and accessibility of information has brought a new reality for systems security and risk, which is why a new area called Cybersecurity was developed.

Cybersecurity is an important area of research, as can be seen by the very large number of scientific papers that have been published recently (see Fig. 1). Searching for the keyword Cybersecurity (C) in Google Scholar, approximately 397k papers are obtained. Focusing on the theme of present paper, approximately 5k papers under Cybersecurity in "Military Systems" (CMS), 32k under Cybersecurity in Industrial "Maintenance" (CIM), 19k under Cybersecurity in the Context of Maintenance "Data Management" (CCMDM), and 256 Cybersecurity in the Context of Maintenance in "Military Ships" (CCMMS) were obtained. As we can see, even though cybersecurity in the context of maintenance of military ships is a very small part of the overall scientific production in cybersecurity, it is still very relevant.

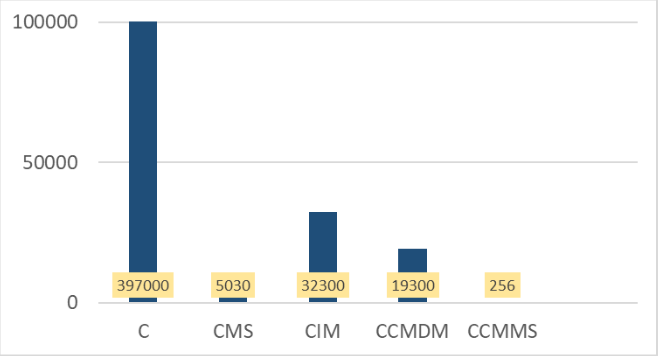


Figure 1. Histogram of the number of papers found in Google Scholar (19/10/2022)

Our interest in this area stems from the increasing automation of the maintenance process and thus greater exposure of navy ship's maintenance systems to cyberattacks.

The motivations for cyber-attacks can be various, such as espionage, organized crime, environmental or other activists, pure "pleasure" hacking. Cyber-attacks can also be due to cyber misuse, including unintentional vandalism, unauthorized access to cyber systems, terrorism, and warfare. The actors in these scenarios may be commercial competitors, members of the ship's crew, cybercriminals, terrorists, or even nation states. These threats and actors may be in direct contact with the ship, or via remote systems [1].

Modern information and control systems, such as the Electronic Chart Display and Information System (ECDIS) used by most ships, expose them to cyber risks [2] identified using risk analysis, since "*ECDIS is critically vulnerable to weaknesses raising from ECDIS backup arrangement and underlying operating system updating and secure setup*." However, not updating the system also represents a risk, since the update may solve known problems with the system. Since most navigation planning (and now even some of its control) is done using the ECDIS, changing the information on that system, or denying its use, can

This work is supported by Portuguese Naval Academy and CINAV and acknowledged for the collaboration of the Instituto Universitário Militar (IUM) from Portugal.

S. LAMPREIA is with the CINAV – Centro de Investigacao Naval, Portuguese Naval Academy, 2810-001 Almada, Portugal (e-mail: suzana.paula.lampreia@marinha.pt).

V. LOBO is with the is with the CINAV – Centro de Investigacao Naval, Portuguese Naval Academy, 2810-001 Almada, Portugal.

V. VAIRINHOS is with the is with the CINAV – Centro de Investigacao Naval, Portuguese Naval Academy, 2810-001 Almada, Portugal.

Digital Object Identifier 10.32754/JMT.2022.2.08

jeopardize the whole ship.

Most modern ships have control and management systems that control most machinery, damage control systems, and, in the case of warships, weapons control systems their weapon systems. Tampering with these systems can lead to potentially catastrophic results, ranging from unintentional stopping or accelerating the engines, rudder blocking, flooding of compartments, etc.

Some modern ships are also introducing integrated maintenance management systems that continuously assess ships´ health, help plan, and execute maintenance actions. Tampering with these systems, as we shall see later, can lead to unnecessary maintenance actions (with increased costs and unavailability of the system) or breakdowns due to lack of maintenance.

Ships, seen as industrial facilities capable of navigating, are complex systems where machinery and humans coexist and interact. Ships have sensors for navigation systems, platform systems, safety systems, cargo systems, crew access systems, and crew management systems. If these assets are damaged or endured a cyber-attack, this may negatively, affect crew health and safety, on the ship operation, on the safety of other ships and maritime structures, and deteriorate ship performance in terms of speed and efficiency [1].

Although it was not the result of a Cyber-attack, the recently stranded ship in the Suez Canal (in March 2021) illustrates the consequences of a ship navigation and control system breakdown. In this case, without person injured, but this accident led to economic loss.

II. Cybersecurity in a Maritime Context

A. *When Data Management of Equipment onboard Ships*

As the number of sensors and automatic systems increases, the vast amount of data available on-board becomes a problem and gives rise to what is known as a "big data" environment. This is a challenge for data management systems and the data managers [3,4]. This data is an opportunity to enhance systems performance, but also an opportunity for cyber-attacks.

Enterprises are now implementing Information Security Management Systems (ISMS) and one main objective is "managing and controlling cyber security risks and ensuring continuous improvement" [5]. To implement and maintain these systems, it is necessary to plan by company policies and rules implemented for cyber security [5], mainly because, whenever the ship is navigating or when it docks and uses port facilities, it must be possible to connect it to some global network. Therefore, both ships and ports must follow international cyber-safe rules and protocols.

Csorna & Carvalho (2017) Also referred that the first procedure to obtain a cyber-secure control system is to follow ensure that the secure systems and personnel´s who operate it, work, and act according to international standards [6].

Other threats to cyber security are ship crews and port personnel´s lack of training in remote control and command systems and their resistance to change, boycotting ships and ports adaptation to new management systems and software. This may represent a greater threat, or even security negligence, than a declared attack with criminal intent.

The access to ships information systems must be tightly monitored, and measures such as two-stage authentications should be used, as happens in areas such as banking where it is a common procedure [7]. However, since in a maritime environment, the mobile phone access used in banking may not be possible, other forms of second-stage authentication should be used.

B. *Cybersecurity risk assessment in ships*

With the objective of reducing the crew, many automated systems for command and control have been implemented on-board ships. Nowadays these systems include "health" monitoring and/or risk management equipment, which collect their data. Using remote control on these automated systems is a cyber-vulnerability, and so cyber-safe software structures have been developed, and implemented [8].

Ports can also represent a risk for ships and vice-versa. As an example, can be the study conducted by European Network and Information Security Agency (ENISA) that identified fragilities in cybersecurity in ports. Ahokas *et al* [9]. This reference presents a simplified scheme for the concepts related to cybersecurity in ports that can guide the design of a cyber-safety program based on risk, considering cyber-threat, cyberattack, system vulnerability that should be secured, and the inherent cyberspace.

Many different approaches can be made for assessing cyber risks aboard ships.

Mednikarov *et al* (2020) describe 3 main steps for the "Ship´s Cyber Risk assessment Process" [10]:

- ✓ Preliminary risk assessment.
- ✓ Ship cybersecurity assessment.
- ✓ Review, assessment, and report on the potential impact of ship cyber vulnerability.

In the first step, a compilation of the control systems, equipment and their functions, networks, and their vulnerability to cyberattacks should be made.

In the second step, beyond the systems and equipment compiled in the first step, crew education and training should also be considered. To improve the ship's cybersecurity, it is important to monitor crew network access to the system [10].

In the third step, the effect of cyberattacks on the whole ship is assessed. To prevent potential cybersecurity impacts and consequently eventual damage to the ship, risk analysis is based on the whole ship information.

The International Maritime Organization (IMO) has already issued guidelines on Maritime Cyber Risk Management) (MSC-FAL.1-Circ.3) [11]. The cybersecurity tasks can be procedure specification, risks identification and assessment, and responses to mitigate the identified risks [12]. In addition, a consortium of maritime organizations recommends a similar approach, and regularly publishes some guidelines for cybersecurity on-board ships [13].

According to its 2020 guidelines, cyber risk management has a few more steps, since it should identify threats and vulnerabilities, assess risk exposure, develop protection and detection measures, establish contingency plans, respond to, and recover from cyber security incidents. Its principles also state that those enterprises should not include sensitive information in their safety management systems (SMS) [13].

Digital Object Identifier 10.32754/JMT.2022.2.08

In 2020, Bolbot et al published an important methodology for cyber risk assessment considering fundamental entry points and attack types. In that work, four levels for the method are defined [14]:

a. Preparation for analysis, considering the system analysis and review, the selection of attack group, and the identification of system components vulnerabilities.
b. Scenario's characterization, identifying potential attacks and consequences.
c. Scenarios ranking, estimating the scenario's likelihoods and the ranking consequences.
d. The system enhancement and requirements with the identification of control obstacles, new scenarios for eventual risk assessment, and, finally, the generation of recommendations.

CCS (2018) presented a discussion of the risk management process used by ISO 31000 [12], which is also used by [13]. To define a risk assessment system, first, we should define the context, then identify the risk, perform risk analysis and evaluation, and then, perform risk management and continuously monitor and review risks, communicating any findings to all those involved.

To characterize the risk of cyber-attacks occurring on a ship, there are conceptual scales of risk measurement that involve probability, frequency, impact, and exposure level [13]. These scales should be adapted to each case, based on involved organizations, or means contexts. In the case study presented in this paper, modified scales will be considered.

It is possible to develop a cyber security model considering the associated risks to cyber management both on ports and ships [15,16].

It is believed that the application of cyber-risk analysis to evaluate the risk assessment to maintenance databases will support a cyber-safe model built for the organization under study.

III. Maintenance Management in the Portuguese Navy

In 1984, Marinha had published in an official book that: "The main objective of naval assets maintenance is to ensure levels of material availability, compatible with established operational programs, using available logistical resources or those that can be acquired at acceptable costs." [18] To accomplish this aim, several publications regulate the operation of ship maintenance in the Portuguese Navy. In addition, it is imperative to apply a supported decision-making online network system for ships equipment and systems maintenance.

It is believed that an online statistical monitoring scheme of equipment and systems operating parameters, using the necessary data, can contribute to a correct and reliable diagnosis of the true machine state.

Maintenance in the Portuguese Navy is a three stages process. The first stage is carried out by the ship's crew, the second stage is carried out by a shore-based technical support workshop hierarchically under the Naval Command (CN - *Comando Naval*, with ships Operational Command) and the third stage, is under the responsibility of the Navy Technical Directorate (DN - *Direção de Navios*). DN makes a deep technical study of the needed maintenance, specifies what work should be done, and if it will be carried out by the Navy's shipyard or by another company.

The maintenance data management system implemented for surface ships is called Data Collection and Treatment System (in Portuguese: "*Sistema de Recolha e Tratamento de Dados*" (SRTD)) [19]. Helicopters and submarines have specific maintenance management systems. This raises some problems, namely for the financial management, existing widespread agreement that a single global system should be used. In this paper, the focus is on surface ships.

SRTD is a Portuguese Navy Maintenance Management System (SGM - Sistema de Gestão da Manutenção) component. The other component subsystem is the Planned Maintenance System (SMP – Sistema de Manutenção Planeada), which specifies all maintenance procedures, together with the tools, components, and specialized technicians needed for each procedure. SMP even specifies "registering cards" for equipment and system condition control [18]. In this paper, we will not study the cyber threats to the whole SMP.

The SGM in turn is part of the Portuguese Navy logistic system [18], and it was inspired in the USA Navy 3M System [19].

In addition, the 92/2019 Council of Ministers Resolution defines the National Cyberspace Security Strategies [20], so it is in the National interest that risk assessment of the Portuguese Navy maintenance database may be imperative and developed to guarantee safe data storage and management.

A. *The database structure for surface ships*

The SRTD guarantees the collection of historical and operational information on maintenance, namely the record of interventions occurrences (preventive, corrective, or of any other nature), the description of the work carried out (what, who, where) what spare parts, and other materials were spent and eventually costs. The objective is to allow a data-driven formulation of maintenance policies, the evaluation of the policies in force and its alteration when necessary [21].

However, the available software shows serious shortcomings when the time arrives to transform this data into useful information for reliability, logistic, and maintenance support decision policies at CN, SM, and EMA. Supply Direction (DA – Direção de Abastecimento), responsible for spare parts and fluid supply is linked by servers to SRTD. For small ships, there is a specific technical solution.

Maintenance needs are identified, reported and its evaluation and execution are requested to the administrative command (ENS – Esquadrilha de Navios de Superfície[1]) by the ship, through SICALN[2]. ENS is responsible for processing the request forwarding it to the 2nd stage workshop or sending it to the 3rd stage (DN).

Arsenal do Alfeite SA (AA) is the Portuguese Navy shipyard charged by law with the execution of ship third stage maintenance, unless it cannot execute or schedule it. Currently, a restructuring is underway at AA, which will produce some changes in these procedures and links, namely software.

[1] ENS - Surface Ship Squadron (SSS)

[2] SICALN - an ORACLE language software, which represents the Navy Logistic Integrated System software for the area of maintenance

Digital Object Identifier 10.32754/JMT.2022.2.08

SRTD uses SICALN oracle software, for interface human/computer. The servers of the SRTD are not in DN. This system feed the Integrated Logistic System (SLI - *Sistema Logístico Integrado*), which is connected to DN. The DN is the organism responsible for SICALN software management. The SLI is also connected to Armed General Staff (EMA - *Estado Maior da Armada*), other Material Superintendence (SM - *Superintendência do Material*) organs and the CN. These organisms should have the maintenance information available and statistically treated to support ship operations decisions, but this type of system is not, yet implemented, but are under study.

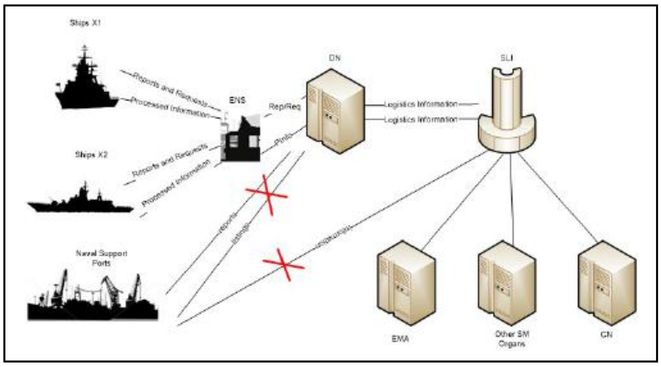


Figure 2. Modified SRTD model

Fig. 2 is an adaptation of an image present on [18], modified to correspond to current practice.

The connections between ships, ENS, DN, and SICALN, are supported by three forms: DSM58 (in these form there are several maintenance codes that identify the anomaly type, and also there is a text space where the ships report or request maintenance support), DSM59 (ship monthly report covering equipment working hours, oil and fuel consumption, and the selected equipment's state), and DSM60 (used by technical services or departments on-board to request or document on-board spare parts consumption in maintenance interventions) [18], the DSM60 is connected to the DSM58 form. These three documents - its digital images - are visualized and validated by the ENS and DN.

Experience and new realities suggest the need for a reconfigured and full-integrated SICALN database, making data, information, and knowledge resulting from analytics, dynamically available to all involved, both technical and operational organizations.

Although an integrated logistic system enhances the decision-making process, it brings other cyber security concerns and challenges; hopefully, the risks associated with eventual network attacks will be minimized or mitigated with proper cyber safety.

IV. Case Study – Maintenance Databases Risk Analysis

A. Factors that can influence the cybersecurity in Maintenance System

For the implemented system, factors and risks are stable and not increased because there are few connections among the involved organization.

The effects of networking on various organizations will lead to monitoring, risk analysis, control, and network blocking systems increase.

The characteristics that can influence cybersecurity, and enhance the risk exposure on maritime systems maintenance are:

- ✓ All equipments/system integrated;
- ✓ Eventual inexistence of cybersecurity protocol in the organisms;
- ✓ Eventual inexistence of cybersecurity between the organisms;
- ✓ Lack of means of controlling computers network navigation;
- ✓ Eventual resistance to change of involved personnel;
- ✓ Eventual lack of training of personnel in the use of the software;
- ✓ Eventual users negligence in software operation;
- ✓ Eventual use of inappropriate language to the type of maintenance report.

In the ship cybersecurity environment several factors should be considered: the ship itself, the crew, equipment, or systems continuous risk analysis. Identified factors with a well-documented system and management will contribute to a cyber-safe environment.

B. Risk of Cyber Exposure in Maintenance Data

BIMCO (2020) and Kavallieratos & Katsikas (2020), enunciated an assessment to risk exposure. In this investigation, a modified risk matrix was designed to evaluate the risk of cyber exposure of a frigate propulsion diesel engine maintenance data [15]. For risk assessment, six criteria were considered: Exposure, Likelihood, Environment Impact, Safety Impact, Security Impact, and Maintenance Impact.

For Exposure criteria, four levels were assumed (see Table I) from sporadically to permanently.

Table I. Scale for Risk Assessment – Exposure (E)

Value	*Exposure*
0	Sporadic
1	30% of the time
2	60% of the time
3	Permanently

Likelihood of a cyber-attack (see Table II). For the impact, there were considered 2 events, the extraction of information or anomalies in the system by cyber-access.

Table II. Scale for Risk Assessment – Likelihood (L)

Value	Likelihood
0	Did not occur in the last 3 years
1	It may have occurred in the last 3 years
2	Occurred in the last 3 years
3	Occurred 1 time in the last year
4	Occurred more than 2 times in the last year

For Environment Impact, also four levels were considered, from "without impact" to "ship inoperative" (see Table III).

Table III. Scale for Risk Assessment – Environment Impact (EI)

Value	Environment Impact
0	Without impact
1	Software mild anomaly
2	Serious anomaly in the maintenance software
3	Ship Inoperative / May cause personal injury.

Safety impact means consequences of the attack for database maintenance, putting at risk the on-board safety; for example, a wrong maintenance procedure execution.

Digital Object Identifier 10.32754/JMT.2022.2.08

TABLE IV. SCALE FOR RISK ASSESSMENT – SAFETY IMPACT (SI)

Value	Safety Impact
0	Without safety impact.
1	Mild access/software of safety - mild anomaly.
2	Access/serious anomaly in the safety software.
3	Safety database inoperative/without access to system information. Possible personnel injury.

The security impact is considered related to information integrity and an eventual vulnerability in the ship security assessment system (see Table V).

TABLE V. SCALE FOR RISK ASSESSMENT – SECURITY IMPACT (SECI)

Value	Security Impact
0	Without security impact
1	Security software mild anomaly
2	Serious anomaly in the security software
3	A fatal breach in Ship security, loss of data, possible people injury.

The maintenance impact is related to the access to maintenance information, misinformation, and equipment maintenance, which can lead to equipment anomaly or bad operation. Four levels were assumed, from without impact to maintenance database inoperative (Table VI).

TABLE VI. SCALE FOR RISK ASSESSMENT – MAINTENANCE IMPACT (MI)

Value	Maintenance Impact
0	Without maintenance impact.
1	Mild access/software mild anomaly.
2	Access/serious anomaly in the maintenance software.
3	Maintenance database inoperative/without access to system information.

Impact significance is estimated considering all six defined criteria:

$$SI = E + L(EI + SI + SecI + MI)$$

This significance represents the Risk (R) of a Cyber-attack.

TABLE VII. SCALE FOR RISK ASSESSMENT – SIGNIFICANCE IMPACT

Valuation	*Levels*	*Action*
0-1	Insignificant	None
2-4	Not significant	Monitoring
5-6	Not significant	Monitoring
7-8	Acceptable	Monitoring e study improvements of the cyber-security system
9-13	Significant	Implement Improvement Measures
14-15	Significant	Implement Improvement Measures
15 or more	Not Acceptable	Cut Network till cyber-security is reestablished

For a propulsion diesel engine risk assessment, seven activities related to SICALN use were assumed, and can be found in Appendix A. These activities were chosen to represent part of the information that can be analyzed, because these diesel propulsion engines are a complex system with hundreds of maintenance activities that are included in its Maintenance Planned System. The article has a point of view of the ship, so all the original actors of the presented activities are from the ship, but because of the network connection and access, the DN and the others administrative organizations from the Navy may interact with the information introduced by the ship and the data registration on SICALN, and that network and interaction represent the risk which was analyzed.

For the considered criteria and the obtained results, the risk of cyber-access was considered acceptable. Eventually, if SRTD was linked to equipment operational working parameters and other network connections, the risk can be higher.

The safety of the system must be monitored, and improvements of system cyber-security must be researched and, eventually, implemented.

In future work, another factor to be considered is that, for different networks, the security system procedure and access should be adapted to various security levels. For example, if maintenance software requests are introduced by access to the World Wide Web (WWW) or on a private web, or even ship to land. For different situations, the cyber risk is different, the security levels and aggregated security software should be adapted.

In the appendix, we can observe the results for the ship propulsion diesel engine assessment, where the obtained higher cyber risk exposure was for the SICALN library access. This may have happened because mostly the operators of SICALN can access it; if there is a networking hacker, access to some confidential information can be obtained, or some maintenance information can be changed or lost.

C. *Cybersecurity Factors in Maintenance Data*

The main risk in maintenance data will be the loss, mixing or alteration of its history for erroneous data, for example, alteration of operating hours, the recording of condition control readings, among others. In the present investigation, only maintenance data is mentioned, when there is a cybernetic connection between the control of the ship's propulsion and ground stations, the consequences may be more harmful.

A cybersecurity model for maintenance database must assume that connection of SRTD, SLI, and various navy organisms will be maintained or established. SRTD should be adapted to a system that allows the development of analytics related to system and equipment reliability and anomaly detection, trends, and prediction. Therefore, it should be fed by the machinery control system.

One procedure that should be implemented is the second stage authentication to enter maintenance database software platforms, not using personal mobile, but with a single touch in a procedure to show that, the person is not a “robot”. A procedure that we can find in various similar networking platforms.

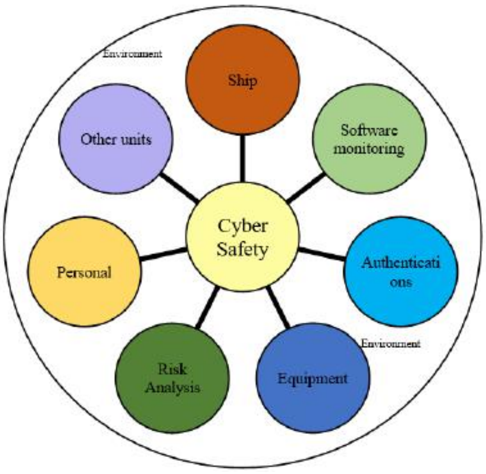


Figure 3. Maintenance database cyber-safety factors

Portuguese Navy network already has a monitoring and safety system; it is believed that the maintenance database should have a dedicated system that diagnoses the state and its assessment in the Naval Base and out of it, reporting

Digital Object Identifier 10.32754/JMT.2022.2.08

when there are some menaces in development, so the ship database managers can monitor its state.

Fig. 3 displays the factors that can contribute to maintenance cyber-safe model. The factors that must be accounted for in the model are the ship itself with the technical systems and equipment’s, the units, which has functions in the maintenance processes, personnel involved, the cyber-software monitoring, the risk analysis systems, and the implemented procedures to access the maintenance database and the environment and context that involve other factors.

It is believed that the existence of continuous training of the personnel on-board and in the land organizations and the continuous alert to the compliance with cybersecurity procedures are very important for a maintenance cyber-safe environment.

V. Conclusion

The networking environment among information systems is a today reality, and although cyber safe procedures implemented among the organizations, that doesn´t mean that cyber risk was eradicated.

Today the ship’s equipment is mostly connected to a central process that allow the systems monitoring. And the ships itself sometimes are connected to shore when they are on ports or by satellite. Therefore, cyber risk occurrence is a reality in ships maintenance database systems.

The maintenance system in the organization understudy has a dedicated software named SICALN, but the working equipment parameters are not collected and object of statistical treatment. In the future, a system integrating the various information systems with data treated with statistically algorithms should be implemented. And this fact can represent a higher risk for equipment.

The maintenance data base risk characteristics, in the organization, can be the inexistence of cybersecurity protocol in and between the Navy organisms, the lack of safety software and the resistance to change of the involved personnel.

The network safety depends on whether the software operates in a WWW or in a private network. The maintenance database in the Portuguese Navy is not always available online.

To guarantee cyber-safety, maintenance network risk analysis should be permanently upgraded, by monitoring the network.

Ship maintenance database, although with risk analysis acceptable results for cyber risk exposure, represents a ship cyber vulnerability. In Appendix A it is verified that a simple action like library access can put the maintenance database in risk of a cyber-attack.

A dedicated system to monitor the cyber-safety with the ship in the Naval Base and out of it should be developed when the databases are available online.

An implemented cyber-safe environment should be based in continuous personnel conferences, training, and periodical warning to remember the operative procedures.

Acknowledgment

This work is supported by Portuguese Naval Academy and CINAV and acknowledged for the collaboration of the Instituto Universitário Militar (IUM) from Portugal.

References

[1] H. Boyes & R. Isbell, Code of Practice – Cyber Security for Ships. IET (Institution of Engineering and Technology) Standards Department for Transport, England, 2017.

[2] B. Svilic, D. Brcic, S. Zuskin & D. Kalebic, “Raising Awareness on Cyber Security of ECDIS”, The International Journal on Marine Navigation and Safety of Sea Transportation, vol. 13, no. 1, pp. 231-236, 2019.

[3] S. Yee, N. Zainal & P. Fanam, “Challenges and Opportunities of Digitization on Container Shipping Industry in Supply Industry in Supply Chain Perspective”, Presented at the 10th Asian Logistics Round Table Conf., ALRT2039, Tasmania, 2020.

[4] N. Pajunen, “Overview of Maritime Cybersecurity. Bachelor Thesis – Marine Technology”, South-Eastern Finland University of Applied Sciences, Finland, 2017.

[5] Cyber security resilience management for ships and mobile offshore units in operation, Recommended Practice - DNVGL-RP-0496. DNV.GL [Online], Available in: https://www.dnv.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html [Consulted 27 mar.2021], 2016.

[6] M. Csorba & C. Carvalho, Plain Sailing? Observations of Cybersecurity and Network Health Problems in Control Systems at Sea. OTC-28039-MS, OTC Brasil, Rio de Janeiro, Brazil, 2017.

[7] A. Bamrara, “Evaluating Database Security and Cyber Attacks: A Relational Approach”, Journal of Internet Banking and Commerce, vol. 20, no. 2, 2015.

[8] M. Diulio, R. Halpin, M. Monaco, H. Chin, T. Hekman & D. Frank, “Advancements in Equipment Remote Monitoring Programs – Providing Optimal Freet Support in a Cyber-Safe Environment”, Naval Engineers Journal, vol. 127, no. 3, pp.109-118, 2015.

[9] J. Ahokas, T. Kiiski, J. Malmsten & L. Lauri, “Cybersecurity in Ports: A Conceptual Approach”, in: Kersten, Wolfgang Blecker, Thorten Ringle, Christian M. (Ed.): Digitalization in Supply Chain management and Logistis: Smart and Digital Solutions for an Industry 4.0 Environment. in Proc. of the Hamburg Int. Conf. of Logistics (HICL), vol. 23, Berlin, pp. 343-359, 2017.

[10] B. Mednikarov, Y. Tsonev & A. Lazarov, “Analysis of cybersecurity Issues in the Maritime Industry”, ISIJ, vol. 47, no. 1, pp. 27-43, 2020.

[11] IMO, Guidelines On maritime Cyber Risk Management, MSC-FAL. 1/Circ. 3/Rev.1, 14 June 2021.

[12] CCS, Practice of Cyber Security Management System on Cargo Ship. China Classification Society [Online]. Available in: https://www.asef2015.com/asef-forum/pdf/ASEF 7-Practice of Cyber Security Management System on Cargo Ship - Zhibiao Chen - CCS.pdf [Consulted 27 mar.2021], 2018.

[13] BIMCO, The guidelines on cyber security onboard ships, [Online], BIMCO and CLIA and ICS and INTERCARGO and INTERMANAGER and INTERTANKO and IUMI and OCIMF and WORLD SHIPPING COUNCIL Available in: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships [Consulted 28 mar.2021], 2020.

[14] V. Bolbot, G. Theotokatos, E. Boulougouris & D. Vassalos, “A novel cyber-risk assessment method for ship systems”, Journal of Safety Science, vol. 131, no. 104908, pp. 0925-7535, 2020.

[15] G. Kavallieratos & S. Katsikas, Managing Cyber Security Risks of the Cyber-Enabled Ship. Journal of Marine Science and Engineering, 8, 768, 2020.

[16] BIMCO, In the Guidelines on Cyber Security Onboard Ships, BIMCO and CLIA and ICS and INTERCARGO and INTERMANAGER and INTERTANKO and IUMI and OCIMF and WORLD SHIPPING COUNCIL, Technical Report; BIMCO: Bagsværd, Denmark, 2018.

[17] Marinha-EMA, ILA 5(A)–Instruções para a Organização da Manutenção das Unidades Navais e Outros Meios de Acção Naval, Marinha, Lisboa, 1997.

[18] Marinha. Data Collection and Processing System Manual (Manual do Sistema de Recolha e Tratamento de Dados (SRTD)) (ILMANT512). Direção de Navios, 1984.

[19] Navy, Ships´ 3-M Manual. Navseainst 4790.8D ed. s.l.: Navsea - Naval Sea Systems Command, 2021.

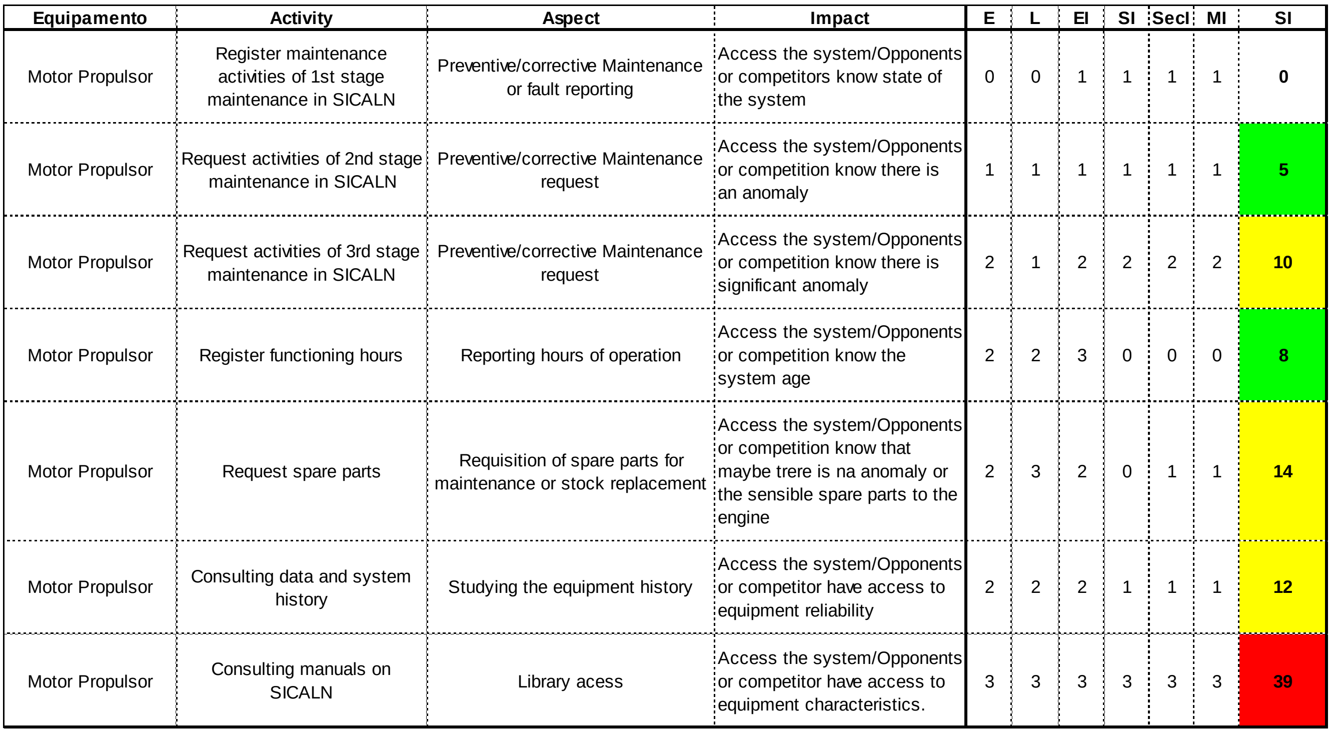
[20] Resolução do Conselho de Ministros nº92/2019. Estratégia Nacional de Segurança do Ciberespaço, Portugal.

[21] S. Lampreia, “Condition Based Maintenance. An Approach Using Modified Control Charts” (“Manutenção Baseada no Estado de Condição. Uma Abordagem Utilizando Cartas de Controlo Modificadas”). PhD Thesis, Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa, Almada, 2013.

Appendix A

Appendices represent the risk matrix.

Digital Object Identifier 10.32754/JMT.2022.2.08



Equipamento	Activity	Aspect	Impact	E	L	EI	SI	SecI	MI	SI
Motor Propulsor	Register maintenance activities of 1st stage maintenance in SICALN	Preventive/corrective Maintenance or fault reporting	Access the system/Opponents or competitors know state of the system	0	0	1	1	1	1	**0**
Motor Propulsor	Request activities of 2nd stage maintenance in SICALN	Preventive/corrective Maintenance request	Access the system/Opponents or competition know there is an anomaly	1	1	1	1	1	1	**5**
Motor Propulsor	Request activities of 3rd stage maintenance in SICALN	Preventive/corrective Maintenance request	Access the system/Opponents or competition know there is significant anomaly	2	1	2	2	2	2	**10**
Motor Propulsor	Register functioning hours	Reporting hours of operation	Access the system/Opponents or competition know the system age	2	2	3	0	0	0	**8**
Motor Propulsor	Request spare parts	Requisition of spare parts for maintenance or stock replacement	Access the system/Opponents or competition know that maybe trere is na anomaly or the sensible spare parts to the engine	2	3	2	0	1	1	**14**
Motor Propulsor	Consulting data and system history	Studying the equipment history	Access the system/Opponents or competitor have access to equipment reliability	2	2	2	1	1	1	**12**
Motor Propulsor	Consulting manuals on SICALN	Library acess	Access the system/Opponents or competitor have access to equipment characteristics.	3	3	3	3	3	3	**39**

Digital Object Identifier 10.32754/JMT.2022.2.07