Maritime Cybersecurity Risk Assessment: the Ship Maintenance Databases' Case Study

Suzana Lampreia
Science & Tecnology Department
Portuguese Naval Academy - CINAV
Almada, Portugal
suzanalampreia@gmail.com

Vitor Lobo
Science & Tecnology Department
Portuguese Naval Academy - CINAV
Almada, Portugal
vlobo@novaims.unl.pt

Valter Vairinhos
CINAV
Portuguese Naval Academy - CINAV
Almada, Portugal
valter.vairinhos@sapo.pt

***Abstract*— Nowadays, to decrease the crew, ships are being automated with complex systems. The objective is to minimize navigations costs, risks, and pollution. The operation of equipment and systems on board, is usually controlled and monitored by management software on board the ship itself, but sometimes it may be done also from shore installations. This may lead to an unsafe situation, from a cybersecurity point of view. A cyberattack on the control and monitoring system can put the crew and ship in danger. In this paper, cyber-attack evaluation risk matrix is defined, considering maintenance data from a diesel engine propulsion system of a navy frigate. To obtain that matrix, the occurrence probability, the impact, and the level of exposure to unsafe internal and external interventions was considered. From this matrix the impact significance is computed.**

Keywords— Cybersecurity, Ship, Maintenance, Database

I. INTRODUCTION

Cybersecurity is an important area of research, by a quickly research in the GoogleScholar, we can seen a very large number of scientific papers that was recently published.

Our interest in this area stems from the increasing automations in the platform ship control, and of the maintenance process, and thus greater exposure of our ships maintenance systems to cyberattacks.

Ships may be considered an industrial facility capable of navigating, on it there is 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 suffered a cyber-attack, they may have a negative impact on the health and safety of the people on board, on the ship operation, on the safety of other ships and maritime structures, and deteriorate the ship performance in terms of velocity and efficiency [1].

II. CYBERSECURITY IN A MARITIME CONTEXT

A. Data Management of Equipment onboard Ships

With the objective reducing the crew, many automated systems for command and control have been implemented on board ships. Nowadays these systems include equipment "health" monitoring, which collect their own data. The possibility of using remote control on these automated systems is a cyber vulnerability, and so cyber-safe software structures have been developed and implemented [2].

Ports can also represent a risk for ships and vice-versa. An example of it is a study conducted by European Network and Information Security Agency (ENISA) that identified fragilities in cybersecurity in ports referred by Ahokas *et al* [3].

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

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

[4] describe 3 main steps for the "Ship´s Cyber Risk assessment Process":

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

The International Maritime Organization (IMO) has already issued guidelines on Maritime Cyber Risk Management) (MSC-FAL.1-Circ.3). The cybersecurity tasks can be the establishment of procedures, the identification of the risks and risk assessment, and the responses to mitigate the identified risks [5].

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

III. MAINTENANCE DATABASES IN THE PORTUGUESE NAVY

The maintenance data management system implemented on surface ships in Portuguese Navy is called Data Collection and Treatment System (in Portuguese: "*Sistema de Recolha e Tratamento de Dados*" (SRTD)) [6].

The SRTD it is a subsystem of the Portuguese Navy Maintenance Management System (SGM - Sistema de Gestão da Manutenção). The SGM in turn is part of the Portuguese Navy logistic system [6].

The SRTD is processed by the SICALN (SICALN (an ORACLE language software), which the servers are not physical in DN, this system feed the Integrated Logistic

System (SLI - *Sistema Logístico Integrado*). The logistic information it is in SLI, and it is connected to DN, the organism responsible for 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, and the shipyard [Fig. 2].

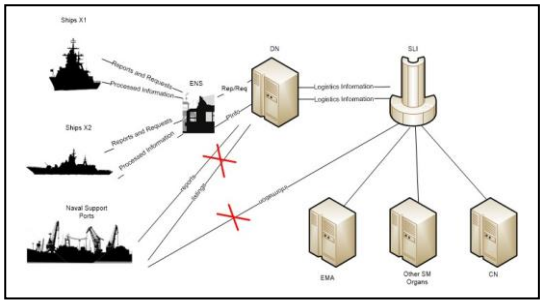

Fig. 2. Modified SRTD model.

The connections between ships and the ENS (Squadron of Surface Ships) and ENS and DN mean ships, sending processed information or requests in three type of registering data models, for example report or request maintenance support, report monthly the equipment's hours of functioning and request for spare parts [6].

IV. Case Study - Maintenance Databases Risk Analysis

A. *Factors that can influence the cybersecurity in Maintenance System*

The effects of networking on various organizations will lead to monitoring implementation and risk analysis, control, and network blocking systems need in case of the event of a threat. The characteristics that can influence the cybersecurity in Navy maintenance system are:

- ✓ All equipment´s/system integrated.
- ✓ Inexistence of cybersecurity protocol in the organisms.
- ✓ Inexistence of cybersecurity between the organisms.
- ✓ Lack of means of controlling computers network navigation.
- ✓ Resistance to change of involved personnel.

B. *Risk of Cyber Exposure in Maintenance Data*

In this investigation, it was designed a modified risk matrix to evaluate the risk of cyber exposure of maintenance data of frigate propulsion diesel engine.

For the impact, it was considered two events, the extraction of information or anomalies in the system by cyber-access, and four levels of impact (from minimum to maximum impact.

The considered likelihood criteria has six levels, from the non occurrence to the occurrence of 16 times or more in the last year.

The exposure criteria has four levels, from sporadically to permanently.

And then THE significance impact is calculated by (SI)=LxI+E, with nine valuation levels, from insignificant to not acceptable.

For risk assessment on propulsion diesel engine, it was considered seven activities related with SICALN use.

For the considered criteria and the obtained results, the risk of cyber-access was considered acceptable. The safety of the system must be monitored, and improvements of cyber-security system must be studied and maybe implemented.

TABLE I. PROPULSION DIESEL ENGINE RISK ASSESSMENT[a]

Activity	Aspect	Impact	L	I	E	SI
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	1	1	2	3
Request activities of 2nd stage maintenance in SICALN	Preventive/corrective Maintenance request	Access the system/Opponents or competition know there is an anomaly	2	2	2	6
Request activities of 3rd stage maintenance in SICALN	Preventive/corrective Maintenance request	Access the system/Opponents or competition know there is significant anomaly	1	3	2	5
Register functioning hours	Reporting hours of operation	Access the system/Opponents or competition know the system age	2	3	2	8
Request spare parts	Requisition of spare parts for maintenance or stock replacement	Access the system/Opponents or competition know that maybe there is an anomaly or the sensible spare parts to the engine	1	2	2	4
Consulting data and system history	Studying the equipment history	Access the system/Opponents or competitor have access to equipment reliability	1	2	2	4
Consulting manuals on SICALN	Library acess	Access the system/Opponents or competitor have access to equipment characteristics.	2	2	2	6

a. L-Likelihood, I-Impact, E-Exposure, SI-Significance

C. *Proposed Cybersecurity Model 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 the maintenance data are mentioned, if there is a cybernetic connection between the control of the ship's propulsion and ground stations, the consequences may be more harmful.

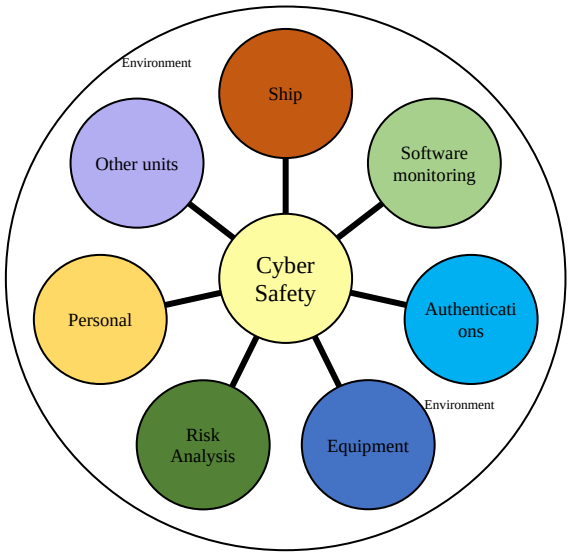

Fig. 3. Maintenance database cyber-safety factors.

The Portuguese Navy network already have a monitoring and safety system, but it is believed that for the maintenance database should have a dedicated system that diagnosis the state and its assessment in the Naval Base and out of it, reporting if there are some menaces in development, so the ship database managers can monitor its state.

In Fig. 3 it is exposed the factors that can contribute do maintenance cyber-safe model.

It is considered 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. CONCLUSIONS

A cyber risk attack is a reality in ships maintenance data base systems.

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

To guarantee cyber-safety, risk analysis should be permanently actualized.

The ship maintenance database, although with risk analysis acceptable results to cyber risk exposure, it is considered a vulnerability in ships.

The network safety, from where the database is accessed and the information changed between Portuguese navy units, can be different and depends on if it is national, international, in the naval base or out of it.

It should be developed a dedicated system that monitor the cyber-safety with the ship in the Naval Base and out of it.

A cyber-safe environment should be based in continuous personnel 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] 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, nr 3, 2015, pp.109-118.

[3] 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. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23, Berlin, pp. 343-359, 2017.

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

[5] China Classification Society. Practice of Cyber Security Management System on Cargo Ship. [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.

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