IAMU
International Association of Maritime Universities

THE NIPPON FOUNDATION

International Association of Maritime Universities

IAMU 2022 Research Project
(No. YAS20220301)

Determining Maritime Cyber Security Dynamics And Development of Maritime Cyber Risk Check List for Ships

By

Istanbul Technical University, Maritime Faculty

August 2023

IAMU
International Association of Maritime Universities

This report is published as part of the 2022 Research Project in the 2022 Capacity Building Project of International Association of Maritime Universities, which is fully supported by The Nippon Foundation.

Published by the International Association of Maritime Universities (IAMU) Secretariat
Meiwa Building 8F, 1-15-10 Toranomon, Minato-ku,
Tokyo 105-0001, JAPAN
TEL : 81-3-6257-1812 E-mail : info@iamu-edu.org URL : http://www.iamu-edu.org

ISBN978-4-907408-49-7

IAMU 2022 Research Project
(No. YAS20220301)

Determining Maritime Cyber Security Dynamics And Development of Maritime Cyber Risk Check List for Ships

By
Istanbul Technical University, Maritime Faculty

Contractor : Ozcan Arslan
Research Coordinator : Gizem Kayisoglu

Determining Maritime Cyber Security Dynamics And Development of Maritime Cyber Risk Check List for Ships

Theme: 3

Istanbul Technical University, Maritime Faculty

Research Coordinator

Gizem Kayisoglu

Research Assistant, Ph.D, Istanbul Technical University, Maritime Faculty, yukselg@itu.edu.tr

Abstract The digitalization in maritime industry rises the integration of the information and operational technologies on the vessels. The high level of connectivity and the rising of digitalization in maritime sector increase the cyber security issue. The systems of vessels can be exposed to errors of digital world and encounter some malicious attacks. At this point, cyber security in maritime sector is an important topic in terms of not only securing the systems, preventing the accidents, loss of life, and damage to the environment but also national security, and global economy. Accordingly, in the context of IAMU 2022 Research Project for Young Academic Staff, it is aimed to determine maritime cyber security dynamics based on informational technology (IT) and operational technology (OT) for ships, by considering the breaches, the liabilities, responsibilities, rules and enforcements in the scope of maritime cyber security. Thus, it is aimed to develop maritime cyber risk checklist for ships by performing maritime cyber risk management with the help of these dynamics in the project. The considered risk assessment framework in this project is CORAS risk assessment approach. Then, the outputs are visualized and sequenced hierarchically by using bow-tie framework. All in all, in this report, the issues of maritime cyber security on the perspective of maritime cyber risk assessment and suggestions on solutions of them is tried to be emerged in order to create a maritime cyber-checklist for integrating safety management systems of ships.

Keyword: *Maritime cyber security, Maritime cyber risk, Maritime cyber-physical system, Cyber-checklist for ships*

Contents

1. Introduction

The high level of digitalization and connectivity in maritime sector make the cyber security issue come to the force. In particular, ships became connected to universal networks, incorporated complex digital industrial systems, and integrated with the information and operational technologies. This integrated network makes a great risk in terms of malicious attacks and unauthorized access to the ship's systems and networks [1]. From this perspective, all machinery, navigation and communication systems of a ship can be exposed to cyber threats. These threats can be performed by technical human error in the system or software or by cybercriminals by finding weak points or vulnerabilities of the system. In this regard, cyber security is not only a concept of information risks any more where many potential risks have emerged for the safe operation of the ships, but also it requires to be understand and analyze those risks. At this point, cyber security in maritime sector is an important topic not only with respect to the particular of securing the systems, preventing the accidents, loss of life, and damage to the environment but also with respect to national security, and global economy. Furthermore, a cyber-breach gives rise to financial loss, disruption in the business procedures, and damage to reputation. Against all of these dangers, a company wants to get rid of the incident quickly and secure itself to work normally again. For this purpose to be achieved, both the issue of ship protection systems against physical attack, the design of the systems and supporting process should be taken into consideration at first.

The cyber environment of ships contain interconnected networks of both Information Technology (IT) such as the computer-based systems, personal computers, tablet devices, laptops, routers, servers and switches, etc. and operational technology (OT) such as, control systems, actuators, sensors, radar, etc. The cyber space onboard provide services, information, business and social functions. As well as for the secure and safe continuity of these mentioned functions, there is an agreement that capabilities of the human factor, and the strengths of humans working together with the management of cyber vulnerabilities, are key in establishing and maintaining robust cyber security and in preventing cyber-attacks [2]. At this point, the appropriate measures for maritime cyber resilience, especially for ships' cyber resilience, should be also taken in the framework of these assets. .

When the historical developments of cyber security in maritime are evaluated, a hierarchical improvement is observed as in Figure 1 and it has been noticed that the above-mentioned framework is specified at every stage of this development. After the 2010 Strategic Defense and Security Review made publication about cyber security as a top threat for national security, in the maritime sector, it has become a prominent issue [3]. In 2011, ENISA highlighted the low cyber security awareness for maritime sector and suggested some titles about cyber security in maritime for raising the awareness [4]. In 2016, International Maritime Organization (IMO) has issued a circular about Guidelines on maritime cyber risk management. As per this circular, cyber risks are appropriately addressed in the International Safety Management (ISM) Code until 1st of January 2021. With these amendments, various guidelines relating with cyber security on board ships were issued by BIMCO, DNV-GL, CLIA, INTERMANAGER, INTERCARGO, INTERTANKO, OCIMF etc. [1] When the researches on the cyber security in maritime in the literature are analyzed, it is observed that the level of cyber security awareness in maritime is visibly high in 2018 and the maritime sector has passed the operation level for cyber security [5]. Cyber security risk assessment and management studies have shown up as of years 2019, 2020 and 2021 [6]–[10].

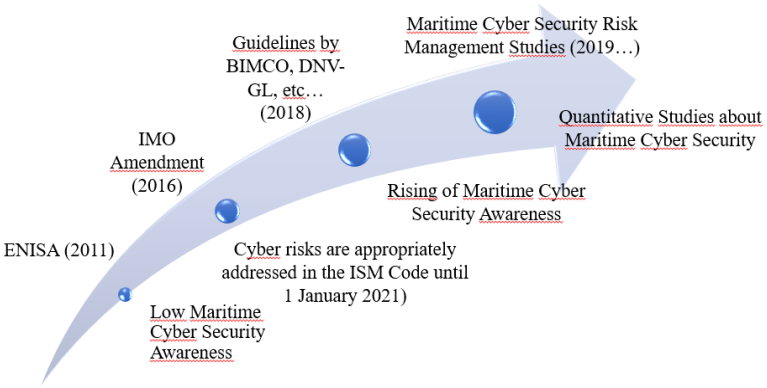


Figure 1. Historical developments of cyber security in maritime

Maritime cyber risk indicates the level of threat on a digital asset due to potential attacks caused by a malicious event, person, situation, or malware, and the level of corruption and loss of information or operating systems due to ship-related safety, security or operation error. Cyber security has an impact on every aspect of a maritime organization such as, logistics, shipping, supply chain, company process, transportation, etc... Thus, maritime cyber risk must be integrated into organizational risk management and decision making structures to ensure high-level cyber security in a maritime organization. Maritime cyber risks include operational risk, financial risk, legal risk such as regulations, partnerships, contract etc…In this respect, cyber risk, cyber risk management and a check list as the output of them should be considered.

At this point, the significance of this project is to emerge with the issues of maritime cyber security on the perspective of maritime cyber risk and maritime cyber risk management. Accordingly, in the context of IAMU 2022 Research Project for Young Academic Staff, it is aimed to develop maritime cyber risk check list for ships, which can create a base for maritime cyber security insurance for ships, by performing maritime cyber risk management with the help of determining maritime cyber security dynamics based on IT and OT for ships and liabilities and responsibilities. The created checklist also provides a standard for safety management systems of ships.

1.1. Research Objectives

The purpose of the project is;

i. to identify the ship cyber environment by determining all systems on the ship, technologic and communication infrastructure of the systems, and their integrations.
ii. to identify cyber risks of all systems on the ships by determining the vulnerabilities of technologic and communication infrastructure of the systems, possible threat scenarios against the systems due to the vulnerabilities, and unwanted incidents resulted from occurring threat scenarios.
iii. to present a cyber risk management approach for ships.
iv. to create a checklist for managing cyber risk on ships under ships' safety management manuals (SMM) in their international safety management (ISM) systems by considering not only technologic mitigations but also integrating them with people and process elements. The check list for cyber risks is a systematic control procedure including work process diagram for cyber security of ships. For this reason, the checklist, which is the research objective of the project, ensures that the ships are prepared technically and systematically against cyber risks and take precautions, and can also be included in their own safety management system (SMS).

2. Methodology

While there is a several potential cyber losses, different approaches exist for mitigating these losses. The approaches involve two different methods in general. The first one is design method that is aimed to develop system activities and architecture. The other one is operational methods which include alterations regarding trade operations [11], [12]. There are also some approaches for managing cyber risks, such as security software and investments in the cyber workforce. On the other hand, for mitigating cyber risk, protective technical measures such as software encryption, firewalls, system separation, virus detection, can be also used as well as developed theoretical approaches. Organizational measures for cyber risk can be categorized as procedural measures involving operational and management systems, structural measures including hardware and software, and responsive measures, which means damage and response management when an attack or incident is found out [13]. Institutions must recognize that mentioned measures cannot prevent cyber risk as whole and they must manage properly residual risks and should use cyber insurance for transferring the risks to third parties [14].

The risk management approach, which is stipulated in "The Guidelines on Cyber Security Onboard Ships", is proposed for improving maritime cyber risk assessment and creating a background for maritime cyber insurance policy [1]. It is developed with the aim to explain why and how cyber risks should be managed in a shipping context. It includes pro-documents, process, components, and responsible parties for risk assessment. Besides, in searching for a standardized approach to compliance, it is seen that the ISO27000 family of standards are suitable for ship owners and other stakeholders in the maritime sectors [15]. They can be considered as a guideline to make high the perception for not only on-board but also on-shore, adopting compliance for cyber risk management in maritime and certifying an Information Security Management System (ISMS).

Accordingly, the steps of the cyber risk management approach for maritime sector is proposed as in Figure 2 under this project. The five columns in Figure 2 are realized based on CORAS risk assessment framework for ship cyber security assessment and the demonstration of the treatments for cyber security of specific ship systems is implemented based on bow-tie framework.

In this context, firstly, the process of CORAS and bow-tie frameworks are presented in next sections. Then, overall ship cyber physical system is mapped. After that, for understanding how CORAS risk assessment framework can be used for cyber security of ship system, a case study is shown by applying the CORAS framework on the RADAR system, which is the one of the ship cyber physical system. At this point, the integration of specific guidelines, standards, regulations, and code of best practices (e.g. The National Institute of Standards and Technology (NIST) framework, International Association of Classification Societies (IACS) Unified Requirements (UR) for cyber security, which are E26 and E27, DNV-GL class guideline for cyber security, IEC 62443-3, ISO/IEC 27001, ISO/IEC 27033-3, code of practice: cyber security for ships) with ship cyber security is also presented and used for developing systematic treatments for ship cyber security. The treatments are developed for each ship cyber physical system by considering similar steps of the CORAS framework for each ship system. Accordingly, a check list table is created for ship cyber security. The developed treatments are shown on the bow-tie framework for ECDIS system as a sample demonstration in this project.

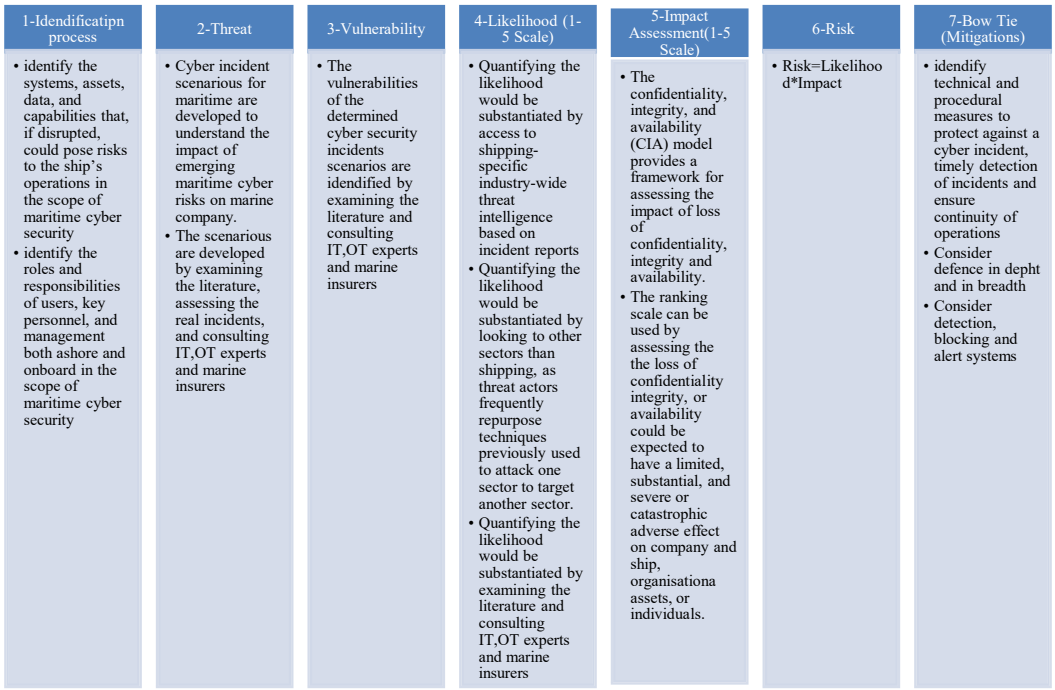


Figure 2. Maritime cyber risk management.

The steps of the project is summarized as in Figure 3 by integrating the steps in Figure 2. Accordingly, step 1-4 in Figure 3 is useful for the step of development of treatment in the risk assessment.

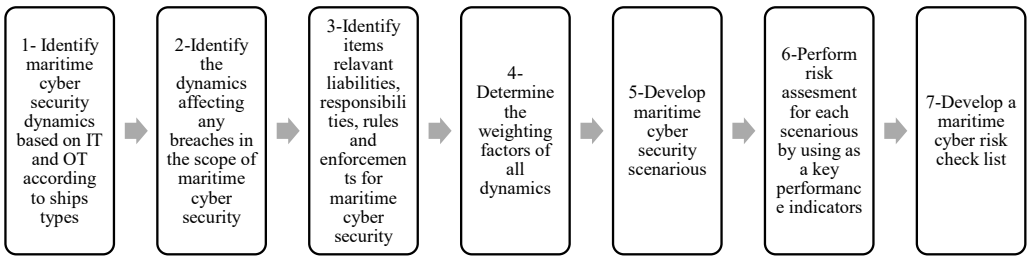


Figure 3. Summary of the Methodology.

2.1 CORAS Framework

The CORAS framework is developed as part of the EU-funded CORAS project (IST-2000-25031) in order to serve as a model-based risk assessment tool specifically designed for the security of critical systems [16] . The CORAS framework offers the practical and simple usage of the Unified Modelling Language (UML), which addresses the attributes, operations, and relationships of a system, the possible states in the system, example scenarios of system usage, including different user types and relationships between user tasks, and the behavior of the overall system in the context of a usage scenario [17]. Furthermore, Fault Tree Analysis (FTA) [18], Hazard and Operability Analysis (HazOp) [19], the Failure Mode and Effect Analaysis (FMEA) [20], and Markow Analysis [21] are just a few examples of traditional analysis techniques for security issues that are rigorously integrated into CORAS. The Australian/New Zealand Standard for Risk Management [22], the ISO/IEC 13335 Guidelines for the

management of IT-Security [23], and other international standards, such as system documentation in the form of the Reference Model for Open Distributed Processing [24], the ISO/IEC 17799 Code of Practice for Information Security Management [25], are also included in this approach.

The CORAS framework provides milestones within the realm of IT security, as posited by Stolen et al. [16]. The employment of this approach enhances the precision and dependability of the evaluation's objectives, context, and security concerns. Additionally, it facilitates communication and data exchange among the parties involved in the risk assessment. Furthermore, it simplifies the documentation of risk assessment outcomes and enables assumptions to be made regarding their reliability and validity. Lastly, it establishes a robust foundation for the grouping of assessment techniques and the management of risks within the system. Enhancing the probability of reutilizing and revising evaluation outcomes upon resumption of the assessment target leads to an improvement in the quality of risk assessment outcomes, a reduction in maintenance expenses, and the assurance of the stipulated security level.

The CORAS Risk Management Process is illustrated in Figure 4. The initial phase involves setting the context by disclosing the organizational setting and engaging with system users, authorized personnel, and decision makers to comprehend the purpose of the analysis, the assets to be safeguarded within the system, and the scope of the analysis. Subsequently, the technical configuration and communication technologies employed by the system are expounded with the aim of delineating its vulnerabilities. This is followed by the development of threat scenarios that are triggered by the vulnerabilities, and the identification of unwanted incidents that may arise due to the threats. This step is commonly referred to as risk identification. During the third phase, a risk analysis is conducted through the assessment of the likelihood of threat and potential incidents, as well as the severity of the consequences resulting from an undesirable event. This evaluation is based on expert judgment or previous system data. The establishment of the tolerable risk value is based on the evaluation of the targeted criteria of the system, in accordance with the acquired risk values of the examined system. In situations where risks cannot be tolerated, the implementation of mitigation techniques becomes necessary. These techniques may include the incorporation of additional technical specifications, the establishment of defined security policies, the assignment of security duties and responsibilities, as well as the implementation of monitoring and testing processes. The objective of these measures is to ensure the effectiveness and reliability of the treatment methods employed. In order to successfully carry out the CORAS risk management process for shipboard RADAR in the case study section, it is imperative to adhere to the actions and sub-tasks outlined in the steps as depicted in Figure 4.

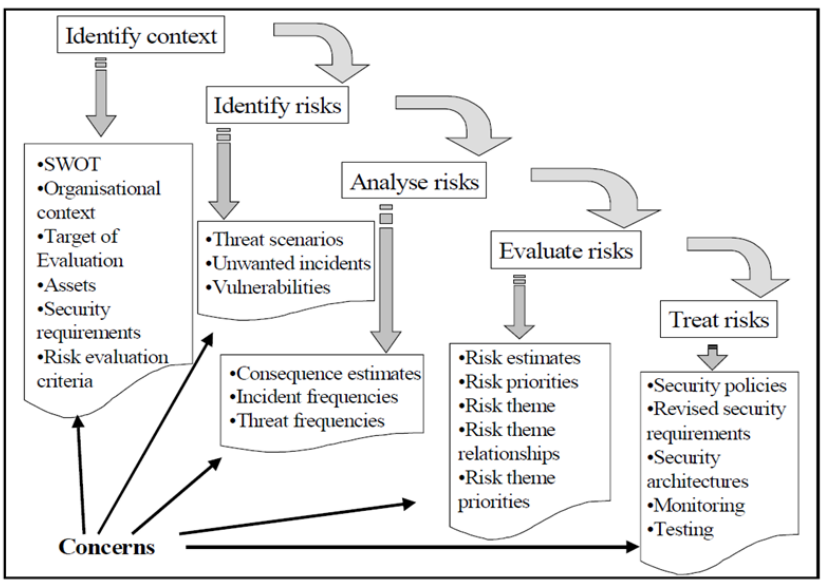


Figure 4. The CORAS risk management process [16].

The nomenclatures used in the framework language include specific terms such as threat and asset. The nomenclature and its relationship in CORAS are depicted in Figure 5. The process of defining a system involves identifying relevant questions, determining the constituent components of the system's responses to these questions, and analyzing the interrelationships among these components. This approach facilitates the development of a comprehensive risk assessment for the system.

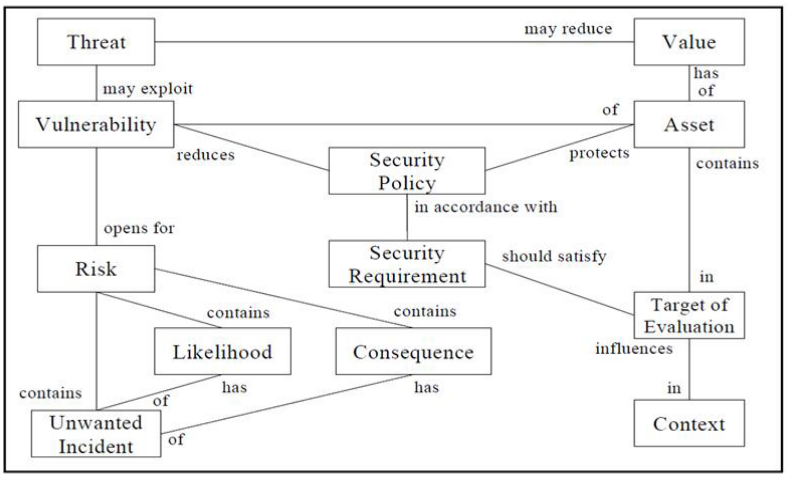


Figure 5. CORAS terminology [16]

The CORAS tool employs distinct symbols to represent the aforementioned nomenclatures, with the aim of enhancing visual retention and design, as illustrated in Figure 6.

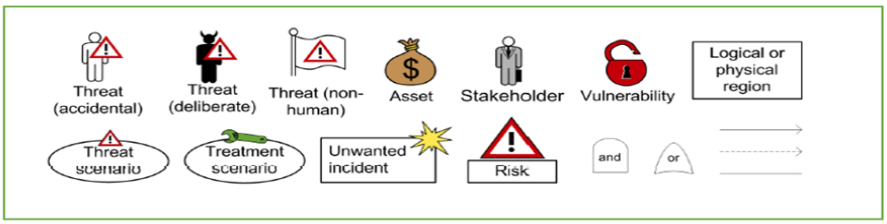


Figure 6. Symbols in the CORAS framework [26].

2.2 Bow-Tie Framework

The bow-tie model is created to provide both reactive and proactive risk management in the case of an accident by displaying the cause of the undesirable event on the left side and potential consequences on the right side, should the event have occurred. When applying fault tree or event tree analysis, it can produce a quantitative assessment and indicate an acceptable risk threshold. The bow-tie method's benefits include easy reading and an awareness of dangers, obstacles, and repercussions in a system. Additionally, it must clearly depict the initial situations, escalators and keyhole barriers, potential results, remedial actions, and the way in which these factors interact. The linking of the obstacles, in turn, creates a safety management system [27]. In the literature, Abdo et al.'s [28] presents a security risk assessment with bow-tie for industrial control systems, and Bernsmed et al.'s [29] suggests the bow-tie diagrams for visualizing cyber security risks. The bow tie's purpose is depicted in Figure 7 [30]. Due to these benefits, the bow-tie diagram is employed in this project by integrated with CORAS framework. The bow tie diagram's placement of identified components can be understood using the prioritizing values received by using a method for multi criteria decision making such as Analytic Hierarchical Process (AHP). Therefore, in this project, the bow-tie model offers a useful single diagram to illustrate the ECDIS cyber security system as a sample.

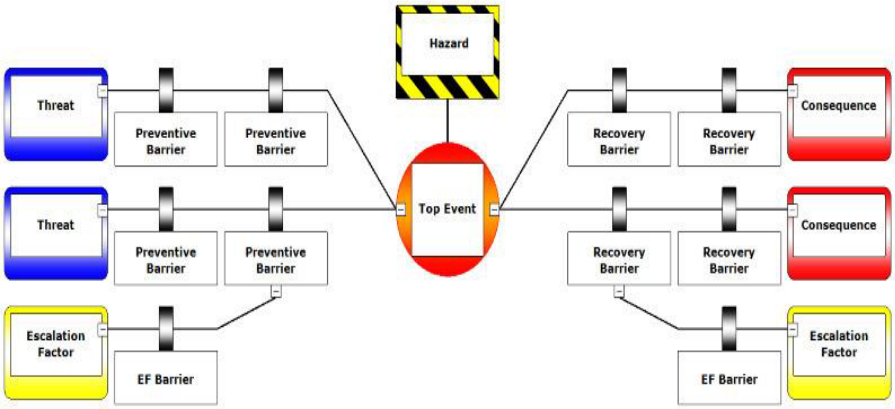


Figure 7. Typical Bow-tie Diagram [30].

3. Shipboard Cyber Physical Systems

In order to understand the cyber physical systems onboard ships, the general system categorization is needed to define. At this point, the system onboard ships, which is stated by Vassallo Associates [31], is considered as in Figure 8 regardless of ship type. Accordingly, the general systems onboard ships are categorized as bridge systems, onboard security systems, cargo management systems, communication systems, propulsion and machinery control systems, and passenger and crew systems. According to the ship system, it is recognized that mostly cargo tanks and cargo lines are differ each other. For instance, in tanker ships cargo management systems have more sensors and control system than a bulk carrier ships. However, they have similar IT and OT mapping in terms of cyber space. Therefore, the developed checklist under this project is created according to the technologic categorization.

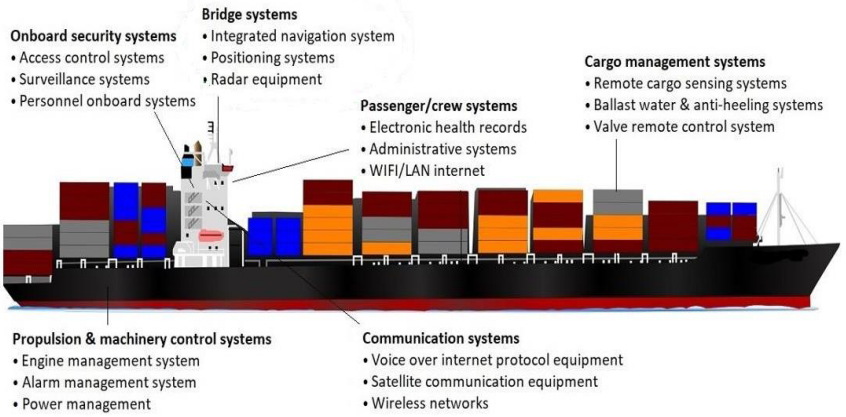


Figure 8. General systems onboard ships [31].

As shown in Figure 9, on-vessel infrastructure can be segmented into two systems: electro-mechanical and communications. For the electromechanical system the data is transferred to programmable logic controllers (PLCs) via sensors. Ship bridge has indicators and alert system for seeing the situation of electromechanical system rather than controlling them. Additionally, PLCs are generally used to automate a process and on-vessel PLCs are combined with the power management system, alarms and

engines. PLCs are integral to the control of the navigation system and to prevent defaults delivering high operational efficiency with low maintenance cost. Moreover, PLCs provide critical data such as temperature, engine status, pressures and electrical defaults, as well as information to execute the overall management of the vessel.

Propulsion and machinery management and power control systems is one of the mechanical and electrical systems of a ship allowing the crew to maintain their basic professional functions throughout exploitation. Some of the systems might be accessible from the shore side like engine performance or Emergency Shut Down Systems (ESD).

The modern integrated bridge command system is a computer-based ship cyber-physical system the functionality of which is provided by local Internet network technologies, satellite communication, and navigation systems making the bridge system vulnerable to cyberattacks. The data communication between systems on the bridge such as RADAR, ECDIS, GPS, or AIS is provided by NMEA 0183 (IEC 61162/1-2) protocol, NMEA 2000 protocol, and Ethernet (IEC 61162/450) connection. Therefore, serial data and network data transferring occur between the bridge systems.

Access control systems are systems for controlling access to ship's equipment and infrastructure, ensuring the reliability, physical security, and safety of the ship and its cargo, as well as systems for monitoring, announcing, and warning of circumstances related to on-board security.

Passenger servicing and management systems are electronic systems for passenger service and management – digital systems used for passenger property management, boarding, and access control; these systems may contain data related to passengers. Also, smart devices, such as tablets, smart-phones, scanners, etc.) should be under control, such as potential targets of a cyber-attack.

In terms of passenger network access, the local and Internet network access of passengers is a potential risk to the ship's cybersecurity. Network passenger services, such as Internet access, mail servers, must be outside the on-board computer networks used to control the ship and crew operations.

For administrative and crew welfare systems, onboard computer networks used for administrative management and crew actions are also extremely vulnerable to cyberattacks, especially if they also provide access to the Internet and an email server. This can be used for unauthorized access to onboard systems and data. Therefore, these systems should be considered uncontrolled and should not be linked to a critical safety system onboard. Software provided by ship management companies or owners is also included in this category.

Shipboard communication systems for the Internet and satellite and/or other wireless communication increase the risk of cyber-attacks on the ship's systems. This requires the use of reliable software security tools to achieve the necessary cybersecurity.

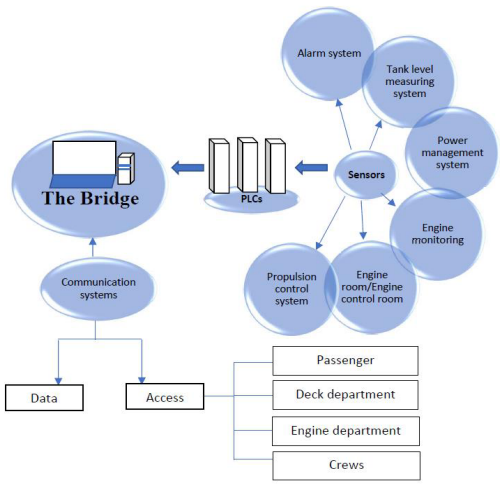


Figure 9. Interaction of vessel systems [32].

The appeal of hacking maritime systems and PLCs arises from their lack of built-in security. Furthermore, maritime vessel networks have typically been flat and isolated, with air-gapping being the "security solution" of choice. As a result, security had not been a priority until today. However, as these networks become increasingly interconnected, the attack surface on a vessel grows. With little or no segmentation between the IT and vessel networks, the potential of malware infiltrating the vessel networks and spreading laterally to crucial controls exists. Accordingly, for network segregation, Mission Secure [33] suggest the framework in Figure 10.

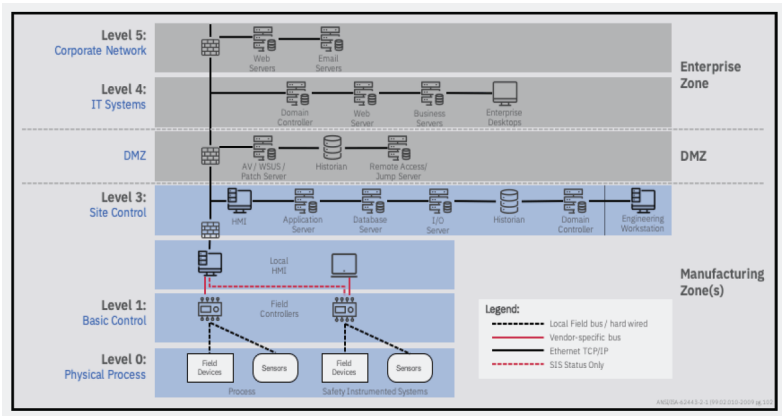


Figure 10. Network Segregation Framework [33].

4. Cyber Risk Assessment based on CORAS: A Case Study for Shipboard RADAR

The purpose of presenting this section is to show an example to the implementation proposed for the project. In this project, in the overall perspective, it is aimed to determine maritime cyber security dynamics based on informational technology (IT) and operational technology (OT) for ships, by considering the breaches, the liabilities, responsibilities, rules and enforcements in the scope of maritime cyber security. Thus, it is aimed to develop maritime cyber risk checklist for ships by performing maritime cyber risk management with the help of these dynamics in the project. The considered risk assessment framework in this project is CORAS risk assessment approach. Then, the outputs are visualized and sequenced hierarchically by using bow-tie framework. This section is an example where processes related to achieving these goals are shown on shipboard RADAR. In this context, the risk assessment procedure based on the CORAS architecture specifically designed for RADAR cyber security is introduced in Figure 11 as a case study.

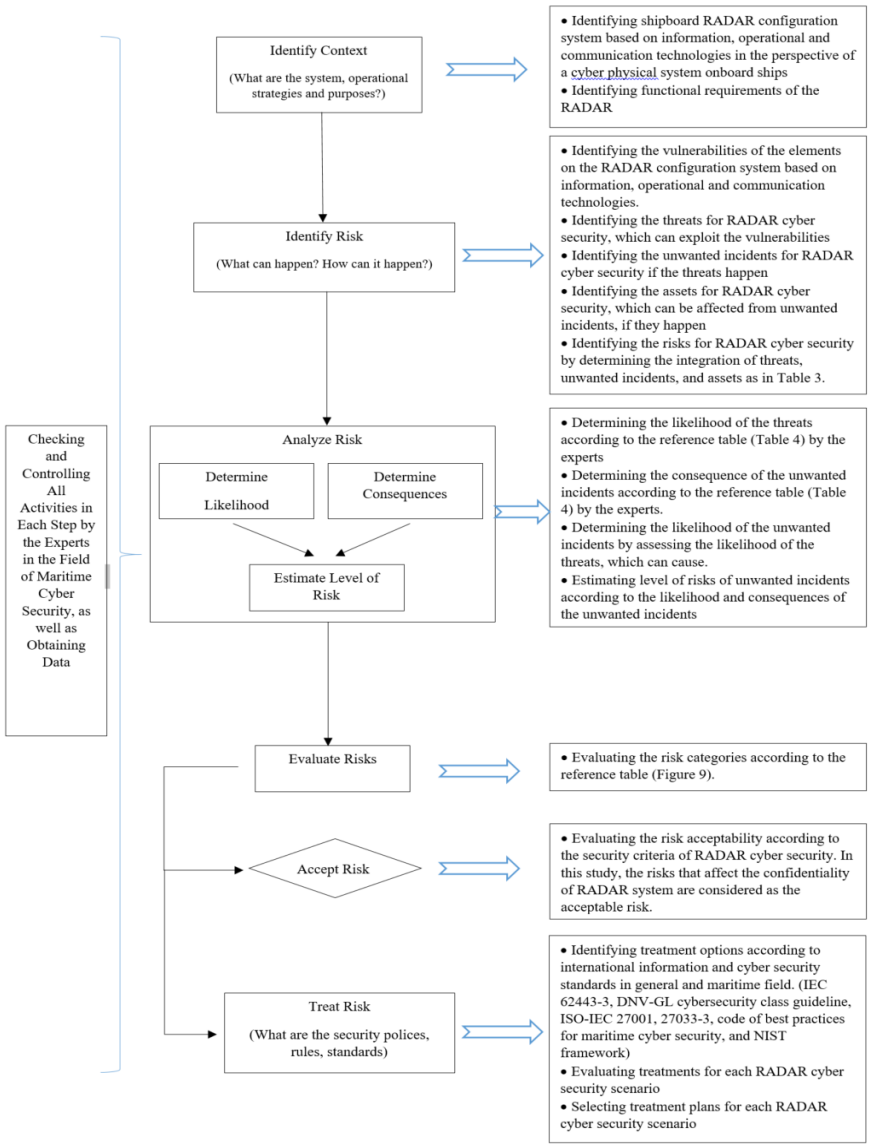


Figure 11. Cyber Risk Assessment Process for RADAR.

4.1 Identify Context

In terms of determining the goals and assets of a system based on the CORAS framework, the identification of context is an essential stage. In this step, the RADAR design objective, configuration system, components, communication protocols, integrated system devices, data processing system, and user function are comprehended. The ensuing processes determine the shipboard RADAR system's target points, whose weaknesses may be exploited by attackers, and the assets that may be compromised by the attacks.

The design aim of a RADAR system in this situation is to identify and track physical things in its surrounding environment. Figure 12 depicts a specific configuration system of a shipboard RADAR that conforms to IMO performance specifications. Consequently, it consists of a display unit, a processor unit, a keyboard control unit, a trackball control unit, an antenna unit for X band and S band, a power supply unit, a performance monitor, a remote control unit, a gyro interface, a digital visual interface

analog RGB conversion kit, an RGB connector, a memory card interface unit, a junction box, and a switching hub. Although the RADAR configuration system comprises stand-alone mechanisms, it is also integrated with other cyber-physical systems and sensors on the bridge through a variety of interfaces. The processing unit receives signals from RADAR antennas via wire as well as other external navigational devices and sensors such as GPS, SDME, AIS, Gyrocompass via NMEA serial interfaces (IEC 61162-1), and ECDIS, other RADAR, and integrated navigation system over 100Base-tx Ethernet.

Moreover, the processor unit sends the collected signals to the VDR via an RGB connector so that the RADAR display image can be recorded in the VDR, and it sends the same signal to the RADAR display unit via a digital visual interface (such as the ASTERIX standards [34]) so that the bridge officers can see all of the information regarding the detected objects.

Own ship status, different navigational data, radar plotting data, water temperature, wind, and data from other sensors on the ship are displayed on the cells of the display unit. It can display both AIS and ARPA symbols on the screen, depending on how the GPS determines the AIS positions and how the ARPA target signal and data are determined by bearing and range from its own ship. Through operator-defined conditions, these two types of symbols can be combined. In accordance with the various target vector demonstrations, the operators can identify the targets as asleep, chosen, lost, or dangerous. By deactivating automatic acquisition and tracking excluding them, they can also define an automatic acquisition zone on the display unit to reduce processor overload and clutter. When targets enter the operator-specified zones or when targets or their ships depart from the established zone in an anchoring situation, guard zones on the display unit can generate audience and visual alarms. The electronic bearing line (EBL) and variable range marker (VRM), respectively, are used by the operators to measure the bearing and distance of any fixed-positioned object from their own ship. In order to determine whether a target is in a collision situation, they can also establish the closest point of approach (CPA) and time to CPA (TCPA) [35]. The keyboard control unit and the trackball control unit are used by the operators to set and manage all of these RADAR operations.

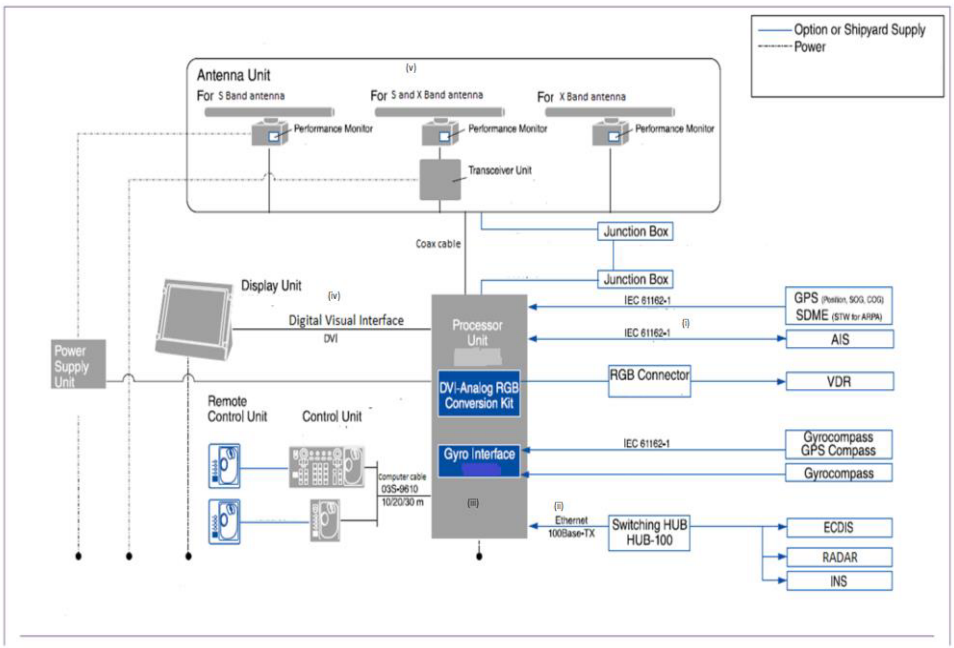
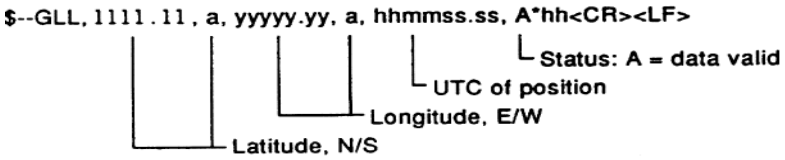


Figure 12. Shipboard RADAR Configuration System [36].

The input and output data phrases for shipborne RADAR are constructed in accordance with Figure 13 of the IEC 61162-1 [37] and a manufacturer's guidance [38]. These data phrases, which are described in IEC 61162-1, are used to transport the aforementioned data between the talker and the listener in an acceptable data format. For instance, "GLL" data, which indicates the geographic position of the current vessel and includes its latitude and longitude as well as the moment when its position was fixed and its status, follows the general format shown below in written form:



Input		Output	
ABK	AIS addressed and binary broadcast acknowledgement	ABM	AIS Addressed binary and safety related message
ACK	Acknowledge alarm	ACK	Acknowledge alarm
ACN	Alert command	ALC	Cyclic alert list
ALR	Set alarm state	ALF	Alert sentence
BWC	Bearing and distance to waypoint – great circle	ALR	Set alarm state
BWR	Bearing and distance to waypoint – rhumb line	ARC	Alert command refused
CUR	Water current layer – multi-layer water current data	BBM	AIS Broadcast binary message
DBT	Depth below transducer	DDC	Display Dimming Control
DDC	Display Dimming Control	EVE	General event message
DPT	Depth	HBT	Heartbeat supervision sentence
DTM	Datum reference	OSD	Own ship data
GGA	Global positioning system (GPS) fix data	RSD	Radar system data
GLL	Geographic position – latitude/longitude	TLB	Target label
GNS	GNSS fix data	TTD	Tracked Target Data
HBT	Heartbeat supervision sentence	TTM	Tracked target message
HDT	Heading true	VSD	AIS voyage static data
MTW	Water temperature		
MWV	Wind speed and angle		
OSD	Own ship data		
RMB	Recommended minimum navigation information		
RMC	Recommended minimum specific GNSS data		
ROT	Rate of turn		
RTE	Routes		
THS	True heading and status		
VDM	AIS VHF data-link message		
VDO	AIS VHF data-link own-vessel report		
VDR	Set and drift		
VHW	Water speed and heading		
VSD	AIS voyage static data		
VTG	Course over ground and ground speed		
ZDA	Time and date		

Figure 13. Data Sentences (IEC 61162-1/2) for Shipborne RADAR.

Identify targets and threats

According to the shipboard RADAR configuration system in Figure 12, the target/exploitation points for cyber-attacks against shipboard RADARs can be as follows: (i) IEC 61162-1 standard NMEA 0183 interface, while serial data is sending to RADAR from various sensors such as AIS, GPS, or SDME because of the lack of authentication or encryption ; (ii) IEC 61162-450 standard Ethernet interface, while network data is sending to RADAR from ECDIS, second RADAR, or other integrated navigation systems because of the lack of authentication or encryption; (iii) Computer based-RADAR processor unit, while collected data and user command are processed via RADAR software and operating system because of the lack of authentication or encryption, lack of software updates, and lack of vendors' security patch; (iv) Digital visual interface such as ASTERIX standard, while processed data is send to RADAR display unit for users because of the lack of authentication or encryption; (v) RADAR receiver antenna, while surrounding targets send to signal to RADAR receiver antenna because of the allowing to receive high-power noise signal. The possible cyber-attacks considered in this study can exploit these points, and are detailed in Table 1. On the other hand, Cohen et al. (2019) presented various cyber-attacks such as spoofing, reverse engineering, sidelobe eavesdropping, jamming, DoS, and supply chain attack by considering airplanes RADAR systems. Leite Junior et al. (2021) demonstrated an electronic attack against RADAR and ECDIS/AIS which sends attacker's command on the malware injection in the system via removable media or supply chain attack. Longo et al. (2022) showed malware injections and man in the middle attacks for maritime RADAR systems by using the vulnerabilities of ASTERIX and NMEA protocols. Boris Svilicic et al. (2020) demonstrated the vulnerabilities of Windows based RADAR operating and software systems. This study stated that remote code execution and DoS attacks can be performed due to the obtained vulnerabilities.

Table 1. Target Points on the Shipboard RADAR for Cyber-attacks.

IEC 61162-1 standard NMEA 0183 interface	- Malware injection via portable external devices
IEC 61162-450 standard Ethernet interface	- denial-of-service (DoS) attacks - spoofing attacks - man-in-the-middle (MiTM) attacks - Malware injection via remote unauthorized access
Computer based-Processor Unit	- Malware injection via remote and physical unauthorized access - Remote code execution - DoS Arbitrary code injection Supply chain attack
Digital visual interface such as ASTERIX standards	- Malware injection via portable external devices - Internal or external sabotage
RADAR receiver antenna	- Electronic attack via RADAR jammers

Identify assets

The step of identifying context also involves the sub-task of identifying assets.

Assets are entities that the users, owners, or stakeholders in a system desire to protect and do not want to be harmed by cyber-attacks, such as software and hardware, data, or physical objects. The risk analysts typically perform an initial identification of assets based on the information provided by the context of the system and target documentation. To limit the size of the analysis, the number of assets should not grow too large; typically the 4-6 most important assets suffice [43].

By examining the configuration system of RADAR shipboard system, it is understood that RADAR system mainly consists of hardware, software, data, applications and integrated critical systems as an asset. In particular, the data the RADAR gathers comes from multiple IT/OT sources, user data and operational data. This data is processed in in a computing device (including an operating system and specific software) and then sent to the user through a visual, application interface. These are therefore critical, and must be properly managed and protected every step of the way.

According to von Solms & van Niekerk (2013), the security objects of a system or data are based on the triangular of Confidentiality, Integrity, and Availability (CIA). CIA triangular provides to be ensure the cyber security of a system. Confidentiality is about keeping a system's data private that only authorized users and processes should be able to access or modify data. For the integrity, data can be trusted by

keeping it in correct condition, tamper-proof and accurate, authentic, and reliable. For availability object, it should be ensured for the usability object to exclude unauthorized users from a system data, the data should be accessible to authorized users when they need it. Therefore, availability covers to keep networks, systems and devices working. Accordingly, the assets of RADAR system must be protected by considering and ensuring their CIA functions.
According to the context of the shipboard RADAR, the assets to be protected in the RADAR system are as in Table 2.

Table 2. Assets for Shipboard RADAR Systems.

Asset Number	**Assets for the Shipboard RADAR system**
A1	Confidentiality of the serial data sent to the RADAR
A2	Integrity of the serial data sent to the RADAR
A3	Availability of the RADAR system
A4	Integrity of the RADAR data
A5	Confidentiality of the RADAR system
A6	Confidentiality of the network data sent to the RADAR
A7	Integrity of the network data sent to the RADAR

4.2. Identify Risks

All in all, the known vulnerabilities of ship RADAR systems, the threats caused by these vulnerabilities, and the undesirable consequences that may occur in the event of these threats are created as in Table 3 with the help of the literature and expert opinions in the maritime cyber field. In this study, five experts opinions are utilized to (i) check and control the created context, assets, targets, threats, vulnerabilities, threat scenarios, unwanted incidents, and risks for shipboard RADAR system, (ii) determine the likelihood and consequence of the determined risks, (iii) evaluate them, and (iv) suggest treatment ways for risky cases. Experts consist of computer, electronics, and maritime transportation engineers, and they are members of the laboratory research group that conducts academic and sectoral studies in the field of maritime cyber security. Their average experience level is 7 years. The three of them are women, and the others are men, and they are all members of the laboratory research group that conducts academic and sectoral studies in the field of maritime cyber security. This laboratory is one of the leading laboratories in the field of maritime cyber security in the world.

The completed CORAS threat assessment for shipboard RADAR system is as in Figure 14. This figure provides a holistic view in terms of elements of cyber-attacks for RADAR. It is important to note that, more than one cyber-vulnerability can lead to the same unwanted incident and affect the same asset.

Table 3. CORAS Risk Management Functions for Shipboard RADAR Cyber Security.

Scenarios	Who/What causes it?	What makes this possible?	How?	What is the incident?	What does it harm?
	Threat	**Vulnerability**	**Threat Scenarios**	**Unwanted Incident**	**Asset**
Scenario 1	Man-in-the-middle attack via physical unauthorized acc.	Due to the lack of authentication on the NMEA 0183 and digital visual interface such as ASTERIX standards	Attacker monitors the serial data on the NMEA 0183 or on the digital visual interface via an external portable malicious device, which can be used for man-in-the middle attacks and only used for monitoring the traffic. [T1]	RADAR serial data traffic is monitored and inspected by the attacker.	Confidentiality of the serial data sent to the RADAR
Scenario 2	Malware injection to serial data traffic via physical unauthorized acc.	Due to the lack of authentication and encryption on the NMEA 0183 and digital visual interface such as ASTERIX standards	Attacker uses external portable malicious device, which includes malware and used for man-in-the-middle attack, on the NMEA 0183 or digital visual interface. By this way, RADAR system is infected by malware via physically access.[T2]	Serial data sent to RADAR is deleted or modified.	Integrity of the serial data sent to the RADAR
				RADAR system is crashed.	Availability of the RADAR system
Scenario 3	Malware injection to RADAR processor Unit via physical unauthorized acc.	Due to the lack of authentication on RADAR Processor Unit software	Attacker uses external portable malicious device such as USB stick, which includes malware, on the RADAR processor unit. By this way, RADAR system is infected by malware via physically access.[T3]	RADAR data is deleted or modified.	Integrity of the RADAR data
				RADAR system is crashed.	Availability of the RADAR system
Scenario 4	Man-in-the-middle attack via ARP spoofing as a remote unauthorized acc.	Due to the lack of authentication and encryption on the Ethernet interface (IEC 61162-450 standard)	Attacker monitors the network data on the Ethernet via ARP spoofing as a man-in-the middle attacks. By this way, attacker gains access to the RADAR network data and transmit false data to the RADAR by impersonating other devices, which send network data to the RADAR. [T4]	RADAR network data traffic is monitored and inspected by the attacker	Confidentiality of the network data sent to the RADAR
				Network data sent to RADAR is deleted or modified.	Integrity of the network data sent to the RADAR
				RADAR system is crashed.	Availability of the RADAR system
Scenario 5	Remote code execution	Due to the lack of authentication on RADAR software	Attacker scans the RADAR processor unit across local area network (LAN) seeking known vulnerabilities that may support a successful attack. Once a targeted vulnerability is identified, attacker performs the exploit to gain access. When the attacker is in, attacker executes remote malicious code on the RADAR processor unit software across local area network (LAN) in order to exfiltrate data, perform detail surveillance, and disrupt service. [T5]	Attacker runs remote code to navigate and assess the RADAR data.	Confidentiality of the RADAR system
				RADAR data is deleted or modified	Integrity of the RADAR data
				RADAR system is crashed.	Availability of the RADAR system

Scenario 6	Arbitrary code injection via physically or remotely unauthorized access	Due to the lack of authentication RADAR software or operating system, lack of update for RADAR processor unit software, lack of vendor's security patch for RADAR processor unit software	Attacker gains control over the instruction pointer of the RADAR processor unit and has privilege escalation exploit via arbitrary code injection by unauthorized access with physically or logical access. RADAR processor unit includes user/operator-provided data via RADAR control unit (keyboard control unit and trackball control unit) within commands executed in the shell of the computer running the program. The command can be modified or stopped by attacker-provided data and shell commands, which are selected by the attacker is run. Accordingly, RADAR processor unit does not have ability to discriminate between injected code and data, therefore malicious code is hided like innocuous input data. [T6]	Attacker runs arbitrary code to navigate and assess the RADAR data.	Confidentiality of the RADAR system
				RADAR system is crashed.	Availability of the RADAR system
Scenario 7	Denial of service (DoS)	Due to the industrial control systems with including a low tolerance to bogus traffic or connected via low bandwidth links which can be easily saturated	Attacker creates a denial-of-service (DoS) attack on the RADAR system by sending specially crafted requests to the server. (For instance, RADAR system software (e.g. The Microsoft Server Message Block 1.0 (SMBv1)) permits denial of service when crafted requests by an attacker sends to the server. On the other side, attacker flood RADAR network with network packets to produce a DoS attack. [T7]	RADAR system is crashed.	Availability of the RADAR system
Scenario 8	Electronic attack via RADAR jammers	Due to the function of enabling to blind the RADAR via high-power noise or generating fake targets with false location	Radar jammers are a type of electronic attack technology that either produce fake targets with false location or blind the RADAR via high-power noise. Accordingly, the range and sensitivity of the RADAR receiver antenna decreases in consequence of increasing a noise floor of the RADAR receiver by transmitting high-power noise. [T8]	Attacker either blinds a radar or generate false targets	Confidentiality of the RADAR system
					Integrity of the RADAR system

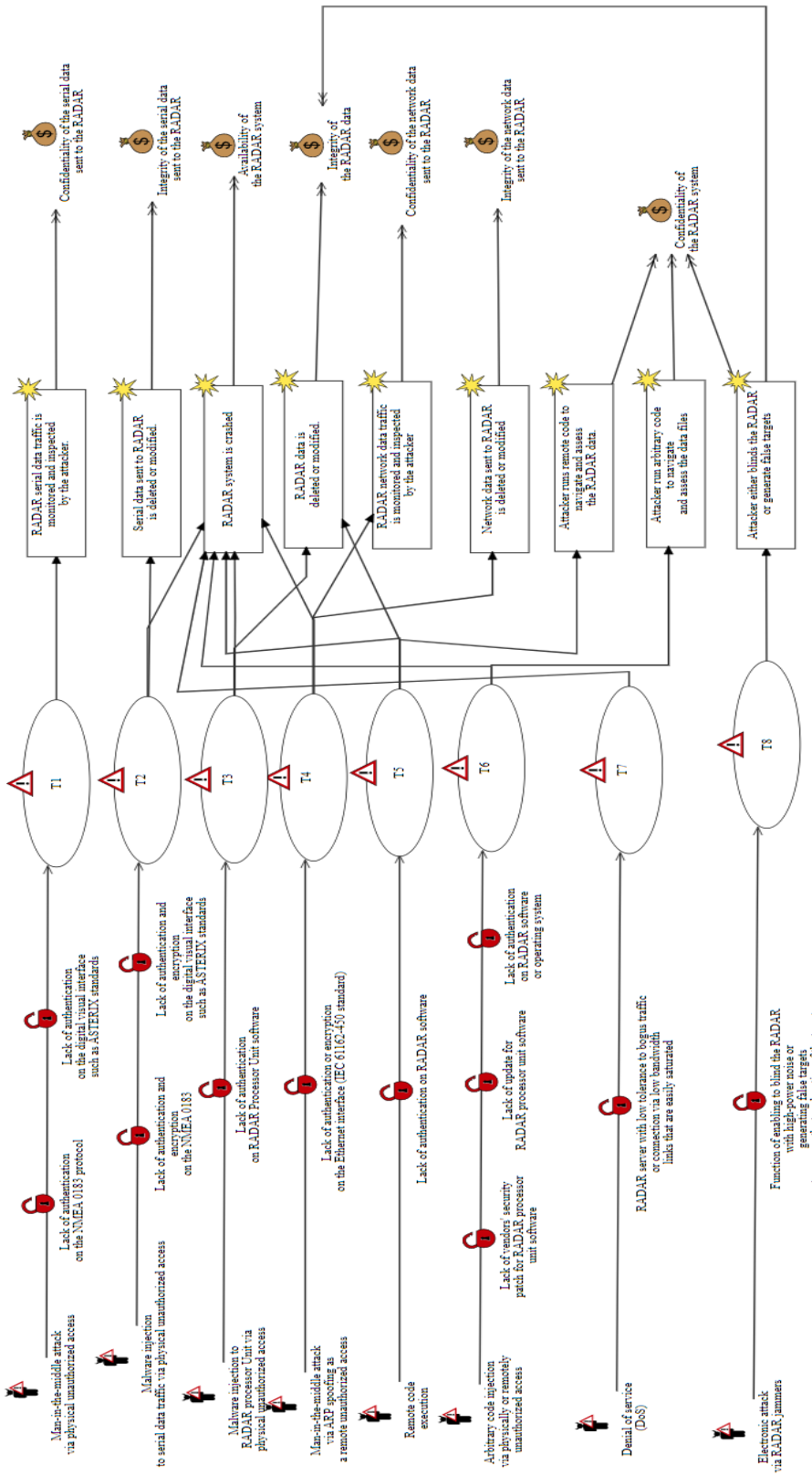


Figure 14. Threat Scenarios for Shipboard RADAR Systems.

4.3. Analyze Risks

Risk evaluation criteria

The purpose of this step is to specify what level of risk the owner of the ship, bridge officer onboard as a user, and other stakeholders are able to accept, via considering what losses can be tolerated over a given period of time.

The level of risk is defined as the overall effect of likelihood, which expresses the probability of the occurrence of this risk, and the consequence, which expresses what the loss is for the asset affected by the risk. The values of consequence and likelihood can be defined as quantitative values such as amount of money lost and statistical probability, respectively. On the other hand, the measured values are not generally applicable/suitable for the assets under consideration or the require data are not available to calculate the correct values. In this case, qualitative values for consequence and likelihood, such as "low", "medium", and "high", are used through expert opinion [43]. In this context, utilizing the sample value definition table suggested by Braber et al., (2006), the values used for likelihood and consequence for the shipboard RADAR system are documented by the experts in a value definition table as in Table 4 for this study.

Table 4. Risk Evaluation Criteria for Shipboard RADAR Created by Experts.

Value Type	Value	Definition	Reference Point
Likelihood	Rare	Less than once per ten years	[43]
	Unlikely	Less than once a year	
	Possible	About once a year	
	Likely	2-5 times a year	
	Certain	More than 5 times a year	
Consequence	Insignificant	No impact on RADAR operation, minor delays	E.g. when only RADAR data traffic is monitored or range of [0%,1%> of RADAR data are influenced
	Minor	Loss of a part of RADAR data	E.g. when specific RADAR data such as only some of serial data, only AIS data belongs to one target is deleted or modified during monitoring RADAR data traffic. Or range of [1%,10%> of RADAR data are influenced
	Moderate	Loss of significant part of RADAR data	E.g. when huge part of specific RADAR data such as only some of serial data or only network data, or only AIS data belongs to much more one target is deleted or modified during monitoring RADAR data traffic. Or range of [10%,20%> of RADAR data are influenced
	Major	Loss of whole part of RADAR data	E.g. when all RADAR data such as both network and serial data is modified or deleted. Or range of [20%,50%> of RADAR data are influenced
	Catastrophic	Out of RADAR operation	E.g. when RADAR is entirely shut down. Or range of [50%,100%> of RADAR data are influenced

There are various type of risk function table, which includes the different risk tolerance level, in the CORAS-based researches [43], [45], [46]. However, for RADAR cyber risk security, experts assent the risk tolerance matrix in Figure 15, which is suggested by Lund et al. (2011). Accordingly, the risks with green color can be acceptable, but the risks in other color should be evaluated and implemented treatments.

RISK OUTCOME
Low
Moderate
Significant
High

Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

Figure 15. Risk Tolerance Matrix (Lund et al. 2011).
(Green: Acceptable, Other: Evaluate Risk)

Estimate Risks

Experts in the field of maritime cyber-security evaluate the likelihood of the threats in Table 5 and provided severity levels of the unwanted incidents in the "Consequence" column in Table 6. After that, to identify the risk category of unwanted incidents, combined likelihood values of them are determined by aggregating the likelihood values of the threat scenarios that affect the same incident. The aggregation method is implemented by referencing Braber et al. (2006)'s study about the CORAS model-based method for security risk analysis. Accordingly, the likelihood values of each threat scenario is aggregated linearly and experts checked it before deciding the final value. However, this method can be resulted huge values when there is more than one threat scenario exit. For this reason, it is considered that calculating the average of the likelihood values of the threat scenarios that affect the same incident provides better results than linearly aggregation method. Finally, by intersecting the final likelihood and consequence values in the risk matrix table, it is determined whether the risks of the unwanted incidents are acceptable or should be evaluated.

Table 5. Likelihood of Threat Scenarios.

Who/What causes it?	**What makes this possible?**	**How?**		**What is the possibility of frequency of the threat scenario?**
Threat	**Vulnerability**	**Threat Scenarios**	**Threat Number**	**Likelihood**
Man-in-the-middle attack via physical unauthorized access	Due to the lack of authentication on the NMEA 0183 and digital visual interface such as ASTERIX standards	Attacker monitors the serial data on the NMEA 0183 or on the digital visual interface via an external portable malicious device, which can be used for man-in-the middle attacks and only used for monitoring the traffic.	T1	Unlikely
Malware injection to serial data traffic via physical unauthorized access	Due to the lack of authentication and encryption on the NMEA 0183 and digital visual interface such as ASTERIX standards	Attacker uses external portable malicious device, which includes malware and used for man-in-the-middle attack, on the NMEA 0183 or digital visual interface. By this way, RADAR system is infected by malware via physically access.	T2	Unlikely
Malware injection to RADAR processor Unit via physical unauthorized access	Due to the lack of authentication on RADAR Processor Unit software	Attacker uses external portable malicious device such as USB stick, which includes malware, on the RADAR processor unit. By this way, RADAR system is infected by malware via physically access.	T3	Possible
Man-in-the-middle attack via ARP spoofing as a remote unauthorized access	Due to the lack of authentication and encryption on the Ethernet interface (IEC 61162-450 standard)	Attacker monitors the network data on the Ethernet via ARP spoofing as a man-in-the middle attacks. By this way, attacker gains access to the RADAR network data and transmit false data to the RADAR by impersonating other devices, which send network data to the RADAR	T4	Possible
Remote code execution	Due to the lack of authentication on RADAR software	Attacker scans the RADAR processor unit across local area network (LAN) seeking known vulnerabilities that may support a successful attack. Once a targeted vulnerability is identified, attacker performs the exploit to gain access. When the attacker is in, attacker executes remote malicious code on the RADAR processor unit software across local area network (LAN) in order to exfiltrate data, perform detail surveillance, and disrupt service.	T5	Possible
Arbitrary code injection via physically or remotely unauthorized access	Due to the lack of authentication RADAR software or operating system, lack of update for RADAR processor unit software, lack of vendor's security patch for RADAR processor unit software	Attacker gains control over the instruction pointer of the RADAR processor unit and has privilege escalation exploit via arbitrary code injection by unauthorized access with physically or logical access. RADAR processor unit includes user/operator-provided data via RADAR control unit (keyboard control unit and trackball control unit) within commands executed in the shell of the computer running the program. The command can be modified or stopped by attacker-provided data and shell commands, which are selected by the attacker is run. Accordingly, RADAR processor unit does not have ability to discriminate between injected code and data, therefore malicious code is hided like innocuous input data. [T6]	T6	Possible
Denial of service (DoS)	Due to the industrial control systems with including a low tolerance to bogus traffic or connected via low bandwidth links which can be easily saturated	Attacker creates a denial-of-service (DoS) attack on the RADAR system by sending specially crafted requests to the server. (For instance, RADAR system software (e.g. The Microsoft Server Message Block 1.0 (SMBv1)) permits denial of service when crafted requests by an attacker sends to the server. On the other side, attacker flood RADAR network with network packets to produce a DoS attack. [T7]	T7	Likely
Electronic attack via RADAR jammers	Due to the function of enabling to blind the RADAR via high-power noise or generating fake targets with false location	Radar jammers are a type of electronic attack technology that either produce fake targets with false location or blind the RADAR via high-power noise. Accordingly, the range and sensitivity of the RADAR receiver antenna decreases in consequence of increasing a noise floor of the RADAR receiver by transmitting high-power noise. [T8]	T8	Likely

Table 6. Risk Estimation Results.

Asset	Threat Scenarios	Risk	Unwanted Incidents (UI)	Combined Likelihood	Final Likelihood	Consequence	Risk of UI
Confidentiality of the serial data sent to the RADAR	T1	R1	RADAR serial data traffic is monitored and inspected by the attacker.	Unlikely	Unlikely	Insignificant	Acceptable
Integrity of the serial data sent to the RADAR	T2	R2	Serial data sent to RADAR is deleted or modified.	Unlikely	Unlikely	Moderate	Unacceptable
Availability of the RADAR system	T2	R3	RADAR system is crashed.	(Unlikely+4* Possible+Likely)/6=Possible	Possible	Catastrophic	Unacceptable
	T3						
	T4						
	T5						
	T6						
	T7						
Integrity of the RADAR data	T3	R4	RADAR data is deleted or modified.	(Possible+Possible)/2=Possible	Possible	Major	Unacceptable
	T5						
Confidentiality of the network data sent to the RADAR	T4	R5	RADAR network data traffic is monitored and inspected by the attacker	Possible	Possible	Insignificant	Acceptable
Integrity of the network data sent to the RADAR	T4	R6	Network data sent to RADAR is deleted or modified.	Possible	Possible	Moderate	Unacceptable
Confidentiality of the RADAR	T5	R7	Attacker runs remote code to navigate and assess the RADAR data.	Possible	Possible	Moderate	Unacceptable
Confidentiality of the RADAR	T6	R8	Attacker runs arbitrary code to navigate and assess the RADAR data.	Possible	Possible	Moderate	Unacceptable
Integrity of the RADAR	T8	R9	Attacker either blinds a radar or generate false targets	Likely	Likely	Catastrophic	Unacceptable

4.4. Evaluate Risks

The results of the risk categories for unwanted incidents are shown in Table 7. The dark areas in Table 7 show that the risks of the unwanted incidents should be evaluated, and some mitigations should be developed for them. Experts decide that the risks that affect only the confidentiality of the serial and network data, which sent to the RADAR, can be considered as acceptable risk for RADAR cyber security in reasonable perspective. Because these risks include only assessing and monitoring the data of the RADAR and the RADAR data has already monitored via other open sources such as some online AIS data providers on the websites. Only R1 and R5 can be acceptable risks, so they do not require treatment, but for more security and for not open backdoor to other attack scenarios. The mitigations for them are also presented in this study.

Table 7. Risk Evaluation Matrix with Risks.

Frequency/Consequence	Insignificant	Minor	Moderate	Major	Catastrophic
Rare					
Unlikely	R1		R2		
Possible	R5		R6-R7-R8	R4	R3
Likely					R9-R10
Certain					

4.5. Treat Risks

The final activities in the RADAR cyber security analysis are mitigation identification. All risks found unacceptable are evaluated to find ways to reduce them. The contribution of a treatment should provide to let fall the likelihood and/or consequence of an unwanted event. Accordingly, the threat-risk relationship is shown as a well-design in IEC 62443-3 standard (2008) as in Figure 16.

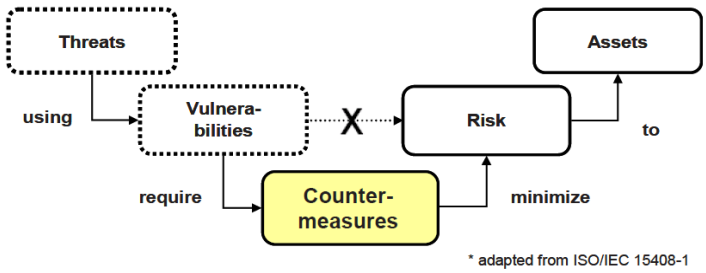


Figure 16. Threat-risk Relationship [47].

In this study, for identifying the treatments systematically for RADAR cyber security, the three main pillars for the cybersecurity (i.e., technology, people, and process) offered by DNV-GL (2020) are considered. It is important to cognized that an exhaustive cyber security framework is based on a cyber security management plan (CSMP) under the safety management systems (SMS) onboard ships that manage the activities and behavior of people onboard according to procedures and policies and sets the doctrines for the functionality of technical security barriers. The CSMP should also provide that cyber security risks are systematically and adequately managed that includes identifying and evaluating and reducing them to an acceptable level. Reducing the risk to a tolerable level is carried through enforcing barriers and mitigations. Barriers can include technical (such as firewall) or organizational (such as awareness training or procedures). Mitigations are much more related to the skill of the organization (economic skill, or investments for training) to response to cyber-attacks and to recovery the system. If the technical barriers are nor managed and supported by procedures and policies in the CSMP via defining the responsibilities and roles of people for all cyber security activities, they are unlikely to be effective.

In this context, in order to develop the integration of the technical cyber security mechanisms, the responsibilities of sides such as crews onboard ships, ship owners and managers, and vendors and suppliers, and the policies for cybersecurity onboard ships, both DNV-GL class guideline for cyber secure [48], international security standards (IEC/PAS 62443-3, 2008; ISO/IEC 27001, 2017; ISO/IEC 27033-3, 2010) and other code of best practices for maritime cyber security [51]–[53] are taken as references. As a result, mitigation solutions for RADAR cyber security is developed by considering the integration of technology, people, and processes in addition defining them according to Institute of Standards and Technology (NIST) Cyber Security Framework (Identify –I, Protect –P, Detect – D, Respond – R, Recovery – Rec) [54] as in Table 8 The RADAR cyber security operations are determined by considering both overall cyber security implementations on the ships and specific to RADAR cyber risks.

Table 8. Shipboard RADAR Cyber Treatments.

RADAR Cyber Security Operations			
Treatment Group	**NIST Framework Category**	**Treatment Number**	**Treatment**
Process			
T1 Policies and procedures in the context of cyber security management plan (CSMP) under safety management system (SMS)	I	1.1	Shore-based Company Cyber Security Officer, who is responsible for the security of all information and operational technology including RADAR, is defined in CSMP.
	I	1.2	Ship-based Cyber Security Officer, who is responsible for the security of all information and operational technology including RADAR, is defined in CSMP.
	I	1.3	The contractual agreement between ships' officers and their employer, which states their and the companies' responsibilities for information security onboard, is provided in the shipping company.
	I	1.4	The agreement between vendors / suppliers and shipping company, which include cybersecurity requirements and the responsibilities they need to adhere to in the delivery of their service, is provided.
	I-P	1.5	A risk assessment policy for RADAR cyber security including such as CORAS framework processes is defined in the CSMP onboard a ship and implemented onboard ships.
	I-P	1.6	The risk management process is established and managed for RADAR by integrating all responsibilities of ship, company, and third-parties.
	I-P	1.7	A checklist for RADAR cyber security is identified in CSMP and used onboard a ship. (This table can be used as a checklist for RADAR cyber security onboard ships)
	I-R	1.8	An information sharing policy about reporting any cyber near misses or incidences, which includes organizational communication and data flows between ships, shipping companies, and third parties, is defined and used.
	I-R	1.9	A response plan for RADAR cyber security is defined in CSMP and executed during or after a cyber-attack. If it is require, the response plan also cover third parties.
	I-Rec	1.10	A recovery plan for RADAR cyber security is defined in CSMP and executed after a cyber-attack. (Recovery plan includes skill and competence of shipping company supply and ship in order to recover the damaged asset, system, hardware, software, or data. For instance, in any case of DoS attack to the RADAR system, it is defined in the recovery plan that what ways and how much time are required to restore the system to its previous state. It generally depends on the skill of the shipping company IT support or exist personnel on boars ship who is responsible for hardware and software maintenance, such as electro technical officer. If it is require, the recovery plan also covers third parties.)
	I-R-Rec	1.11	A policy for annual physical security inspection, audit or survey for hardware and software maintenance of RADAR is defined in CSMP. After inspection, audit, or survey, the reports of them are kept in the ship's documentation records. The reports are analyzed in the context of defined risk assessment policy. Accordingly, defined risk management process, the response plan, and the recovery plan are updated.
	I-R-Rec	1.12	A record policy for any cyber security suspicious activity or incidence is defined in CSMP and implemented in any noticed suspicious cyber activity. The records are analyzed in the context of defined risk assessment policy. Accordingly, defined risk management process, the response plan, and the recovery plan are updated.

People			
T2 Cybersecurity awareness and training in the context of CSMP under SMS	P	2.1	Company policies in the CSMP require adequate cyber security awareness and training for all users onboard a ship to perform and understand their information security-related duties and responsibilities, including RADAR to bridge officers who they will employ.
	I-P	2.2	Drill scenarios for cyber security onboard ships including RADAR cyber security are identified and carried out regularly in order to keep the active and update cyber knowledge of ship personnel.
	P	2.3	The international policies, rules, regulations, and law for RADAR cyber security are encouraged by the company to be adopted and implemented by the ship.
T3 Navigation responsibilities of bridge officers with the cyber knowledge in the context of CSMP under SMS	D	3.1	Officers use cross-checking methods to confirm the accuracy of targets displayed on the RADAR screen (e.g. from ECDIS, visual fix, paper charts if exist or via communication) against any manipulation on the RADAR targets by attackers.
	D	3.2	Officers check the AIS data of the targets and GPS information on the RADAR screen via controlling AIS and GPS devices against any modification AIS or GPS data on the RADAR by the attackers.
	D	3.3	Officers check the ECDIS chart overlay function on the RADAR screen via controlling ECDIS device.
T4 Relationship between vendors, shipping company and ship in the context of CSMP under SMS	P	4.1	Subsequent updates by RADAR manufacturers for the operating system, processor unit or software used own RADAR are carried out only after appropriate testing, and there are release notes for masters and navigating officers to distinguish any changes.
	D	4.2	If manufacturers detect any inconsistency in RADAR performance, they issue technical bulletins to all ship owners/operators who manage ships equipped with their systems to highlight issues.
	R-Rec	4.3	The manufacturers' technical bulletin includes mitigating measures for masters and navigating officers with future plans to correct the inconsistencies.
	D-R	4.4	Ship owners/operators communicate with RADAR manufacturers and ensure that relevant information is shared with ships under management immediately and acted upon with necessary mitigations according to Original Equipment Manufacturer (OEM) technical bulletins.
	Rec	4.5	Any noted defect or inconsistency in RADAR performance are promptly reported to the RADAR manufacturer, with appropriate notices to Flag State Administrations or recognized organization.
	D-Rec	4.6	RADAR manufacturers issue safety bulletins or software upgrades as soon as an error or inconsistency in RADAR-related data or functionality is detected by a navigating officer. The operating system is updated with a security patch sent by the manufacturer.
Technical			
T5 Control physical access to devices	P	5.1	An access control system such as identified id card or physical key is installed for the room, which taken place the servers that RADAR connects. Navigating officers and master have the authorization for this room.
	P	5.2	RADAR work station central units (processor unit) is in locked cabin on the bridge.
	P	5.3	All the network cable and sockets connected to RADAR is protected access.
T6 Network segregation and	I-P	6.1	A map for RADAR network flow is established as in Figure 12 in the SMM.
	P	6.2	The network segmentation for RADAR network flow is provided for separating network from other critical ship system network or infrastructure network.
	I-P	6.3	The IP-addresses and network communication protocols and data flows needed for RADAR system is identified to function properly.

Firewall configuration	P	6.4	RADAR network flow is filtered by a firewall. Firewall policies is analysed and ensured that only necessary communication is allowed to and from the assets connected to RADAR
	P-D-Rec	6.5	Firewalls with a default-deny configuration is set up that blocks and logs all non-approved network communication. The anomalies are detected by tracing and analyzing the rejected traffic.
T7 Management of portable devices and media	P	7.1	USB ports on RADAR system are deactivated.
	I-P	7.2	If USBs are needed to use for maintenance or vendors' updates, the type of media is defined in CSMP and only clean portable devices such as pre-scanned and pre-defined ones in the whitelisting application are used for these purpose.
	P	7.3	If it is possible, software restriction policies are activated on the RADAR system against non-defined portable devices functions.
T8 Account management (logical access)	I-P	8.1	Default admin password on vessel systems that RADAR connects is created such as for serial-to-IP converters, and networks that connects RADAR.
	I-P	8.2	User authentication policy for RADAR onboard ships is defined in CSMP.
	P	8.3	Strong passwords, which comply with an international policy, such as NCCIC/US-CERT's password policy, are used for the authentication on the RADAR and admin access.
	P	8.4	The passwords are changed regularly.
T9 Configuration hardening	P	9.1	Remote configuration and programming modes on RADAR systems are deactivated.
	I-P	9.2	Non-Disclosure / remote access agreements that outline the company requirements for accessing vessel networks (VPN connections, personal users, strong passwords/MFA, anti-malware protection on computers, etc.) are created when third-party and supplier need to access remotely to vessel networks that RADAR connects.
	P	9.3	Firewall policies to grant third-parties and internal users access remotely to the vessel network they need are updated.
T10 Management of event logs and alarms	D	10.1	If the RADAR operating systems and software ("Windows Event", text file, etc.) permit that traceability functions on the RADAR are activated.
T11 Malware protection	P	11.1	The RADAR vendors, which provides security patches for own operating system and anti-malware protection system, is preferred by the shipping companies.
	P	11.2	The malware protection tools on the RADAR system are regularly and automatically updated.
T12 Network Authentication and Encryption of the data	P	12.1	For the network data package between RADAR and other assets, data encryption methods, which can be integrated with specifically on the NMEA 0183 protocol, is used. For instance, one protocol that can be incorporated in existing marine network protocols is the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol, which is a variation on traditional asymmetric cryptography. Or the network protocol for RADAR can be integrated with such as encrypted using TLS / SSL protocols
	P	12.2	In addition to traditional encryption method, hashing method is also used for ensuring the integrity of the data.
T13 RADAR Antenna Set Up	P	13.1	Shipping companies prefer the RADAR with Dynamic Frequency function, which could operate by changing its frequency before transmission, making jammers ineffective, in theory.

4.6. Results

The security control table for RADAR cyber security in Table 8 contains the key points for a cyber security infrastructure such as technical protection and detection dynamics for RADAR cyber-attacks, identification of process and documentation on RADAR cyber security, requirements of the users and responsible people to protect and detect the RADAR cyber-attacks, skill of the ship and shipping company to response and recover the RADAR cyber-attacks. Each treatment is evaluated for each cyber scenario. The proper mitigations for each scenario are specified in Table 9. The mitigations are categorized as identification of policy and process and technical protection items in Table 8 are specified as a preventative barrier against cyber-attacks. The treatments categorized as detection dynamics, response or recovery for RADAR cyber-attacks in Table 8 are specified as a mitigation that works to protect systems during or post-incident.

In this context, CORAS mitigation framework is created for each scenario according to Table 9 in from Figure 17 to Figure 24. For instance, if scenario 3 in Figure 19 is examined as a scenario, which includes the most treatments, it is seen that there is a cyber-attack that includes malware injection to RADAR processor unit via physical unauthorized access. In this scenario, attacker uses external portable malicious device such as USB stick, which includes malware, on the RADAR processor unit. Through this infection vector, the RADAR system is infected by malware through physically access due to the lack of protected physical access to the RADAR processor unit, open ports for external portable device, lack of authentication on the processor unit, lack of RADAR software and operating system updates, and lack of policy and training for the ship personnel. These vulnerabilities shown in Figure 19 are created by considering them hierarchically. It means that firstly attacker needs to have physical access to the RADAR processor unit. To prevent that, it is proposed that RADAR processor unit should be in locked cabin in the bridge. Before that, some security control functions state that an access control system with ID card or password for the bridge should exist. However, according to the International Ship and Port Facility Security (ISPS) code, ship bridges have already required to be locked in the ports. In general, they are locked via a physical key. Access control system with ID card or password can be also integrated to the ship bridges providing that the system can be deactivated while ship is underway on the water. Otherwise, this security control function may prevent the quick action in the case of other maritime accidents such as ship collision, grounding or sinking. Therefore, based on what is explained in this example, it is important to state for this study that, although a holistic approach for RADAR cyber security is tried to be considered, only cyber security control functions have been tried to be presented, if the partial or full security measures required by the contracts in force are adopted by ships. Therefore, it is assumed that ships have already adopted a bridge access control system. Moreover, it is also important to state that bridge access of the attackers can only happen, if they are authorized people in the port such as surveyor, inspector for port state control, responsible people for cargo handling and they can be on the ship for one of these purposes. In these cases, attackers can use them as an insider threat and these people may be aware of this situation or not.

If a human threat has physical access to the bridge in some way, if the processor unit is not locked in a cabin, the second physical access to the target point (RADAR processor unit) would happen. If the access ports for portable devices on the processor unit are not deactivated, an insider threat can inject the malware to the RADAR processor unit via USB device. If the ports on the processor unit cannot be deactivated for maintenance or vendors' updates, alternatively, the only pre-scanned and unique portable media should be used on the processor and defined in the whitelisting application. The rest of the portable media should be rejected by the system software. Additionally, if it is possible, the authorization and authentication should be provided on the processor unit via use password. This can prevent that attacker installs and runs malware on the processor unit. If the malware is set up on the processor unit in some way, as the final protection step, if it is possible, malware protection tools on the software and operating system should be exist. If they are available, the RADAR vendors, which provides security patches for own operating system and anti-malware protection system, is preferred by the shipping companies. The malware protection tools on the RADAR system should be regularly and automatically updated. For this, subsequent updates by RADAR manufacturers for the operating system, processor unit or software should be carried out, but only after appropriate testing. Additionally, there should be release notes for masters and navigating officers to distinguish any changes. Finally, all these actions

should be identified as a policy or process for RADAR cyber security in CSMP and all ship personnel, responsible people for cyber security of the RADAR and ship' general cyber security on ships and in shipping companies should have adequate cyber security education training and awareness to understand and implement properly all these activities. These two security control functions should take place in the beginning of the Figure.

As a result, if these mentioned barriers are implemented for RADAR cyber security by ships, shipping companies, and RADAR vendors, the threat vectors will be significantly reduced. However, if attacker overcomes these barriers in some way, malware function runs on the RADAR processor unit. Hereby, either RADAR data is deleted and modified RADAR system is crashed. In this case, navigation officers on the bridge should have knowledge and responsibilities in terms of integration of cyber security and navigation rules. Accordingly, they should use cross-checking methods to confirm the accuracy of targets displayed on the RADAR screen (e.g. from ECDIS, visual fix, paper charts if exist or via communication), check the AIS data of the targets and GPS information on the RADAR screen via controlling AIS and GPS devices, and check the ECDIS chart overlay function on the RADAR screen via controlling ECDIS device against any manipulation on the RADAR targets by attackers. These activities help the human element to detect the cyber-attacks affecting RADAR display. If they can be detected, response and recover activities for RADAR cyber security can be implemented. For instance, if the RADAR operating systems and software ("Windows Event", text file, etc.) permit that traceability functions on the RADAR should be activated. Then, the log of it is analyzed to understand the reason of the cyber-attack. Ship owners/operators should communicate with RADAR manufacturers and ensure that relevant information is shared with ships under management immediately and acted upon with necessary mitigations according to Original Equipment Manufacturer (OEM) technical bulletins. Any noted defect or inconsistency in RADAR performance should be promptly reported to the RADAR manufacturer, with appropriate notices to Flag State Administrations or recognized organization. The manufacturers' technical bulletin should include mitigating measures for masters and navigating officers with future plans to correct the inconsistencies. RADAR manufacturers should issue safety bulletins or software upgrades as soon as an error or inconsistency in RADAR-related data or functionality is detected by a navigating officer. The operating system should be updated if it was the source of the vulnerability, with a security patch sent by the manufacturer.

All the above activities should be identified in CSMP as a detection, response and recovery policy. If this scenario is resulted the unwanted incident such a system crashing, the recovery policy should be specified in detail according to the IT skill of the shipping company and the ship. In this step, it is necessary to define how to return the system and the maximum possible time for this, which differ according to the IT personnel skill, IT potentiality and availability of the shipping company, the skill of the ship personnel (For instance, shipping companies should provide an electro technical officer, who is responsible for the hardware and software security and maintenance according to the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), on their ships).

Similarly, the mitigation solutions for all scenarios should be created by considering each vulnerability points, target points, detectability points, and response and recovery activities step-by step hierarchically.

Table 9. Treatments for Each RADAR Cyber Scenario.

Scenarios	Who/What causes it?	What makes this possible?	How?	What is the incident?	What does it harm?	What is the security control mechanisms?	
	Threat	Vulnerability	Threat Scenarios	Unwanted Incident	Asset	Treatments as a Barriers	Treatments as a Mitigations
Scenario 1	Man-in-the-middle attack via physical unauthorized acc.	Due to the lack of authentication on the NMEA 0183 and digital visual interface such as ASTERIX standards	Attacker monitors the serial data on the NMEA 0183 or on the digital visual interface via an external portable malicious device, which can be used for man-in-the middle attacks and only used for monitoring the traffic.	RADAR serial data traffic is monitored and inspected by the attacker.	Confidentiality of the serial data sent to the RADAR	T1(I-P)-T2-5.3-7.1-7.2-12.1-12.2	N/A
Scenario 2	Malware injection to serial data traffic via physical unauthorized acc.	Due to the lack of authentication and encryption on the NMEA 0183 and digital visual interface such as ASTERIX standards	Attacker uses external portable malicious device, which includes malware and used for man-in-the-middle attack, on the NMEA 0183 or digital visual interface. By this way, RADAR system is infected by malware via physically access.	Serial data sent to RADAR is deleted or modified.	Integrity of the serial data sent to the RADAR	T1(I-P)-T2-5.3-7.1-7.2-12.1-12.2	T1(R-Rec)-3.2
				RADAR system is crashed.	Availability of the RADAR system	T1(I-P)-T2-5.3-7.1-7.2-12.1-12.2	T1(R-Rec)
Scenario 3	Malware injection to RADAR processor Unit via physical unauthorized acc.	Due to the lack of authentication on RADAR Processor Unit software	Attacker uses external portable malicious device such as USB stick, which includes malware, on the RADAR processor unit. By this way, RADAR system is infected by malware via physically access.	RADAR data is deleted or modified.	Integrity of the RADAR data	T1(I-P)-T2-4.1-5.2-T7-8.2-8.3-8.4-T11	T1(R-Rec)-3.2-3.3-4.2-4.3-4.4-4.5-4.6-T10
				RADAR system is crashed.	Availability of the RADAR system	T1(I-P)-T2-4.1-5.2-T7-8.2-8.3-8.4-T11	T1(R-Rec)-4.2-4.3-4.4-4.5-4.6
Scenario 4	Man-in-the-middle attack via ARP spoofing as a remote unauthorized acc.	Due to the lack of authentication and encryption on the Ethernet interface (IEC 61162-450 standard)	Attacker monitors the network data on the Ethernet via ARP spoofing as a man-in-the middle attacks. By this way, attacker gains access to the RADAR network data and transmit false data to the RADAR by impersonating other devices, which send network data to the RADAR	RADAR network data traffic is monitored and inspected by the attacker	Confidentiality of the network data sent to the RADAR	T6-T8-T9-T12	T1(R-Rec)-T6.5
				Network data sent to RADAR is deleted or modified.	Integrity of the network data sent to the RADAR	T6-T8-T9-T12	T1(R-Rec)-3.3-T6.5
				RADAR system is crashed.	Availability of the RADAR system	T6-T8-T9-T12	T1(R-Rec)-T6.5
Scenario 5	Remote code execution	Due to the lack of authentication on RADAR software	Attacker scans the RADAR processor unit across local area network (LAN) seeking known vulnerabilities that may support a successful attack. Once a targeted vulnerability is identified, attacker performs the exploit to gain access. When the attacker is in, attacker executes remote malicious code on the RADAR processor unit software across local area network (LAN) in order to exfiltrate data, perform detail surveillance, and disrupt service.	Attacker runs remote code to navigate and assess the RADAR data.	Confidentiality of the RADAR system	T1(I-P)-T2-4.1-T6-T8-T9-T10-T11-	T1(R-Rec)-T6.5
				RADAR data is deleted or modified	Integrity of the RADAR data	T1(I-P)-T2-4.1-T6-T8-T9-T10-T11-	T1(R-Rec)-3.2-3.3-4.2-4.3-4.4-4.5-4.6- T6.5-T10
				RADAR system is crashed.	Availability of the RADAR system	T1(I-P)-T2-4.1-T6-T8-T9-T10-T11-	T1(R-Rec)-4.2-4.3-4.4-4.5-4.6-T6.5

Scenario 6	Arbitrary code injection via physically or remotely unauthorized access	Due to the lack of authentication RADAR software or operating system, lack of update for RADAR processor unit software, lack of vendor's security patch for RADAR processor unit software	Attacker gains control over the instruction pointer of the RADAR processor unit and has privilege escalation exploit via arbitrary code injection by unauthorized access with physically or logical access. RADAR processor unit includes user/operator-provided data via RADAR control unit (keyboard control unit and trackball control unit) within commands executed in the shell of the computer running the program. The command can be modified or stopped by attacker-provided data and shell commands, which are selected by the attacker is run. Accordingly, RADAR processor unit does not have ability to discriminate between injected code and data, therefore malicious code is hided like innocuous input data. [T6]	Attacker runs arbitrary code to navigate and assess the RADAR data.	Confidentiality of the RADAR system	T1(I-P)-T2-4.1-T5-T6-T7-T8-T9-T10-T11-	T1(R-Rec)- 4.2-4.3-4.4-4.5-4.6-T6.5-T10
				RADAR system is crashed.	Availability of the RADAR system	T1(I-P)-T2-4.1-T5-T6-T7-T8-T9-T10-T11-	T1(R-Rec)-4.2-4.3-4.4-4.5-4.6-T6.5
Scenario 7	Denial of service (DoS)	Due to the industrial control systems with including a low tolerance to bogus traffic or connected via low bandwidth links which can be easily saturated	Attacker creates a denial-of-service (DoS) attack on the RADAR system by sending specially crafted requests to the server. (For instance, RADAR system software (e.g. The Microsoft Server Message Block 1.0 (SMBv1)) permits denial of service when crafted requests by an attacker sends to the server. On the other side, attacker flood RADAR network with network packets to produce a DoS attack. [T7]	RADAR system is crashed.	Availability of the RADAR system	T1(I-P)-T2-T6-T7-9.3-10.1	T1(R-Rec)-T6.5
Scenario 8	Electronic attack via RADAR jammers	Due to the function of enabling to blind the RADAR via high-power noise or generating fake targets with false location	Radar jammers are a type of electronic attack technology that either produce fake targets with false location or blind the RADAR via high-power noise. Accordingly, the range and sensitivity of the RADAR receiver antenna decreases in consequence of increasing a noise floor of the RADAR receiver by transmitting high-power noise. [T8]	Attacker either blinds a radar or generate false targets	Confidentiality of the RADAR system	T1(I-P)-T2-13.1	N/A
					Integrity of the RADAR system	T1(I-P)-T2-13.1	T1(R-Rec)- 3.1

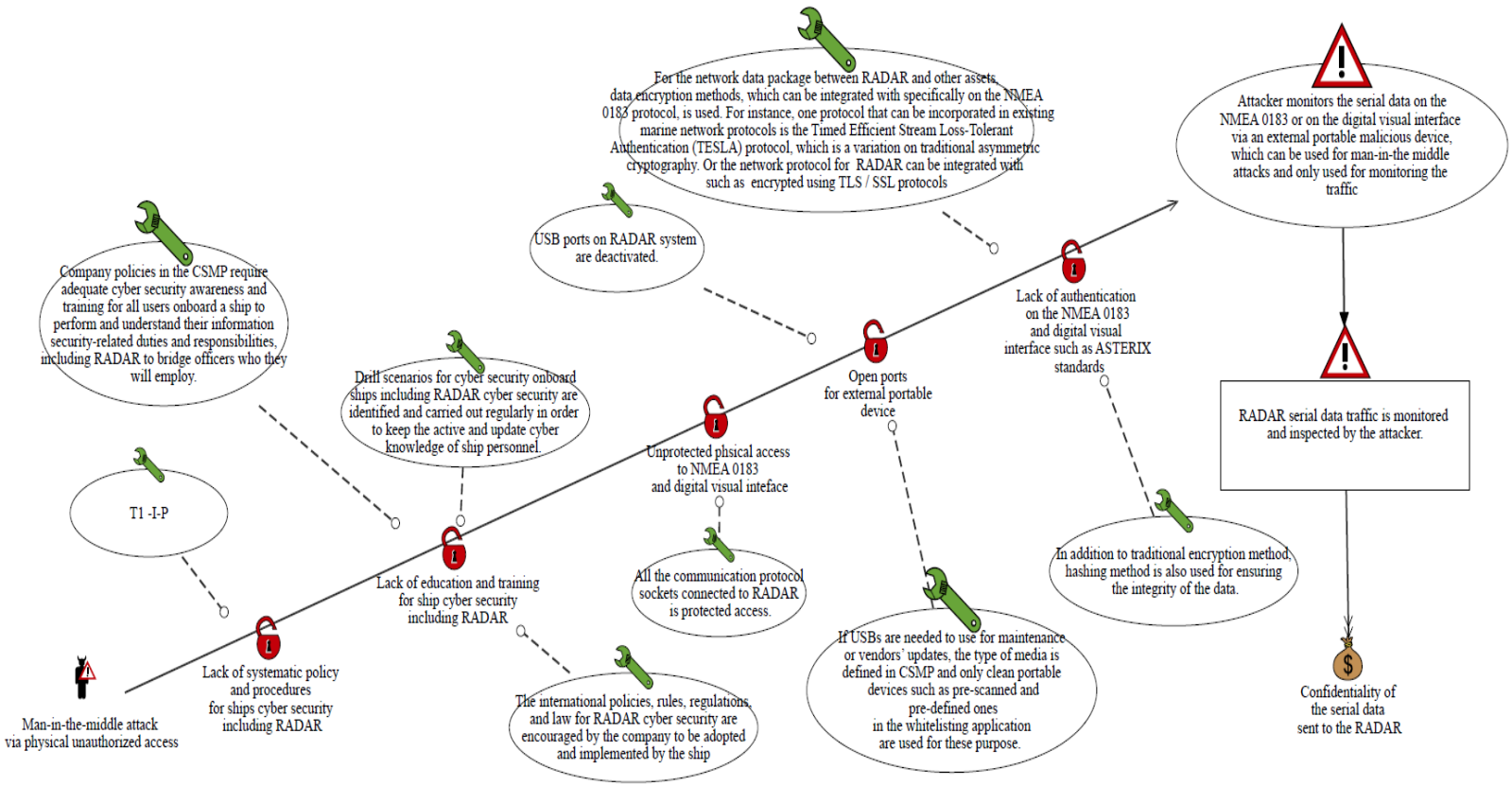


Figure 17. Overall Results for Risk Assessment of Scenario 1.

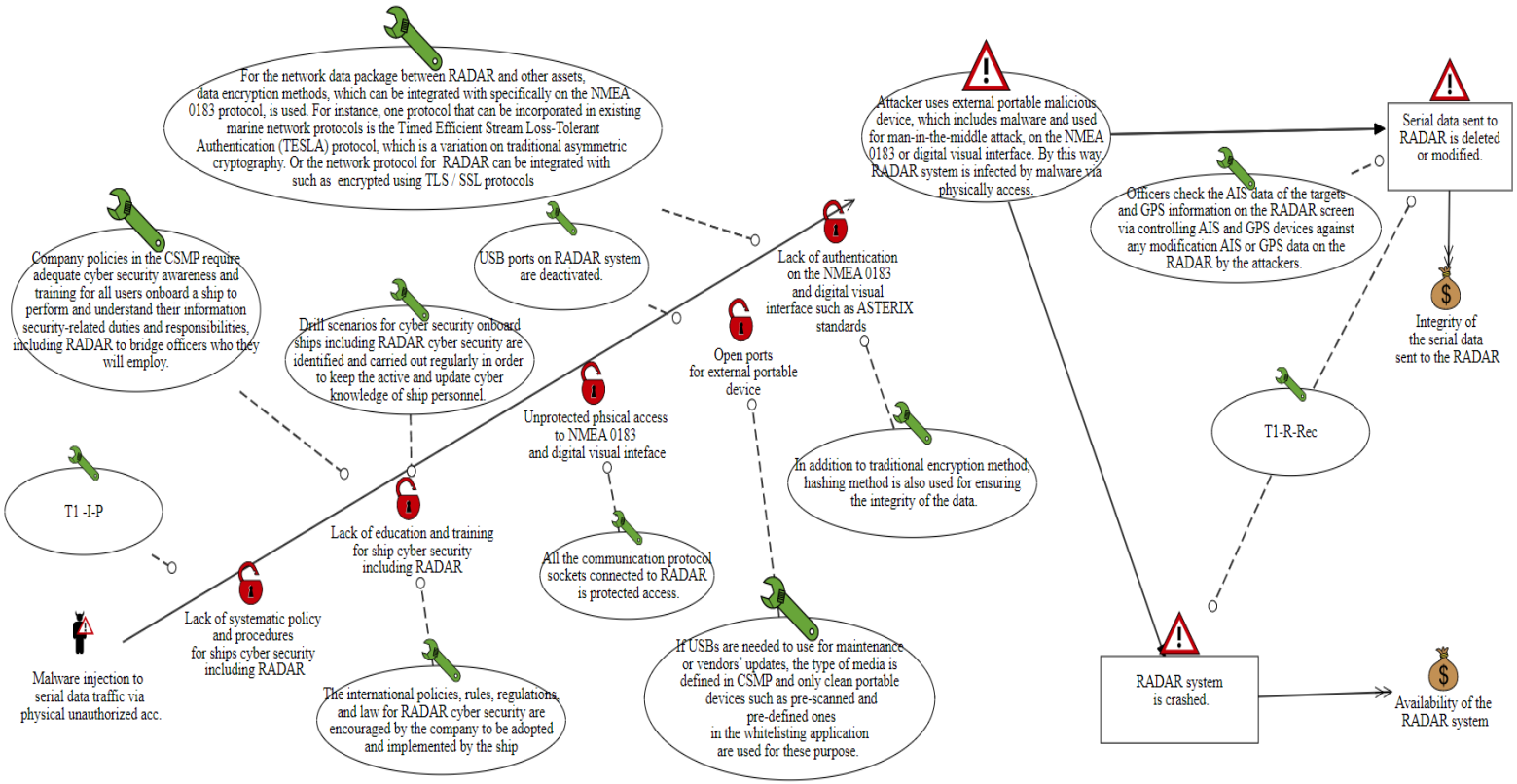


Figure 18. Overall Results for Risk Assessment of Scenario 2.

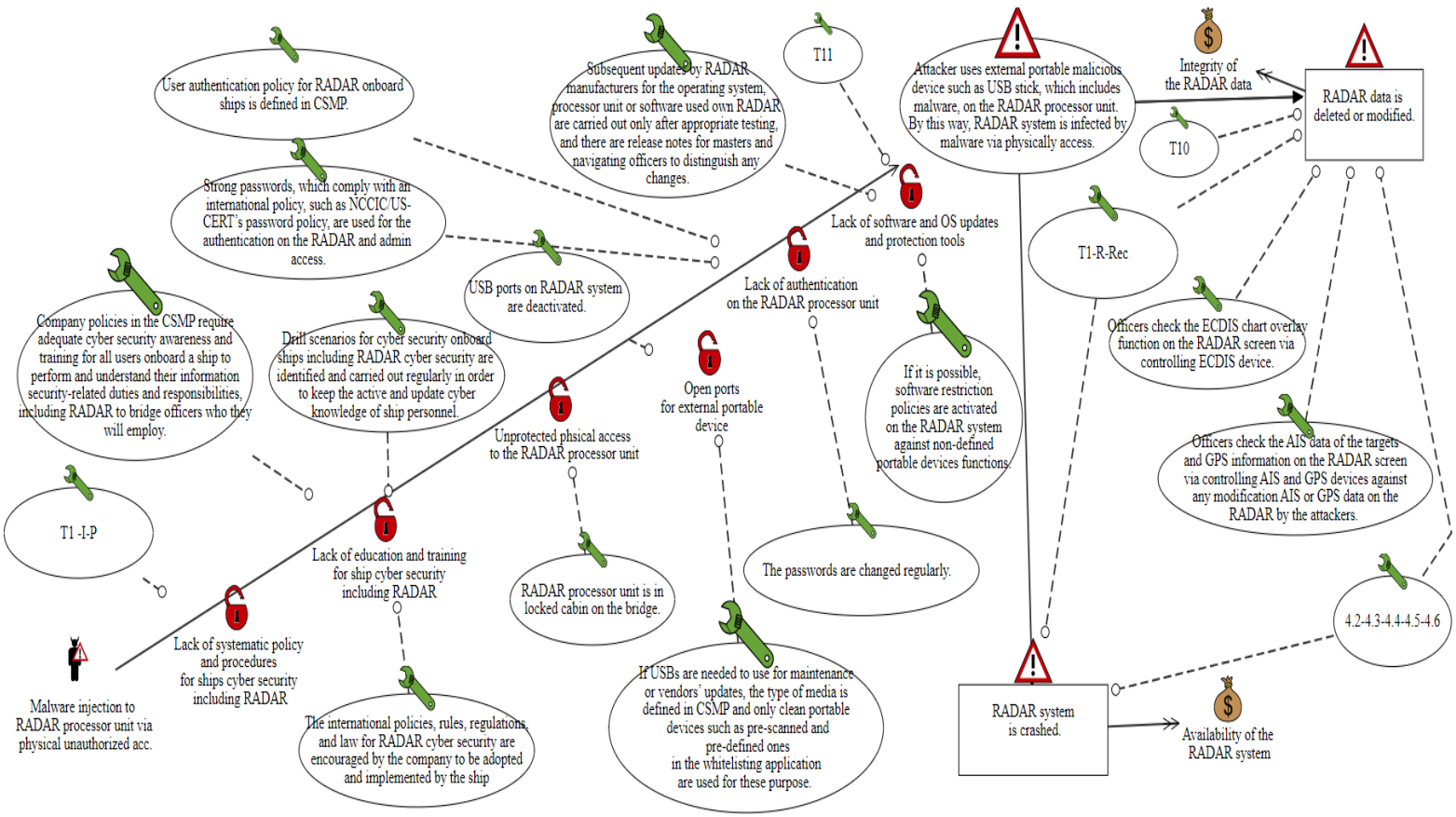


Figure 19. Overall results for risk assessment of scenario 3.

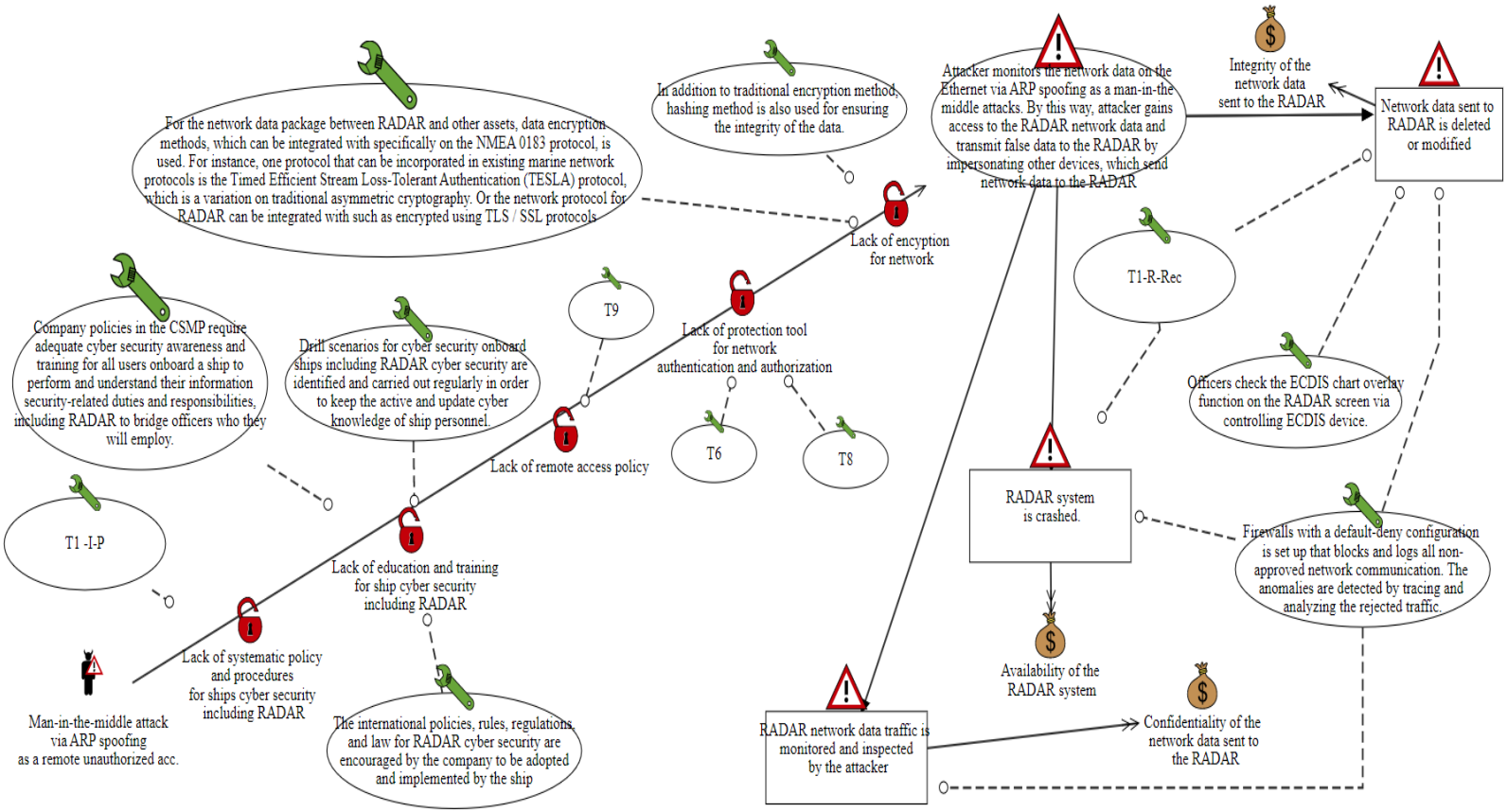


Figure 20. Overall Results for Risk Assessment of Scenario 4.

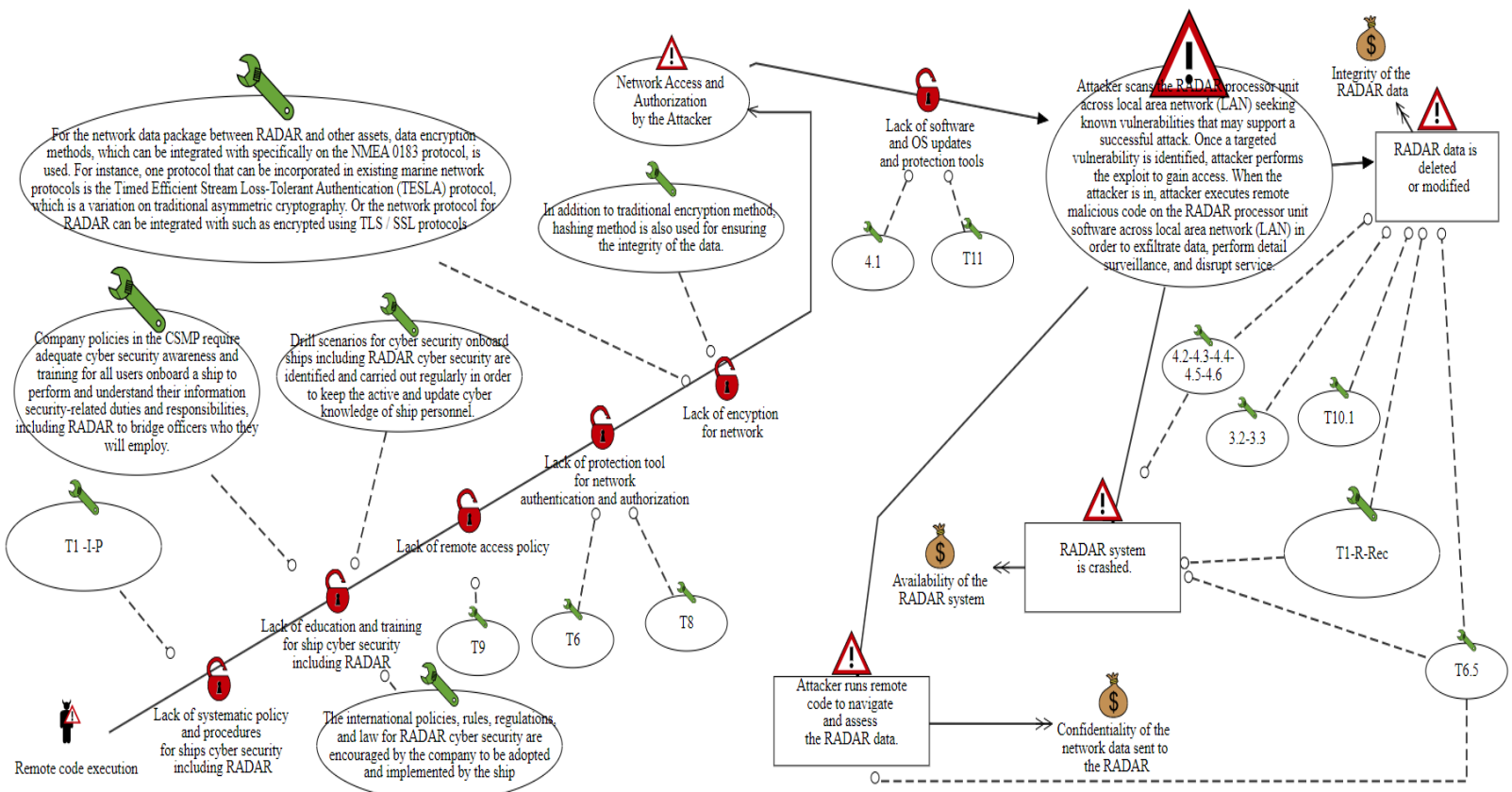


Figure 21. Overall results for risk assessment of scenario 5.

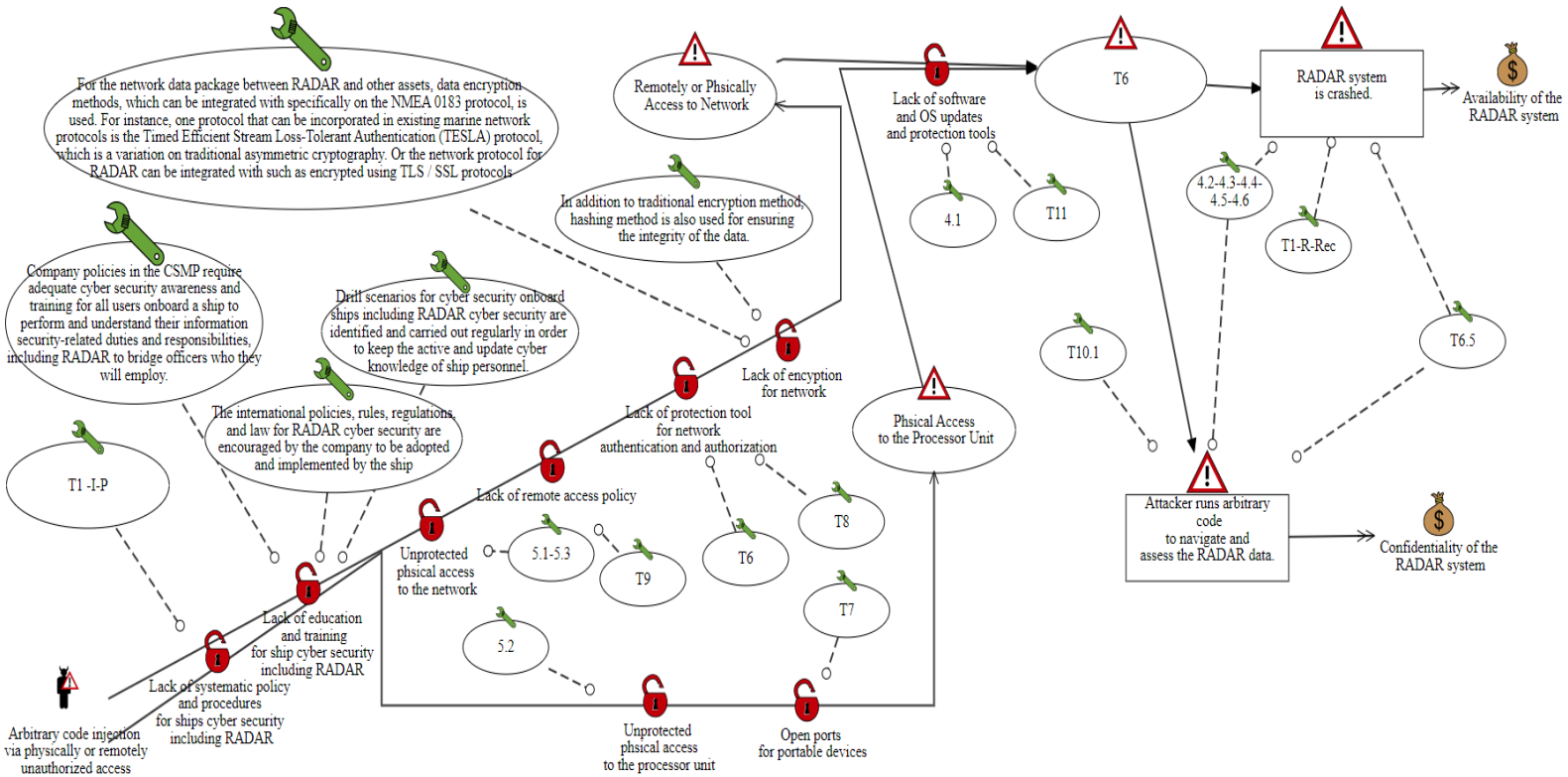


Figure 22. Overall Results for Risk Assessment of Scenario 6.

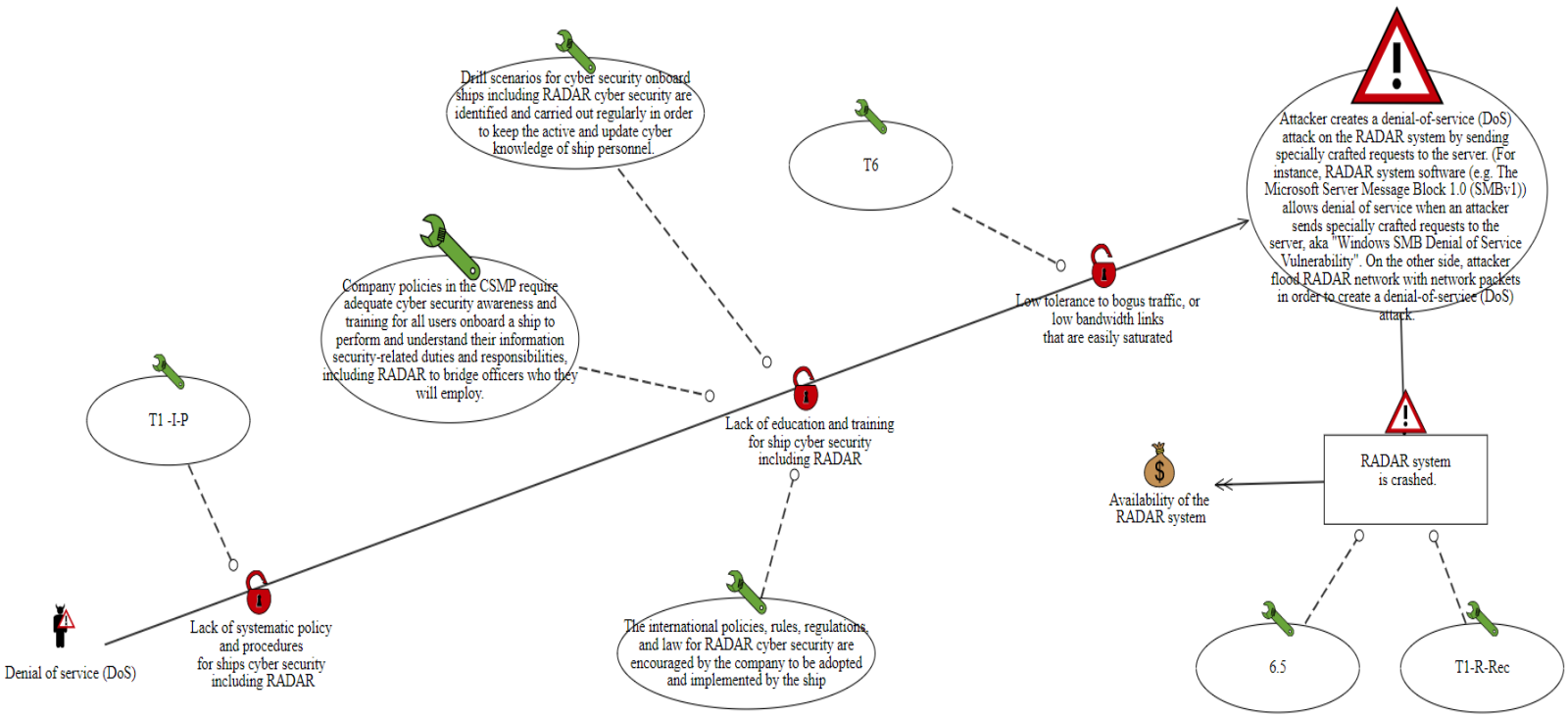


Figure 23. Overall Results for Risk Assessment of Scenario 7

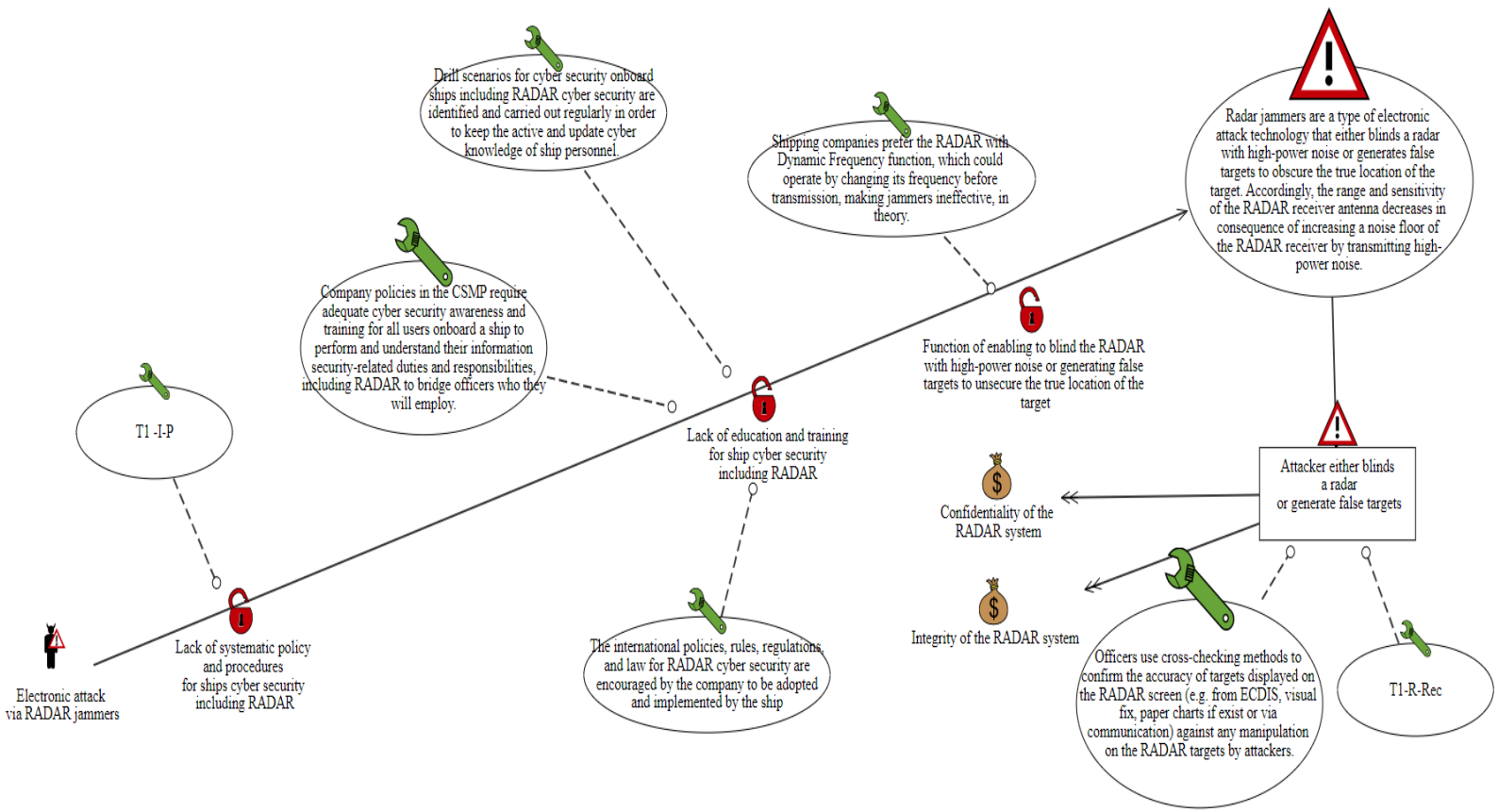


Figure 24. Overall Results for Risk Assessment of Scenario 8

4.7. Discussion

This study presents the vulnerabilities of the shipboard RADAR system by examining the standard RADAR configurations system and existing literature. The vulnerabilities for RADAR systems are determined according to specific serial and network data communication protocols, digital visual interface, processor unit mechanism including operating system and software, and antenna item, which all shipboard RADAR should include. Accordingly, the lack of authentication and encryption on the communication protocols and visual interface, lack of security patches and protection tools on the ship network and in the RADAR processor unit, unavailable dynamic frequency function of the RADAR antenna are specified as the underlying vulnerabilities for shipboard RADAR system.

Based on the vulnerabilities discussed throughout this study, this study considered cyber threats from unauthorized users, removable external data sources such as USB sticks, network segments installed outside of the restricted areas, remotely and physically unauthorized access to ship networks, communication protocols, interfaces, and the processor unit of RADAR. With the available information, the most likely cyber threats for shipboard RADARs as predicted with CORAS is malware injection to the RADAR processor unit via physical unauthorized access, man-in-the-middle attack via ARP spoofing as a remote unauthorized access, remote code execution, arbitrary code injection via physically or remotely unauthorized access, and supply chain attack. From this, the least desired outcomes, which can be caused by these attacks, is the modification or deletion of RADAR serial or network data and corruption of the overall RADAR system.

The risk of an incident is different for each equipment/system, and the mitigating security measures required should be appropriate to the identified risk of incident and proportional to the identified adverse consequences. Accordingly, barriers and mitigations for RADAR cyber security take the form of both physical, such as direct access to the equipment via its ports (e.g., network, USB, import of digital files, software installation) and logical (e.g., connections over a network, transfer of data, operator use). A key tenet of cyber security is authentication of who has provided the data and verification that what is being provided has not been tampered with. For this reason, the security control items in this study are created based on followings:

1) It is suggested to control physical access to items that are integrated to the RADAR, such as the servers, processor unit, network cable, and sockets.
2) Network segregation and firewall configuration should be required to prevent unauthorized access to ship networks containing the RADAR. The monitoring and analyzing of both legitimate and firewall rejected network traffic to detect the anomalies, near-miss cyber incidents, and to inform response and recover efforts in the future.
3) Management of portable devices and medias will help prevent unauthorized access and malicious attacks against RADAR via closing the USB ports. If it is not possible, using pre-scanned and unique portable device is advised, including defining it in a whitelist of acceptable devices.
4) Account management system is suggested for RADAR access, physical or digitally.
5) Configuration hardening for the RADAR system would ensure that deactivating remote configuration and programming modes on RADAR systems, if it is not possible, using remote access agreements that outline the company requirements for accessing vessel networks when third-party and supplier need to access remotely to vessel networks that RADAR connects, securing the RADAR system according to vendors' instructions.
6) Management of event logs and alarms for the RADAR operating systems and software is essential for monitoring and analyzing of the anomalies, near-miss cyber incidents and responding and recovering them for the future
7) Malware protection tools and security patches for the operating system and software is standard practice across many sectors to prevent and detect malicious software.

8) Appropriate authentication for network and encryption for the network data packages between RADAR and other assets would prevent unauthorized remote access and modification of the data.
9) The RADAR with Dynamic Frequency function, which could operate by changing its frequency before transmission, making jammers ineffective, in theory, would be a valuable defense capability in next-generation RADAR manufacture.
10) Company policies should include adequate cyber security awareness and training for all users onboard a ship to perform and understand above-mentioned technical security control items and their information security-related duties and responsibilities.
11) Navigation responsibilities of bridge officers should incorporate appropriate cyber knowledge in order to be on the cyber alarm in every moment.
12) Third parties such as RADAR manufacturers or suppliers are are encouraged to supply shipping companies and ships with safety and technical bulletins on cyber security for RADAR, and information sharing policies for RADAR cyber security.
13) Policies and process, including identification and implementation of above-mentioned security control functions, and responsibilities for identification of the policies and process for RADAR cyber security, implementation, assessment, analyzing, and updating them are required for the ships.

5. A Case Study on ECDIS Cyber Security for Using Bow-Tie Framework

According to step 6 in Figure 2, developed treatments are shown in bow-tie framework. Mainly, CORAS framework covers holistic approach including hierarchic sequence and demonstration of the treatments in a system. However, if only barriers and mitigations are required to be seen in a systematic structure. Where it is desired to see only the general threats, consequences and their barriers and mitigations for the purpose of investment, rather than the detailed flow of the scenario considered, as in the CORAS framework, the bow-tie framework can be useful.

For the aim of depicting bow-tie framework for ship cyber security system, in this section, a case study on ECDIS system is shown as an example. For positioned the treatments for ECDIS cyber security on the framework correctly, Figure 3 states to found importance weighting values of all dynamics. Accordingly, developed treatments for ECDIS cyber security are prioritized by using AHP method. Consequently, in addition to CORAS framework, after creating the developments, bow-tie method integrated with any multi criteria decision making approach such as AHP can be used for seeking the entire cyber security system of the ship in case of any investment decision by the companies. From this point of view, while CORAS framework can be more useful method for tracking the policies and taking the actions on cyber security inside of ship, the bow tie framework includes situations where there is no need to see intermediate and detailed actions related to onboard cyber security and only allows the holistic structure of the system to be systematically seen. It may be a more useful method that can be used by the company for investment decisions where it is needed.

In the above-mentioned context, similar to the steps of CORAS framework, ECDIS configuration system, its IT and OT infrastructure, communication protocols, data transfer mechanism, network structure, and functional requirements are examined. Accordingly, several possible cyber security threats, consequences, and the appropriate cyber security treatments (the treatments that are developed for the threats are called as barriers and the treatments that are developed for the consequences are called as mitigations) are created. They are prioritized by using AHP method.

Analytic Hierarchy Process (AHP) is developed by Thomas Saaty [55] with the aim of creating a hierarchy form for a system. The hierarchical classes are components which are compromise an entire of a system that has been created to select the optimum alternative to achieve the relevant goal by weighting the criteria affecting a specific goal, and each level has its own algorithms. AHP is one of the most used methods for multi criteria decision making (MCDM) problems due to the performing easily

in terms of mathematics process and requiring the interactive solution process. The main process of AHP progress with creating pair wise comparisons of criteria and, if exists, alternatives and assigning weights to them by the experts considering 1-9 ranking scale. There is two significant purposes for understanding the importance weights of criteria. The first one is to help for understanding the key factors related goal by way of ranking or prioritizing via AHP in terms of contributing to scientific researches, and systematic modelling. Secondly, business organizations can effectively make investment on related goal for gaining profit critically by focusing on key criteria. As a result, the key information for trade operations is determined more correct, the commercial decision is given more accurate, or the alternative marketing strategies are evaluated more accurate [56].

In this section, the application demonstration of the AHP method is not shown due to being it as the well-known method. Therefore, the created bow-tie framework as a result of the AHP method is directly presented as in Figure 25. In the figure, the treatments are positioned according to the hierarchical importance weights. The left side of the top event has the barriers role for the each threat and the right side of it has the mitigation role for each consequences. This depiction provide different holistic view for the ship cyber security.

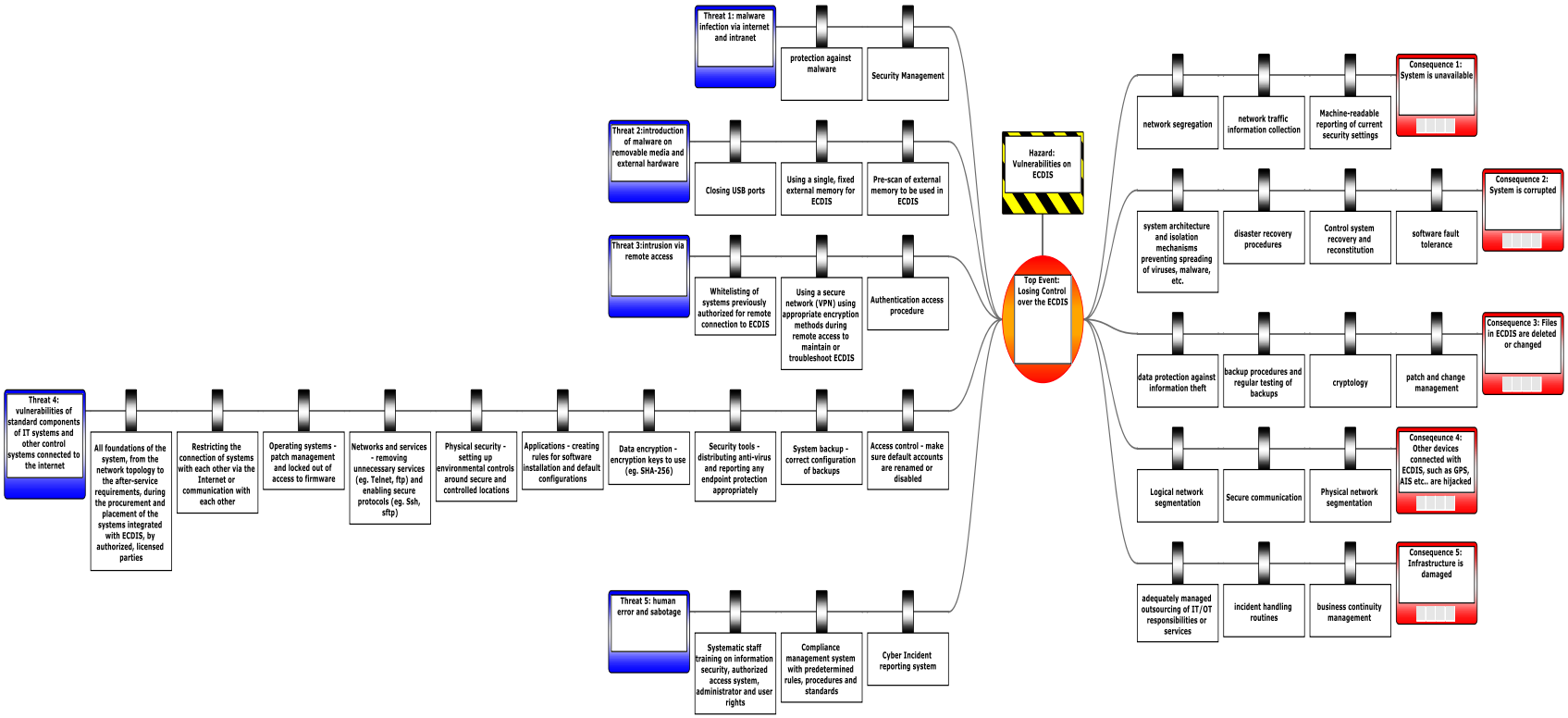


Figure 25. Bow-tie Diagram for Cyber Security of ECDIS.

6. Conclusion

This project aimed to develop maritime cyber risk check-list for two different types of ships for supporting to SMS by performing maritime cyber risk management in the project proposal. The considered risk assessment framework in this project is CORAS risk assessment approach. Then, the outputs are visualized and sequenced hierarchically by using bow-tie framework. However, by examining the general systems onboard ships in terms of cyber space, it is realized that they are categorized as bridge systems, onboard security systems, cargo management systems, communication systems, propulsion and machinery control systems, and passenger and crew systems. Therefore, it is understood that in terms of cyber space onboard ships, it is better to address the check list according to the categorization of the ship system not ship types. According to the ship system, it is recognized that mostly cargo tanks and cargo lines are differ each other for ship types. For instance, in tanker ships cargo management systems have more sensors and control system than a bulk carrier ships. However, they have similar IT and OT mapping in terms of cyber space. Therefore, the developed checklist under this project is created according to the technologic categorization. For this purpose, each system onboard ships is explained in the third section. After understanding the cyber space framework, communication protocols, data transfer mechanism in each systems and between them, in this project, a cyber risk assessment methodology is implemented as a case study for one of these system (RADAR and ECDIS). However, the presented checklist in the deliverables covers all cyber systems onboard a ships. At this point, the created cyber security control functions are tailored for other cyber-physical systems onboard by checking only the technical treatments according to their own configuration system vulnerabilities and if it needs, by re-identifying additional technical treatments. In the content, demonstration of risk assessment for other systems onboard ships is not presented. The CORAS framework and the bow-tie diagram are shown for only RADAR and ECDIS as an example randomly. As a result, the considered risk assessment method and the developed security control items in this project are used as a base in the purpose of adopting an effective system for entire cyber security of ships. Consequently, the developed check list in this project can be used in the SMS of every type of the ships including tankers, bulk carrier, container ships. Similarly, for instance, for tankers, one of the salient changes in the Tanker Management And Self Assessment (TMSA) version 3 is the addition of the 13th performance element which focuses on Maritime Security. This new element will require Members who are subscribed to the Ship Inspection Reporting Programme (SIRE) programme, to incorporate cyber risk security policies and procedures within the company/vessel's operating procedures. To be more specific, operators will be required to have procedures on software management, guidance on how to identify and mitigate cyber threats, availability of latest guidelines on cyber security from industry and classification society, password management procedures, and a cyber security plan which can be shared with staff to promote cyber awareness on board [58]. From this point of view, it is proofed that for all ship types need a standardized cyber security management plan, which can be re-identified the steps of an adoptive cyber risk management methodology according to their specific systems. This project provides all these specified requirements for all types of ships.

This project uses CORAS as one method of cyber risk assessment methodology to suggest basic cyber security requirements for shipboard RADAR as the case study in order to contribute to the CSMP, which should be created within the scope of ISM on ships. The method is considered for all ship cyber-physical systems. The CORAS framework can be used as one effective cyber risk assessment approach for using in CSMS, as it is capable of providing multiple solutions while considering threat sources, vulnerabilities, threats, unwanted incidents, and mitigations in one holistic view. The mitigations, as called as security control items as well, are categorized according to the NIST framework in this study. According to NIST, humans as defenders also reduce cyber risks for any system by being aware of appropriate system protection ways, activating fundamental protections, monitoring system to understand any existing of breach for protections, assessing the ways for increasing system security, tracking cyber threats, which attempted to do harm to the system or system assets, and recovering the damages to the system. Thus, this categorization helps to carry out the integration of technology, people,

and process for ship cyber security systematically. Furthermore, it makes easy that the barriers, which is called a term for protecting the system before realizing the threats, and the mitigations, which is called a term for preventing the unwanted incident after occurring the threats, are specified clearly for ship cyber security. These solutions are significant points for comprising the forceful CSMP by providing systematic and overall security control functions in the context of cyber security for ships and shipping companies. The developed solutions for treatments of ship cyber incident scenarios includes (i) procedural protection measures covering human and process activities such as training and awareness, access of visitors, upgrades and software maintenance, anti-virus and anti-malware tool updates, remote access, use of administrator privileges, physical and removable media controls, (ii) technical protection measures such as limitation to and control of network ports, protocols and services, configuration of network devices such as firewalls, routers and switches, physical security, satellite and radio communication, secure configuration for hardware and software, patch management, and response and recovery capabilities.

For the aim of depicting bow-tie framework for ship cyber security system, a case study on ECDIS system is shown as an example in this project. The developed treatments for ECDIS cyber security are prioritized by using AHP method.

Consequently, the reason of implementation of two approaches (CORAS risk management framework and Bow Tie framework) is that in addition to CORAS framework, after creating the developments, bow-tie method integrated with any multi criteria decision making approach such as AHP can be used for seeking the entire cyber security system of the ship in case of any investment decision by the companies. From this point of view, while CORAS framework can be more useful method for tracking the policies and taking the actions on cyber security inside of ship, the bow tie framework includes situations where there is no need to see intermediate and detailed actions related to onboard cyber security and only allows the holistic structure of the system to be systematically seen. It may be a more useful method that can be used by the company for investment decisions where it is needed.

The impact of the project to individuals, organizations and society will be as follows in more ways:

- To study the importance and essence of cybersecurity as part of a holistic approach throughout a ship's life-cycle.
- To examine the potential impact of cyber-attacks on board a vessel.
- To investigate the nature of the systems on board a vessel along with the significant impacts they can introduce to the maritime environment in case of a cyber-incident.
- To explore the different threat actors and identify their motives in order to map the attack landscape and recognize the origin of the attacks.
- To map out the attack surface and identify the specific system assets that introduce vulnerabilities and impose threats for cyber incidents.
- To identify the main aspects that contribute to the mitigation of the cyber risk and propose a framework for addressing the exposures.
- To introduce a maritime cyber risk check list with state of the art model.

This project is a baseline for a further study, which has been currently under consideration. In this further study, the potential safety and financial effects of cyber security incidents in maritime will be examined by focusing maritime cyber security insurance. At this point, the obtained treatments in this project will be used as an indicator for ships in maritime cyber security insurance. For developing a maritime cyber security insurance policy, an optimization tool will be developed by considering safety issues and financial losses in case of a cyber incidents and the cost of the treatments.

Overall, this project provides an output including a checklist for ship cyber security to be used in all type of ships' safety management system as in appendix. Besides, in appendix, a conference proceeding presented in IAMU AGA22 and a journal article, which is under review process, are shown as the other deliverables of this project.

For achieving project results, the project support has been used as follows: attending the IAMU AGA 22 conference and other maritime cyber security related conferences; to provide the tools to be used in the project; and course with cyber security to better and professionally comment ship cyber physical systems and to decide effectively on the measures developed.

Acknowledgement

This research is funded by the IAMU Young Staff Research Project 2022 as titled of "Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships" [Research project number: YAS20220301].The materials and data in this publication have been obtained through the support of the International Association of Maritime Universities (IAMU) and The Nippon Foundation in Japan.

References

[1] BIMCO, "The Guidelines on Cyber Security onboard Ships," 2016.
[2] White Paper, "The role of human factors in delivering cyber security," 2022.
[3] O. Fitton, D. Prince, B. Germond, and M. Lacy, "The Future of Maritime Cyber Security," 2015.
[4] ENISA, "Analysis of cyber security aspects in the maritime sector," 2011.
[5] P. Bolat and G. Kayisoglu, "Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector," *J. ETA Marit. Sci.*, vol. 7, no. 4, pp. 344–360, 2019, doi: 10.5505/jems.2019.85057.
[6] A. Jain and V. President, "Modelling Cyber Risk," pp. 1–39, 2017.
[7] B. Svilicic, I. Rudan, A. Jugović, and D. Zec, "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System," *J. Mar. Sci. Eng.*, vol. 7, no. 10, p. 364, Oct. 2019, doi: 10.3390/jmse7100364.
[8] B. Svilicic, J. Kamahara, J. Celic, and J. Bolmsten, "Assessing ship cyber risks: a framework and case study of ECDIS security," *WMU J. Marit. Aff.*, vol. 18, no. 3, pp. 509–520, Sep. 2019, doi: 10.1007/s13437-019-00183-x.
[9] B. Svilicic, J. Kamahara, M. Rooks, and Y. Yano, "Maritime Cyber Risk Management: An Experimental Ship Assessment," *J. Navig.*, vol. 72, no. 5, pp. 1108–1120, 2019, doi: 10.1017/S0373463318001157.
[10] K. Tam and K. Jones, "Cyber-SHIP: Developing next generation maritime cyber research capabilities," 2019.
[11] V. Gisladottir, A. A. Ganin, J. M. Keisler, J. Kepner, and I. Linkov, "Resilience of Cyber Systems with Over- and Underregulation," *Risk Anal.*, vol. 37, no. 9, pp. 1644–1651, Sep. 2017, doi: 10.1111/risa.12729.
[12] M. Nogal and A. O'Connor, "Cyber-Transportation Resilience. Context and Methodological Framework," in *Resilience and Risk*, NATO Science for Peace and Security Series C: Environmental Security, 2017, pp. 415–426.
[13] M. -Elisabet. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller, "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies," *Risk Anal.*, vol. 38, no. 2, pp. 226–241, Feb. 2018, doi: 10.1111/risa.12844.
[14] J. P. Kesan and L. Zhang, "Analysis of Cyber Incident Categories Based on Losses," *ACM Trans. Manag. Inf. Syst.*, vol. 11, no. 4, pp. 1–28, Dec. 2020, doi: 10.1145/3418288.
[15] ISO27001, "ISO 27001 Information Security Management System," *International Certification and Auditing Co. Lmt.*, 2014. [Online]. Available: https://belgelendirme.ctr.com.tr/iso-27001.html.
[16] K. Stølen, B. Folker den, T. Dimitrakos, R. Fredriksen, and et al., "Model-based risk assessment – the CORAS approach - Stolen.pdf," *iTrust Work.*, 2002.

[17] N. Medvidovic, D. S. Rosenblum, D. F. Redmiles, and J. E. Robbins, “Modeling software architectures in the unified modeling language,” *ACM Trans. Softw. Eng. Methodol.*, vol. 11, no. 1, pp. 2–57, 2002, doi: 10.1145/504087.504088.
[18] IEC 61025, “Fault Tree Analysis (FTA),” *BS IEC*, 2006.
[19] F. Redmill, “System Safety: HAZOP and Software HAZOP,” *Ind. Manag. Data Syst.*, vol. 100, no. 1, pp. 46–48, Feb. 2000, doi: 10.1108/imds.2000.100.1.46.2.
[20] A. Bouti and D. Ait Kadi, “A State-of-the-art Review of FMEA/FMECA,” *Int. J. Reliab. Qual. Saf. Eng.*, vol. 01, no. 04, pp. 515–543, Dec. 1994, doi: 10.1142/S0218539394000362.
[21] B. Littlewood, “A Reliability Model for Systems with Markov Structure,” *Appl. Stat.*, vol. 24, no. 2, p. 172, 1975, doi: 10.2307/2346564.
[22] AS/NZS 4360, “Australian/New Zealand Standard. Risk Management,” *Stand. Aust. Stand. New Zeal.*, 2004.
[23] ISO/IEC13335, “Information technology - Guidelines for management of IT Security,” *BS ISO/IEC*, 2000.
[24] ISO/IEC 10746, “Basic reference model for open distributed processing,” *BS ISO/IEC*, 1995.
[25] ISO/IEC 17799, “Information technology _ Code of practice for information security management,” *BS ISO/IEC*, 2005.
[26] F. den Braber *et al.*, “The CORAS model-based method for security risk analysis,” *SINTEF, Oslo*, no. September, 2006.
[27] K. Mokhtari, J. Ren, C. Roberts, and J. Wang, “Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals,” *J. Hazard. Mater.*, vol. 192, no. 2, pp. 465–475, 2011, doi: 10.1016/j.jhazmat.2011.05.035.
[28] H. Abdo, M. Kaouk, J. M. Flaus, and F. Masse, “A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis,” *Comput. Secur.*, vol. 72, pp. 175–195, 2018, doi: 10.1016/j.cose.2017.09.004.
[29] K. Bernsmed, C. Frøystad, P. H. Meland, D. A. Nesheim, and Ø. J. Rødseth, “Visualizing Cyber Security Risks with Bow-Tie Diagrams,” in *International Workshop on Graphical Models for Security*, 2017, pp. 38–56.
[30] CGE Risk, “The bowtie method,” *CGE Risk Management Solutions*, 2020. [Online]. Available: https://www.cgerisk.com/knowledgebase/The_bowtie_method.
[31] Vassallo Associates, “Maritime Cyber Security,” 2022. [Online]. Available: https://www.hvassallo.com/practice-areas/maritime-cyber-security/.
[32] M. A. Ben Farah *et al.*, “Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,” *Information*, vol. 13, no. 1, p. 22, Jan. 2022, doi: 10.3390/info13010022.
[33] Mission Secure, *A Comprehensive Guide to Maritime Cybersecurity*. 2021.
[34] EUROCONTROL-SPEC-0149-240, “EUROCONTROL Specification for Surveillance Data Exchange ASTERIX Category 240 Radar Video Transmission,” *EUROCONTROL Specif.*, 2015.
[35] IEC 60936-1, “Maritime navigation and radiocommunication equipment and systems — Radar — Part 1: Shipborne radar — Performance requirements — Methods of testing and required test results,” *BS IEC Br. Stand.*, 2000.
[36] A. G. Bole, A. Wall, and A. Norris, *Radar and ARPA Manual: Radar, AIS and Target Tracking for Marine Radar Users*. Elsevier and Book Aid International, 2013.
[37] BS EN IEC 61162-1, “Maritime navigation and radiocommunication equipment and systems — Digital interfaces —BS EN IEC 61162-1-1996,” 1996.
[38] Furuno, “FURUNO Operator’s Manual -Marine Radar,” 2018.
[39] S. Cohen, T. Gluck, Y. Elovici, and A. Shabtai, “Security analysis of radar systems,” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 3–14, 2019, doi: 10.1145/3338499.3357363.
[40] W. C. Leite Junior, C. C. de Moraes, C. E. P. de Albuquerque, R. C. S. Machado, and A. O. de

Sá, “A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems,” *Sensors (Basel).*, vol. 21, no. 9, pp. 1–22, 2021, doi: 10.3390/s21093195.
[41] G. Longo, E. Russo, A. Armando, and A. Merlo, “Attacking (and defending) the Maritime Radar System,” *Cornell Univ. Cryptogr. Secur.*, pp. 1–16, Jul. 2022, doi: https://doi.org/10.48550/arXiv.2207.05623.
[42] B. Svilicic, I. Rudan, V. Frančić, and D. Mohović, “Towards a Cyber Secure Shipboard Radar,” *J. Navig.*, vol. 73, no. 3, pp. 547–558, 2020, doi: 10.1017/S0373463319000808.
[43] F. den Braber *et al.*, *The CORAS Model-based Method for Security Risk Analysis*. 2006.
[44] R. von Solms and J. van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.
[45] M. S. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis - The CORAS Approach*. Springer, 2011.
[46] T. Dimitrakos, B. Ritchie, D. Raptis, and K. Stølen, “Model based Security Risk Analysis for Web Applications: The CORAS approach,” in *EuroWeb 2002 Conference (EW)*, 2002.
[47] IEC 62443-3, “Security for industrial process measurement and control — Part 3: Network and system security,” *BS IEC Br. Stand.*, 2008.
[48] DNV-GL, “DNVGL-CG-0325 Cyber secure,” *DNV-GL Cl. Guidel.*, vol. October, 2020.
[49] ISO/IEC 27001, “Information technology- Security techniques-Information security management systems-Requirements -BS EN ISO-IEC 27001-2017,” *BS ISO/IEC Br. Stand.*, 2017.
[50] ISO/IEC 27033-3, “Information technology-Security techniques-Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues,” *BS ISO/IEC Br. Stand.*, 2010.
[51] The Finnish Shipowners’ Association, “MARITIME CYBERSECURITY - BEST PRACTICES FOR VESSELS,” *Finnish Natl. Emerg. Supply Organ. Marit. Transp. Pool*, 2021.
[52] ANSSI, “Cybersecurity for Industrial Control Systems,” *French Netw. Inf. Secur. Agency*, vol. Version 1., no. June, p. France, 2012.
[53] H. Boyes and R. Isbell, “Code of Practice: Cyber Security for Ships,” *IET Stand. Dep. Transp.*, p. 73, 2017.
[54] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018.
[55] T. L. Saaty, *The Analytic Hierarchy Process: Planning. Prior. Setting. Resour. Alloc.* New York Int. B. Co.: MacGraw-Hill, 1980.
[56] Y. Chen and L. Qu, “Evaluating the selection of logistics centre Location using fuzzy MCDM model based on entropy weight,” *Proc. World Congr. Intell. Control Autom.*, vol. 2, pp. 7128–7132, 2006, doi: 10.1109/WCICA.2006.1714468.
[57] G. Kayisoglu, P. Bolat, and K. Tam, “Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships,” in *22nd International Association of Maritime Universities Student Session (IAMU)*, 2022, pp. 19-21 October, Batum, Georgia.
[58] Shipowners, "Cyber Security On Board Ships - Tanker Management And Self Assessment And Upcoming Changes To The International Safety Management Code," 2018, accessed in 15 May 2023 from https://www.shipownersclub.com/media/2017/12/TMSA-3-Cyber-Security-On-board-ships-1217.pdf

Appendix: Deliverables

The project output is a checklist for ship cyber security to be used in safety management systems of ships. The checklist is as below:

Ship Cyber Security Operations			
Treatment Group	**NIST Framework Category**	**Treatment Number**	**Treatment**
Process			
T1 Policies and procedures in the context of cyber security management plan (CSMP) under safety management system (SMS)	I	1.1	Shore-based Company Cyber Security Officer, who is responsible for the security of all ship information and operational technology is defined in CSMP.
	I	1.2	Ship-based Cyber Security Officer, who is responsible for the security of all ship information and operational technology is defined in CSMP.
	I	1.3	The contractual agreement between ships' officers and their employer, which states their and the companies' responsibilities for information security onboard, is provided in the shipping company.
	I	1.4	The agreement between vendors / suppliers and shipping company, which include cybersecurity requirements and the responsibilities they need to adhere to in the delivery of their service, is provided.
	I-P	1.5	A risk assessment policy for ship cyber security including such as CORAS framework processes is defined in the CSMP onboard a ship and implemented onboard ships.
	I-P	1.6	The risk management process is established and managed for ship by integrating all responsibilities of ship, company, and third-parties.
	I-P	1.7	A checklist for RADAR cyber security is identified in CSMP and used onboard a ship. (This table can be used as a checklist for RADAR cyber security onboard ships)
	I-R	1.8	An information sharing policy about reporting any cyber near misses or incidences, which includes organizational communication and data flows between ships, shipping companies, and third parties, is defined and used.
	I-R	1.9	A response plan for ship cyber security is defined in CSMP and executed during or after a cyber-attack. If it is require, the response plan also cover third parties.
	I-Rec	1.10	A recovery plan for ship cyber security is defined in CSMP and executed after a cyber-attack. (Recovery plan includes skill and competence of shipping company supply and ship in order to recover the damaged asset, system, hardware, software, or data. For instance, in any case of DoS attack to the ship system, it is defined in the recovery plan that what ways and how much time are required to restore the system to its previous state. It generally depends on the skill of the shipping company IT support or exist personnel on boars ship who is responsible for hardware and software maintenance, such as electro technical officer. If it is require, the recovery plan also covers third parties.)
	I-R-Rec	1.11	A policy for annual physical security inspection, audit or survey for hardware and software maintenance of ship is defined in CSMP. After inspection, audit, or survey, the reports of them are kept in the ship's documentation records. The reports are analyzed in the context of defined risk assessment policy. Accordingly, defined risk management process, the response plan, and the recovery plan are updated.
	I-R-Rec	1.12	A record policy for any cyber security suspicious activity or incidence is defined in CSMP and implemented in any noticed suspicious cyber activity. The records are analyzed in the context of defined risk assessment policy. Accordingly, defined risk management process, the response plan, and the recovery plan are updated.
People			

T2 Cybersecurity awareness and training in the context of CSMP under SMS	P	2.1	Company policies in the CSMP require adequate cyber security awareness and training for all users onboard a ship to perform and understand their information security-related duties and responsibilities to bridge officers who they will employ.
	I-P	2.2	Drill scenarios for cyber security onboard ships are identified and carried out regularly in order to keep the active and update cyber knowledge of ship personnel.
	P	2.3	The international policies, rules, regulations, and law for ship cyber security are encouraged by the company to be adopted and implemented by the ship.
T3 Navigation responsibilities of bridge officers with the cyber knowledge in the context of CSMP under SMS	D	3.1	Officers use cross-checking methods to confirm the accuracy of targets displayed on the RADAR screen (e.g. from ECDIS, visual fix, paper charts if exist or via communication) against any manipulation on the RADAR targets by attackers. [Stating RADAR is an example for understanding the action purpose. This action can be implemented suitable other system.*]
	D	3.2	Officers check the AIS data of the targets and GPS information on the RADAR screen via controlling AIS and GPS devices against any modification AIS or GPS data on the RADAR by the attackers. [*]
	D	3.3	Officers check the ECDIS chart overlay function on the RADAR screen via controlling ECDIS device. Stating RADAR is an example for understanding the action purpose. This action can be implemented suitable other system. [*]
T4 Relationship between vendors, shipping company and ship in the context of CSMP under SMS	P	4.1	Subsequent updates by RADAR manufacturers for the operating system, processor unit or software used own RADAR are carried out only after appropriate testing, and there are release notes for masters and navigating officers to distinguish any changes. Stating RADAR is an example for understanding the action purpose. [*]
	D	4.2	If manufacturers detect any inconsistency in RADAR performance, they issue technical bulletins to all ship owners/operators who manage ships equipped with their systems to highlight issues. [*]
	R-Rec	4.3	The manufacturers' technical bulletin includes mitigating measures for masters and navigating officers with future plans to correct the inconsistencies. [*]
	D-R	4.4	Ship owners/operators communicate with RADAR manufacturers and ensure that relevant information is shared with ships under management immediately and acted upon with necessary mitigations according to Original Equipment Manufacturer (OEM) technical bulletins. [*]
	Rec	4.5	Any noted defect or inconsistency in RADAR performance are promptly reported to the RADAR manufacturer, with appropriate notices to Flag State Administrations or recognized organization. [*]
	D-Rec	4.6	RADAR manufacturers issue safety bulletins or software upgrades as soon as an error or inconsistency in RADAR-related data or functionality is detected by a navigating officer. The operating system is updated with a security patch sent by the manufacturer. [*]
Technical			
T5 Control physical access to devices	P	5.1	An access control system such as identified id card or physical key is installed for the room, which taken place the servers that RADAR connects. Navigating officers and master have the authorization for this room. [*]
	P	5.2	RADAR work station central units (processor unit) is in locked cabin on the bridge. [*]
	P	5.3	All the network cable and sockets connected to RADAR is protected access. [*]
T6 Network segregation and	I-P	6.1	A map for RADAR network flow is established as in Figure 12 in the SMM. [*]
	P	6.2	The network segmentation for RADAR network flow is provided for separating network from other critical ship system network or infrastructure network. [*]
	I-P	6.3	The IP-addresses and network communication protocols and data flows needed for RADAR system is identified to function properly. [*]

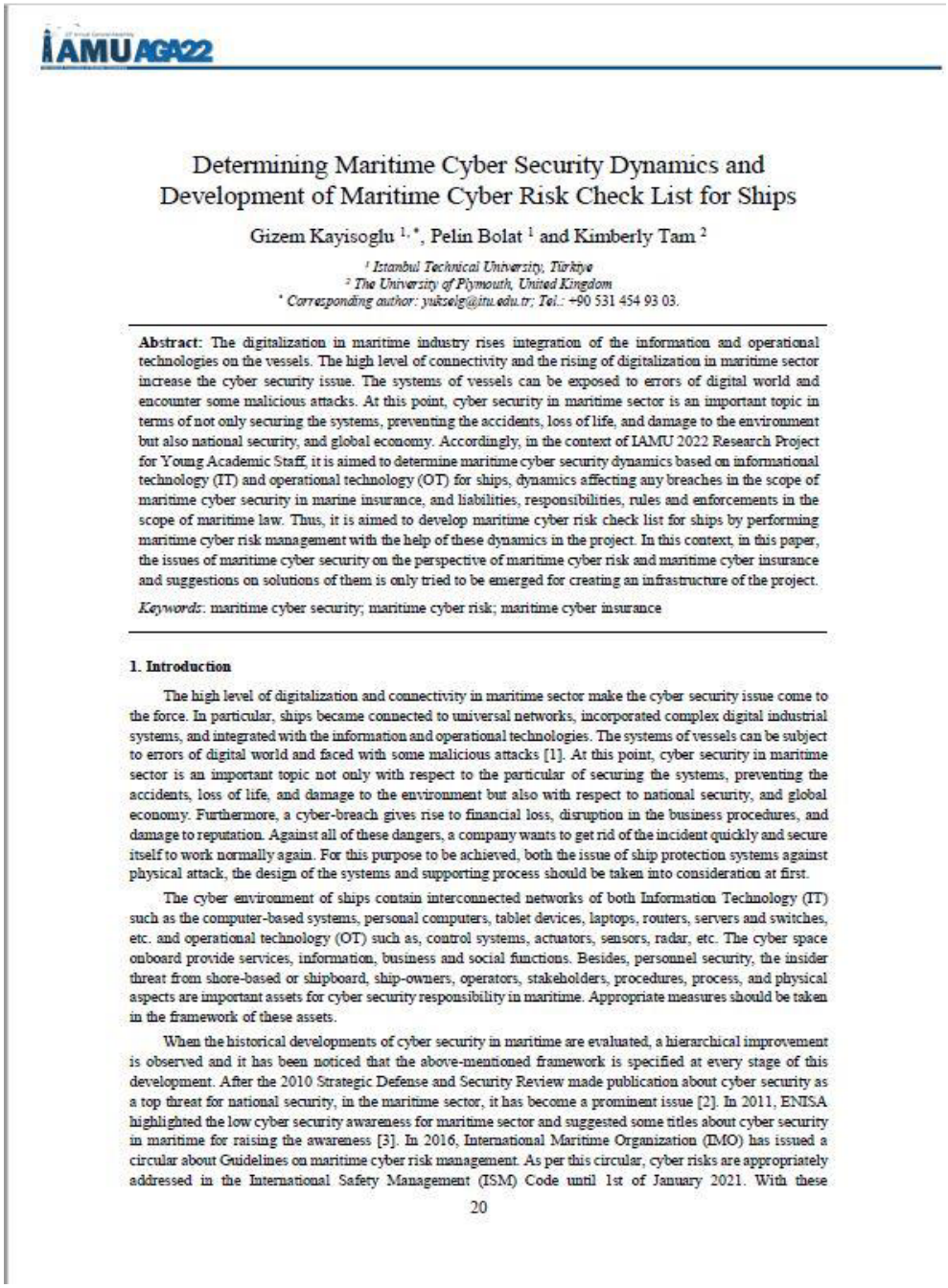
Firewall configuration	P	6.4	RADAR network flow is filtered by a firewall. Firewall policies is analysed and ensured that only necessary communication is allowed to and from the assets connected to RADAR [*]
	P-D-Rec	6.5	Firewalls with a default-deny configuration is set up that blocks and logs all non-approved network communication. The anomalies are detected by tracing and analyzing the rejected traffic.
T7 Management of portable devices and media	P	7.1	USB ports on RADAR system are deactivated. [*]
	I-P	7.2	If USBs are needed to use for maintenance or vendors' updates, the type of media is defined in CSMP and only clean portable devices such as pre-scanned and pre-defined ones in the whitelisting application are used for these purpose.
	P	7.3	If it is possible, software restriction policies are activated on the RADAR system against non-defined portable devices functions. [*]
T8 Account management (logical access)	I-P	8.1	Default admin password on vessel systems that RADAR connects is created such as for serial-to-IP converters, and networks that connects RADAR. [*]
	I-P	8.2	User authentication policy for RADAR onboard ships is defined in CSMP. [*]
	P	8.3	Strong passwords, which comply with an international policy, such as NCCIC/US-CERT's password policy, are used for the authentication on the RADAR and admin access. [*]
	P	8.4	The passwords are changed regularly.
T9 Configuration hardening	P	9.1	Remote configuration and programming modes on RADAR systems are deactivated. [*]
	I-P	9.2	Non-Disclosure / remote access agreements that outline the company requirements for accessing vessel networks (VPN connections, personal users, strong passwords/MFA, anti-malware protection on computers, etc.) are created when third-party and supplier need to access remotely to vessel networks that RADAR connects. [*]
	P	9.3	Firewall policies to grant third-parties and internal users access remotely to the vessel network they need are updated.
T10 Management of event logs and alarms	D	10.1	If the RADAR operating systems and software ("Windows Event", text file, etc.) permit that traceability functions on the RADAR are activated. [*]
T11 Malware protection	P	11.1	The RADAR vendors, which provides security patches for own operating system and anti-malware protection system, is preferred by the shipping companies. [*]
	P	11.2	The malware protection tools on the RADAR system are regularly and automatically updated. [*]
T12 Network Authentication and Encryption of the data	P	12.1	For the network data package between RADAR and other assets, data encryption methods, which can be integrated with specifically on the NMEA 0183 protocol, is used. For instance, one protocol that can be incorporated in existing marine network protocols is the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol, which is a variation on traditional asymmetric cryptography. Or the network protocol for RADAR can be integrated with such as encrypted using TLS / SSL protocols [*]
	P	12.2	In addition to traditional encryption method, hashing method is also used for ensuring the integrity of the data.
T13 Antenna Set Up	P	13.1	Shipping companies prefer the RADAR with Dynamic Frequency function, which could operate by changing its frequency before transmission, making jammers ineffective, in theory. [*]

Above table is mainly created by considering RADAR system. The table below acts as a checklist, showing whether the tasks given in the above table can be adapted to each ship's cyber-physical system.

Checklist for Ship Cyber Security Operations According to Its Cyber-Physical System																
				Communication Systems				Propulsion, Machinery and Control Systems	Bridge Navigation System					Cargo Management Systems		
Category	**Treatment Group**	**NIST Framework Category**	**Treatment Number**	**Satellite Communication**	**Integrated Communication System**	**Voice Over Internet Protocol (VOIP)**	**Wireless Local Area Network (WLAN)**		**ECDIS**	**RADAR**	**AIS**	**GPS**	**VDR**	**Cargo Control Room**	**Ballast Water System (BWS)**	**All Systems**
Process	T1 Policies and procedures in the context of cyber security management plan (CSMP) under safety management system (SMS)	I	1.1													x
		I	1.2													x
		I	1.3													x
		I	1.4													x
		I-P	1.5													x
		I-P	1.6													x
		I-P	1.7													x
		I-R	1.8													x
		I-R	1.9													x
		I-Rec	1.10													x
		I-R-Rec	1.11													x
		I-R-Rec	1.12													x
People	T2 Cybersecurity awareness and training in the context of CSMP under SMS	P	2.1													x
		I-P	2.2													x
		P	2.3													x
Technical	T3 Navigation responsibilities of bridge officers with the cyber knowledge in the context of CSMP under SMS	D	3.1					x	x	x	x	x		x	x	
		D	3.2							x	x	x				
		D	3.3						x	x						
	T4	P	4.1													x
		D	4.2													x

	Relationship between vendors, shipping company and ship in the context of CSMP under SMS	R-Rec	4.3													x
		D-R	4.4													x
		Rec	4.5													x
		D-Rec	4.6													x
	T5 Control physical access to devices	P	5.1					x	x	x	x	x	x	x	x	
		P	5.2						x	x	x	x	x			
		P	5.3				x	x	x	x	x	x	x	x	x	
	T6 Network segregation and Firewall configuration	I-P	6.1													x
		P	6.2													x
		I-P	6.3													x
		P	6.4													x
		P-D-Rec	6.5													x
	T7 Management of portable devices and media	P	7.1					x	x	x	x	x	x	x	x	
		I-P	7.2					x	x	x	x	x	x	x	x	
		P	7.3					x	x	x	x	x	x	x	x	
	T8 Account management (logical access)	I-P	8.1					x	x	x	x	x	x	x	x	
		I-P	8.2					x	x	x	x	x	x	x	x	
		P	8.3					x	x	x	x	x	x	x	x	
		P	8.4					x	x	x	x	x	x	x	x	
	T9 Configuration hardening	P	9.1													x
		I-P	9.2													x
		P	9.3													x
	T10 Management of event logs and alarms	D	10.1					x	x	x			x	x	x	
	T11 Malware protection	P	11.1					x	x	x			x	x	x	
		P	11.2					x	x	x			x	x	x	
	T12 Network Authentication and Encryption of the data	P	12.1													x
		P	12.2													x
	T13 Antenna Set Up	P	13.1	x	x	x				x	x	x				

In the scope of the project, one proceeding is presented in the IAMU 22 student session [57] .



IAMU AGA22

Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships

Gizem Kayisoglu [1,*], Pelin Bolat [1] and Kimberly Tam [2]

[1] Istanbul Technical University, Türkiye
[2] The University of Plymouth, United Kingdom
* Corresponding author: yukselg@itu.edu.tr; Tel.: +90 531 454 93 03.

Abstract: The digitalization in maritime industry rises integration of the information and operational technologies on the vessels. The high level of connectivity and the rising of digitalization in maritime sector increase the cyber security issue. The systems of vessels can be exposed to errors of digital world and encounter some malicious attacks. At this point, cyber security in maritime sector is an important topic in terms of not only securing the systems, preventing the accidents, loss of life, and damage to the environment but also national security, and global economy. Accordingly, in the context of IAMU 2022 Research Project for Young Academic Staff, it is aimed to determine maritime cyber security dynamics based on informational technology (IT) and operational technology (OT) for ships, dynamics affecting any breaches in the scope of maritime cyber security in marine insurance, and liabilities, responsibilities, rules and enforcements in the scope of maritime law. Thus, it is aimed to develop maritime cyber risk check list for ships by performing maritime cyber risk management with the help of these dynamics in the project. In this context, in this paper, the issues of maritime cyber security on the perspective of maritime cyber risk and maritime cyber insurance and suggestions on solutions of them is only tried to be emerged for creating an infrastructure of the project.

Keywords: maritime cyber security; maritime cyber risk; maritime cyber insurance

1. Introduction

The high level of digitalization and connectivity in maritime sector make the cyber security issue come to the force. In particular, ships became connected to universal networks, incorporated complex digital industrial systems, and integrated with the information and operational technologies. The systems of vessels can be subject to errors of digital world and faced with some malicious attacks [1]. At this point, cyber security in maritime sector is an important topic not only with respect to the particular of securing the systems, preventing the accidents, loss of life, and damage to the environment but also with respect to national security, and global economy. Furthermore, a cyber-breach gives rise to financial loss, disruption in the business procedures, and damage to reputation. Against all of these dangers, a company wants to get rid of the incident quickly and secure itself to work normally again. For this purpose to be achieved, both the issue of ship protection systems against physical attack, the design of the systems and supporting process should be taken into consideration at first.

The cyber environment of ships contain interconnected networks of both Information Technology (IT) such as the computer-based systems, personal computers, tablet devices, laptops, routers, servers and switches, etc. and operational technology (OT) such as, control systems, actuators, sensors, radar, etc. The cyber space onboard provide services, information, business and social functions. Besides, personnel security, the insider threat from shore-based or shipboard, ship-owners, operators, stakeholders, procedures, process, and physical aspects are important assets for cyber security responsibility in maritime. Appropriate measures should be taken in the framework of these assets.

When the historical developments of cyber security in maritime are evaluated, a hierarchical improvement is observed and it has been noticed that the above-mentioned framework is specified at every stage of this development. After the 2010 Strategic Defense and Security Review made publication about cyber security as a top threat for national security, in the maritime sector, it has become a prominent issue [2]. In 2011, ENISA highlighted the low cyber security awareness for maritime sector and suggested some titles about cyber security in maritime for raising the awareness [3]. In 2016, International Maritime Organization (IMO) has issued a circular about Guidelines on maritime cyber risk management. As per this circular, cyber risks are appropriately addressed in the International Safety Management (ISM) Code until 1st of January 2021. With these

Additionally, the case study section about CORAS-based cyber risk assessment for shipboard RADAR has been under-review process in a journal.

A Novel Application of the CORAS Framework for Ensuring Cyber Hygiene on Shipboard RADAR

Gizem Kayisoglu[a*], Pelin Bolat[b], Kimberly Tam[c]

[a]*Department of Maritime Transportation Management Engineering, Istanbul Technical University, Istanbul, Türkiye;* [b]*Department of Basic Sciences, Istanbul Technical University, Istanbul, Türkiye;* [c]*School of Engineering, Computing, and Mathematics, University of Plymouth, Plymouth, UK*

*Corresponding Author. E-mail: yukselg@itu.edu.tr

A novel application of the CORAS framework for ensuring cyber hygiene on shipboard radar

Abstract

Radio Detection and Ranging (RADAR) equipment is a significant information and navigational system onboard vessels and a critical part of a ship's cyber space. It is an electronic system used for not only detecting surrounding objects, indicating their positions, and tracking targets by using radio waves, but also providing safe navigation by receiving and displaying data from other navigational devices. Therefore, it is concerning to see that marine RADAR systems have various cyber vulnerabilities, including data deletion and data relocation. Accordingly, shipboard RADAR systems can be manipulated and penetrated via malicious software, unauthorized remote access, human error, or sabotage by internal and external attackers. This is critical to the cyber hygiene of the ship, which affects its reliability and safety. This study performs a cyber-risk assessment using the CORAS framework for RADAR cyber security by developing case-based RADAR cyber scenarios. The CORAS framework is a methodology for risk assessment in this study to understand a ship's RADAR cyber-attack surface in terms of both its specific information technology subsystems and the cyber control measures. The output of this study includes a holistic, visual assessment of RADAR's cyber security for both its cyber vulnerabilities and cyber hygiene to better protect shipboard RADAR in the future.

Key words: shipboard RADAR; maritime cyber security; CORAS risk assessment; RADAR cyber security; cyber security risk assessment

Funding details

This study is funded by the IAMU Young Staff Research Project 2022 as titled of "Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships" [Research project number: YAS20220301].The materials and data in this publication have been obtained through the support of the International Association of Maritime Universities (IAMU) and The Nippon Foundation in Japan.

International Association of Maritime Universities

Meiwa Building 8F, 1-15-10 Toranomon, Minato-ku, Tokyo 105-0001, Japan

Tel : 81-3-6257-1812 E-mail : info@iamu-edu.org URL : http://www.iamu-edu.org

ISBN No. 978-4-907408-49-7