TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology

Dariana Khisteva 194237IVCM

A PROPOSAL OF INTEGRATING OPEN-SOURCE IDS INTO VESSEL'S BRIDGE NETWORK

Master Thesis

Supervisor
Olaf Manuel Maennel
Professor, Dr. rer. nat.
Co-supervisor
Gabor Visky

Tallinn 2021

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Dariana Khisteva .....
(signature)

Date: 14.05.2021

Abstract

The problem with the cybersecurity in the maritime industry is an approach to defend against cyber threats by general IT-oriented cybersecurity solutions. The shipowners prefer to buy a commercial tool to assure compliance with the new regulations, ignoring the unique nature of the network communication environment on a ship that needs to be protected. That is why this thesis is aimed to analyse the possibilities of open-source IDS solutions to serve as a cybersecurity tool on a ship's bridge network taking into account the maritime-specific properties of the ecosystem.

In order to identify the need and appliance of IDS in the system, we analysed the possible attack scenarios that can intervene in the safe navigation operations of the ship with the help of attack tree modelling methodology.

In addition, the ship communication protocol data were collected and analysed in a ship simulator with the real equipment that was built in NATO Cooperative Cyber Defence Centre of Excellence. We analysed the time intervals of the messages and draw conclusions on possible novel attack scenarios.

Finally, the placement of IDS on the bridge was proposed, what benefits it will bring to the system were discussed and the way of how to advance detection mechanisms in IDS in order to address the novel attack was introduced. The application of IDS onboard is quite diverse: it can be used as passive monitoring, it can help prevent attacks in IPS mode, it can be used for forensics analysis, and all these features can be directed not only for IT attacks but also industrial protocol attacks.

This thesis is opening a continuous discussion about how industrial world can get an advantage of open-source IDS solutions and what challenges are there.

The thesis is written in English and contains 53 pages of written text, 6 chapters, 25 figures, 2 tables.

Acknowledgements

I would like to express my unlimited gratitude to the people who helped me during this research study. This Master thesis would have never happened without you.

First of all, I would like to thank my supervisor, Prof Olaf Manuel Maennel, for the weekly meetings that helped me to stay on track; for making me smile even when it was a bad day. For fast feedbacks on my work and invaluable support. You were always there for me.

I would like to thank Gabor Visky, who introduced me to the maritime research community, helped a lot during the data acquisition process. For the interesting, full of great conversations research trips to ships. Thank you for speeding up the process of building ship bridge in NATO CCDCOE center.

Thank you, my reviewer, Prof Risto Vaarandi, who provided fast and insightful comments and suggestions that helped to estimate the quality of the work. Thank you for giving detailed and explanatory feedback, pointing out thighs that can help to make my thesis stronger. Also, thank you for inspiring me to connect my thesis with monitoring solutions, your “Cyber Defense Monitoring Solutions” class is incredible.

Thank you, my manager, Kaur Virunurm, at Starship Technologies, who always supported my study leave days, understanding my situation and motivating me to do my best. Thank you for belief in me.

Finally, many thanks to my mum and dad for supporting my decision on studying in Estonia, never doubting my choices and motivating me to continue. Even though, I know that you do not know English, I will translate this for you!

List of abbreviations and terms

AIS	Automatic Identification System
BNWAS	Bridge Navigation Watch Alarm System
COG	Course Over Ground
COSCO	China Ocean Shipping Company
DCS	Distributed Control System
DoS	Denial of Service
DPU	Data Processing Unit
DSC	Digital Selective Calling
ECDIS	Electronic Chart Display and Information System
EPIRB	Emergency Position Indication Radio Beacon
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HIDS	Host Based Intrusion Detection System
ICS	Industrial Control System
IDS	Intrusion Detection System
IMO	International Maritime Organization
INS	Inertial Navigation System
ISM	International Safety Management
IT	Information Technology
LAN	Local Area Network
NIDS	Network Intrusion Detection System
OS	Operating System
OT	Operational Technology
RADAR	RAdio Detection And Ranging
RDP	Remote Desktop Protocol
S-AIS	Satellite-based Automatic Identification System
SIS	Safety Instrumented System
SIEM	Security Information and Event Management
SMB	Server Message Block
SOG	Speed Over Ground
TCP	Transmission Control Protocol

TOS	Terminal Operating System
UDP	User Datagram Protocol
VDR	Voyage Data Recorder
VHF	Very High Frequency
VTS	Vessel Traffic Service

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Motivation

Nowadays the importance of the shipping industry for modern society is hard to underestimate: more than half of goods across the world are being transported by the sea [1]. A global trend in progressive digitalization of the world is affecting different industrial structures including the maritime transport sector [2]. Electronic navigation is actively developing in the maritime domain: ships increase in size and crews decrease in number due to the automation of processes; the onboard systems receive updates during the voyage; the teams have access to the Internet – this all makes the life of the shipping industry much faster and easier thus more vulnerable to cyberattacks [3].

The work of chart plotters, echo sounders, radars, automatic systems, and other sources of onboard information is interconnected, and information from them can be aggregated, aligned and processed. This interaction makes it possible to speed up the decision-making process on the selection of the direction of movement from the proposed options offered by the navigation system.

"Along with the growing reliance on automation, the risk of external interference and disruption of key systems is greatly exacerbated; hackers can interfere with the management of the ship or the operation of navigation systems, cut off all external communications of the ship, or obtain confidential data," says Allianz's Shipping Safety Report [4].

Electronic navigation equipment used onboard modern ships have undoubtedly decreased the ships collision incidents over years [5]. However, it brought the problem of crew total trust in what they see on the displays rather than what they can spot in the window, opening a completely new way for an adversary to intervene in ships operations. "We have seen serious losses from an overreliance on electronic chart displays and human error on the part of crew," says Captain Andrew Kinsey in his interview [6]. Several past incidents have shown the impact of cyber interference into digital navigation that can cause real damage [7, 8, 9]. Sometimes, due to weather conditions (fog, storm, etc.), the only way to control the situation at the sea is to rely on navigational equipment. In those situations, an attacker has an advantage in exploiting navigational systems in order to affect human actions which

can lead to not only financial impact but catastrophic consequences for the environment, safety of the people and overall transportation business development.

However, sometimes the threat is lying in accidental mistakes of the crew on board who might not understand the importance of cyber hygiene on a ship. Phishing emails, personal devices, suspicious websites - those are still an old and well-worked way of delivering malware to the system. While people working in the IT sector are having an understanding of cybersecurity awareness, ship crews are still behind the schedule in cybersecurity education [10, 11].

The crew's unintentional misuse and mistakes that led to cyber incidents on ships can be easily preventable with correct cybersecurity tooling. Currently, even simple protection of computer systems on ships, like antivirus, is being disabled. The reason behind this is laying in the fact that automation and navigation integrator companies prioritise safe navigation and correct operation of the equipment above cybersecurity risk. Accidental blockage of the valid communication channels between ship components is an unacceptable risk for the shipowners. Bringing IDS solution to the network that alerts on potential malicious activity can become the first step towards a compromise between undisruptive sailing and IT/OT security on board.

Nonetheless, the unique nature of network communication inside the ship is making it difficult to use standard defence mechanisms for IT networks. This lays in the fact that on the ship we can find not only TCP/IP packet transmission but also industrial protocol communication like NMEA 0183/2000 for ship sensor data or AIS messages, etc. And that data is being encapsulated into TCP/IP packets to "feed" computer systems, however, regular cybersecurity solutions will not be able to spot malicious behaviour in industry-specific communication.

That is why an idea of a well-known IDS solution that can be adopted for ship security needs was born. For the feasibility analysis of this proposal, Snort IDS was chosen. We studied the idea of detecting and mitigating "classical" cyber threats by existing signatures as well as if we can advance detection mechanisms to notice specific threats that are unique to the maritime sector. A detailed explanation behind choosing Snort is provided later in the thesis in Section 5.1.

Interviews with the experts in the maritime domain have shown slight doubt about the shipowners' business needs to consider cybersecurity as part of the budget, as, even though, the ship's equipment can run outdated software, it is still secure enough due to the fact that the ship system is most of the time offline and well isolated from other networks

(such as ship's guest network). However, we are living right now in fast-changing world conditions where autonomous shipping will sooner or later become a common way of transportation where IT and OT systems will be tightly interconnected and require a constant Internet connection. This is opening a discussion about the high importance of addressing cybersecurity on the ship.

1.2 Problem statement

"There are few reports that hackers have compromised maritime cybersecurity. But researchers say they have discovered significant holes in the three key technologies sailors use to navigate: GPS, marine Automatic Identification System (AIS), and a system for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS)" [12].

Cybersecurity subject and maritime operations have become significantly interconnected nowadays. On the 1st of January 2021, the IMO's Resolution MSC.428(98) [13] came into effect, which forces the shipowners and ship companies to report any cyber risk in their ISM (International Safety Management) Code [14]. This made a clear point for the shipowners that to continue worldwide operations, they need to make an effort to address cybersecurity.

Attackers are far ahead of defence mechanisms on ships. That is why it is crucially important to understand the attackers' behaviour as well as develop domain-specific countermeasures at a reasonable cost.

"My message to companies that think they haven't been attacked is: "You're not looking hard enough" says James Snook [15]. This statement emphasises the importance of the information systems being monitored and people understand what they are trying to protect against.

The regulations that exist [16, 17, 18] are giving the requirements for shipowners to be cybersecurity complaint but not giving the exact methods of how to achieve this. Therefore, almost all standards emphasize the importance of the ability to observe and detect potentially malicious activity. However, there are no clear, well-structured and understandable methods on how to implement the network monitoring solution for the ship's bridge system to achieve observability. Moreover, how to achieve this goal in a cost-efficient and pragmatic way. That is why the main research question of this paper is:

"Can "open-source" intrusion detection software be incorporated into commercial ship's

bridge navigation integrator package to properly address the existing and industry-specific cyber threats?"

Nevertheless, there is just growing attention to the maritime sector in terms of cybersecurity, therefore there is no free, out-of-the-box solution that can help ships to stay secure.

Due to the type of ship bridge environment, where a complex mixture of TCP/IP and industrial protocol communications takes place, the bridge system is open to both off-the-shelf known attacks as well as unstudied protocol-specific attacks. This brings the importance of the multiplex approach to detect potentially malicious activity on the ship. The NIDS (Network Intrusion Detection System) that was chosen to conduct the feasibility study is Snort [19], the detailed explanation behind this decision is provided in Section 5.1.

In order to answer the main research question, we needed to state and clarify several sub-questions, namely:

1. What are the threats posed to the ship electronic navigation equipment?
2. Can open-source IDS detect the attack vectors posed to navigation equipment on the ship?
3. How to advance the detection functionality of the open-source IDS to address the novel attack vectors on the ship bridge network equipment?

1.3 Goal and Scope

This work is aimed to study the feasibility of the proposal of integrating an open-source intrusion detection system into the commercial environment on the vessel's bridge. To achieve this, we mapped possible resemblances between the office IT network and IT network on the vessel, potentially applying existing countermeasures for detecting malicious information activity. Moreover, we described the unique nature of the communication protocols used of the vessel to suggest a modification to detection mechanisms.

The goal is to understand what the critical informational and system assets on the ship are; what threats pose the high-risk level; how to detect and respond to the potential attack happening on the ship. We want to achieve a monitored and predictable system condition, network traces and history of the events on the ship's bridge navigational system.

The scope of this research is limited to analysing and building a threat landscape and proposing the implementation of the network intrusion detection solution - Snort - for the electronic navigational system on the non-military vessel bridge.

The scope of conducting the network traffic analysis is data collection in the simulation laboratory, with some parts being real ship equipment, in the NATO Cooperative Cyber Defence Centre of Excellence. Detailed description is provided in Chapter 4. This technical feasibility analysis gives the author insights into domain-specific protocol details and their behavioural patterns.

Based on the network traffic analysis scope, this research paper has a limitation of analysing the normal behaviour patterns and proposing potential detection mechanisms for the system components on the ship's bridge, narrowed down to ECDIS, RADAR and AIS transmitter. The detailed explanation of ship's bridge components and their impact on sailing operations is provided in Section 2.3. This limitation comes from the fact that NATO CCDCOE center has not built an exact copy of the ship's bridge, virtualizing or leaving some parts setup for later stages.

The thesis contains the description of the novel attack scenario in the industrial protocols - NMEA and AIVDM/AIVDO. However, it is not posing ethical concerns as it is a theoretical conclusion based on the real ship data analysis, otherwise, not being technically tested and not calling for action. The author is also proposing a way to mitigate discovered new branch of attack scenarios called timing attacks.

The outcome of the study is a systematised method of detecting the treats on the electronic navigational system on the vessel and addressing them by open-source intrusion detection solution proposing possibilities of software customisation in order to achieve advanced threat detection in industry-specific protocol communication.

1.4 Contribution

The contribution of this research paper is to produce a feasibility analysis of addressing existing and novel attacks vectors on the navigational equipment on the ship by a well-known open-source NIDS - Snort. To prevent the reinvention of existing countermeasures for the known cyber threats, we are going to analyse the possibilities of Snort as well as introduce the way how we can advance the detection mechanisms in Snort based on the data analysis.

The systematisation of the existing threats is conducted based on the literature review. The representation format that was chosen for drawing the threat landscape is graphical-based attack tree models. This modelling method allows seeing the key aspects of the presented approaches, which helps select the appropriate defence methods.

This works also introduces the message time intervals analysis for NMEA and AIVD-M/AIVDO communication protocol. The findings can be found in Chapter 4. Data collection was conducted in NATO CCDCOE center where the ship bridge simulator was built.

The network traffic analysis has shown a novel attack vector that can breach the integrity of navigation data. We introduce possible scenarios in Section 4.4.

1.5 Research Methods

The main research method used in this thesis is a feasibility study. The main subparts of feasibility study include legal, operational and technical feasibility of proposed idea. The economical feasibility is being briefly discussed and scheduling feasibility is not relevant for our research.

In addition, here are several research methods used to complement the feasibility study. Those include:

- Secondary data analysis / archival study on the past academic and research documents;
- Threat analysis using Attack Trees method which is being described in Section 2.2;
- Experimental data analysis - based on the fact that we are using the simulation of the real ship bridge system (electronic navigational ship system) and mapping the behaviour of the real ship to the simulated environment;
- Semi-structured interviews;
- Use case approach to observe the new attack vectors and propose mitigation.

For the purpose of this research paper, it is needed to identify the threat model for the ship navigation electronic equipment which can be controlled and observed by the monitoring system installed on the ship. The threat modelling method that was used is the Attack Tree method. During the literature review, it was identified that the Attack Tree method was used for threat modelling for ships [20] recently, focusing on broader aspects of attacks including human behaviour and misuse of the systems, whereas this research is using attack tree methodology to illustrate the attack flows and threats posed to navigational equipment only. Also, as attack trees are capturing the dynamic picture of the world, it was proven to be one of the best application for identifying network attacks [21].

The method for the literature review that was mostly used is “forward snowball” – after finding the particular relevant paper and seeing where this paper was cited to find related

literature.

The criteria that can be used for selecting the relevant resources are publications, academic papers with a high number of citations, international IT conferences that are recognized throughout the world. Also, the research is conducted starting from the latest updated documents and coming to the older versions in order to analyse the evolution of the mitigation of the possible attack options. The publications date boundary is limited to the papers published between 2001-2021.

In this research area it is not enough to operate with existing data due to the fact that the ship network structures, inside protection mechanisms are not available for public use. Therefore, semi-structured interviews were conducted with the focus group identified as people working in the maritime industry and maritime cybersecurity researchers, namely with:

- technical solutions managers and chief engineers during several research trips to the real ships from November 2020 to March 2021 (Leiger and Tiiu ships at Rohuküla port) as well as Teams calls in April 2021;
- maritime cybersecurity researchers from NATO CCDCOE center;
- lecturers from Estonian Maritime Academy of Tallinn University of Technology.

In respect of peoples' privacy, the personalities are being anonymised and permission for using the feedback was received.

1.6 Thesis Structure

The thesis structure organised as follows. Chapter 2 gives the background and information related to the research paper topics, namely: What are attack trees? What are the main components of the bridge navigational system on the ship? What is NIDS? Chapter 3 gives an analysis of the created attack trees. Chapter 4 describes the simulator network schema and gives an analysis of the network traffic of the ship's bridge. Chapter 5 gives a proposal for monitoring solution and recommendations. Chapter 6 gives a conclusion and final thoughts of the author.

2 Background Information

2.1 Legal Basis of Maritime Cybersecurity

An understanding of the need to take appropriate actions regarding cybersecurity onboard is recognised both at the international and national levels. Worldwide, classification societies are actively involved in the development of recommended practices, guidelines and standards for cybersecurity in the maritime domain. Cybersecurity became a regulatory requirement for shipowners.

The importance of addressing the aspects of detecting malicious activity on the ship IT network is being described and required by almost all official directives and guidelines that are applied to vessels' cybersecurity approaches.

The IMO (International Maritime Organization) Maritime Safety Committee in June 2017 adopted Resolution MSC.428 (98) – Managing maritime cyber risks in safety management systems [13]. The resolution calls on administrations to ensure that cyber risks are adequately addressed in existing security management systems no later than the first annual review of the company's document of compliance after January 1, 2021. The IMO recommends the measures to enhance maritime security as well as guidelines for formal safety assessment republished in 2018 [22]. The guidelines are showing the way how to achieve total visibility and control over assets, including risk control options.

The document written by one of the largest international shipping associations BIMCO [23] provides recommendations for ensuring the safety of onboard IT systems, as well as examples of the possible consequences of violation of these recommendations.

In particular, the largest classification society DNV GL in 2016 developed the recommended practices "Cybersecurity resilience management for ships and mobile offshore installations in operation" [24], and Japan's leading classification society Class NK is developing its approaches [25] to ensuring onboard cybersecurity for ships.

The process of developing and improving the structured, standardised and complex approach for building connections between maritime and cybersecurity aside from legislation

also include understanding of threats and vulnerabilities that exist and how to evaluate the consequences with the proper risk assessment. The International Maritime Organization recommends that cyber risk management be pursued through a natural extension of existing maritime and ship safety management practices. IMO views cybersecurity as part of maritime security and safety [18]. That leads to the indisputable importance of conducting the risk assessment for the shipping industry.

This technical report [26] provides high-level agency recommendations, good practice for handling specific cyber threats to the maritime sector. It serves as a pattern towards making the advancement of cybersecurity in this specific place through desk research, individual interviews, questionnaires and validation workshop. Several important parts were highlighted and strongly recommended: proposals of the conceivable approaches that can be taken for mitigating the possible risks in the maritime industry; the public relations between different stakeholders and investing into cybersecurity awareness of the people inside the organization; policy creation.

The Guidelines on Maritime Cyber Risk Management proposed by IMO [18] give a high-level overview of the ways to cope with cybersecurity administration for the shipowners. The vulnerable systems described are including the bridge vessel's system which we are targeting in this research paper.

This is not a full list of the documents that insist on taking cybersecurity of the vessels seriously, dedicating resources (human, financial, etc) to ensure an acceptable level of security in order to operate on the market. Consequently, we are going to propose a method how to address the common pattern within the requirements, called "Assess and Detect".

2.2 Attack Tree Methodology

For the purpose of this research paper, attack trees are going to be used to define a network security monitoring strategy and to define the real threats that are posing danger for the vessel network infrastructure as by using this methodology we can visually build the interconnection between cyber and cyber-physical parts of the system as well as clearly see the evolution of the attack scenario in order to understand at which stage we will be able to catch potentially malicious activity.

Attack tree is a model that describes different possible scenarios on how to achieve the predefined goal. In the field of information technology, it is used to describe potential threats to a computer system and the possible attack methods that implement these threats. In our case, we going to use attack trees as diagrams that show how a target (vessel

network system) can be attacked simulating the adversary behaviour. However, the use of an attack tree threat modelling method is not limited to the analysis of conventional information systems. They are also widely used in computer control systems (especially, related to power grids), aviation and defence to analyse the probable threats associated with tamper-resistant electronic systems (for example, to the avionics of military aircraft [27]).

Attack trees are multilevel diagrams with a single root, leaves, and descendants [28]. There is an objective at the top as a root node of the attack tree with the leaves coming down from the root to address the specific sub-actions (leaf nodes; attack vector nodes) that needed to be completed in order to achieve the objective [28]. Child nodes are the conditions that must be met for the parent node to become true. When the root becomes true, the attack is successful. Each node can only be brought into its true state by its direct descendants.

By including the prior probabilities at each node, it is possible to calculate the probabilities for the nodes higher in the tree structure by Bayes' rule [29]. However, in reality, accurate estimates of the likelihood are either unavailable or too approximate to give a certain conclusion. As we are using the attack tree threat modelling approach to complement the monitoring solution directions, the quantitative analysis is out of the scope.

As Sjouke Mauw and Martijn Oostdijk [30] advise "the most efficient way to prevent a threat in the attack tree is to prevent it as close to the root as possible", the monitoring setup is going to be proposed in a way to follow this direction.

2.3 Navigation System Assets Description

In order to continue observation of the current cyber-related problems of the passenger vessels, it is necessary to briefly highlight the information systems and technologies used to better understand the cyber-physical assets that are needed to be protected on the vessel's bridge. It is worth noting that it is not a complete list of the systems used on the bridge, however, it is highlighting the main ones which are mandatory to be installed on the passenger vessels which are making commercial trips [31].

- ECDIS (Electronic Chart Display and Information System) is an electronic cartographic navigation information system that visualizes navigational related information based on AIS messages, data from RADAR (RAdio Detection And Ranging), GPS and other ship sensors. Also, ECDIS provides aid to handle embedded charts. It is used for navigation and automation of some tasks of the navigator. This highly sophisticated device increases navigational safety. It should be noted that starting

from 2019, it was obligatory to install ECDIS on all vessel types specified in Chapter 5 in [17]. Most of the machines that are running ECDIS's set of applications are usually running Windows operating systems (often Windows 7 or even XP, referring to interviews in Appendix 2) and located on the bridge of the ship. Other systems are connected to the workstation of ECDIS, via the on-board LAN network, from which the Internet is most often available: NAVTEX (Navigation Telex) - a unified transmission system for navigation, meteorological and other line information; AIS; RADAR and GPS equipment, as well as other sensors [32].

- AIS (Automatic Identification System) is an automatic identification system that serves to transfer the identification data of the vessel, information about its condition, current position and course [33]. It is also used to prevent collisions of ships and provide communication between courts. "The device works by transmitting signals in the VHF band between ships, floating repeaters and coastal AIS gateways that are connected to the Internet" [34]. All ships on international voyages, ships of over 500 gross tonnage, and all passenger ships must be equipped with AIS. [31]. The system helps to search for objects in the sea and their location as well as in case of incident, transmit request of assistance signal. The ship's AIS display systems can be ECDIS, ARPA (Automatic Radar Plotting Aid), depending on the availability of appropriate interfaces. ARPA's capability can create tracks using RADAR contacts. The system can calculate the tracked object's course, speed and CPA (Closest Point of Approach), in order to warn captain in case of possibility of collision or natural obstacles.

- VDR (Voyage Data Recorder) is like a flight data recorder, an analogue of the "black box" used in aviation. "The main tasks are to record important voyage information of the vessel, including both technical and heading data, as well as voice recordings from the captain's bridge, and its preservation in case of an emergency" [34].

- GMDSS (Global Maritime Distress and Safety System) serves as an interconnected maritime communications network that helps ships avoid dangerous water emergencies and alert others about the danger. It provides radio communication with ships in case of distress, transmits information on the safety of navigation, including navigational and meteorological warnings [35]. Modern means of digital and satellite radio communications installed on ships and coastal radio stations made it possible to switch to an automated method of receiving distress signals, to increase the reliability and efficiency of communication. The devices of GMDSS can include:
  - EPIRB (Emergency Position Indication Radio Beacon) - an emergency radio beacon, a transmitter that, when activated, sends a distress signal, the transmission of which, depending on the technology of execution, can be carried out via

satellite, in the VHF range or in combination [35]. In addition to the distress signal, some EPIRBs can also transmit ship information (when synchronised with AIS).
  - NAVTEX - a receiver that operates at 518 kHz in the midrange [36]. Sometimes, the frequency 490 kHz can be used by some countries for transmissions in their national languages [36]. It serves to transmit and receive information about navigational, meteorological forecasts and warnings, even the state of the ice at the sea. This is not the full list of the warning types that NAVTEX can receive and process.
  - VHF radio with DSC (Digital Selective Calling) - the core of GMDSS.
  - HF radio with Telex as an alternative.

- RADAR (Radio Detection and Ranging) is a high-frequency electromagnetic device designed to detect air, surface and coastal targets, determine their parameters, including movement parameters, transmit information to ship visualization and analysis equipment [37]. The operation of maritime radars is based on the principle of reflection of electromagnetic waves from objects, analysing information about the range, size and characteristics of the movement of objects, which is most in-demand primarily for military purposes, as well as in civilian purposes from the point of view of organising the safety of navigation.

- INS (Inertial Navigation System) is a centralized computing unit that receives and processes the signals and measurement indicators coming from ship's sensors. "The inertial navigation system is a self-contained navigation technique in which measurements provided by accelerometers and gyroscopes are used to track the position and orientation of an object relative to a known starting point, orientation and velocity" [38]. The systems computes and gives the relative location values based on the last "known" location report.

It is important to understand how the navigational bridge system components work in order to define the critical threats which are going to serve as root goals in this research paper. A detailed analysis of the attack scenarios is given in Chapter 3.

2.4 NMEA Communication Standard

NMEA is a standard of the American National Marine Electronics Association [39]. NMEA 0183 was introduced in 1983 as a free industry standard for transferring data between electronic devices in marine vessels. It uses a simple ASCII serial communication protocol that records the transmission of a message from one 'talker' to another or other

'listeners' per unit of time. Although the standard is quite old, at the same time, it is still widely used and is well suited in situations of direct communication of one device (for example, a GPS navigator, which requires combining several data sets) with another. NMEA 2000 - can be considered a successor to the NMEA-0183 - was accepted as a standard IEC 61162-3 on IEC technical committee 80, working group 6 [40]. Although, many modern devices are designed to support both standards.

This standard works today in the international maritime industry. NMEA 2000 is more complex than the NMEA 0183 standard, it allows a combination of many elements in one network and transmit information simultaneously. When multifunctional displays are connected to the network system, the user can independently choose any combination of receiving data that he or she needs in a particular case and a given situation. NMEA 2000 has made possible the development of integrated navigation and control systems that can now be used on ships of all sizes and standards.

The NMEA format includes a message system for two-way information exchange between the ship's navigational equipment such as ECDIS, RADAR, GPS receiver, AIS, Gyro compass and information consumers (such as MFD). NMEA 2000 is based on CAN which is standardised by ISO [40]. ISO 11898 specifies the physical and data link layer of serial communication technology called Controller Area Network that supports distributed real-time control.

In the concept of NMEA protocol communication, we are going to view this type of communication as "pushing messages to a single device". That means we are neither keeping track of the received acknowledgements for the messages, nor can rely on the state of the communication. Each individual message is independent of the others and is "complete". The NMEA message includes a header, a set of data in ASCII characters, and a check-sum field to check the validity of the transmitted packet information.

As a single standard, NMEA 2000 allows the shipowners to switch and integrate equipment from different manufacturers allowing them "to talk the same language".

2.5 Network Intrusion Detection Systems

While talking about resistance of the system to cyberattacks, we can assume that we are talking about intrusion detection/prevention mechanisms taken into place (against software, insider, external advisory, etc). Also, we can classify intrusion into two major types: "anomaly" and "misuse" [41], where "anomaly" can be defined as change in the system indicators from normal predefined behaviour profile; and "misuse" is a way of known

system exploitation that can be detected with predetermined set of adversary behaviour patterns (rules/signatures) [41]. This research paper is focusing on the discussion around hybrid approach where anomaly detection can complement misuse detection. And here is coming the term - IDS (Intrusion Detection System), the host or software module that allows analysing the user and system activity behaviour.

The application of dynamic mechanisms for cyber defence can be achieved using IDS. The classification for intrusion detection systems can be separated to host-based or network-based intrusion detection systems. "A host-based IDS will monitor resources such as system logs, file systems and disk resources; whereas a network-based intrusion detection system monitors the data passing through the network" [42].

With the relevant signatures (rules) setup, IDS can detect malicious traffic activity which is trying to exploit specific vulnerability of the system. It is a passive solution designed to monitor a network segment of interest, analyse the packets that are passing through this network segment and make decisions - alert, block, etc.

The incoming traffic is split into TCP, UDP or other transport streams, after which the parsers mark them and split them into high-level protocols and their fields - normalising if required. The resulting decoded, decompressed, and normalised protocol fields are then validated with signature sets that identify whether network traffic contains attempted network attacks or packets inherent in malicious activity.

Having IDS technology around the controlled system is motivated by several facts:

- After two research trips to Port of Tallinn ferries, we discover that machines with navigational software (ECDIS, RADAR, etc.) are running Windows OS with antivirus being disabled. The reason behind this lays in follows: automation and navigation integrator is supplying packages for shipowners and intentionally disabling antivirus protection in there, as antivirus proved to react with false-positive alerts and blockage of the valid packet transmission that can disrupt safe navigation operations. That is why we can see vendors not trusting host-based security tooling. In case of IDS, it can be an external device in the network which, in case of any failure, will not affect the main processes on the ship and not interfere with the communication channel.
- Currently, if a cybersecurity incident has happened on the ship, the shipowner is making an official request to the system integrator to get information from the system logging (according to expect interview provided in Appendix 2), however, it is taking time. IDS on a ship can serve as logging and journaling tool that will help cybersecurity investigators, in case of an incident, perform forensics analysis based

on logs and traces as quickly as possible.

Due to the discovered facts provided in Chapter 5, we consider an analysis of possible implementation of signature-based IDS as in order to take best out of the setup and customise for maritime-specific protocol, we propose developing rules for threat hunting. However, the perspective of the installed IDS can be advanced with anomaly detection, it is out of scope for this research paper. Another aspect to consider - the network analysed can be classified as a small network so the need for enterprise-oriented IDS is eliminated.

The variety of open-source solutions that are fitting the needs of security monitoring on a vessel is quite diverse. There is a number of solutions included but not limited to:

- Snort [19];
- Suricata [43];
- Zeek (Bro) [44].

In Figure 1 we provided a comparison table for Snort and Suricata. Even though the article where this table was adapted from is dated by 2020, the information is partially incorrect as Snort 3 was released which made Snort multithreaded.

Table 1 Comparison of *Snort* and *Suricata IDS*

Parameter	Intrusion detection system	
	Snort	*Suricata*
Multi-threaded	No	Yes
Operating systems	All	All
Developer	Sourcefire	Open Information Security Foundation
Rules	VRT *Snort* rules, SO rules, pre-processor rules, emerging threats rules	Emerging threats rules, VRT *Snort* rules
Installation	Manual or using packages	Manual or using packages
User-friendly	More	Less
Documentation	Well-documented and provides solutions to common issues	Not well-documented
Cost	Commercial version has a price	Free
GUI	Large number of compatible GUIs	Very few
High-speed network support	Not present	Present

Figure 1. *Comparison table for Snort and Suricata [45].*

2.6 Related Work

The current problem state in the ship network monitoring system is becoming a new trend in the cybersecurity research world. In 2020 CyberOwl received a patent [46] for the

new method for threat detection in networks. The method logic lies in the calculation of historical reference activity of the peer node and its current “suspicious score” based on the symptoms. With the help of Bayesian-based framework, each symptom is transferred to probability. Based on the deviation, CyberOwl’s method is supposed to detect malicious activity in the network. This logic was used in the maritime monitoring solution "Medulla" developed by aforementioned company [47].

One more company that is focused on bringing cybersecurity to the shipping industry is Naval Dome [48]. The company is offering an out-of-the-box working solution that can be installed on any ship with Naval Dome 24/7 technical support ready to respond to alarms.

The studies towards bringing IDS solutions to industrial systems has been widely discussed. Mohamed Attia et al. [49] analysed power station threats and identified DoS and price manipulation attacks as attack vectors and proposed new detection policies to IDS. Liang in 2018 [50] proposed a model of detecting abnormal activity in electric power systems.

Snort IDS was studied as a forensics tool for investigating SCADA and control networks cyber incidents showing great results in combination with firewall and honeypots [51].

On the other hand, communication protocols on the vessel are being a subject of research papers. Daniel Blauwkamp et al. [52] proposed "strategy for implementing a behaviour-based anomaly detection system" based on the AIS message transmission trends. Konrad Wolsing et al. [53] introduced the initiative of developing a protocol-independent IDS system for industrial systems. NMEA protocol used in navigation updates on the vessel was part of this research along with Modbus and IEC-60870-5-104. The experiment shows that parsing of NMEA messages is the fastest among presented protocols being a bit more than 0.5 milliseconds.

It shows how IDS solutions can be integrated into industrial systems, hardening the protection layers. Based on those successful results, we are proposing implementing IDS into the internal ship network.

3 Threat Mapping using Attack Trees

In order to properly assess and make the best efficiency out of the monitoring system deployment, we need to understand what types of threats are considered to be the real ones as the nature of the analysed system gives different attack scenarios compared to the ordinary office network setup.

Several studies showed that using attack tree threat modelling method gives valuable results that can easily be analysed and interpreted. The formal method for threat modelling by Seyit Ahmet [54] showed how attack trees can ideally detect and represent network attacks. The problem of cost-effective solution of defence structure and decision for the suitable nodes to put safeguards in place proved to be solved by attack tree methodology as well [55].

Inspired by [56] who showed how attack tree can be used to map the threats in SCADA systems and by [57] who showed BGP (Border Gateway Protocol) attack trees models, it was decided to take a similar approach and apply it to the maritime domain.

Among the variety of the threats posing danger, it was decided to draw the threat landscape based on the literature review and newly developed framework for assessing cybersecurity risks in the maritime domain called MAINFRAME [58]. Therefore, U.S. Coast Guard is giving a proposal on risk assessment [59] using NIST framework. There are several risk assessment models proposed for the ship industry including [60, 61] as well as for autonomous sailing [62, 63]. The authors are giving measures to ensure the security of critical information infrastructure can be provided for in a unified plan for ensuring the security of a critical information infrastructure facility.

Also, for the basis of the threat intelligence gathering multiple standards were used, namely:

- NIST SP 800-53 - RA-5, SI-5, PM-12;
- ISA 62443 - 4.2.3, 4.2.3.9, 4.2.3.12;
- ISO/IEC 27001:2013 - 6.1.2.

The aforementioned standards, guidelines and research works are presenting the base

for choosing the attack vectors. In addition, here and further while talking about MFD (Multifunctional Display), we are going to refer to two separate server applications running on top: ECDIS and RADAR, which are described in detail in Chapter 4.

3.1 MFD attack vectors

Correct operation of the ECDIS system inside MFD is very important, its compromise can lead to the most adverse consequences - injury and even death of people, environmental pollution and large economic losses.

ECDIS systems usually do not come with any information security tools. It should also be noted that Windows systems deployed on ships that are on long voyages do not always have time to receive critical security updates within a reasonable time frame. After interviewing the Chief Engineers of Estonian shipping company, it was found out that on the ships there is no antivirus installed. The explanation that was given to us: "Sometimes the processes that navigation and positioning software needs to run, can be classified by antivirus as malware, so in order to not cause troubles during the voyage, the antivirus software is being disabled". Also, both IT systems of those ships were running on top of Windows 7 OS version.

The vulnerabilities found by the researchers from NCC Group Research & Technology are mainly related to the Apache server installed in conjunction with the system [32]. Malicious code can be injected either by an external adversary via the Internet or by a crew member via a physical medium used to update or supplement navigation maps. The vulnerabilities found made it possible to read, download, replace and delete any files on the workstation. With these evolving events, the attacker gains access to reading and changing data from all service devices connected to the ship's onboard network.

There are several attack scenarios aimed to compromise MFD system on the passenger vessel that we are going to discuss during this research study, namely:

1. ECDIS malware infection;
2. Unauthorised access to MFD;
3. Ship size change in ECDIS system;
4. Ship position change on electronic charts displays;
5. ECDIS displays ghost ships that do not exist in real life;
6. RADAR malfunctioning.

3.1.1 ECDIS malware infection

Malware infection is classified as one of the critical threat by several studies [64, 65, 66]. Business-critical software, being only compatible with legacy systems or protocols, sometimes cannot be upgraded or replaced. Some companies do not have a regular framework for patching and upgrading system components, and their antivirus software is thus obsolete [67].

During the vulnerability scanning of the INS by [68], one of the findings were related to remote code execution vulnerabilities that exist in the SMB service version 1.0. The vulnerabilities explained in the report could be exploited by a remote attacker to execute arbitrary code without authentication [69].

Ransomware has been common to traditional computing systems and could be adapted to the maritime domain [70]. In those situations ransomware impact is more dangerous than conventional ransomware attack on IT systems due to the isolated nature of ships at sea and their dependency on knowing where they are and being able to move further along the course.

In July 2018, one of the largest shipping lines, China Ocean Shipping Company (COSCO), became a victim of a cyberattack [71]. The company was faced with a ransom demand and intimidation of failure of all communication systems. The attack severely damaged the company's internal system. Even though COSCO was able to handle the situation with very little loss to its network and customers, it was an indicator that cybersecurity should have not the lowest priority.

In June 2017, the consequences of a ransomware cyberattack on Maersk caused losses of about $250-300 million: transport and logistics businesses were disrupted, leading to unwarranted impact [72]. Such significant losses for all parties contributed to the realisation of the fact that changes are really necessary. It is worth saying that the cyberattack against Maersk was a lesson for the entire shipping industry.

Another illustrative example of a cyber attack with serious consequences is connected with Norsk Hydro. The company became a victim of the LockerGoga virus which was encrypting the file systems causing $35-40 million financial damage to the company [73].

Cyber Guidelines for onboard ships [16] emphasise the importance of the ship owners to ensure the right protection from ransomware. The recent incidents highlight that many companies also lack a consistent approach for managing their systems' cybersecurity.

In Figure 2 we propose the attack tree model that corresponds to the ransomware infection and propagation scenario.

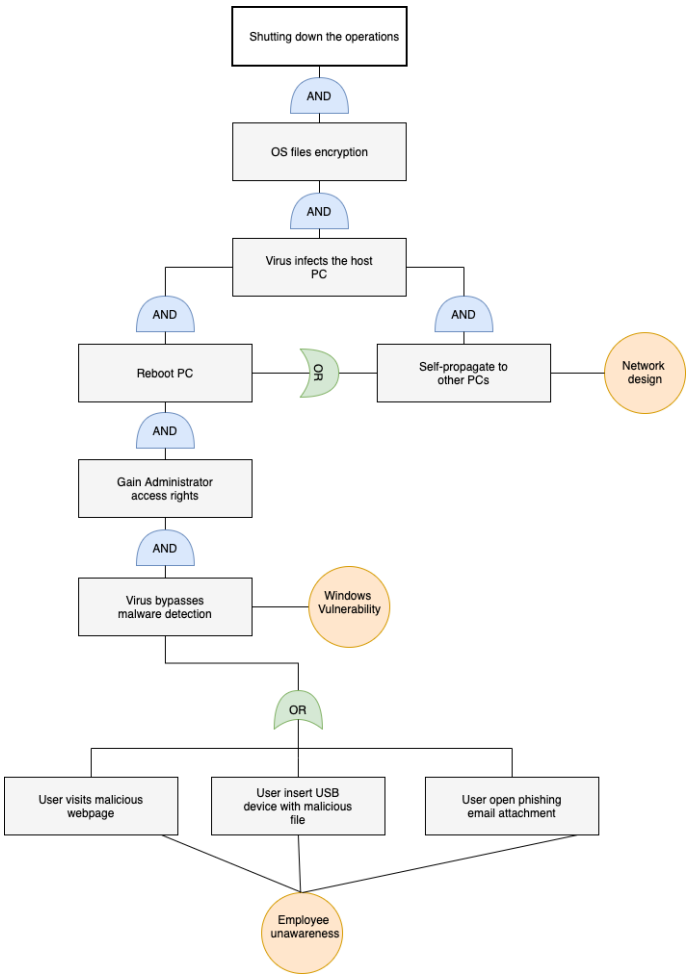

Figure 2. *Attack tree for ransomware scenario.*

Nevertheless, the nature of cyber world is changing every day, most of the incidents that involve system encryption occur due to:

- Malicious mail. The expertise of the attackers in creating fake emails has grown rapidly. The initial trust to some known companies, coupled with the low awareness of the crew about cyber threats, makes such attacks very effective. An attacker can fake the valid email coming from the shipowner company, where malicious attachments can be included that can lead to malware infection of the computer. And, in case of low awareness, computer might be connected to bridge network unintentionally.
- Malicious sites. The crew members being on voyage can use Internet for their own purposes. Unintentional download of content from suspicious online resources, can lead to malware download. Sometimes, it might be enough even to visit the web

resource and without human interaction, the host machine can be infected.

- Removable media. This is the main way of infecting computers on the bridge that either has no network connections at all or are part of small local networks without Internet access. "Most vessels use ECDIS as an offline system, and all updates are done by USB sticks. This results in a lot of interaction between the INS and auxiliary systems." [74] says. This fact was supported by the interviewed ship crew members. It was confirmed that, in most cases, the electronic navigational charts are being updated with a dedicated USB storage device. If a removable medium is infected, and an antivirus program is not updated on a computer, then there is a great risk of system encryption threat. It will be enough to insert the device into the USB connector [75].

These three paths are the main ones to case file encryption in the system, however, the aforementioned Maesk case [72] showed that the self-propagation nature of some ransomware still posing a high risk to the system. As we are limiting our scope to the IT system of the ship, it is worth saying that controlled area should be logically separated in order to quickly react to the possible infection of one single host in the system and be able to isolate infected host from the system.

3.1.2 Ship Position Change in MFD

In 2013, a US navy warship grounded itself on a coral reef due to an error with ECDIS [32]. Studies of this system have found ECDIS to have not been designed securely, e.g. accepting dangerous network methods. The crew, relying on the false information displayed on the navigational charts, caused the situation when the vessel and passengers aboard were held hostage at sea until the issue is resolved.

Another well-known and illustrative example of the compromise of satellite systems is the case that occurred in 2013 when students from the University of Texas were able to deflect an $80 million yacht from the course using a GPS signal simulator [76].

The general description of the attack scenarios for taking control over the vessel is presented in Figure 3.

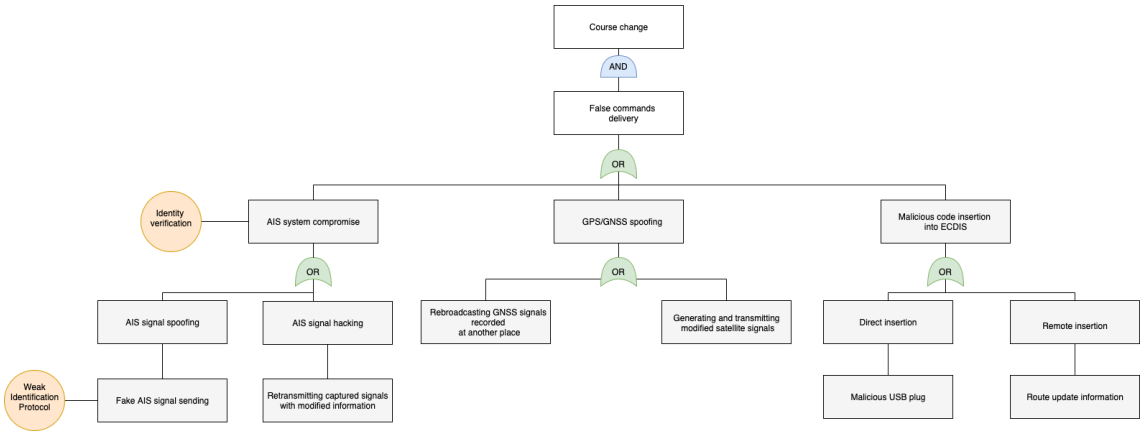

Figure 3. *Attack tree for gaining control over vessel navigational system.*

Passenger vessels are usually transmitting telemetry information about their current direction, cargo and route navigation using a narrow channel bandwidth and a short communication session. This can be enough for an adversary, who is using open data ports, default access settings and even bruteforce method. Thus, they can get access to the "administration panel" of the communication modem and the next step to get the right to execute commands and download data by hacking the network equipment by executing an exploit - a program code that exploits equipment vulnerabilities.

An attack tree model for gaining access to the system is presented on Figure 4.

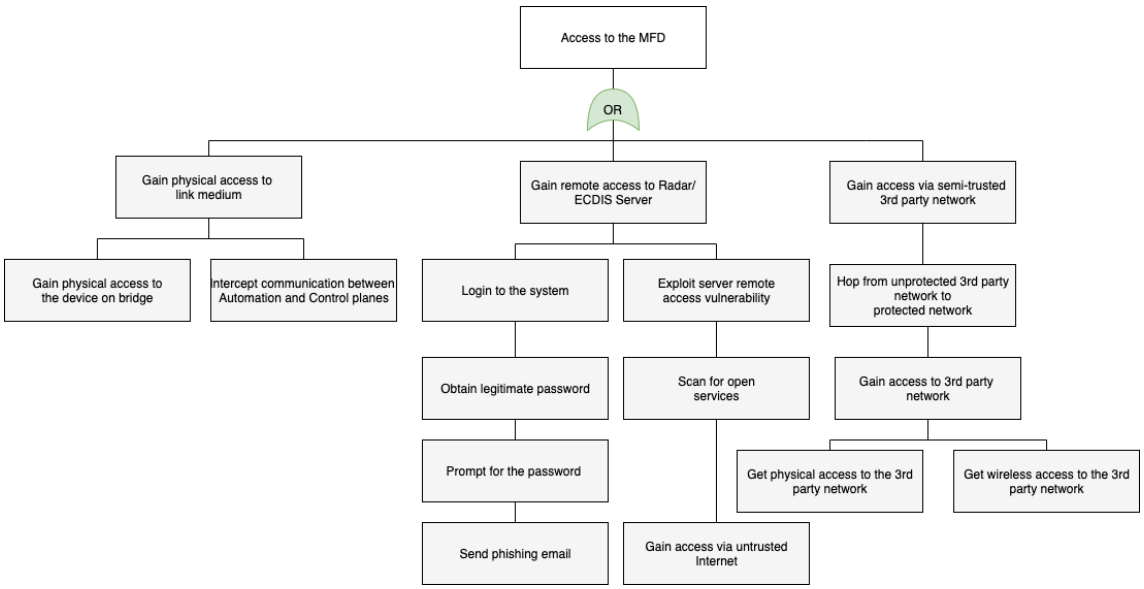

Figure 4. *Attack tree for accessing the administration module.*

After gaining control over the communication equipment and access to the LAN (Local Area Network) of the onboard bridge, attackers can launch an attack on almost any equip-

ment of the ship, be it navigation or ship management systems, passenger management system, administrative equipment, etc.

We can also elaborate the access tree child node with login process to a separate attack tree model presented in Figure 5

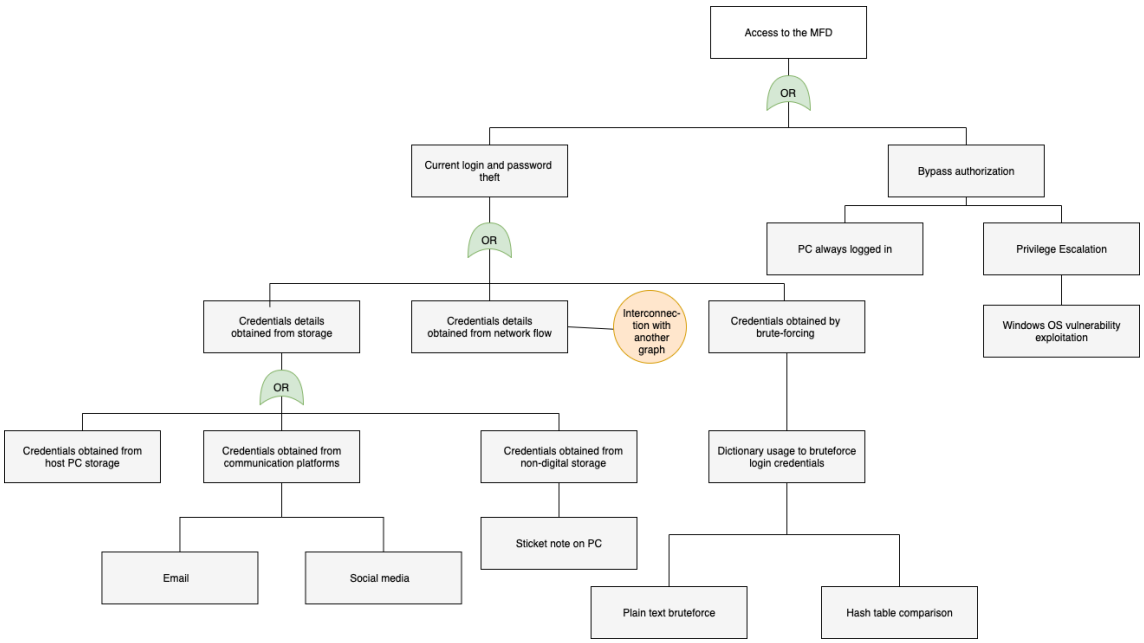

Figure 5. *Attack tree for obtaining login credentials.*

Major problems arise here as the typical countermeasures may not be applicable. Default passwords for the applications running in MFD are stayed unchanged, we can observe them even in publicly available manuals. Also, according to the interviewed technical engineers, all applications are running in a privileged mode which cannot be changed as a requirement from the manufacturer.

The child node "Credentials details obtained from network flow" presented in Figure 5 also can be advanced with the attack tree model displayed in Figure 6. Here the purpose of communication eavesdropping can be not only to gain access credentials but also to obtain sensitive information in the communication channel.

Moreover, at the latest Black Hat 2020 conference, Oxford student James Pavour has demonstrated how satellite communication can be listened in by $300 equipment [77].

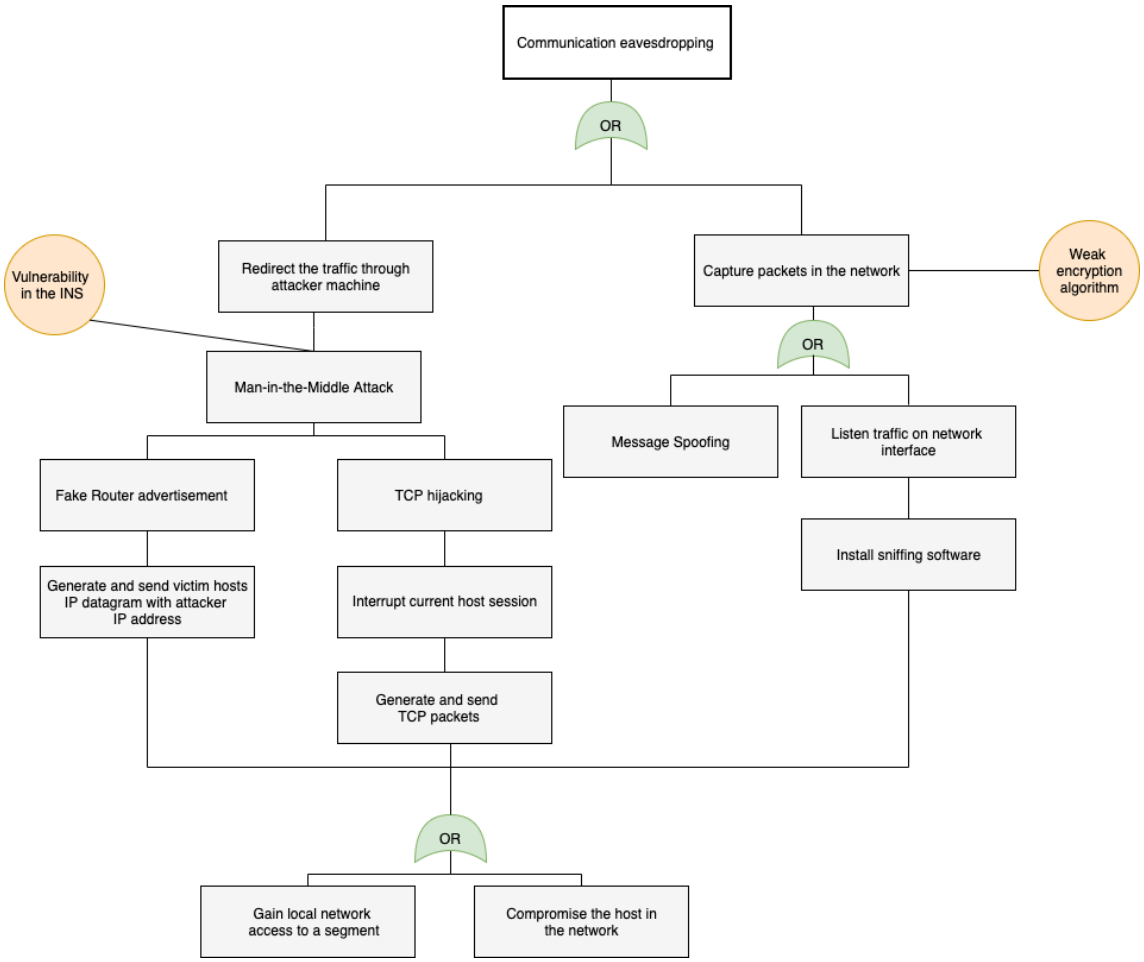

Figure 6. *Attack tree for intercepting the network traffic.*

During the vulnerability scanning of the INS by [68], it was found out the system is vulnerable to man-in-the-middle attack due to low encryption level. The vulnerability can be exploited by a remote attacker to gain access to the INS by RDP Server (Terminal Service). In this research paper, we are not focusing on detailed description of the standard network attack vectors as DoS and DDoS attacks as they are common for the usual IT network and ship IT network. They are well-described and studied so beyond the scope of attack trees modelling.

3.2 AIS attack vectors

The importance of keeping ferries on the correct course on the specified route and not deviating from it hard to underestimate.

The proof of this concept appeared during the research trip organization in February 2021. The company TS Laevad informed customers that they are not able to depart from the port

because one of the cargo ships is stuck in the sailing channel between the mainland and Hiiumaa. Due to this accident, the research trip was cancelled. The ferry cannot just go around the cargo ship - the Rukki channel is quite narrow and deviating from the course will end with running the ship aground. That is why getting the precise coordinates of the objects around the vessel during the sailing has become a principal point for crew members and captain to decide whether to keep the course or make unexpected route changes.

As it was described earlier, AIS serves as an interchange mechanism between ships, as well as between the ship and the coastal service, to transmit information about the call sign and name of the ship for its identification, its coordinates, information about the ship (dimensions, cargo, draft, etc.) and its voyage, parameters of movement (course, speed, etc.) in order to solve problems of preventing collisions of ships, monitoring compliance with the navigation regime and monitoring ships at sea.

The base for classifying AIS attack vectors was taken from the framework for assessing maritime cybersecurity readiness [78] where the authors are describing different approaches to compromise the workflow of AIS. However, the framework is not describing how the mentioned attacks can be achieved, where we are proposing attack tree models in order to understand attacker's needs in order to be successful.

The summarised attack tree model for compromising the work of AIS is provided in Figure 7.

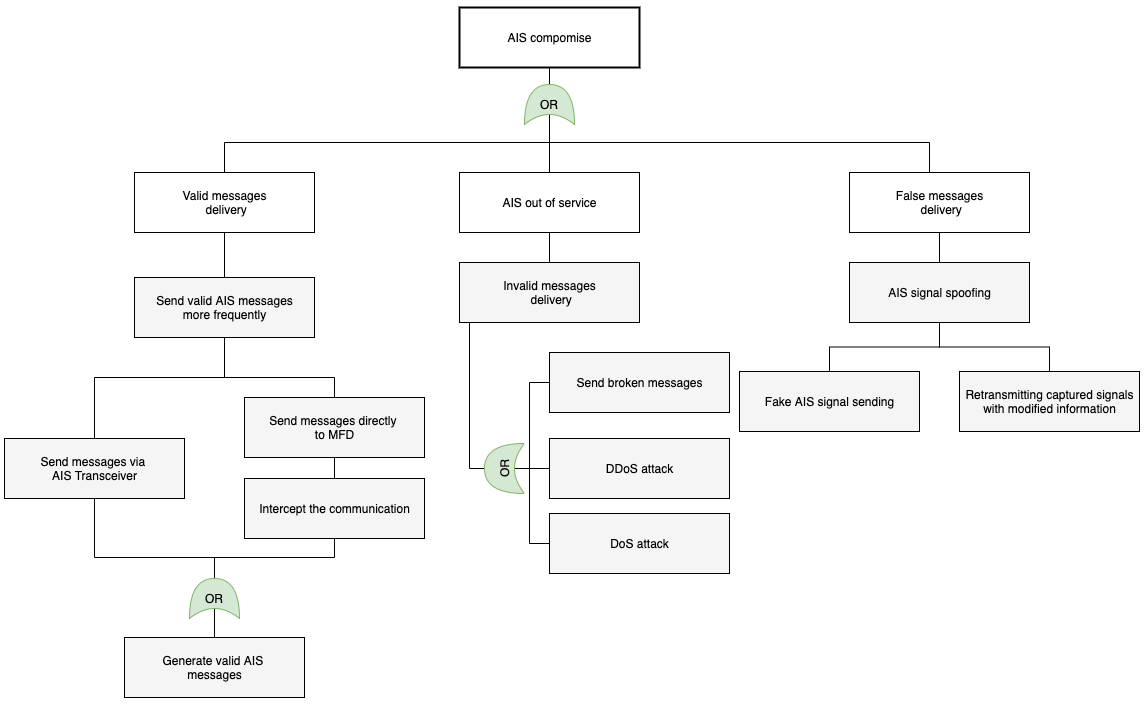

Figure 7. *Attack tree for AIS work compomise.*

Several scenarios are possible in order to compromise the work of AIS [78]:

- changes in ship data, including its position, course, speed and name;
- creation of "ghost ships", recognised by other ships as a real ship, in any location in the world or vice versa - make the real ship invisible on the electronic displays;
- sending false weather information to specific ships to force them to change course to avoid a non-existing storm;
- activation of false collision warnings, which can also cause the ship to automatically correct the course;
- the ability to conduct a DoS attack on the entire system by initiating an increase in the frequency of transmission of AIS messages [34].

By sending false data to the vessel AIS transponder it is possible to create enormous amount of "ghost ships" so the vessel will not be able to operate further as it will be impossible to differentiate between the real object and attacker's fake ships. This attack is possible due to the fact that AIVDM/AIVDO protocol is designed without security in mind as, back in history, it was a belief that the creation of transmitter is expensive and will not be a potential threat.

Security researchers have found ways to abuse the system, such as generating valid commands, changing ship courses, replaying commands, and tracking ships, for potential physical attacks [33]. The general consensus is that these systems are poorly designed at the protocol level, and at the implementation level [70].

Another attack vector for achieving the goal of changing the vessel route can be done by compromising data in the VHF range, i.e. misusing the AIS protocol [33]. The structure of the protocol was designed quite a long time ago, there are no mechanisms for validating the sender and encrypting the transmitted data, since the likelihood of using expensive radio equipment to compromise the technology was estimated as low. Attackers can deploy fake VHF transmitters, transmitting data ranging from false weather conditions to distress alarms, all of which can be used to mislead the ship's command and force it to correct the route, which can also have consequences when entering the port water area, dangerous, narrow sea areas, and the correctness of the actions of the captain.

The principle of spoofing an AIS signal [33] is the type of attack aimed to create fake signals appearing as multiple transponders which will convince the AIS receiver to be real ones. As a result, AIS receiver would calculate the wrong position of the ships.

Jamming is about flooding the AIS receiver [33] with a much stronger signal which

overpowers and drowns real signals. This type of attack became quite frequent due to the fact that the price for AIS transmitters that can perform jamming significantly decreased.

4 Data collection and analysis

4.1 Experimental environment description

Some of the scenarios introduced in Chapter 3 include the provisioning of the false data to the navigational equipment, namely the MFD (Multifunctional Display) display which aggregates and displays data from several applications like ECDIS or RADAR. This is a visual representation for the crew to understand the situation in the geographical radius of the ship current position in order to make decisions on further movements. This chapter is dedicated to analysing how the data is being provisioned and processed by the main component of the bridge and opening a discussion handled in Chapter 5 if the rules of packet transmission can be exploited by malicious actor in order to stay unnoticed. Moreover, it is giving a solid background knowledge for understanding how IDS detection mechanisms can be advanced in order to tackle those attack scenarios.

There are two main datasets that were collected and analysed:

- sensor packet data coming to MFD in NATO CCDCOE lab;
- AIS packet data received by vessel-based AIS receiver placed in the port.

This research paper is supported by NATO CCDCOE center which recently built the bridge vessel simulator with the real equipment used on modern ships. All equipment used in the center is provided by Transas, the subsidiary of Wärtsilä company [79]. Transas is one of the leaders in the market for providing ship and fleet operating solutions for shipowners. The lab environment is built specifically for cybersecurity research purposes and the equipment was bought from the company providing a solution for real ships.

A detailed description of the current physical setup is provided in Figure 8.

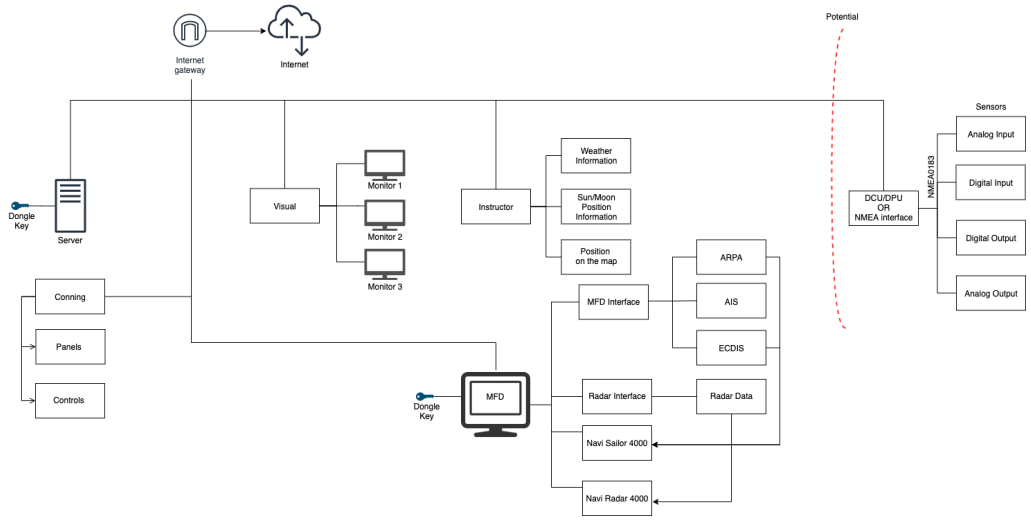

Figure 8. *Schema of the simulator in NATO CCDCOE center.*

Here we can see the main component that is going to be observed and analysed - MFD, which is the "heart" of the e-navigation on the vessel.

We have 3 monitors that are giving visual effect for simulating the view from the captain's cabin; we have a logical component called "Instructor" which is generating the weather condition, wind, position, sun/moon location for correct representation of the visual components. We also have a server, which is generating the actual packets needed for the input to the MFD, simulating the behaviour of the sensors on the real ship. We have "Conning" which is responsible for the Controls and Automation tools - which are the link between OT and IT systems of the ship. For this research paper, OT sector is out of the scope. In our test bench, we do not have all the mandatory components that are installed on the real ship, however, we have the main ones.

MFD is a combination of different software and hardware components. Inside MFD we have two server applications running on top: MFD Interface and RADAR Interface. RADAR Interface creates the UDP data stream and MFD Interface creates the NMEA-0183 data which is encapsulated into TCP packets. Both UDP and TCP packets are sent for MFD application (running on the same computer). This application is responsible for the visual representation of the received data. This includes: drawing maps, RADAR pictures, charts, ship position, different objects positions at the sea, etc. Also, it is responsible for sending back the commands to the MFD Interface that sends it towards the Server. Also, we have sensors interface in place to receive information from different sensors. On the real ship, it is coming from DPU (Data Processing Unit) with is gathering the information from serial connection from the sensors and sending it over to MFD converting signals from digital to analog. The sample IT network configuration of the real ship bridge is provided in Figure

9. The information was provided to the author during one of the research trips on the ferry in the Port of Haapsalu by technical solutions specialist. For confidentiality reasons, all data was anonymised, no real names are provided as well as the model specifications or versions.

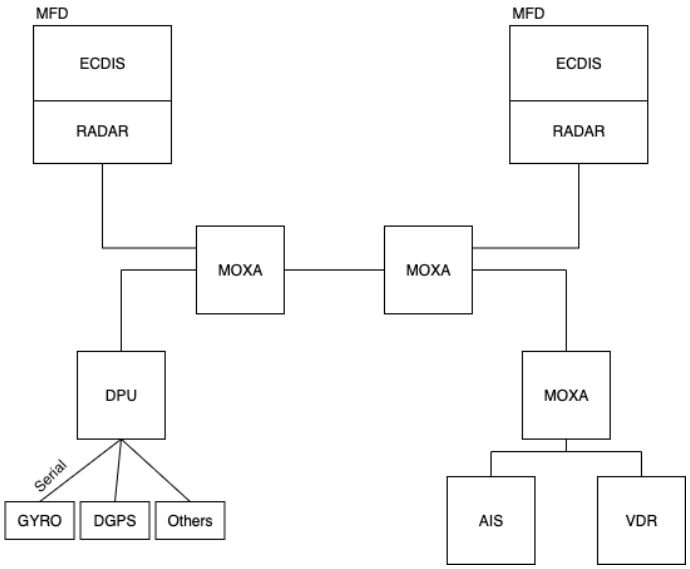

Figure 9. *Sample network schema setup of the ferry.*

There are a few differences between the real setup and the simulator in the NATO CCDCOE center. Firstly, we cannot put the real sensors in the simulated environment, so instead of DPU which is collecting sensor data from the supplementary devices placed around the ship, we have an aforementioned logical unit called "Instructor" which is generating all messages in the valid format that are coming from the sensors to the bridge. Also, on the real ship is it a common practice to have a backup ECDIS system which we do not have in our lab environment.

Inside MFD Application we have different "supplementary applications". Among the route planning systems presented on the market, "Navi-Planner" by Transas [80] is one of the most popular application to be installed on the ship. It provides efficient pre-routing, taking into account the weather forecast and alarm conditions.

Navi-Planner 4000 system allows ensuring safe and effective preliminary routing, as well as the implementation of the transition plan along the route [81]. Navi-Planner 4000 complies with the requirements of IMO Resolution A.916 (22) - “Guidelines for recording events related to navigation” and IMO Resolution A.893 (21) - “Guidelines on flight planning ". From the functionality point of view, the Navi-Planner 4000 system is an application for processing ECDIS electronic maps, as well as a set of databases, applications and services required for preliminary plotting. The system is used for both onboard use and for shore

use as an administrative tool. Navi-Planner 4000 software creates a transition plan based on an electronic course editor [80], including:

- automatic preliminary laying using WGS-84 coordinate system;
- control of the depth under the bottom of a ship;
- checking the preliminary laying for navigational hazards and informing about the found dangers;
- automatic calculation of control points;
- points of presentation of reports by radio;
- integration with the Navi-Sailor 4000 ECDIS system.

The logical presentation of the navigational sensors and support components that are sending data to MFD is presented in Figure 10.

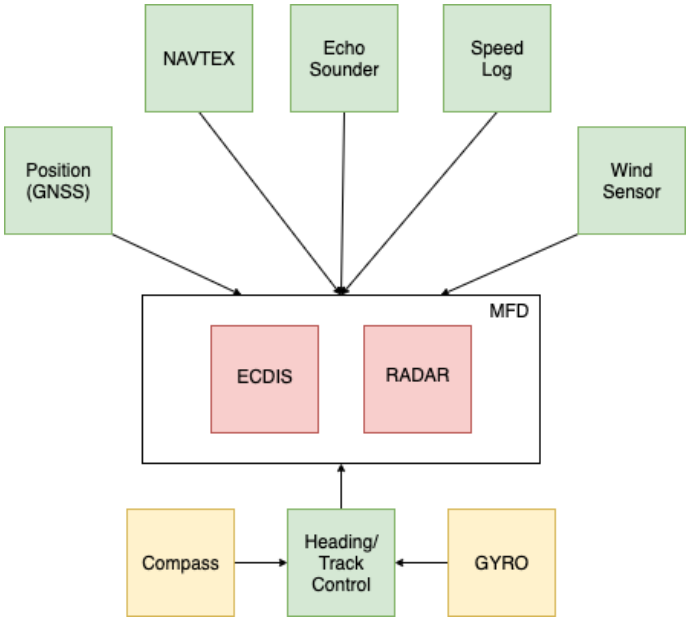

Figure 10. *Logical schema of sensor communication.*

We are going to focus on collecting and analysing the data from the sensors represented on Figure 10.

It is important to understand the limitations of the simulated setup as the primary focus of this research paper is analysing the real ship attack vectors. The only components which are corresponding to the actual equipment of the real ships are MFD and AIS receiver. The devices analysed are actually used on the real ships so it is sufficient enough to state that the data analysed is accurate. NATO CCDCOE environment was built to support the cybersecurity research - the devices are surrounded by a simulated environment in order

to imitate the real situations and supply them with the real data. There is a simulated input with the real protocol that the devices are using for message exchange. That is why the analysis of time intervals described in this chapter is corresponding to the vessel environment as we need to "feed" the real device with the real data that equipment is expecting. The feasibility behind the need of network data analysis lies in the fact that we can draw the behavioural traffic patterns which can serve us as a basis while proposing customisation for IDS.

4.2 Multi Functional Display Data Analysis

This part describes the format of sentences in IEC 61162-1 and NMEA 0183 standards, received from different types of navigational sensors.

In order to operate adequately in conjunction with navigational sensors, the MFD should receive certain data from them. This data is required to be transmitted in accordance with Standard IEC 61162-1 (Edition 4.0, 2010-11) “Maritime navigation and radio communication equipment and systems. Digital interfaces. Part 1: Single talker and multiple listeners” or in NMEA-0183 format. In addition, there is also a range of navigation equipment using specific data exchange protocols. MFD allows operation with several types of such equipment. In the real environment data from ECDIS mandatory sensors (GPS, Gyrocompass and Speed Log) and additional sensors (AIS, RADAR data, NAVTEX) is gathered directly via serial interfaces where, in the case of simulator, it is provided by "Instructor". The scope of analysed data is limited to the messages within the aforementioned standard. Reception of messages sent from NAVTEX receiver to the MFD serial port in ASCII and NMEA format compatible with IEC 61097-6, Second Edition.

Format of the messages consists of the following parts [82]:

$–AAA,x.x,a,c—c,...*hh <CR><LF>, where:

1. "$": Start of sentence;
2. "–": Talker ID;
3. "AAA": Mnemonic code of data type identification;
4. ",": Data field delimiter;
5. "x.x,a,c—c...": Data;
6. "*hh": Checksum field;
7. "<CR><LF>": End of sentence.

While trying to collect some real network flow from a real ship, we found out that, the ex-

tracted traffic represents well-segmented network traffic, and only the MFD communication is recorded.

Different sensors are sending messages to MFD with different time intervals, with the acquired network traffic we can see the rules by which retransmission of the messages can be analysed.

This data flow extracted from the interface of the MFD computer. The average time intervals can be found in Table 1.

Table 1. *A table with time intervals between MFD messages*

Nr	**Message Prefix**	**Meaning**	**Sensor**	**Average time interval (seconds)**
1	$HEHDT	Heading from True North	Compass	0.1094
2	$HEROT	Rate and direction of turn	Rate of turn indicator	0.0994
3	$VBVHW	Speed through the water	Speed log	0.0546
4	$VMVBW	Speed through the water	Speed log	0.0546
5	$GPVTG	Speed and course over ground	GPS	1.1
6	$GPDTM	Used datum	GPS	1.1
7	$GPGLL	Explained below	GPS	0.05
8	$GPRMC	Explained below	GPS	0.05
9	$GPGGA	Explained below	GPS	0.0937

There are two types of packets observed which are displayed in Figures 11 and 12. They are coming together with the average interval between Type 1 and Type 2 less then 1 millisecond, while the interval between each pair of messages is 0.9565 seconds. This messages include following prefixes:

- $INGLL (Geographic position);
- $INZDA (UTC Time and Date): the message contains information about the time, calendar day, month, year, and local time zone;
- $INVDR (Set and Drift);
- $IIRTE (Route name);
- $IIHTC (Heading/track control command);
- $IIAPB ((Heading/Track Controller (Autopilot)).

The messages described above are sent by position (GPS, GLONASS, DECCA, LORAN) sensor.

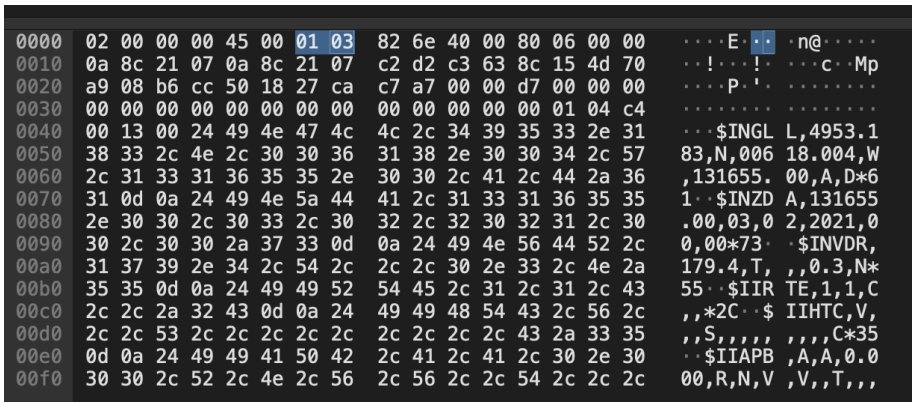

Figure 11. *Wireshark INGLL packet payload. Type 1.*

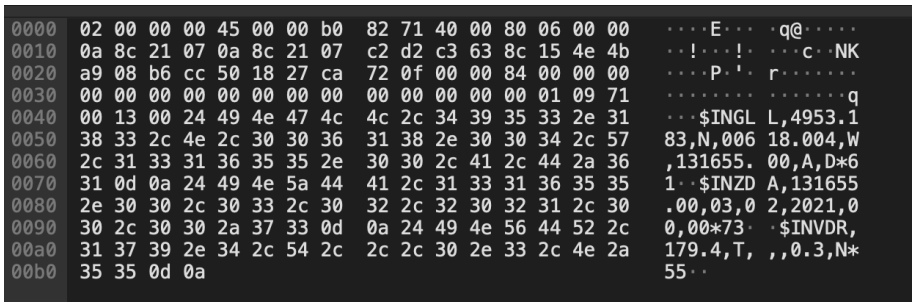

Figure 12. *Wireshark INGLL packet payload. Type 2.*

Messages with the prefixes $GPGGA, $GPGLL, and $GPRMC are sent by GPS sensor to update the information about the ship's position (latitude and longitude) [83].

$GPGGA - The message contains data on position, time of position determination, data quality, number of satellites used, factor of degradation of accuracy of horizontal coordinates, information on differential corrections and their age [83].

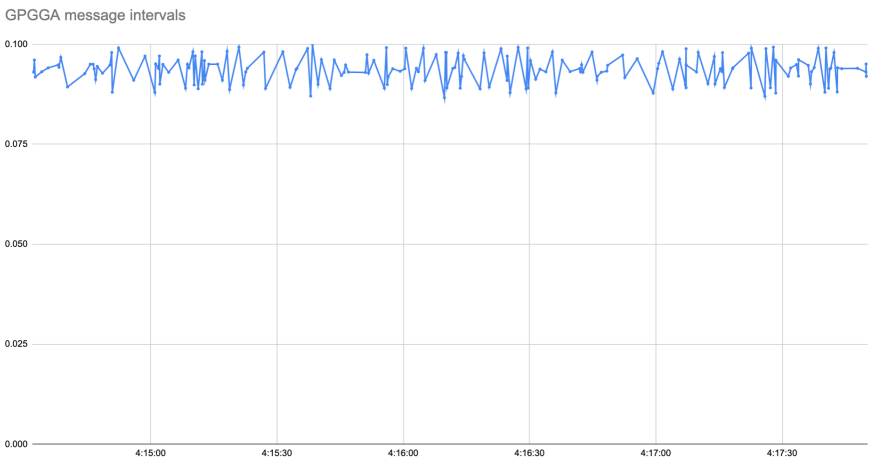

Figure 13. *GPGGA intervals line chart.*

$GPGLL - The message contains data on geographic latitude, longitude and time of coordinates determination [83].

$GPRMC - The message contains information about the location, time and date of the coordinates, speed, direction of travel and magnetic declination [83].

Messages with the prefixes $GPVTG and $GPDTM (the used datum) also sent by GPS sensor to provide data about SOG (speed over ground) and COG (course over ground) [83]. This data is sent twice in a 1.1 second with almost imperceptible difference.

$GPVTG - The message contains information about the direction and speed of movement [83].

4.3 AIS Messages Analysis

For the purpose of this research paper, we analysed AIS records collected on the real equipment used on the vessels. The model is Comar Systems RECEIVER: R500Ni. The Comar R500Ni with WiFi is an AIS receiver interfaced to a Raspberry Pi 3 computer [84]. This receiver was located onshore in the port so the amount of received records is higher than the object in the sea would have received during the voyage. Python script was used for data extraction adding the needed timestamps. Later then the records were imported to Excel spreadsheet for continuous analysis.

While talking about AIS receivers, it is worth noting that the receiver was used is a vessel-based AIS transceiver. Another type can be Satellite-based AIS (S-AIS) which is out of the scope for this research paper.

Collected data was grouped by the 'sourceMmsi' message part as it is the unique 9-digits sequence aimed to identify the object that has sent the packet.

The example of AIS message is presented below, according to IEC 61993-2 regulation:

!AIVDM,1,1,,A,33a1A>0OiVQhECtR35t:THQ@01V0,0*72, where:

1. First field: !AIVDM - AIVDM packet identifier;
2. Second field: 1 - segment count;
3. Third field: 1 - segment number of this message;
4. Forth field: empty - sequential message ID for multi-segment messages;
5. Fifth field: A - radio channel code;

6. Sixth field: message data.

The tool used to decode the AIS message is [85]. It is using the AIVDM/AIVDO protocol decoding method described in [82].

Different indicators were calculated, namely: average time between packets from the same source, minimum and maximum times between received packets from the same source, as well as standard deviation. In order to visually display the received results, we plotted histograms of the time distances between the packets from different ships.

On the histogram, presented in Figure 14, we can see how many messages from different AIS objects were received by our equipment per minute.

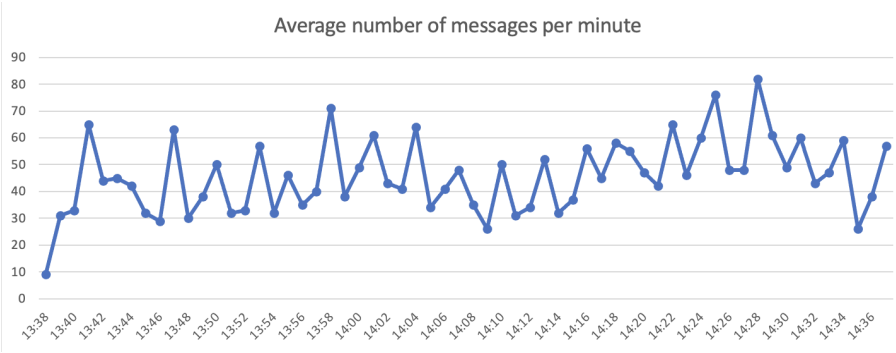

Figure 14. *Average number of messages per minute.*

As we can see from this line chart diagram, the number of AIS messages received varies too much in order to draw conclusions for the possible DDoS attack with the fake AIS messages. Nevertheless, by classifying the received messages by types of the 'sender' we can see different behavioural patterns. There are different sender types, e.g. slow ships, fast ships, navigational aids, buoys, etc.

Detailed analysis of the groups of the same object messages gave us the output presented below.

- "!AIVDM,1,1,,A,13a1A>..." message analysis is presented of Figure 15. This is Vessel Type - Generic: Cargo. This information we can get from its 'sourceMmsi' code. The names of the ships are not going to be presented, however, it is open information available online.

Most of the data in the 14-21 seconds time interval. We can see time differences around 20, 40 and 60 seconds. They are 20 seconds intervals multiplied by 2, 3, etc. It means that the packets are sent every 20 seconds but sometimes we miss the reception. By replacing the

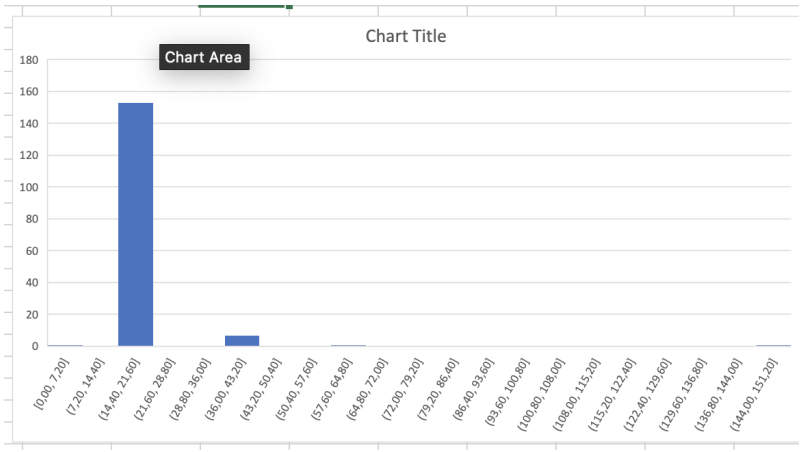

Figure 15. *Time intervals for "13a1A>" message.*

resulted values with the median value of the time difference, we can draw the histogram presented on Figure 16:

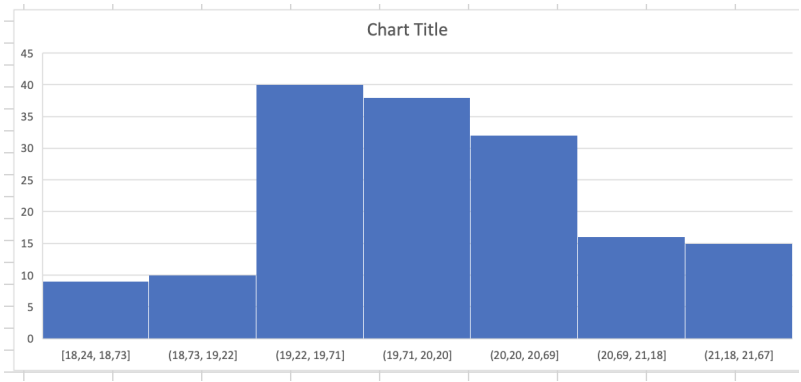

Figure 16. *Median value for the time difference of "13a1A>" message.*

So, we can expect the time difference between messages n * (18-22) seconds for the "!AIVDM,1,1,,A,13a1A>. . . " message type.

- "!AIVDM,1,1,,A,13lqAn. . . " message analysis is presented of Figure 17. The Vessel Type - Generic: Tanker.

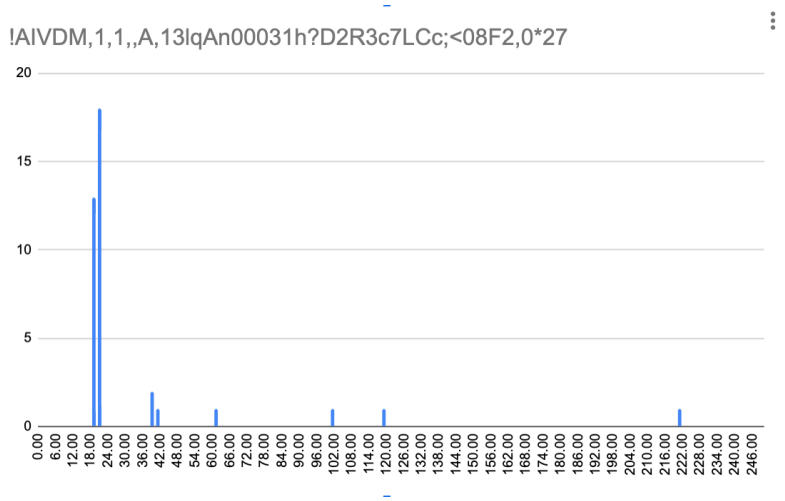

Figure 17. *Time intervals for tanker ship class type.*

As we can see on of the histogram above in Figure 17, we can see the same timing pattern: messages are mostly coming in 18-22 seconds with some results breaking this interval, indicating us the loss of some perception (at 40, 102, 120 and 222 seconds). So, the same conclusion applies to this object type at the sea.

- The next object type that we are going to analyse is Bulk carrier ship. The example AIS message for this object is "!AIVDM,1,1,,A,33=c‘b10011h=uLR2OkhUqHn0DM:,0*0A".

In Figure 18 we can see a new timing pattern that indicates the importance of object classification to identify the expected behaviour.

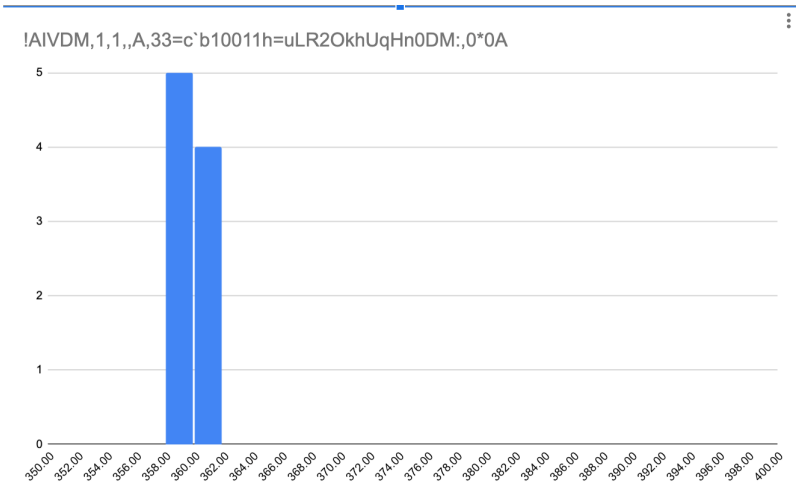

Figure 18. *Time intervals for bulk carrier ship class type.*

This histogram presented in Figure 18 shows us quite strict results, the possible conclusion

why we have no deviant values is that our receiver was close to the object. On histogram, we can see a new time pattern: messages from the bulk carrier are coming within 358-362 seconds time window, i.e. 5.96 - 6.03 minutes.

- Another type of object can be Generic: Tug. The sample message is "!AIVDM,1,1,,A,B481Ed0000L>C
  The time intervals are presented in Figure 19.

Figure 19. *Time intervals for tug ship class type.*

More statistical results for different messages are presented in Appendix 1.

Our assumption was that, after we analyse the timing and the content of the packets, we can define what is normal and what is abnormal behavior for the system. To finalise, now, we can see several facts:

- the deviation is too high, so, it is impossible to compare the periodicity of the data with its average without separation of the messages to different classes;
- the received data is periodical but the periodicity is based on the transmitter as each type of transmitter is sending packets with different frequency;
- the content of the messages (speed, station type, etc.) correlates with the repetition time;
- shown data analysis can be a base for anomaly detection as we can define the normal behaviour based on the timing of the received messages.

4.4 Novel Attack Description

Based in the message data, time intervals and attacks vectors analysis, we can see the way how to circumvent the monitoring system. The signature-based detection relies on

the existing database of the malicious payloads and behaviour analysis of the potential attack. However, due to the lack of studies in the NMEA industrial protocol behaviour, there are no resources describing how to detect abnormal behaviour in the messages with the valid payload. NMEA sequences are plain text and contain authentication messages. It is not difficult for an adversary to intercept information either in the GPS receiver, or in the autopilot controller or on another part of the network, and change the course of the vessel. That is how we came up with the novel attack on electronic navigational system on the ship bridge which we called "timing based attack". The ship is suspected to be vulnerable to the following offensive technology: by sending valid packets but within fewer time windows, we can force navigational equipment to display information that is needed for the attacker. We cannot physically force a ship to change the course but with manipulation of the display data, the adversary can force the captain to make a different decision.

Addressing the results from AIS messages analysis where uniquely objects at the sea are sending their location inside the time window between 18 and 21 seconds, adversary can overwrite the information received by AIS receiver on the victim ship by sending messages with the same 'sourceMmsi' packet part as it is unique identified of the object, with less time interval, changing the position report of the objects around the ship. This use case shows that adversary can possibly deceive the recipient navigation display. This particular scenario is assuming that the attacker gained initial access to the bridge and, by running a script which takes the real packets and shifting the time a bit, makes a danger of the ships collision. With this example, we wanted to highlight the impact that timing attack can cause on navigational equipment.

5 Results and Discussions

This chapter is going to summarize the findings of the author and discuss the feasibility of putting open-source IDS into ship's bridge. There are several aspects to consider: how to place IDS sensors in the system, how IDS can perform under network load on the bridge. As an example, Snort IDS is going to be discussed and its possibilities to fit into maritime needs as well as how Snort can detect timing attack scenario discovered in Chapter 4. However, according to the comparison of the needs IDS should meet, in essence, Suricata can also fulfil those. It is worth highlighting that this research paper is not aimed to promote Snort solution but rather show a method of detecting and preventing known and unknown attack scenarios described in details in Chapter 3. Snort is taken to show a use case example of embedding open-source IDS solutions and adapting it to maritime needs.

5.1 Attack Vectors Detection and Prevention

Due to the mixed nature of the communication happening between navigational equipment (TCP/IP packets as well as NMEA-over-Ethernet), the thread is becoming more complex as well. We need to be ready to detect well-known IT attacks as well as maritime-specific attacks.

The proposal on placing Snort in the ship's bridge network is motivated by several facts:

1. Any software or hardware placed on the ship's bridge should be certified. This puts constraints on the ability to perform any testing of open-source product's functionalities on the real ship as it does not have needed certifications. This is an obstacle that any researcher interested in maritime cybersecurity might face with. Previously, Snort creators have shown the ability of Snort to transform into commercial, certified product. Cisco company took Snort solution into their routers, successfully customised and certified it [86]. This example shows that open-source solution can be a good fit for commercial products and receive certification.
2. Snort has become a standard for IDS systems. It is not only supported by top-lists of cybersecurity tools [87, 88], but also by awards granted to Snort software [89];
3. Snort is an open-source solution that is supported by cybersecurity enthusiasts and a strong development community. This is extremely important nowadays as new

exploits and attacks are coming every day and Snort community is reacting fast enough to update the database of detection rules. And the solution itself is actively being improved. Recently, Snort announced stable release of Snort 3 completely rewritten in C++ [19];

4. Due to the fact that it is open-source - the product itself is easily customisable which makes it possible to adjust the features to specific needs. The need for customization is described later in Section 5.3;
5. Due to the fact that it is open-source - the product is free.

As mentioned above, this year Snort community announced the next stable version of Snort - Snort 3 [90]. It brought Snort software to a new level of competitiveness. With the new release, big changes came [91] which outweighs the decision on using Snort 3 over 2, namely:

- The engine for detecting attacks has been modernized, the rules have been updated, the ability to bind buffers in the rules (sticky buffers) has been added. The Hyperscan search engine was used, which made it possible to use fast and more accurately triggered patterns based on regular expressions in the rules;
- The performance of the deep packet inspection mode has been significantly improved. Added the ability to multithreaded packet processing, allowing simultaneous execution of multiple threads with packet handlers and providing linear scalability depending on the number of CPU cores;
- Automatic detection of running services, eliminating the need to manually specify active network ports;
- And a lot more, but the points provided above are affecting the author's decision on using Snort 3 over Snort 2.

The study of optimal bandwidth of the ship network topology [92] has shown the amount of the transferred packets in case of different typologies (e.g. bus, star, ring) within the 0.6-1.5 seconds window. It was proved that the ship network can be classified as a small network. At the same time, Snort has shown the ability to be an effective solution for small medium networks. Recent studies examined the performance of the Snort under different workloads [93]. The testbed results showed that Snort can provide relatively high efficiency with 1 Gbps of traffic generated. Although the performance of the Snort can reduce while the traffic is becoming over 5 Gbps [94], it is proved to be not the case when working with a single ship network.

The abilities of Snort to perform its stated functions was covered by different research papers. Although the studies discussed below are concerning Snort version 2, we do believe

that successful results of older version are going to be carried out to the newer version. There is no solid research basis covering Snort 3 performance or detection efficiency due to the fact, that is it relatively new.

Snort performance of detecting ransomware attacks was studied by several papers [95, 96], providing satisfying and reasonable results. Ransomware, being one of the biggest concerns in the maritime industry which was discussed in Chapter 3 should be considered among the first factors to be addressed while choosing cybersecurity protection mechanisms.

Chakrabarti et al. provided a comprehensive review of the Snort capabilities showing the results of the detection ratio by Snort for various attacks, namely: DDoS, virus and malware infection, exploits, etc. "For testing out various attacks, Snort was configured with some rules that are inherent to Nmap – Zenmap" [97]. This study proves that Snort is able to successfully detect the typical cybersecurity world attacks which can also occur on the ship computer network.

There are several attack branches discussed in Chapter 3 that cannot be mitigated with the IDS placement on the bridge. This includes the possibility of detecting an infected removable device plugged in the computer. This case of host-based attack cannot be detected by NIDS. However, with the IPS being in between ECDIS and backup ECDIS, we are able to prevent the infection from spreading, leaving the possibility for the ship to operate even if the main ECDIS was compromised. To advance to possible effects of the IDS in the system, we analysed and proposed a placement option for IDS sensors in the network.

5.2 Implementation Recommendations

As long as we are not performing action research focusing on one vessel and trying to propose the best implementation of the NIDS in the network, we are trying to draw common patterns of the network setups in order to provide a unified solution that will fit the need of any non-military vessel. There are several recommendations on how network setup on the bridge should look like [98, 99, 100]. Literature review showed that the way of how the network equipment is placed can vary from ship to ship, depending on its size and purpose, however, the general purpose and types of the equipment components are staying the same. The main parts that are going to be found of any vessel: RADAR, ECDIS, Backup ECDIS, Conning, AIS, GPS, VDR, GMDSS - making no difference what is the type of this vessel (being it tug, cargo or passenger ship, big fishing boat, etc.). In Figure 20 we introduce the possible placement of Snort in the system.

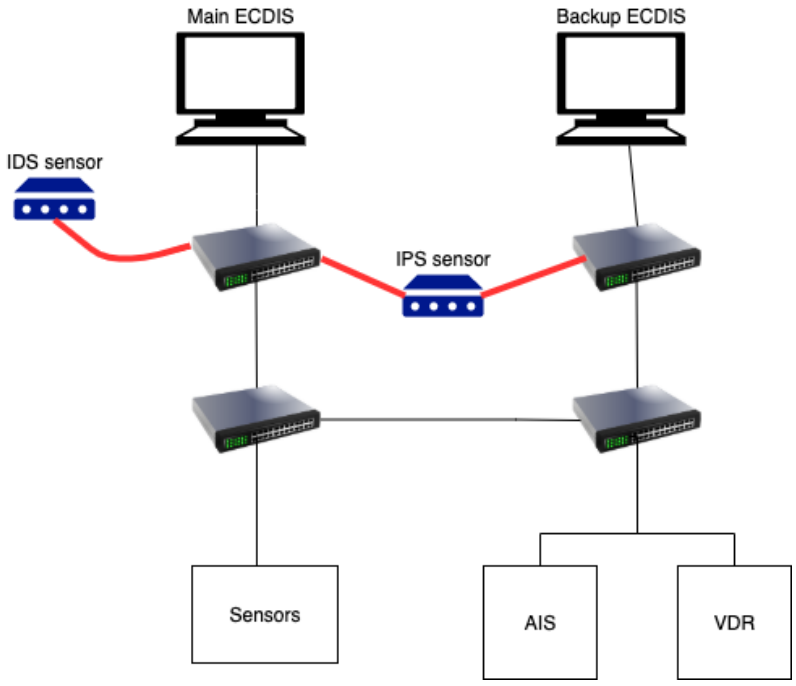

Figure 20. *Proposal on IDS and IPS sensors placement.*

There are a few things that should be taken into account while choosing the best placement option for an intrusion detection system:

- Firstly, computers and software running on top for navigation equipment is licensed. That means that installing additional software of the host machine is prohibited unless it is approved by the vendor or automation and navigation integrator. Also, referring to the interviewed experts answers provided in Appendix 2, this statement was confirmed. This limitation shows us that we cannot consider installing a host-based intrusion detection solution as we need to keep the licence.
- Secondly, from interviews we discovered that it won't be allowed to put additional components inside the same network where navigation network is located unless the device or appliance is approved by the navigation integrator. In this case, we can consider IDS only as a listener and logger. In this scenario, we can mirror the traffic from navigation network and forward it to Snort in a different network segment, leaving it the possibility of alerting and analysing the network activity.
- According to the technical requirements for installing ECDIS on the ship, it is required to have a connectivity cable between main ECDIS and backup ECDIS [101]. If we want to get the best use out of Snort on a bridge, we propose to use it as an inline device in navigation network between main and backup ECDIS. The IPS sensor placed between main ECDIS and backup ECDIS will prevent malware from spreading in case of infection. In this case, Snort should be certified by navigation

and automation integrator. This is not the case right now, however, during the interviews maritime experts have shown interest in adapting open-source solution to ship needs.

5.3 Proposed Improvements for the Novel Attack Detection

And as we can see from our hypothesis, the potential indicator of the attack is the wrong interval of the messages. Hence, it can be an indicator of the position mislead and possible intrusion.

We need to consider improving current detection mechanisms. The ways of doing this are only limited by research community imagination as this appliance domain (maritime) is relatively unstudied in terms of complementing cybersecurity on a ship with open-source solutions. However, we propose two different approaches to change the detection architecture of IDS:

- a custom preprocessor is a part of IDS codebase sending log messages to separate detection module for further analysis;
- a protocol analyser being a part of IDS codebase passes further to IDS detection processes where messages are matched against NMEA and AIVDM/AIVDO signature sets.

The first option can be explained as follows:

1. First part: a custom preprocessor as a part of the IDS codebase can be developed to parse a single message and create a log entry for it. It is going to be written in C or C++ as Snort 3 was rewritten in C++ [102], Suricata is written in C [103], Zeek is mostly written in C++ [104].
2. In the second part, we consider having a separate attack detection module that tracks the log messages from the preprocessor and completely separated from the IDS codebase. It can be written in a higher-level language (rather than C or C++) in order to facilitate rapid development and testing of different timing attack detection algorithms.

Following the second option scenario, the idea of preprocessor development stays the same, however, instead of passing logs outside IDS, we consider developing rule sets against which log messages are going to be matched. As a result, only maritime-specific protocol messages are going to be sent to the detector, to which the rules are applied. For example,

in case of Snort, detection_filters with rules [105] can used to set an alert on more than specific amount of packets received per defined interval discovered in Chapter 4.

The motivation for writing a custom preprocessor for IDS lies in the fact that we need to decode the AIVDM/AIVDO protocol (used for AIS messages) and NMEA (0183/2000) where IDS can allow us to build protocol-specific decoders. By implementing the new way of parsing the packet data by custom preprocessor we can keep track of the sensor NMEA and AIS messages received by MFD to draw conclusions about the type of activity. The tracking points can be:

- the number of packets is significantly increased within the time window defined;
- the received coordinates from the ship in AIS message have changed a lot from the previously received message.

What we are trying to achieve with the custom preprocessor as plugin design is an understanding of the behaviour of industrial protocols, unknown for IDS. Nevertheless, it is encapsulated into standard IP packet, after it passes the stage of packet decoder, we need to instruct IDS on how to process this type of payload data. When we are talking about the messages coming from sensors on the ship, it does not require additional non-standard procedures as we can treat payload of the sensor messages as a string and provide rules for the matching against custom rules as well as define interval windows. This is trivial due to the fact that messages coming from the sensors on the vessel are passed in unencrypted way. That is why we can differentiate between the messages using prefix filtering. The used prefixes were described in Chapter 5.

The need for additional decoding is coming when we are operating with AIS messages, as they passed in encrypted way according to AIVDM/AIVDO protocol specifications. The problem of fast and efficient decoding of AIS messages has been well-studied. Scientists from non-profit research institute RISE Viktoria [106] showed in their paper a way of extracting the fields information from AIS sentences using C++. As a part of the bigger scope, [107] showed the logical process of decoding AIS sentences as well. There are a few repositories available with the C++ source code solving the problem of decoding AIS messages, namely [108, 109]. These resources can become a basis for IDS preprocessor source code, solving the problem for AIS messages decoding. However, it is worth noting that this approach can be used for initial studies only. When going deeply into upgrading IDS detection mechanisms, for better performance and correct packet interpretation, NMEA plugin development should also be considered.

To sum up, the proposal for the advancing detection mechanisms for detecting attempts to

mislead the ship or trick the captain can be described as follows.

In the first case, we are talking about string matching against particular parts of the packet (prefix), which will identify the type of the packet received and the sender of the packet. The second case includes detection of the behaviour that is against the rules that were concluded from data analysis provided in Chapter 4. As we are keeping track of the messages coming to MFD, we can give a rough classification for two major groups of "senders": sensors on the ship and AIS receiver.

1. If the message received has a prefix from the list of sensors groups (described in Chapter 5), we are going to apply the time interval checking for the next message with the same prefix comes. If the intervals appear to be significantly less than defined (this number exceeds a threshold) in the rule for IDS (the quantitative value was taken based on the data analysis), the alert will be created.
2. If the message received has a prefix from AIVDM/AIVDO protocol specification, then the decoding mechanisms will apply and the 'sourceMmsi' data fields will be extracted, which is a unique identifier for the object at the sea and the interval for this object will be calculated. After the pattern observed, if the intervals appear to be significantly less (this number exceeds a threshold), the alert will be created, indicating the potential external ship direction or coordinates silent change.

This research paper is not aimed to provide benchmarking analysis of the available open-source IDS solutions but rather discuss the possibilities of different platform to extend their detection functionality to meet maritime needs.

- Developing preprocessor in Snort 3

"Preprocessors specifically, and plug-ins in general, give Snort the capability to be more than an IDS. They give it the capability to be an extensible intrusion detection framework onto which most any detection method can be built" [110].

However, Snort 3 documentation [91] provides general guidelines for developers on how to properly embed the new plugin into the existing system.

The current documentation of Snort++ is lacking end-user friendly guidelines on writing preprocessors, and the only available resources are currently quite outdated. The newly introduced Snort 3 shows how industrial protocols can be integrated into a standard IDS solution. Recently, in Snort 3, the new ways of Modbus and DNP3 protocol parsing were introduced. Modbus and DNP3 are communication protocols used in SCADA systems.

This shows growing attention to industrial protocols from Snort development community, where NMEA and AIVDM/AIVDO can be also classified as industrial protocols. Modbus and DNP3 examples show how industrial protocols can be added into open-source IDS with unique rule options needed for detection.

For better performance results, in the ship bridge network, we can turn off most of the available preprocessors. For example, in the case of Modbus and DNP3, it was needed to leave turned on only stream5, frag3 and enabling PAF (Protocol Aware Flushing) [91].

Based on the current requirements for correct industrial protocols processing, future development of the NMEA and AIVDO preprocessors will require minimum dependencies to be enabled.

- Developing preprocessor in Suricata

The newly updated documentation of Suricata 6.0.2 [111] describes the example of protocol decoder in a sketchy way. The documentation is incomplete and can be significantly improved. However, Suricata is actively organizing developer trainings as well as SuriCon conferences [112] which can help future enthusiasts, aimed for extending Suricata detection functionalities to the maritime domain, to learn internals better.

- Developing preprocessor in Zeek

Zeek's documentation on developing scripts is well-written and easy to understand for the development community. It provides extensive guidelines on how to embed additional scripts for further processing of the captured data.

All aforementioned open-source IDS solutions are showing how industrial protocols can live inside detection modules, as all three solutions are providing support for detecting Modbus and DNP3 protocols in their latest stable versions.

Based on the interviews with the experts in the maritime field, we figured out that one of the important aspects that technical people want to see in the future cybersecurity tool on a ship is the possibility to keep the logs for faster investigation. And the more detailed log journal is going to be - the better. This puts one of the aspects that IDS should be complaint with - it should keep a detailed log journal of packets in the ship bridge network. And the proposed 2-separate-part approach (first scenario on changing the detection architecture that has been described earlier) has one fundamental advantage – one will have a detailed log of all messages that have passed the bridge network which allows for detailed investigation of

past incidents.

It is hard to estimate which IDS can be best suited for this purpose, however, we can discuss strengthens and weaknesses of each solution to fit our particular needs. To speed up the performance of the log writing process in Snort, logs are usually written in unified2 binary format. It is increasing the writing to disk speed, however, it is also bringing the difficulty of further parsing the log entities. For this, the Barnyard2 option is available in Snort, however, it has been not updated for more than 5 years now [113], which creates additional vulnerabilities in the system. Also, it is possible to log all traffic to pcap files, however, the performance can get lower.

On the other hand, Suricata and Zeek are offering easier to maintain solution for logging functionality.

Suricata allows logging all traffic passed through the network interface easier, saving it to EVE.json (Extensible Event Format) and, from here, another process can take file for further analysis and testing different timing attack detection algorithms. Also, it is possible to configure suricata.yaml for the "outputs" configuration module. Suricata documentation advises not to log all network traffic as it will result in slower performance as well as the possibility of packet loss. However, in our case, we can configure this functionality to log all NMEA and AIVDM/AIVDO messages in the network, where the rest of the traffic will be covered with the standard detection modules.

As it is stated in Zeek documentation "Zeek offers transaction data and extracted content data, in the form of logs summarizing protocols and files seen traversing the wire" [104]. This means that the possibilities of Zeek to fulfil the requirements of easy and detailed logging is the best fit, nevertheless, it is not offering an extensive suite of alerting mechanisms.

To sum up, for future researchers who want to investigate the behaviour of the NMEA and AIVDM/AIVDO protocols in real life, as well as test custom-written detection modules, Zeek can serve its purpose of providing extensive input. Moreover, it can be used for investigation purposes without impacting the performance of the system. For further processing of the log entities, Zeek offers different output formats, where TSV (Tab-separated Values) [104] can be the fastest and easiest to operate with.

A summary of the author's thoughts is provided in Table 2 below.

Table 2. *A comparison table for open-source IDS*

	Snort 3	**Suricata**	**Zeek**
Industrial protocol detection support (Modbus/DNP3)	Yes	Yes	Yes
Easy to customize/add modules	No	No	Yes
Detailed documentation on preprocessor development	Can be improved	Can be improved	Yes
Extensive detection mechanisms	Yes	Yes	No
Maritime protocols support	No	No	No

Summarizing the discussion, the author sees Zeek software as a great way to continue the research of detection mechanisms development, where placing Zeek in the network as a logger will allow researcher to get the log entities without organizational problems (for example, getting permission from automation and navigation integrator company). However, as we want to detect and react to both known attacks (using conventional signatures) as well as, in the research paper the novel attack was introduced called "timing attack" on the navigation displays, we see that the best efficiency can be achieved with either Snort 3 or Suricata as Zeek does not pose itself as an advanced attack detection solution but rather network monitoring and logger solution.

6 Summary

In conclusion, we observe poor preparedness of the industry, for the times when cyberattacks are no longer something new and are widely used. In addition to software vulnerabilities and other security holes in these systems, there is also a severe problem of the inability to instantly apply security updates to systems on ships in the voyage. It is doubling the chances for adversary and minimising the chance for shipowners to be ready to respond fast enough.

Implementing cybersecurity tools with a deep understanding of how vessel network can differ from ordinary enterprise network, the difference in vulnerabilities and realising the impacts can be the only way to win against the adversary in the digital world.

This research paper had investigated the feasibility of putting open-source cybersecurity tool on the vessel and if an open-source solution can be modified in order to meet commercial world of water transportation needs. The current state on ship in terms of being cyber secure is in its incipient phase where even naive and straightforward misuse can lead to major consequences - and such kind of attacks can be easily preventable. An intrusion detection/prevention system can prevent a lot of known attacks and dangers posed to the ship.

To summarize the findings of the feasibility study performed, we divided the finding into several categories:

- We showed with the help of visual attack scenario modelling - attack tree methodology - the common attacks on bridge navigational systems.
- From a legal perspective, after having interviews with experts from Port of Tallinn, we found out that the possibility of implementing an open-source solution without giving notice in advance to automation and navigation integrator can cause shipowner to lose the license. However, there are two possibilities to get out of this situation: In the first case, in order to make the best out of the IDS, the customised solution can be certified. We studied the possibility of open-source product - Snort - being transformed into commercial use, being inspired by the Cisco model, where Cisco company took the open-source version of Snort, modified it, certified it and then

started to sell it as a product. It combines the best of two worlds: open-source community brings the latest innovations into the system, and a strong company fulfilling legal and certification requirements of their customers who do not have the knowledge to maintain open-source software themselves and on top of - it needs certification.

In another case, if getting the licence for IDS is not a priority for automation and navigation integrators, IDS (or network logger) can still be placed on a bridge but with limited functionalities: it can serve only as a passive monitoring and logging tool, where the log entities are going to be analysed with the help of external module/program/software. In this case, we cannot prevent attacks, however, it can be an initial step to gain "credit of trust".

- From an economic perspective, an advantage of open-source tooling is that it is free. However, experts have shown some slight doubt about the cost of human hours implementing this type of solution onboard. The calculation and prognoses of human efforts are out of the scope of this research paper.
- From technical and operational feasibility, we studied several points, namely: placement, network load, speed of processing, protocol decoding and advancing detection mechanisms. As an example, Snort IDS was chosen to show how the solution can be adapted to the bridge network system. We considered both intrusion detection and prevention capabilities of Snort while proposing the placement of the Snort sensors in the network.
- Finally, scheduling feasibility is not relevant for this research as we are not considering or predicting any time frames for implementation.

Individual shipping companies seem to be interested in trying new and free ways of tackling security of the ship, but they obviously cannot risk the certification status of their equipment. This leaves a perspective for future researchers to work in collaboration with large ship equipment integrator companies to develop cybersecurity tooling based on the open-source recognised products.

We proposed in the thesis how with modifications to the Snort, we can detect industry-specific attacks in NMEA and AIS protocol communications.

It is just the tip of iceberg showing the real problem and lack of attention to possible threats that the maritime industry can face. We cannot tell that any kind of system is 100% secure but at least we can make a solid basement for future improvements.

The perspective of the work is to implement the proposed model for Snort or Suricata preprocessor for maritime protocol processing, test the resulted performance as well as

detection rates. Moreover, to test IDS in a simulated environment in order to be able to suggest processing power and memory utilization limits for the hardware components.

Bibliography

[1] Siri Pettersen Strandenes and Helen A Thanopoulou. “GDP and international seaborne trade: past trends, present breaks and future directions”. In: *Geographies of Maritime Transport*. Edward Elgar Publishing, 2020.

[2] Aziz Muslu. “The Future of Seafarers and the Seafarers of the Future from the Perspective of Human Resources Management”. In: *Contemporary Global Issues in Human Resource Management*. Emerald Publishing Limited, 2020.

[3] Joan Mileski, Christopher Clott, and Cassia Galvao. “Cyberattacks on ships: a wicked problem approach”. In: *Maritime Business Review* 3 (Nov. 2018). DOI: 10.1108/MABR-08-2018-0026.

[4] Greg Dobie, H Kidston, T Chamberlain, and C Fields. “Safety and shipping review 2015”. In: *Allianz Global Corporate and Specialty* (2015).

[5] Sun-Bae Hong. “A study on the effects of e-navigation on reducing vessel accidents”. In: (2015).

[6] *Shipping safety - Human error comes in many forms*. https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/human-error-shipping-safety.html. [Accessed: 2021-20-04].

[7] Resilient Navigation and Timing Foundation. *Ships Collide, but AIS-GPS Says They Passed Safely*. [Accessed: 2020-11-23]. 2017. URL: https://rntfnd.org/2017/06/08/ships-collide-but-ais-gps-says-they-passed-safely/.

[8] National Transportation Safety Board. *Collision between US Navy Destroyer John S McCain and Tanker Alnic MC Singapore Strait*. [Accessed: 2020-11-23]. 2017. URL: https://www.ntsb.gov/investigations/AccidentReports/Pages/MAR1901.aspx.

[9] Allianz Global Corporate & Specialty Team. *Safety and Shipping Review 2019*. Allianz Global Corporate & Specialty, 2019.

[10] *Norwegian cruise company Hurtigruten hit by cyberattack*. https://www.thelocal.no/20201214/norwegian-cruise-company-hurtigruten-hit-by-cyberattack/. [Accessed: 2021-18-04].

[11] *Carnival Cruise Lines Hacked*. https://www.infosecurity-magazine.com/news/carnival-cruise-lines-hacked/. [Accessed: 2021-18-04].

[12] *NORTHERN CALIFORNIA AREA MARITIME SECURITY COMMITTEE CYBER SECURITY NEWS LETTER*. https://www.sfmx.org/wp-content/uploads/2017/03/Cyber-Security-Newsletter-2014-1.pdf. [Accessed: 2021-04-03]. 2014.

[13] International Maritime Organization. *RESOLUTION MSC.428(98) - MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS*. https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf. July 2017.

[14] *Cyber incidents: Changing the narrative*. https://safety4sea.com/cm-cyber-incidents-changing-the-narrative/. [Accessed: 2021-02-25].

[15] *Q&A: James Snook talks the UK government's cybersecurity strategy*. https://www.uktech.news/news/qa-james-snook-talks-the-uk-governments-cybersecurity-strategy-20160418. [Accessed: 2021-17-04].

[16] BIMCO. *The Guidelines on Cyber Security Onboard Ships*. BIMCO, 2016.

[17] International Maritime Organization (IMO). *MSC.282(86): Adoption of amendments to the International Convention for the Safety Of Life At Sea*. [Accessed 31-01-2021], Annex 1. London. June 2009.

[18] International Maritime Organization (IMO). *MSC-FAL.1-Circ.3 - GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*. [Accessed: 15-11-2020]. July 2017.

[19] *Snort - Network Intrusion Detection & Prevention System*. https://www.snort.org/. [Accessed: 2021-03-01].

[20] Karl Lubja. "Systematic Generation of Cyber Attack Scenarios against a Ship". MA thesis. Tallinn University of Technology (TalTech), 2020, p. 51.

[21] Indrajit Ray and Nayot Poolsapassit. "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders". In: *Computer Security – ESORICS 2005*. Ed. by Sabrina de Capitani di Vimercati, Paul Syverson, and Dieter Gollmann. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 231–246.

[22] International Maritime Organization (IMO). *MSC-MEPC.2-Circ.12-Rev.2 - Revised Guidelines For Formal Safety Assessment*. [Accessed: 02-12-2020]. Apr. 2018.

[23] CLIA BIMCO, INTERCARGO ICS, INTERTANKO INTERMANAGER, and OCIMF IUMI. "WORLD SHIPPING COUNCIL". In: *The Guidelines on Cyber Security Onboard Ships. Versión* 3 (2018).

[24] DNVGL AS. "Cyber security resilience management for ships and mobile offshore units in operation". In: (2016).

[25] Koji Kutsuna, Hideyuki Ando, Takuya Nakashima, Satoru Kuwahara, and Shinya Nakamura. "NYK's approach for autonomous navigation–structure of action planning system and demonstration experiments". In: *Journal of Physics: Conference Series*. Vol. 1357. 1. IOP Publishing. 2019, p. 012013.

[26] Dan Cimpean, Johan Meire, Vincent Bouckaert, Stijn Vande Casteele, Aurore Pelle, and Luc Hellebooge. "Analysis of cyber security aspects in the maritime sector". In: (2011).

[27] William Vesely, Michael Stamatelatos, Joanne Dugan, Joseph Fragola, Joseph Minarick, and Jan Railsback. "Fault tree handbook with aerospace applications". In: *NASA Office of Safety and Mission Assurance* (2002), pp. 1–218.

[28] Bruce Schneier. "Attack trees". In: *Dr. Dobb's journal* (2007).

[29] Marco Gribaudo, Mauro Iacono, and Stefano Marrone. "Exploiting Bayesian networks for the analysis of combined attack trees". In: *Electronic notes in theoretical computer science* 310 (2015), pp. 91–111.

[30] Sjouke Mauw and Martijn Oostdijk. "Foundations of attack trees". In: *International Conference on Information Security and Cryptology*. Springer. 2005, pp. 186–198.

[31] International Maritime Organization (IMO). *International Convention for the Safety of Life At Sea*. `https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx`. [Accessed: 25-01-2021]. Nov. 1974.

[32] Yevgen Dyryavyy. "Preparing for cyber battleships–electronic chart display and information system security". In: *NCC Group* (2014).

[33] Marco Balduzzi, Kyle Wilhoit, and Alessandro Pasta. "A security evaluation of AIS". In: *Trend Micro* (2014), pp. 1–9.

[34] *Cybersecurity in shipping and port technologies: examples of cyber attacks in maritime*. `https://marine-digital.com/cybersecurity_in_shipping_and_ports`. [Accessed: 2021-02-04].

[35] Z Kopacz, W Morgas, and J Urbanski. "The maritime safety system, its main components and elements". In: *The Journal of Navigation* 54.2 (2001), p. 199.

[36] Aaron P Dahlen. *Navigational Telex (NAVTEX) Modeling*. Tech. rep. Coast Guard New London Ct New London, 2017.

[37] Boris Svilicic, Igor Rudan, Vlado Frančić, and Djani Mohović. "Towards a cyber secure shipboard radar". In: *The Journal of Navigation* 73.3 (2020), pp. 547–558.

[38] SA Berrabah and Y Baudoin. "GPS data correction using encoders and inertial navigation system (INS) sensors". In: *Using Robots in Hazardous Environments*. Elsevier, 2011, pp. 269–282.

[39] *National Marine Electronics Association*. `https://www.nmea.org/`. [Accessed: 2021-02-28].

[40] Srećko Krile, Danko Kezić, and Franc Dimc. "NMEA communication standard for shipboard data architecture". In: *NAŠE MORE: znanstveni časopis za more i pomorstvo* 60.3-4 (2013), pp. 68–81.

[41] Ajith Abraham, Crina Grosan, and Yuehui Chen. "Cyber security and the evolution in intrusion detection systems". In: *Journal of Engineering and Technology, ISSN* (2005), pp. 0973–2632.

[42] H Günes Kayacik, A Nur Zincir-Heywood, and Malcolm I Heywood. "Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets". In: *Proceedings of the third annual conference on privacy, security and trust*. Vol. 94. Citeseer. 2005, pp. 1723–1722.

[43] *Suricata*. `https://suricata-ids.org/`. [Accessed: 2021-21-04].

[44] *Zeek: An Open Source Network Security Monitoring Tool*. `https://zeek.org/`. [Accessed: 2021-21-04].

[45] Alka Gupta and Lalit Sen Sharma. "Performance Evaluation of Snort and Suricata Intrusion Detection Systems on Ubuntu Server". In: *Proceedings of ICRIC 2019*. Springer, 2020, pp. 811–821.

[46] Harsha Kumara Shaikh Siraj Ahmed; Kalutarage. *Relating to the monitoring of network security*. U.S. Patent 10,681,059. June 2020.

[47] *Medulla*. `https://www.cyberowl.io/solutions/`. [Accessed: 2021-04-04].

[48] *Naval Dome*. `https://navaldome.com/`. [Accessed: 2021-16-01].

[49] Mohamed Attia, Sidi Mohammed Senouci, Hichem Sedjelmaci, El-Hassane Aglzim, and Daniela Chrenko. "An efficient Intrusion Detection System against cyber-physical attacks in the smart grid". In: *Computers & Electrical Engineering* 68 (2018), pp. 499–512.

[50] Liang Liang. "Abnormal detection of electric security data based on scenario modeling". In: *Procedia computer science* 139 (2018), pp. 578–582.

[51] Craig Valli. “SCADA forensics with Snort IDS”. In: (2009).

[52] Daniel Blauwkamp, Thuy D Nguyen, and Geoffrey G Xie. “Toward a Deep Learning Approach to Behavior-based AIS Traffic Anomaly Detection”. In: *Dynamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop, San Juan, PR. Retrieved from http://faculty. nps. edu/Xie/papers/ais_analysis_18. pdf*. 2018.

[53] Konrad Wolsing, Eric Wagner, and Martin Henze. “Facilitating Protocol-independent Industrial Intrusion Detection Systems”. In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 2020, pp. 2105–2107.

[54] Seyit Ahmet Camtepe and Bülent Yener. “A formal method for attack modeling and detection”. In: *SA Camtepe, B. Yener* (2006).

[55] Ping Wang and Jia-Chi Liu. “Threat analysis of cyber attacks with attack tree+”. In: *Journal of Information Hiding and Multimedia Signal Processing* 5.4 (2014).

[56] Eric J Byres, Matthew Franz, and Darrin Miller. “The use of attack trees in assessing vulnerabilities in SCADA systems”. In: *Proceedings of the international infrastructure survivability workshop*. Citeseer. 2004, pp. 3–10.

[57] Sean Convery, David Cook, and Matthew Franz. “An attack tree for the border gateway protocol”. In: *IETF ID* (2004).

[58] Nikolaos Pitropakis, Marios Logothetis, Gennady Andrienko, Jason Stefanatos, Eirini Karapistoli, and Costas Lambrinoudakis. “Towards the Creation of a Threat Intelligence Framework for Maritime Infrastructures”. In: *Computer Security*. Springer, 2019, pp. 53–68.

[59] Andrew E Tucci. “Cyber risks in the marine transportation system”. In: *Cyber-Physical Security*. Springer, 2017, pp. 113–131.

[60] Boris Svilicic, Jasmin Celic, Junzo Kamahara, and Johan Bolmsten. “A Framework for Cyber Security Risk Assessment of Ships”. In: *Proceedings of the 19th International Association of Maritime Universities Conference*. 2018, p. 21.

[61] Kimberly Tam and Kevin Jones. “MaCRA: a model-based framework for maritime cyber-risk assessment”. In: *WMU Journal of Maritime Affairs* 18.1 (2019), pp. 129–163.

[62] Jan Erik Vinnem and Ingrid Bouwer Utne. “Risk from cyberattacks on autonomous ships”. In: *Safety and Reliability-Safe Societies in a Changing World* (2018).

[63] Kimberly Tam and Kevin Jones. “Cyber-risk assessment for autonomous ships”. In: *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE. 2018, pp. 1–8.

[64] Boris Svilicic, Junzo Kamahara, Jasmin Celic, and Johan Bolmsten. “Assessing ship cyber risks: a framework and case study of ECDIS security”. In: *WMU Journal of Maritime Affairs* 18.3 (2019), pp. 509–520.

[65] Vivian Louis Forbes. “The global maritime industry remains unprepared for future cybersecurity challenges”. In: *Future Directions, Nedlands* (2018).

[66] CH Chang, S Wenming, Z Wei, P Changki, and CA Kontovas. “Evaluating cyber-security risks in the maritime industry: a literature review”. In: *Proceedings of the International Association of Maritime Universities (IAMU) Conference*. 2019.

[67] Dennis Bothur, Guanglou Zheng, and Craig Valli. “A critical analysis of security vulnerabilities and countermeasures in a smart ship system”. In: (2017).

[68] Boris Svilicic, Igor Rudan, Alen Jugović, and Damir Zec. “A study on cyber security threats in a shipboard integrated navigational system”. In: *Journal of marine science and engineering* 7.10 (2019), p. 364.

[69] Boris Svilicic, Igor Rudan, Vlado Frančić, and Mateo Doričić. “Shipboard ECDIS cyber security: third-party component threats”. In: *Pomorstvo* 33.2 (2019), pp. 176–180.

[70] Kevin D Jones, Kimberly Tam, and Maria Papadaki. “Threats and impacts in maritime cyber security”. In: (2016).

[71] Naveen Goud. *Cyber Attack on COSCO*. [Online]. Available from: https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/. Aug. 2018.

[72] Mr. Apostolos Belokas. *Maersk Line: Surviving from a cyber attack*. [Online]. Available from: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/. May 2018.

[73] *Norsk Hydro lost about $35-40 million after cyber attack*. https://safety4sea.com/norsk-hydro-lost-about-35-40-million-after-cyber-attack/. [Accessed: 2021-02-25].

[74] Odd Sveinung Hareide, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes, and Kirsi Helkala. “Enhancing navigator competence by demonstrating maritime cyber security”. In: *The Journal of Navigation* 71.5 (2018), pp. 1025–1039.

[75] Nir Nissim, Ran Yahalom, and Yuval Elovici. “USB-based attacks”. In: *Computers & Security* 70 (2017), pp. 675–688.

[76] *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea*. July 2013. URL: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/.

[77] James Pavur. *Whispers Among the Stars: Perpetrating (and Preventing) Satellite Eavesdropping Attacks*. https://i.blackhat.com/USA-20/Wednesday/us-20-Pavur-Whispers-Among-The-Stars-Perpetrating-And-Preventing-Satellite-Eavesdropping-Attacks.pdf. BlackHat USA2020. 2020.

[78] Gary C Kessler, J Philip Craiger, and Jon C Haass. "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system". In: *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 12.3 (2018), p. 429.

[79] *Transas - Wärtsilä*. https://www.wartsila.com/transas. [Accessed: 12-05-2021].

[80] Thorlabs. *Multi-Functional Display: Functional Description*. English. Version 3.00.340. Transas. Dec. 2, 2016. 320 pp. 2016-12-02.

[81] Lech Kasyk, Krzysztof Pleskacz, and Grzegorz Bugajski. "An analysis of discrepancies in search areas in a diagram of an expanding square search". In: *Zeszyty Naukowe Akademii Morskiej w Szczecinie* (2016).

[82] *AIVDM/AIVDO protocol decoding*. https://gpsd.gitlab.io/gpsd/AIVDM.html_introduction. [Accessed: 2021-02-02].

[83] *GPS - NMEA sentence information*. http://aprs.gids.nl/nmea/. [Accessed: 2021-04-02].

[84] *Comar Systems RECEIVER: R500Ni*. https://shop.marinetraffic.com/comar-systems-r500ni.html. [Accessed: 2021-02-02].

[85] *Online AIS Message Decoder*. http://ais.tbsalling.dk/. [Accessed: 2021-02-02].

[86] *Snort IPS Deployment Guide*. https://www.cisco.com/c/en/us/products/collateral/security/router-security/guide-c07-736629.html. [Accessed: 2021-16-04].

[87] https://www.softwaretestinghelp.com/intrusion-detection-systems/. [Accessed: 2021-04-03].

[88] *10 Best Network Intrusion Detection Systems Software & NIDS Tools*. https://www.comparitech.com/net-admin/nids-tools-software/. [Accessed: 2021-04-03].

[89] *Globee Business Awards: BUSINESS AWARDS FOR EVERY INDUSTRY IN THE WORLD*. https://globeeawards.com/business/snort/#business-awards. [Accessed: 2021-04-03].

[90] *New Snort 3 release available — Here are all the updates and fixes*. https://blog.snort.org/2021/05/new-snort-3-release-available-here-are.html. [Accessed: 2021-05-12].

[91] *Snort++ Developers Guide*. https://github.com/snort3/snort3/releases/download/3.1.4.0/snort_devel.html. [Accessed: 09-05-2021].

[92] Mi-Jin Kim, Jong-Wook Jang, and Yun-sik Yu. "Topology Configuration for Effective In-Ship Network Construction". In: *International Conference on Advanced Communication and Networking*. Springer. 2011, pp. 380–392.

[93] Imdadul Karim, Quoc-Tuan Vien, Tuan Anh Le, and Glenford Mapp. "A comparative experimental design and performance analysis of snort-based intrusion detection system in practical computer networks". In: *Computers* 6.1 (2017), p. 6.

[94] Pritika Mehra. "A brief study and comparison of snort and bro open source network intrusion detection systems". In: *International Journal of Advanced Research in Computer and Communication Engineering* 1.6 (2012), pp. 383–386.

[95] Guohang Lu, Yi Liu, Yifei Chen, Chengwei Zhang, Yayu Gao, and Guohui Zhong. "A Comprehensive Detection Approach of Wannacry: Principles, Rules and Experiments". In: *2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE. 2020, pp. 41–49.

[96] M Satheesh Kumar, Jalel Ben-Othman, and KG Srinivasagan. "An investigation on wannacry ransomware and its detection". In: *2018 IEEE Symposium on Computers and Communications (ISCC)*. IEEE. 2018, pp. 1–6.

[97] S Chakrabarti, Mohuya Chakraborty, and Indraneel Mukhopadhyay. "Study of snort-based IDS". In: *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*. 2010, pp. 43–47.

[98] OJ Rodseth, Morten Jagd Christensen, and K Lee. "Design challenges and decisions for a new ship data network". In: *ISIS* (2011), pp. 15–16.

[99] Odd Sveinung Hareide and Runar Ostnes. "Scan pattern for the maritime navigator". In: *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 11.1 (2017).

[100] *Electronic Chart Display and Information System ECDIS EC-8100, EC-8600 with Track Control System*. https://www.tokyokeiki.jp/e/products/detail.html?pdid=158. [Accessed: 2021-18-04].

[101] International Maritime Organization (IMO). *ECDIS – GUIDANCE FOR GOOD PRACTICE*. MSC.1/Circ.1503/Rev.1. June 2017.

[102] *Snort++*. https://github.com/snort3/snort3. [Accessed: 12-05-2021].

[103] *Suricata*. https://github.com/OISF/suricata. [Accessed: 12-05-2021].

[104] *The Zeek Network Security Monitor*. https://github.com/zeek/zeek. [Accessed: 12-05-2021].

[105] *Snort 3 User Manual*. https://usermanual.wiki/Pdf/snortmanual.1346323497/view. [Accessed: 12-05-2021].

[106] Henrik Holm and Niklas Mellegård. "Fast decoding of automatic identification systems (AIS) data". In: *Proceedings of the International Conference on Computer Applications and Information Technology in the Maritime Industries (COMPIT)*. 2018.

[107] Changchuan Lin, Fang Dong, Lin Hai, Lina Le, Jianwen Zhou, and Yangping Ou. "AIS information decoding and fuzzy fusion processing with marine radar". In: *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE. 2008, pp. 1–5.

[108] Kurt Schwehr. *libais*. https://github.com/schwehr/libais. [Accessed: 12-02-2021]. 2019.

[109] Mario Konrad. *marnav*. https://github.com/mariokonrad/marnav. [Accessed: 12-02-2021]. 2020.

[110] Brian Caswell and Jay Beale. *Snort 2.1 intrusion detection*. Elsevier, 2004.

[111] *Suricata Developers Guide*. https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Developers_Guide. [Accessed: 2021-09-05].

[112] *SURICON – 2021 SuriCon in Boston presented by OISF*. https://suricon.net/. [Accessed: 2021-09-05].

[113] *Barnyard2*. https://github.com/firnsy/barnyard2. [Accessed: 12-05-2021].

Appendices

Appendix 1 - AIS Message Analysis

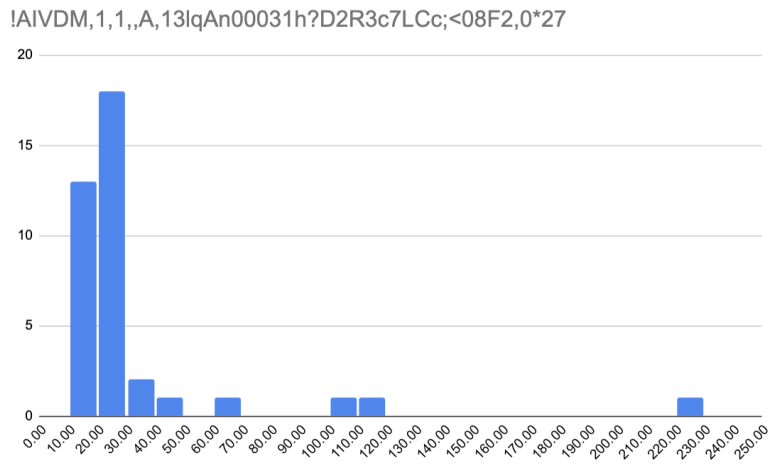

Figure 21. *Time intervals deviation for 13LqAn0003.*

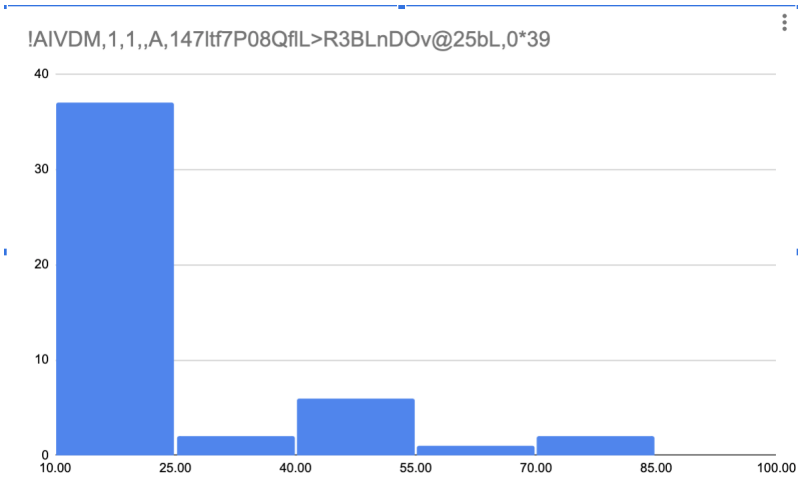

Figure 22. *Time intervals deviation for 147ltf7P08.*

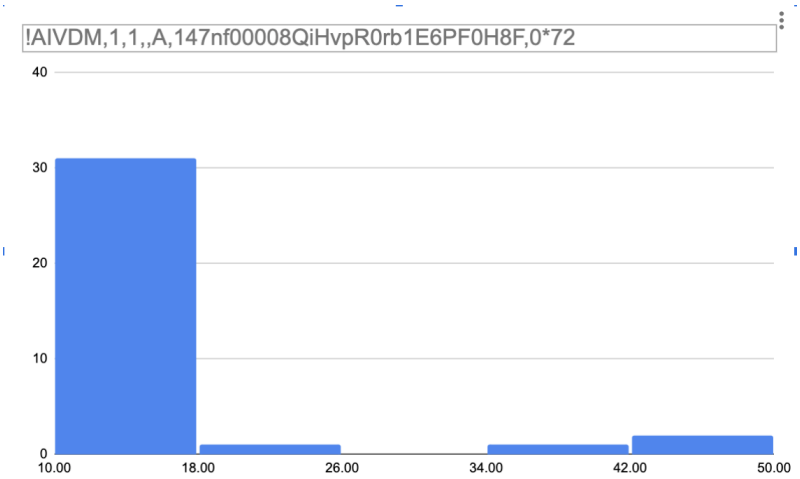

Figure 23. *Time intervals deviation for 147nf00008Q.*

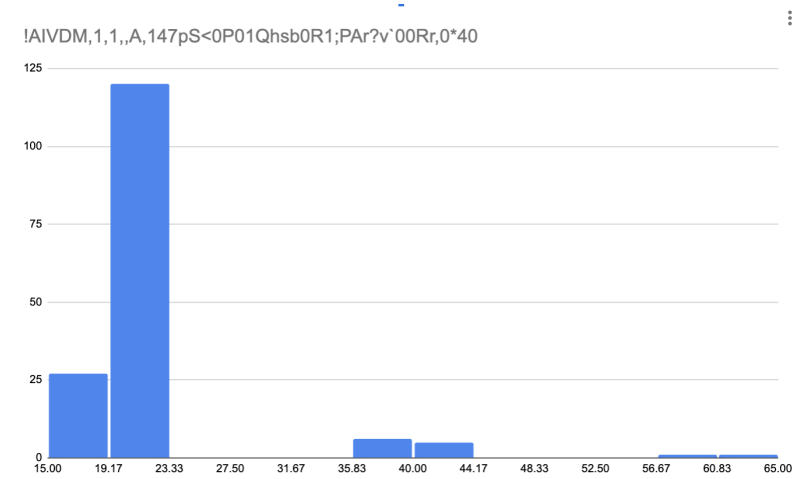

Figure 24. *Time intervals deviation for 147pS<0P01.*

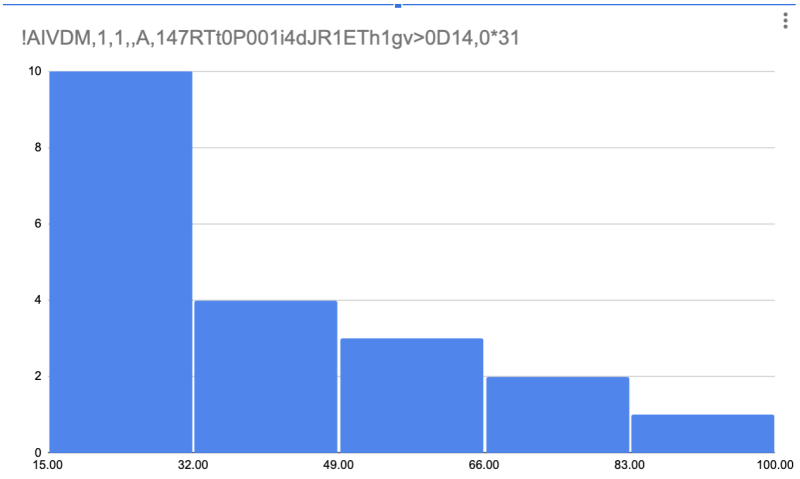

Figure 25. *Time intervals deviation for 147RTt0P00.*

Appendix 2 - Expert Interviews

Questions to ship crew during the trip to ferry Leiger on 17th of February 2021

- Which systems vessel relies on during course-keeping process? (GPS only/GPS+onboard compass/INS/something else).
- Which OS version is used on the vessel for the most important hosts?
- What is the average time the vessel system is online? (During one trip)
- Is it possible to install additional software to the machine running ECDIS/AIS/Automation hosts? And if no, then how it is being prevented.
- What is the current authorization mechanics in the computers? How many users exist in the system?
- How often the systems are being updated? And is there anything that can prevent from updating? (System incompatibility, for example)
- Describe the network setup on the ship - how many switches/routers/firewalls/other? What are the manufacturer and version installed?
- How the guest network is being separated from the crew network?

Questions to Port of Tallinn engineers during the Teams call on 12th of April 2021

1. Is it possible to use open-source software on the vessel? What can prevent from using one?

Expert 1: The first concern about this idea: I do not know if big companies that produce the automation and navigation integrators like Warstsila or Transas, thinking about adding open-source solutions to their systems that are certified for safe navigation. As I understood, open-source is a tool that can be developed by everyone so it is opening new vulnerability vectors, companies will not add to their packages such tooling.

When it is certified as a package, it will be included in the navigation integrator package inside, it should be accepted by the integrator. And when it is already accepted it will be locked: they will take it, customise, certify and then it will be taken on board but after that it will be not anymore customizable.

Expert 2: I agree, there might be problems integrating open-source into commercial product because it is against open source community behaviour. We had this problem: there was a good open-source but we could not use it because the end product was commercial.

Expert 1: The easiest way to still use open-source product on bridge without additional certification is to use it in a navigational system as a listener. It should be not placed inside the network, but, what nowadays navigational systems allow, is to take NMEA data from automation and navigation as serial data only from transmit channel. This data that be used to evaluate the cyber danger and if Snort will discover something, it can alert a separate system but not as a part of the automation and navigation system. It will be a separate device that is listening to serial communication. That is what companies allow to do nowadays, this doesn't require any certification. As an example, right now we have a separate energy monitoring system working on board. We have a system that is monitoring the energy and fuel consumption in real-time and what we using is that we are taking from Watsila the same: we listen to the serial communication RC422 or RS485, convert to TCP/IP and take to another network. It will communicate only by reading but not intervening the communication. Integrator is not allowing third party services as it should be agreed and developed in cooperation with navigation equipment integrator.

Expert 3: I would like to add, that Snort as a listener - it is fine. Open-source products are bringing quite significant resource overhead compared to commercial tools. You need to have the know-how and a really capable team delivering such solutions. Commercial products can be just installed and working but open-source can be daily maintenance. The cost is hidden in human hours. Shipping companies prefer to pay for commercial products rather than for human resources.

Expert 1: The idea of open-source is good and companies might be interested in advancing open-source solution for their needs. As we know, right now, most of the navigation equipment do not have any antivirus or any cyber protection. This is because the antivirus can disrupt the processes needed for safe navigation or deliver false positives.

As a listener even if it cannot avoid or prevent an attack, it is still going to log the information and leave traces. Today if somebody is attacking the system and locking down the system, you have no idea what happened. The equipment providers are having some kind of system logging but it is not easy to reach the logs by shipowners. If the listener has a data about how the attack happened, shipowners might start investigating who is behind it, why and how it happened, what happened, how we can recover, etc. That can be a really useful appliance.

2. What are the criterias for choosing cybersecurity products to be installed on a ship?

Expert 1: The common answer: it is all about the money. What today is shipowners are looking at is budget. The budget is one of the most important things. It is definitely will limit some products. Secondly, integration to the system - how easy it can be integrated, what are the possible side effects, if it requires human hours, etc. The product should be working as independent, reliable, approved by a navigational integrator solution as the main responsibility of the officer is safe navigation and cybersecurity tools should not deliver any additional problems.

3. Is it possible to install additional software on machines running ECDIS?

Expert 1: Short answer: not allowed.

4. What is the common network topologies on the ship's bridge?

Expert 1: I don't know if I can be specific on this question. Expert 2: We can mention the ring topology.

General discussion

Expert 3: We are currently in initial step of risk assessment. At the current situation OT attacks are not that common as IT systems. So in rder to consider additional protection, the business case should be there. Nowadays, it ia hard to see how IT system attacks can affect OT systems on ship. If you take MITRE ATTACK strategies, when it comes to maritime and OT systems, there are a lot of gaps - only when someone fills in those gaps, then IDS can become more relevant. Right now it is not that relevant.

Expert 2: Yes, right now, yhey are separated: OT and IT systems, but it is going to be changed as transportation is changing towards autonomous ships where IT and OT will become closely interconnected.

Expert 1: I agree that we are moving towards automonous shipping where systems running Windows 7 or XP is going to be unacceptable.