

IAMU 2021 Research Project
(No. 20210302)

Towards a Cyber Secure Shipboard ECDIS
Theme: 3

By

Faculty of Maritime Studies, University of Rijeka

August 2022

IAMU
International Association of Maritime Universities

International Association of Maritime Universities

This report is published as part of the 2021 Research Project in the 2021 Capacity Building Project of International Association of Maritime Universities, which is fully supported by The Nippon Foundation.

The text of the paper in this volume was set by the author. Only minor corrections to the text pertaining to style and/or formatting may have been carried out by the editors.

All rights reserved. Due attention is requested to copyright in terms of copying, and please inform us in advance whenever you plan to reproduce the same.

The text of the paper in this volume may be used for research, teaching and private study purposes.

No responsibility is assumed by the Publisher, the Editor and Author for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in this book.

Editorial

IAMU Academic Affairs Committee (AAC)

Head of Committee : Professor Dr. Adam Weintrit
Rector, Gdynia Maritime University (GMU)

Editorial committee : Adam Przybylowski (GMU)
Avtandil Gegenava (BSMA)
Christian Matthews (LJMU)

Contractor : Alen Jugovic

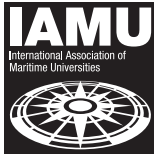
Research Coordinator: Boris Svilicic

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

Copyright ©IAMU 2022

All rights reserved

ISBN978-4-907408-39-8



IAMU 2021 Research Project
(No. 20210302)

Towards a Cyber Secure Shipboard ECDIS
Theme: 3

By
Faculty of Maritime Studies, University of Rijeka

Contractor : Alen Jugovic
Research Coordinator : Boris Svilicic
Research Partner : Jeric Bacasdoon, MAAP
Ahmed K. Tawfik, AAST-MT
Sam Pecota, CSUM

Contents

1. Introduction	2
2. Shipboard ECDIS systems	4
2.1 Training ship Kraljica mora	4
2.2 Training ship AIDA IV	5
2.3 Training ship Kapitan Gregorio Oca	6
3. Cyber Security Resilience Examination Process	8
3.1 Ship Crew Interview	9
3.2 Cyber Vulnerability Scanning	11
4. Experimental Results	13
4.1 Training ship Kraljica mora	13
4.2 Training ship AIDA IV	14
4.3 Training ship Kapitan Gregorio Oca.	15
4.4. Radar systems	17
4.4.1 Training ship Kraljica mora	17
4.4.2 Training ship Kapitan Gregorio Oca	18
5. Cyber Risks	20
5.1 ECDIS Systems Cyber Risks	20
5.2 Comparison of ECDIS and Radar Systems Cyber Risks	22
6. Conclusions	24
References	25
Appendix: Deliverable (Conference Abstract)	29
Appendix: Deliverable (Conference Paper)	31

Towards a Cyber Secure Shipboard ECDIS

Theme: 3

Faculty of Maritime Studies, University of Rijeka

Boris Svilicic

*Tenured Professor, Faculty of Maritime Studies, University of Rijeka, Croatia,
boris.svilicic@pfri.uniri.hr*

Jeric Bacasdoon

Maritime Academy of Asia and the Pacific, Philippines

Ahmed K. Tawfik

Arab Academy for Science, Technology and Maritime Transport, Egypt

Sam Pecota

California State University Maritime Academy, USA

Abstract A comparative cyber security resilience examination of ECDIS systems implemented on three training ships is presented. The examination process is adjusted to the ECDIS systems' operating environment and implemented safeguards, and conducted by means of ships' crew interviews and cyber vulnerability scanning of the ECDIS systems. In addition, radar systems implemented on two training ships are examined using the same process and the results are compared with the examination results of the shipboard ECDIS systems. The results obtained suggest that potential sources of cyber risks of the shipboard ECDIS systems are mainly from the ECDIS software underlying operating system maintenance, but also from the maintenance of ECDIS software's third-party components. The results obtained imply that different critical systems and assets of a ship, which are of the same manufacturer, are most probably subjected to the identical cyber security risks. The results suggest that the high level of cyber security is based on the technological and architectural implementation of the ship's critical systems and assets.

Keyword: *navigation safety, ECDIS, maritime cyber security, cyber-physical system*

1. Introduction

The Electronic Chart Display and Information System (ECDIS) has become a major aid for the safe navigation of ships. ECDIS brings the combination of the paper charts workload reduction and real time navigational information provision, so the ship's navigational officers can focus on the actual traffic situation, improving the safety of ship navigation [1]. The International Maritime Organization (IMO) has set up the requirement for the mandatory ECDIS carriage requirement for all SOLAS vessels [2]. With the improvement for nearly three decades, mainly by the integration and networking, ECDIS has developed into a complex cyber-physical system. The initial concerns from the new equipment and the over-reliance have been changed to awareness of cyber risks threatening safe ship navigation [3-13].

The security risks rising from the application of cyber technologies in ECDIS systems have been recognized by the IMO, and therefore the general cyber security guidelines for safeguarding the ship navigation are recently published [14]. In addition, IMO has amended to include cyber security risk management in the safety management systems starting from 1st January 2021 [15]. Namely, the requirement encourages maritime administrations to ensure that cyber security risks are appropriately addressed in safety management systems as well as that cyber security risk management as a part of safety management system follows objectives and functional requirements of the ISM Code. On the other hand, the functionality of the ECDIS software is standardized by IMO with the performance standards [2]. However, the supporting hardware and underlying operating system required for running the ECDIS software are arranged by ECDIS equipment manufacturers.

In this report, we present a comparative cyber security resilience examination of ECDIS systems that are implemented on board three training ships (Figure 1):

- *Kraljica mora* (IMO: 9569358) provided by the University of Rijeka Faculty of Maritime Studies, Croatia (details available at: <https://mmpi.gov.hr/more-86/skolski-brod-116/116>),
- *Aida IV* (IMO: 9018775) provided by the Arab Academy for Science, Technology and Maritime Transport, Egypt (details available at: <https://aast.edu/en/maritime/facilities-training-vessel.html>),
- *Kapitan Gregorio Oca* (IMO: 9859959) provided by the Maritime Academy of Asia and the Pacific, Philippines (details available at: <https://amosup.org/news&updates/mv-kapitan-gregorio-oca-new-ship-to-boost-cadets-on-board-quality-training/>).

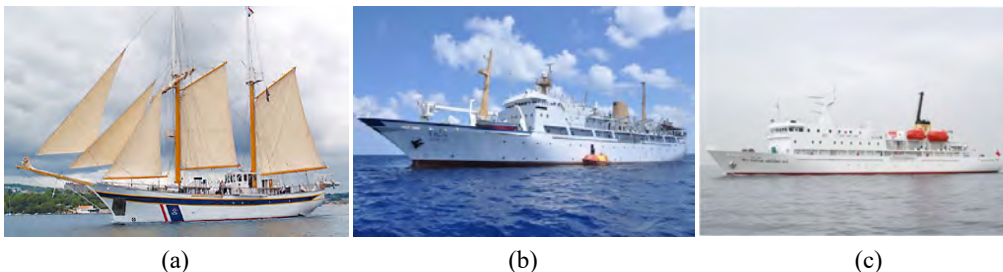


Figure 1.1. The training ships: (a) *Kraljica mora*, (b) *AIDA IV*, and (c) *Kapitan Gregorio Oca*.

In addition to the ECDIS systems cyber security resilience examination, we present the cyber security examination of two radar systems implemented on the training ships in order to compare results with the examination results of the shipboard ECDIS systems. The examination process presented is

adjusted to the ECDIS system operating environment and implemented safeguards. Therefore, we present a questionnaire for the ships' crew interviewing and a model for cyber vulnerability scanning of the ECDIS systems. On the basis of the cyber threats and vulnerabilities identified by the examination process, cyber risks are analysed qualitatively.

2. Shipboard ECDIS systems

Cyber security vulnerabilities in the current deployment of three ECDIS systems have been examined. The ECDIS systems are implemented on the training ships: (i) *Kraljica mora* (IMO: 9569358) provided by the University of Rijeka Faculty of Maritime Studies (Croatia), (ii) *AIDA IV* (IMO: 9018775) provided by the Arab Academy for Science, Technology and Maritime Transport (Egypt), and (iii) *Kapitan Gregorio Oca* (IMO: 9859959) provided by the Maritime Academy of Asia and the Pacific (Philippines). The shipboard EDCIS systems are IMO compliant and meet IMO performance standards.

The examination was not performed on the training ship *Golden Bear* (IMO: 8834407) of the California State University Maritime Academy (California, USA). Unfortunately, due to a number of external factors, including the lingering global pandemic, heightened national security due to war in Europe, and multiple repairs that must be completed before the summer sea voyage commences in early May of 2022, the ship has sharply restricted access to non-essential personnel.

2.1 Training ship *Kraljica mora*

ECDIS system implemented on the training ship *Kraljica mora* is of Wärtsilä Transas manufacturer, model Navi Sailor 4000. The ECDIS software is type approved in the year 2016, it was installed on board the ship in March 2019 and maintained recently. The technical specification of ECDIS system implemented on the training ship *Kraljica mora* is shown in Table 2.1.

ECDIS	<i>Kraljica mora</i>
Manufacturer	Wärtsilä Transas
Model	Navi Sailor 4000
Software version	3.02.350
Approval date	2016
Installation date	2019

Table 2.1. Technical specification of ECDIS system implemented on the training ship *Kraljica mora*.

Figure 2.1 shows the architecture of the ECDIS systems. The ECDIS workstation is networked with a radar workstation and sensors LAN (Local Area Network) switch. The sensors LAN switch is used as a data collector unit for the serial connection of NMEA (National Marine Electronics Association) sensors. The mandatory sensors data (positioning, heading and speed information) and the additional sensors data (AIS and NAVTEX) are gathered to the ECDIS via Ethernet network using the sensors LAN switch.

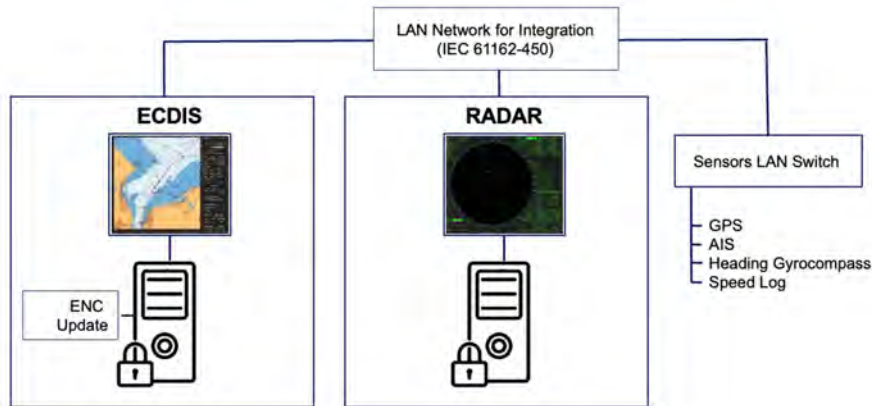


Figure 2.1. Architecture of the ECDIS system implemented on the training ship *Kraljica mora*.

2.2 Training ship AIDA IV

ECDIS system implemented on the training ship *AIDA IV* is also of Wärtsilä Transas manufacturer, model Navi Sailor 4000, but a different version of the ECDIS software compared to the ECDIS system of the training ship *Kraljica mora*. The implemented version of the ECDIS software is type approved in the year 2009 and was installed on board the ship in the year 2010. The technical specification of of ECDIS system implemented on the training ship *AIDA IV* is shown in Table 2.2.

ECDIS	<i>AIDA IV</i>
Manufacturer	Transas
Model	Navi Sailor 4000
Software version	2.00.012
Approval date	2009
Installation date	2010

Table 2.2. Technical specification of ECDIS system implemented on the training ship *AIDA IV*.

The architecture of the ECDIS system is shown in Figure 2.2. The ECDIS is installed in stand-alone mode. The mandatory positioning, heading and speed data, as well as the additional AIS (Automatic Identification System) data, are gathered directly via the serial NMEA interface (standard IEC 61162). Hardware resources of the ECDIS workstation are very limited, in particular no device for ECDIS networking is installed.

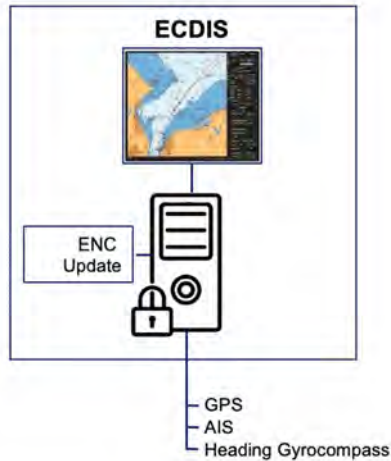


Figure 2.2. Architecture of the ECDIS system implemented on the training ship *AIDA IV*.

2.3 Training ship *Kapitan Gregorio Oca*

ECDIS system implemented on the training ship *Kapitan Gregorio Oca* is of Furuno manufacturer, model FMD-3200. The ECDIS software is type approved in the year 2017 and was installed on board the ship in the year 2020. The technical specification of ECDIS system implemented on the training ship *Kapitan Gregorio Oca* is shown in Table 2.3.

ECDIS	<i>Kapitan Gregorio Oca</i>
Manufacturer	Furuno
Model	FMD-3200
Software version	2450074-03.17
Approval date	2017
Installation date	2020

Table 2.3. Technical specification of ECDIS system implemented on the training ship *Kapitan Gregorio Oca*.

Figure 2.3 shows the architecture of the ECDIS systems. The ECDIS system consists of two identical ECDIS workstations that are networked with two identical radar workstation and sensors LAN switch. The architecture consisting of two regular ECDIS workstations, a primary ECDIS and an independent backup ECDIS with a separate power supply and positioning sensor, allows the paperless navigation of the ship [16, 17]. On the ECDIS workstations, the sensors data are gathered via Ethernet network using the sensors LAN switch.

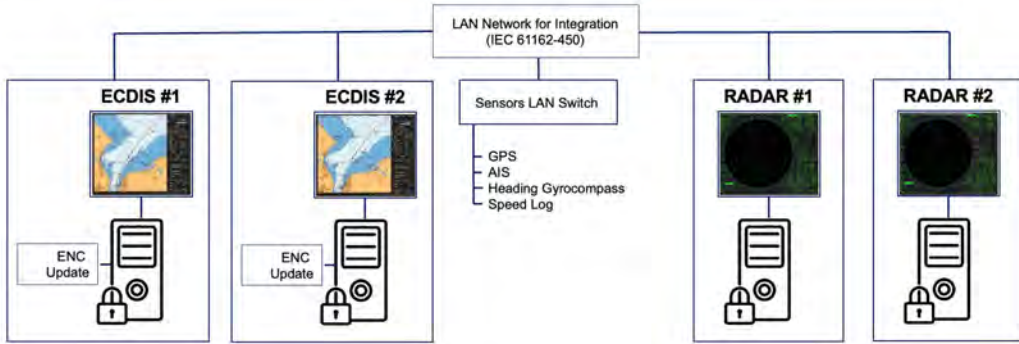


Figure 2.3. Architecture of the ECDIS system implemented on the training ship *Kapitan Gregorio Oca*.

3. Cyber Security Resilience Examination Process

Systematic examination of cyber risks threatening ECDIS systems is essential for improving cyber security of shipboard ECDIS systems. ECDIS cyber security examination represents a complex set of related and interdependent actions that intersect to provide safeguards that are effective and corresponding to challenges presented by ECDIS systems specifics, cyber technology evolution, and human resource capabilities [7]. Results of the ECDIS cyber security examination should provide identification of threats and vulnerabilities in the current deployment of shipboard ECDIS systems and determination of the likelihood and impact magnitude of their exposure caused not only by hardware or software, but also by implemented operational procedures and security policies.

The developed ECDIS cyber risk examination process relies on guidelines and practices [7, 14, 18, 19], and is shown in Figure 3.1. The process consists of three main phases: examination preparation, conduction and results communication.

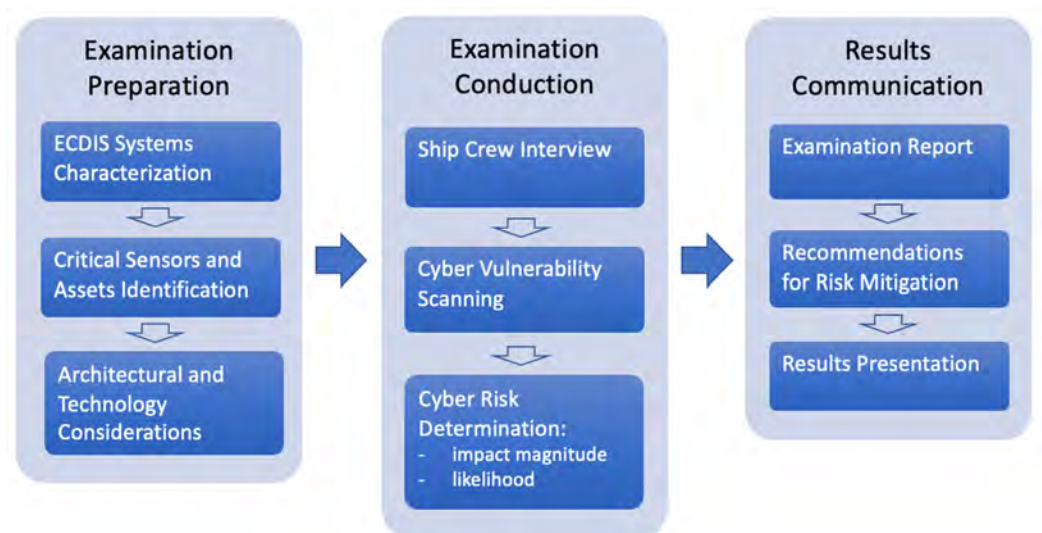


Figure 3.1. ECDIS system cyber security examination process.

In the first phase of the examination process, the shipboard ECDIS systems were characterized by gathering information about general ECDIS systems' technical specifications. The identification of critical ECDIS sensors and assets was conducted based on the ECDIS systems' technical specification documentation and implemented together with the following architectural and technological considerations.

The first phase outputs were used to develop a questionnaire to examine established safeguards by interviewing the ships' crew (second phase of the process). The specific element of the proposed examination process is the conduction of computational vulnerability scanning of the ECDIS systems. Computational cyber vulnerability scanning is a process of reviewing ECDIS systems to locate and identify known weaknesses. In the last segment of the conduction phase, the cyber risks are determined based on the likelihood and impact magnitude of the threats and vulnerabilities detected by the ships'

crew interviewing and vulnerability scanning report. In the final phase of the process, the overall examination results are presented to the ships' crew.

3.1 Ship Crew Interview

The goal of the first part of the examination process is to identify non-existing and/or insufficient safeguard mechanisms and measures. In addition, the cyber security survey is essential to confirm that cyber security safeguard mechanisms and measures are in place on ECDIS system. The collection of the relevant information was conducted by interviewing the ships' crew with a questionnaire developed on the basis of the characterization of ECDIS systems. The form used for the survey conducted by interviewing the ship crew is given in Figure 3.2.

The questionnaire for interviewing the ships' crew is segmented into five parts regarding the critical assets of the ECDIS systems: ECDIS cyber security management system, implemented operational procedures and security policies, cyber security training and awareness, incident handling and response management, and regular audits (Figure 3.2). Data collection was conducted by interviewing the ships' navigation officers.

The survey results indicate that the ECDIS systems demonstrated an equal level of cyber security. Cyber security is integrated in the ships' policies and procedures, and policies and procedures mainly dedicated to cyber security are not fully developed. However, the policies and procedures are well communicated and periodically reviewed. The ships' crew is trained by the ECDIS systems vendors. On the ECDIS systems, an Internet connection is not established, a physical access policy is in place, the handling of portable devices is controlled, logical authentication is in place, authorization using strong control mechanisms is enforced and confidentiality agreements with all suppliers and sub-suppliers are in place. The results are further analyzed in the context of the ECDIS systems cyber security risks in Chapter "5 Cyber Risks".

Assets of the Critical System	What are the threats?	What are the vulnerabilities?	Are any measures in place to eliminate or reduce threats/vulnerabilities?	Yes/ No	Corrective actions required	Risk Evaluation		
						Impact Magnitude	Likelihood	Overall risk Rating
ECDIS	Involved before in cyber risk assessment	- Hardware - Software						
	Cyber security incident handling procedures are in place	Incidents: - detection - analysis - response						
	Authentication and access control are in place	- Logical and physical access is provided to authorized personnel only - Remote users authentication by using cryptographic based techniques (token, VPN) - All default manufacturers passwords have been changed - All mechanisms of authentications and access controls are enforced - Long and complex passwords are required - Regular changes of passwords are required - Sharing of passwords is never done, common accounts are not used						
	Audit and logs	- Audit logs recording user activities, exceptions and information security events are produced and kept						
	Software security	- Operating system and applications are patched to the latest version and opened necessary services and ports - Unnecessary services and applications are removed or disabled - Operating system is installed anti-virus with latest signatures and enabled real-time scanning - Separation of duties through assigned access authorisations - A limit of consecutive invalid access attempts is enforced						
	Communication Security	- Connections to the Internet, or other external networks or information systems is established - The connections are through managed interfaces (e.g. Secure Shell, SSH) consisting of appropriate boundary protection devices (e.g. proxies, gateways, routers, rewrites - Management access to a network device is secured using validated encryption (AES, 3DES, SSH or SSL) - All network management ports and services are disabled (except those needed to support the operational commitments of the site)						
Physical and environmental protection	- Policies and procedures relevant to physical and environmental protection are in place - Awareness and dissemination of policies and procedures to crew are sufficient - Policies and procedures are reviewed periodically or at planned intervals.							
Policies and procedures	Policies and procedures related to cyber security are developed	- Roles and responsibilities are not clearly defined - Incidents detection, analysis and response						
	The policies and procedures are communicated to the all crew	Incidents: - detection - analysis - response						
	The policies and procedures are reviewed periodically	Incidents: - detection - analysis - response						
	Confidential agreements are in place for all sub-suppliers							
Training program and security awareness	Security training and awareness program is developed							
	Appropriate security training and awareness program is conducted to the crew							
Incident handling and response management	All information security incidents are reported							
	Mechanism to monitor and quantify security incidents is identified							
Regular audits for cyber security are performed								

Figure 3.2. Questionnaire to examine established safeguard measures by interviewing the ships' crew.

3.2 Cyber Vulnerability Scanning

Cyber vulnerability scanning is a process of reviewing ECDIS systems in order to detect, classify and report on known security flaws and vulnerabilities. The cyber vulnerability scanning process (Figure 3.3) starts with gathering all relevant information about the target ECDIS system. This phase relied on the data collected by the interview, which was enhanced with technical documentation of the ECDIS system. The second phase of the process was started by breaking the model preparation for effective scanning into three distinct steps: (i) determining turned-on and communicable ECDIS systems, (ii) identifying active ports and services on the ECDIS system, and (iii) obtaining appropriate credential to gain access to the ECDIS system.

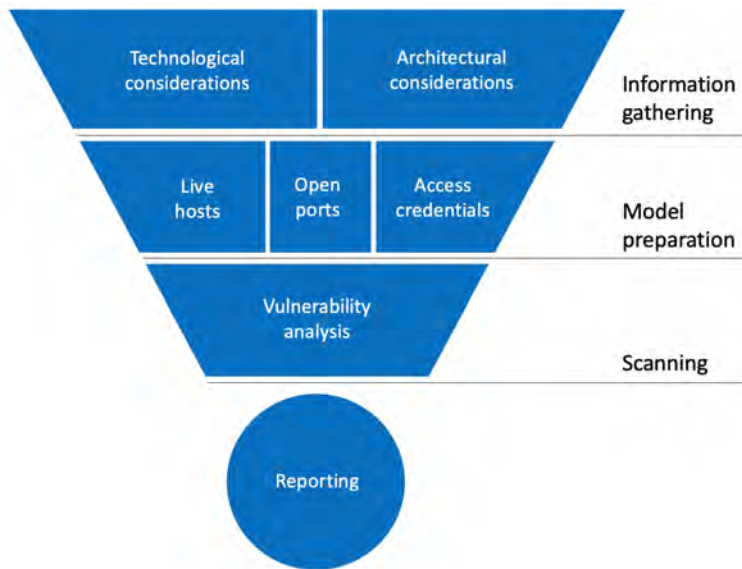


Figure 3.3. Cyber vulnerability scanning process.

The vulnerability scanning was conducted using a piece of commercial software running on a laptop that was connected to the ECDIS systems. The vulnerability scanner uses a database to compare details about the scanned ECDIS system. The database references known flaws, coding bugs, packet construction anomalies, default configurations, and potential paths to sensitive data that can be exploited by attackers. After the vulnerability scanner checks for possible vulnerabilities, it reports security fixes or missing service packs, identifies malware as well as any coding flaws, and monitors remote access. The scanning results in the report were then analyzed to improve their security posture.

The vulnerability of the ECDIS systems was conducted by using a software tool that is most widely used in the industry, the Nessus Professional, version 8.15.2. [20]. Nessus Professional is the most comprehensive vulnerability scanner and possess the ability to perform multiple types of scans across heterogeneous environments that include on-prem, Unix, Linux, Windows, cloud, off-site, and onsite. The ECDIS systems were tested individually, by networking a laptop with the preinstalled vulnerability scanner to the ships' local area network or directly to ECDIS (Figure 3.4).



(a) (b) (c)
 Figure 3.4. Cyber security testing of the ECDIS systems implemented on the training ships:
 (a) *Kraljica mora*, (b) *AIDA IV*, and (c) *Kapitan Gregorio Oca*.

The main advantages of the vulnerability scanner usage are the ability to scan a large number of systems for common cyber vulnerabilities. However, the process is limited to only detecting vulnerabilities and exposures for which the vendor of the tool used has released plugins. The plugin is a program that contains information about newly discovered cyber vulnerabilities, a generic set of remediation actions, and the algorithm to test for the presence of the security issue. Nessus Professional vulnerability scanner supports the Common Vulnerability Scoring System (CVSS) and supports both v2 and v3 values simultaneously [20]. The vulnerability scanner contains 172,763 plugins, covering 69,972 CVE IDs and 30,940 Bugtraq IDs. Figure 3.5 shows a part of the plugins implemented in the used Basic Network scan model of the Nessus Professional.

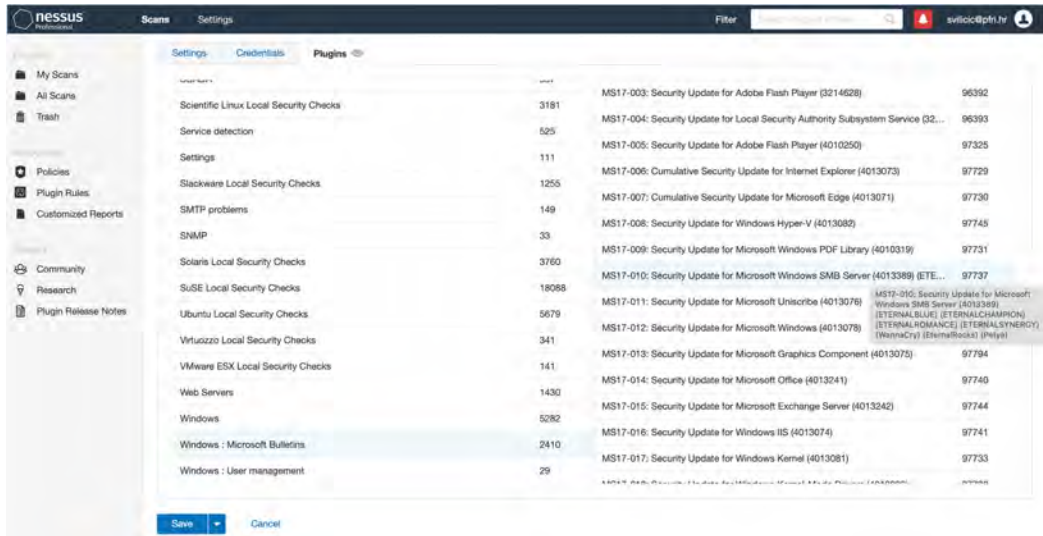


Figure 3.5. Nessus Professional scanning model used.

For example, in Figure 3.5, the selected plugin is related to Server Message Block service (SMB), which is an integral part of Microsoft Windows operating systems, providing file and printer sharing. The vulnerable SMB server [21] represents a threat vector for NotPetya ransomware malicious software to spread and execute arbitrary code on target computers [22]. The ransomware caused probably the most recognized maritime cyber incident, the NotPetya attack on Maersk shipping company [23].

4. Experimental Results

The cyber security resilience examination was performed on three training ships (Figure 1.1), *Kraljica mora* (IMO: 9569358) of the University of Rijeka Faculty of Maritime Studies (Croatia), *Aida IV* (IMO: 9018775) of the Arab Academy for Science, Technology and Maritime Transport (Egypt), and *Kapitan Gregorio Oca* (IMO: 9859959) of the Maritime Academy of Asia and the Pacific (Philippines).

4.1 Training ship *Kraljica mora*

As the training ship *Kraljica mora* is engaged in regular voyage, the examination was conducted in a passive manner, with no disturbance of the ECDIS systems operation, while the ship was docked in the port of Rijeka, Croatia. The laptop with the installed Nessus Professional vulnerability scanner was connected to the sensors LAN switch with an Ethernet cable. While the ECDIS software was running with administrative permissions, the remote cyber vulnerability scanning was performed without administrative rights. Figure 4.1 shows the testing setup.



Figure 4.1. Cyber vulnerability scanning of the ECDIS system implemented on the training ship *Kraljica mora*.

The summary report of the cyber vulnerabilities scanning of the ECDIS system implemented on the training ship *Kraljica mora* is shown in Figure 4.2. The results obtained indicate significant vulnerabilities detected on the ECDIS system.



Figure 4.2. Cyber security vulnerabilities detected on the ECDIS system of the training ship *Kraljica mora*.

The results detected on the training ship *Kraljica mora* (Figure 4.2) indicate 3 critical, 2 high and 7 medium cyber vulnerabilities. The exploitation of vulnerabilities with the critical severity is usually straightforward, meaning that attackers do not need any special knowledge about target systems, and likely results in root-level compromise of target systems. The most critical vulnerability of the ECDIS

system is that the ECDIS software is running on the operating system that is unsupported by its manufacturer. In particular, Microsoft Windows 7 Professional operating system has been used, which is not supported by the manufacturer since January 2020 [24]. The remaining critical and high severity cyber security vulnerabilities are related to the vulnerable web server and unsupported version of a system software. In particular, Apache web server version 2.4.49 [25] and Python interpreter version 2.7.15 [26] are running on the ECDIS system. For both critical vulnerabilities, the support is based on help from members of the communities (Apache and Python communities) who work as enthusiastic volunteers. In addition, the results point out that the significant cyber vulnerabilities exist not only in the software components developed by the manufacturers of the ECDIS software (Wärtsilä Transas) or the underlying operating system (Microsoft), but also in the third-party software components (Apache web server and Python interpreter). A comprehensive list of the cyber vulnerabilities detected is shown in Figure 4.3.

Severity	CVSS v3.0	Plugin	Name
CRITICAL	7.5	153952	Apache 2.4.49 < 2.4.51 Path Traversal Vulnerability
CRITICAL	10.0	148367	Python Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	4.3	153884	Apache 2.4.49 < 2.4.50 Multiple Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Figure 4.3. Comprehensive list of the cyber vulnerabilities detected on the ECDIS system of the training ship *Kraljica mora*.

4.2 Training ship AIDA IV

The cyber vulnerability scanning of the ECDIS system implemented on the ship *AIDA IV* was not performed because the ECDIS software is running on the stand-alone workstation with no hardware for internetworking implemented. However, the examination was performed manually. During the examination the ship was docked in a port. Figure 4.4. shows a display of the ECDIS system implemented on the ship.

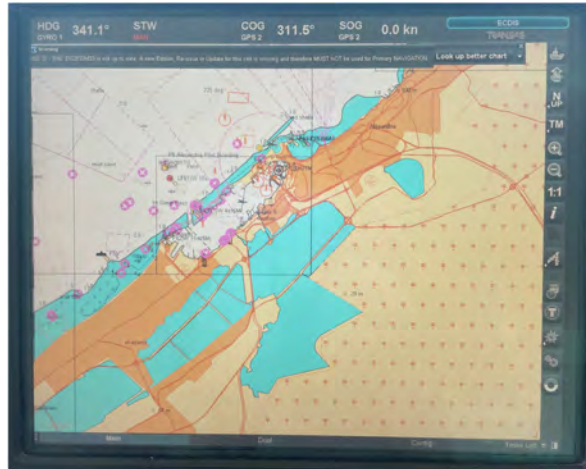


Figure 4.4. Display of the ECDIS system implemented on the training ship *AIDA IV*.

The manual examination has shown that the ECDIS software is running on the Microsoft Windows XP operating system. The version of the operating system is unsupported by the manufacturer (Microsoft company) since the year 2014 [24]. The unsupported operating system implies that no new cyber security patches have been released by the manufacturer for about 8 years now. While the ECDIS software was running on a critically vulnerable operating system, the stand-alone implementation with no internetworking ability provided a high level of cyber security.

4.3 Training ship *Kapitan Gregorio Oca*.

The examination of the primary and backup ECDIS workstations was conducted in a passive manner while the ship was docked in a port. The laptop with Nessus Professional vulnerability scanner was networked with the Sensors LAN Switch. The testing setup is shown in Figure 4.5.

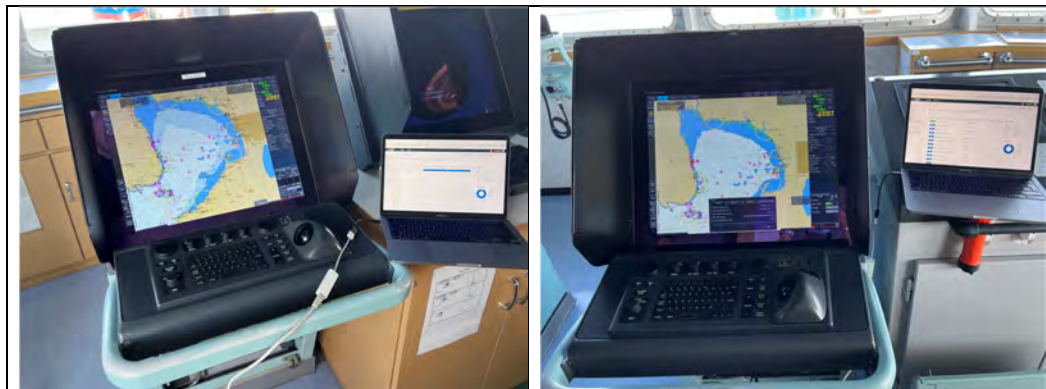


Figure 4.5. Cyber vulnerability scanning of the ECDIS system implemented on the training ship *Kapitan Gregorio Oca*.

The summary reports (the primary and backup ECDIS workstations) of the cyber vulnerabilities scanning of the ECDIS system implemented on the training ship *Kapitan Gregorio Oca* are shown in

Figure 4.6. The results obtained indicate high security level of the ECDIS system. In addition, the summary reports of the ECDIS workstations are identical.



Figure 4.6. Cyber security vulnerabilities detected on the ECDIS system of the training ship *Kapitan Gregorio Oca*.

The only vulnerability detected, classified as the low-level, is related to an X11 server running on the ECDIS system. The same vulnerability is detected on both ECDIS workstations. The basis for the excellent cyber security results is in the usage of a Linux operating system, which makes the ECDIS system less susceptible to potential cyber security threats. In addition, adequate setup and maintenance of the operating system enhance the level of the ECDIS system cyber security. A comprehensive list of the detected cyber vulnerability and information is shown in Figure 4.7.

Severity	CVSS v3.0	Plugin	Name
LOW	2.6	10407	X Server Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	11389	rsync Service Detection
INFO	N/A	78428	rsync Writeable Module Detection

Figure 4.7. Comprehensive list of the cyber vulnerabilities detected on the ECDIS system of the training ship *Kapitan Gregorio Oca*.

4.4. Radar systems

On the training ships *Kraljica mora* and *Kapitan Gregorio Oca*, radar systems are implemented. In order to compare the cyber security level of the ECDIS and radar systems implemented, the cyber security resilience examination of the radar systems was performed.

4.4.1 Training ship *Kraljica mora*

The radar system has been examined using the same cyber vulnerability scanning process (Figure 4.8). The implemented radar system is Wärtsilä Transas Navi-Radar 4000.

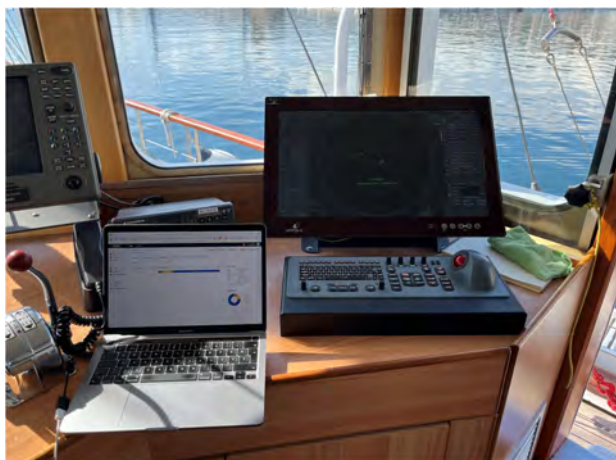


Figure 4.8. Cyber vulnerability scanning of the radar system implemented on the training ship *Kraljica mora*

The summary report of the cyber vulnerabilities scanning of the radar system implemented on the training ship *Kraljica mora* is shown in Figure 4.9. The results obtained indicate significant vulnerabilities detected on the radar system and are identical to the vulnerabilities detected on the ECDIS system (Figure 4.2).



Figure 4.9. Cyber security vulnerabilities detected on the radar system of the training ship *Kraljica mora*.

As in the case of the ECDIS system, the results detected (Figure 4.9) indicate 3 critical, 2 high and 7 medium cyber vulnerabilities. The most critical vulnerability of the radar system is that the radar software is running on the operating system that is unsupported by its manufacturer, Microsoft Windows 7 Professional [24]. The remaining critical and high severity cyber security vulnerabilities are related to the third-party software components, Apache web server version 2.4.49 [25] and Python interpreter version 2.7.15 [26]. The vulnerabilities detected are identical to vulnerabilities detected on the ECDIS system (Figure 4.3).

4.4.2 Training ship *Kapitan Gregorio Oca*

The primary and backup radar workstations have been examined using the same cyber vulnerability scanning process (Figure 4.10). The implemented radar system is Furuno Radar FAR-3320.

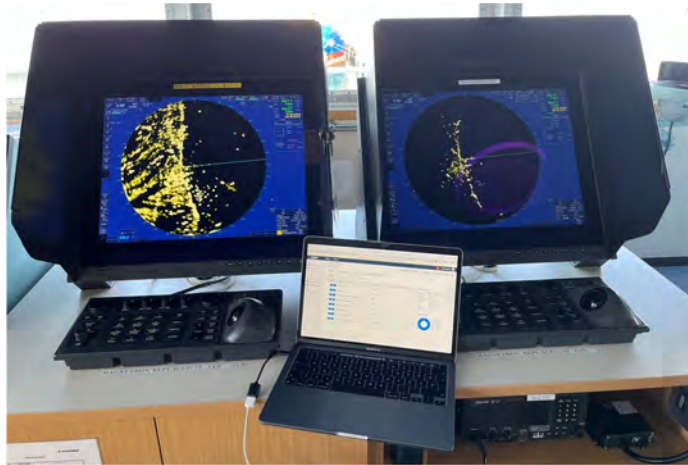


Figure 4.10. Cyber vulnerability scanning of the the radar system implemented on the training ship *Kapitan Gregorio Oca*.

The cyber vulnerabilities scanning reports of the primary and backup radar workstations implemented on the training ship *Kapitan Gregorio Oca* are shown in Figure 4.11. As in the case of the ECDIS systems, the results obtained indicate high security level of the radar system. In addition, the summary reports of the radar workstations are also very similar to the cyber vulnerabilities detected on the ECDIS system (Figure 4.6).

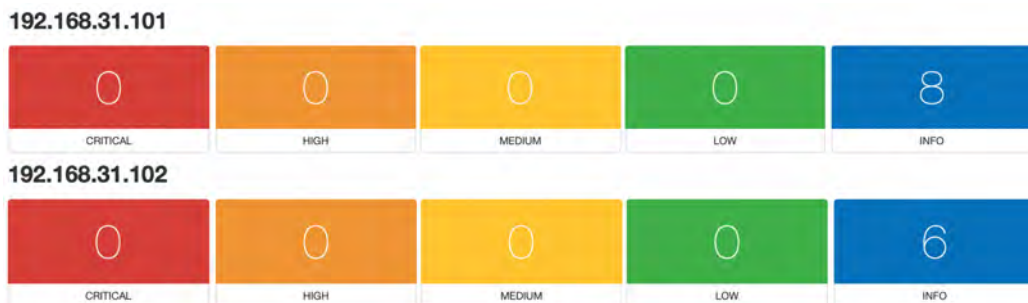


Figure 4.11. Cyber security vulnerabilities detected on the radar system of the training ship *Kapitan Gregorio Oca*.

Compared to the cyber vulnerabilities detected on the ECDIS system (Figure 4.6), no cyber vulnerabilities have been detected on the radar system implemented on the training ship *Kapitan Gregorio Oca* (Figure 4.11).

5. Cyber Risks

The cyber risks determination, as part of the ECDIS systems cyber security examination process (Figure 3.1), was conducted on the basis of a qualitative analysis of cyber threats identified by the ships' crew interview and cyber vulnerability scanning performed. While the cyber vulnerabilities scanning with the general industry tool (Nessus Professional) is used to detect all known vulnerabilities existing in the ECDIS systems, the results could inaccurately reflect the actual severity of threats due to ship environment specifics. Therefore, the vulnerability scanning results were analyzed in the context of the ECDIS systems operating environment and implemented safeguards that are identified with the ships' crew interview.

The qualitative risk analysis is performed by evaluating the impact magnitude and likelihood of threats determined that could exploit detected vulnerabilities to harm the cyber security of ECDIS systems. The method provides a relatively simple, but satisfactory basis for cyber risk analysis. The cyber threat likelihood is a rating of the probability that a detected vulnerability is exploited. The likelihood levels were given with a value from 0 up to 1. The impact refers to the magnitude of damage resulting from the exploitation of a detected vulnerability. The impact magnitude rates were given with a value from 0 (no impact) to 100 (total impact). The cyber risk levels were calculated by multiplying the threat likelihood ratings with the impact magnitude of the vulnerability exploited. The given result indicates qualitative risk level: (i) acceptable low risk level, (ii) medium risk level which may be acceptable over a short period of time, (iii) high risk level requiring an action plan to mitigate the risk, and (iv) critical risk level requiring immediate action.

5.1 ECDIS Systems Cyber Risks

In total, eight cyber risks were determined. Table 5.1 shows the determined cyber risks of the ECDIS systems, together with an estimated impact magnitude rate and a likelihood level. As the examined ships are of the same class (the training ships), the impact magnitudes of all cyber risks were estimated at the same rate for all the ships. Four cyber risks were estimated with the highest (total) impact magnitude (Table 5.1, cyber risks 1-3, and 5). These cyber risks were related to the maintenance of the ECDIS systems' underlying operating system (abandoned, out of date and with an insecure setup), maintenance of the ECDIS software third-party components and Internet connection establishment. However, the likelihood levels were estimated differently for each ship. The highest likelihood levels of the cyber risks were estimated for the ship *Kraljica mora* because of the unsupported and vulnerable versions of the ECDIS software underlying operating system and the third-party software components, Apache web server and Python interpreter (Chapter "4.1 Training ship *Kraljica mora*"). The lowest likelihood levels of the cyber risks were estimated for the ship *AIDA IV* because of the hardware limitation and not possibly for the Internet connection establishment (Chapter "4.2 Training ship *AIDA IV*").

Cyber Risk	Description	<i>Kraljica mora</i>		<i>AIDA IV</i>		<i>Kapitan Gregorio Oca</i>	
		Impact magnitude	Likelihood	Impact magnitude	Likelihood	Impact magnitude	Likelihood
1 ECDIS underlying operating system out of date.	Allows exploitation of well-known vulnerabilities of the ECDIS underlying operating system	100	0.6	100	0.1	100	0.2
2 ECDIS underlying operating system insecure setup	Backdoors are open for possible intrusions and performance are reduced	100	0.6	100	0.1	100	0.2
3 ECDIS software third-party components out of date	Allows exploitation of well-known vulnerabilities of the ECDIS software third-party components	100	0.6	100	0.1	100	0.2
4 Crew training and awareness	Ship crew is not able to adequately perform their duties and adhere procedures	50	0.2	50	0.2	50	0.2
5 Internet connection establishment	Remote attacker is provided with access to ECDIS navigational tools	100	0.3	100	0.0	100	0.1
6 Unauthorized access	Attacker is provided with physical or logical access to ECDIS navigational tools	50	0.1	100	0.1	100	0.1
7 Cyber security policies and procedures	Ship crew is not aware of their roles and responsibilities	20	0.5	20	0.5	20	0.5
8 Continuous assessment and improvement	Lack of ability to respond to rapid technological development	20	0.5	20	0.2	20	0.2

Table 5.1. Cyber risks of the ECDIS systems determined.

The cyber risk levels, calculated by multiplying the impact magnitude rates and the likelihood ratings, are shown in Figure 5.1. The acceptable low risk level cyber threats determined for all the ECDIS systems (Table 5, cyber risks 4, 6–8) were associated with the crew training and awareness, unauthorized access controls, the development of cyber security dedicated policies and procedures, and continuous evaluation and improvement. The slightly higher risk level, but still acceptable low risk level, was associated with the ECDIS system of the training ship *Kraljica mora* due to vulnerable versions of the ECDIS software third-party components, needing more frequent updating (Chapter "4.1 Training ship *Kraljica mora*"). The results were attributed to the fact that the ships are of the same class and therefore the same ECDIS systems' operating environment and implemented safeguards. On all the ships, the crew is continuously trained and familiarized with cyber security issues, strong access controls, cyber security dedicated policies and procedures are implemented, and continuous evaluation and improvement of the critical ship's systems and assets are conducted.

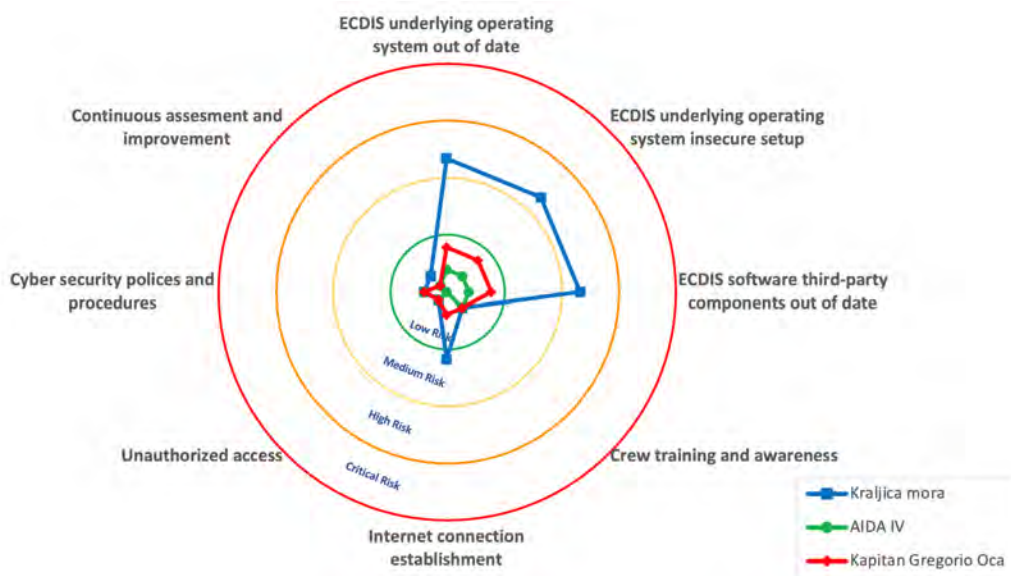


Figure 5.1. Radar graph of the ECDIS systems cyber risks determined.

The cyber risk raised from the possible Internet connection establishment was assigned with the medium risk level (the risk is acceptable over the short period of time) is associated with the ECDIS system of the ship *Kraljica mora*, mainly due to usage of the ECDIS software underlying operating system that is not supported by its manufacturer for a long time (Chapter "4.1 Training ship *Kraljica mora*"). The risk for the training ship *Kapitan Gregorio Oca* is assigned with the low level (acceptable risk) on the basis of the high security level of the ECDIS system determined with the cyber vulnerability scanning (Chapter "4.3 Training Ship *Kapitan Gregorio Oca*"). In the case of the training ship *AIDA IV*, practically there is no risk due to hardware limitations of the ECDIS system (Chapter "4.3 Training Ship *AIDA IV*").

The three high cyber risks were associated to the ECDIS system of the ship *Kraljica mora* (Figure 5.1) and are related to the maintenance of the ECDIS software underlying operating system (unsupported and not securely setup operating system) and the third-party software components (vulnerable and not supported versions of the third-party software). The assigned high level risk indicates that an action plan for cyber risk mitigation is required (Chapter "4.1 Training ship *Kraljica mora*"). The cyber risks are assigned with an acceptable low level for the highly secured ECDIS system of the training ship *Kapitan Gregorio Oca* (Chapter "4.3 Training Ship *Kapitan Gregorio Oca*") and the hardware-limited ECDIS system of the training ship *AIDA IV* (Chapter "4.3 Training Ship *AIDA IV*").

5.2 Comparison of ECDIS and Radar Systems Cyber Risks

The qualitative risk analysis of the cyber risk related to the radar systems implemented on the training ships *Kraljica mora* and *Kapitan Gregorio Oca* was also performed. As in the case of the ECDIS systems, eight cyber risks were determined. The cyber risks of the radar systems are listed in Table 5.2.

Threat	Description	<i>Kraljica mora</i>		<i>Kapitan Gregorio Oca</i>	
		Impact magnitude	Likelihood	Impact magnitude	Likelihood
1 Radar underlying operating system out of date	Allows exploitation of well-known vulnerabilities of the radar underlying operating system	100	0,6	100	0,2
2 Radar underlying operating system insecure setup	Backdoors are open for possible intrusions and performance are reduced	100	0,6	100	0,1
3 Radar software third-party components out of date	Allows exploitation of well-known vulnerabilities of the radar software third-party components	100	0,6	100	0,2
4 Crew training and awareness	Ship crew is not able to adequately perform their duties and adhere procedures	50	0,2	50	0,2
5 Internet connection establishment	Remote attacker is provided with access to radar navigational tools	100	0,3	100	0,1
6 Unauthorized access	Attacker is provided with physical or logical access to radar navigational tools	50	0,1	100	0,1
7 Cyber security policies and procedures	Ship crew is not aware of their roles and responsibilities	20	0,5	20	0,5
8 Continuous assessment and improvement	Lack of ability to respond to rapid technological development	20	0,5	20	0,2

Table 5.2. Cyber risks of the radar systems determined.

By comparing Tables 5.1 and 5.2, it is indicative that there are no significant differences in the cyber risks given impact magnitude rates and likelihood levels. The calculated cyber risk levels of the

radar systems are shown in Figure 5.2. As for the training ship *Kraljica mora*, the cyber risks determined for the radar system (Figure 5.2) are identical to the ECDIS system (Figure 5.1). The only cyber risk that is slightly different (but of the same acceptable low level) is cyber risks determined for the radar system for the training ship *Kapitan Gregorio Oca* and is related to the underlying operating system insecure setup (Tables 5.1 and 5.2, cyber risk 2). On the radar system, the cyber vulnerability related to an X11 server running on the ECDIS system is not detected (Chapter "4.3 Training Ship *Kapitan Gregorio Oca*").

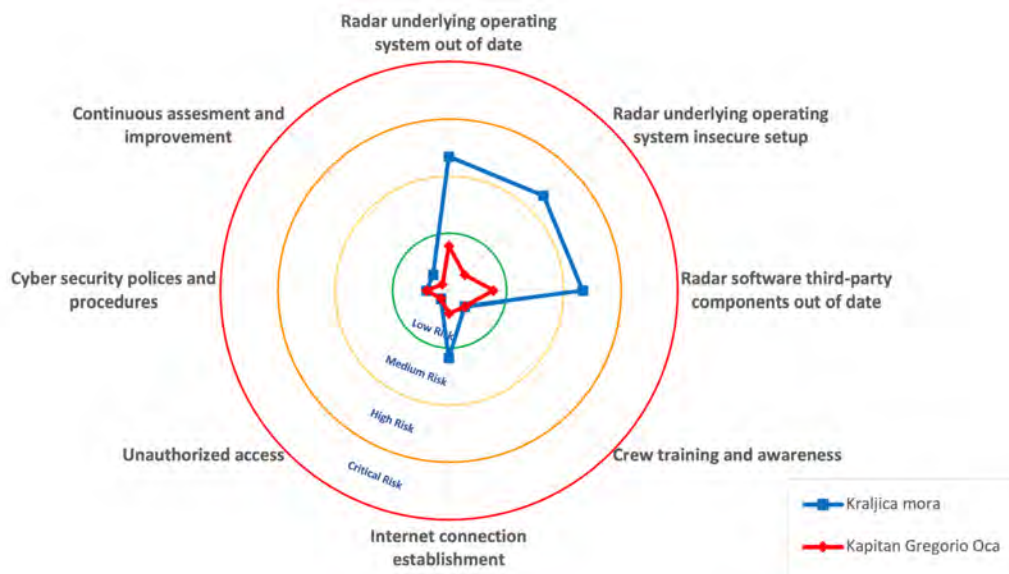


Figure 5.2. Radar graph of the radar systems cyber risks determined.

The results obtained imply that different critical systems and assets of a ship (in this case, ECDIS and radar system), which are of the same manufacturer, are most probably affected by the same cyber security risks. The comparison results confirm that a high level of cyber security is based on the technological and architectural implementation of the ship's critical systems and assets.

6. Conclusions

The comparative cyber security resilience examination of ECDIS systems implemented on three training ships is presented. The ECDIS systems examined were chosen from different manufacturers and models. In addition, radar systems implemented on two training ships were examined using the same process and the results were compared to the examination results of the shipboard ECDIS systems. The examination process was adjusted to the ECDIS system operating environment and implemented safeguards, and conducted by means of ships' crew interviews and cyber vulnerability scanning of the ECDIS systems. The questionnaire for the ship's crew interview was developed and the cyber vulnerability scanning was performed using the world leading industry software tool. The cyber risks identified were analyzed qualitatively.

The cyber risk analysis revealed eight cyber risks in total. The acceptable low risk level cyber risks determined for all the ECDIS systems were associated with the crew training and awareness, unauthorized access controls, the development of cyber security dedicated policies and procedures, and continuous evaluation and improvement. The results were attributed to the fact that the ships are of the same class and therefore the same ECDIS systems' operating environment and implemented safeguards. The cyber risk raised due to the possible Internet connection establishment was assigned with the medium risk level and is associated to the ECDIS system of the training ship *Kraljica mora*, mainly due to usage of the ECDIS software underlying operating system that is not supported by its manufacturer for a long time. Three high cyber risks were also associated to the ECDIS system of the training ship *Kraljica mora* and are related to the maintenance of the ECDIS software underlying operating system (unsupported and not securely set up operating system) and third-party software components (vulnerable and not supported versions of the third-party software). The same cyber risks (high and medium level risks for the training ship *Kraljica mora*) are assigned with acceptable low level for the highly cyber secured ECDIS system of the training ship *Kapitan Gregorio Oca* and the hardware limited ECDIS system of the training ship *AIDA IV*.

The equal cyber security resilience examination process was conducted on the radar systems of the two training ships. The comparison of cyber risk analysis showed that practically the same cyber risks threaten the radar and ECDIS systems. The results obtained imply that different critical systems and assets of a ship (in this case, ECDIS and radar system), which are of the same manufacturer, are most probably affected by identical cyber security risks. In addition, the results confirm that a high level of cyber security is based on the technological and architectural implementation of the ship's critical systems and assets.

The results obtained suggest that potential sources of cyber risks of the shipboard ECDIS systems are mainly from the ECDIS software underlying operating system maintenance, but also from the maintenance of ECDIS software's third-party components. The results suggest that even if the ECDIS software and underlying operating system are maintained, the system could be vulnerable due to weaknesses in the ECDIS software's third-party components. In addition, the necessity of conducting the cyber vulnerability scanning for the determination of cyber risks is shown, especially for complex ECDIS systems. The results obtained imply that the cyber security level of different ship critical systems and assets), which are of the same manufacturer, is most probably identical, depending more on the technological and architectural implementation. The obtained results contribute to the knowledge of shipboard ECDIS systems cyber security and are applicable to any shipboard critical system and asset.

References

- [1] Brčić D., Žuškin S., Valčić V., Rudan, I., "ECDIS transitional period completion: analyses, observations and findings", *WMU Journal of Maritime Affairs*, Vol. 18, (2019), pp. 359-377.
- [2] International Maritime Organization, "ECDIS – Guidance for Good Practice, Resolution", MSC.1/Circ.1503/ Rev.1., (2017).
- [3] Svilicic B., Kamahara J., Rooks M., Yano Y., "Maritime Cyber Risk Management: An Experimental Ship Assessment", *Journal of Navigation*, Vol. 72, (2019), pp. 1108-1120.
- [4] Svilicic B., Kristić M., Brčić D., Žuškin S., "Paperless Ship Navigation: Cyber Security Weaknesses", *Journal of transportation security*, Vol. 13, (2020), pp. 1938-7741.
- [5] Svilicic B., Brčić D., Žuškin S., Kalebić D., "Raising Awareness on Cyber Security of ECDIS", *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 13, (2019), pp. 231-236.
- [6] Svilicic B., Rudan I., Frančić V., Doričić M., "Shipboard ECDIS Cyber Security: Third-Party Component Threats", *Scientific Journal of Maritime Research Pomorstvo*, Vol. 33, (2020), pp. 1332- 0718.
- [7] Svilicic B., Kamahara J., Celic J., Bolmsten J., "Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security", *WMU Journal of Maritime Affairs*, Vol. 18, (2019), pp. 509-520.
- [8] Kaleem Awan M.S., Al Ghamdi M.A., "Understanding the vulnerabilities in digital components of an integrated bridge system (IBS)", *Journal of Maritime Science and Engineering*, Vol. 7, (2019), pp. 350–370.
- [9] Lee E., Mokashi A.J., Moon S.Y., Kim G., "The maturity of Automatic Identification Systems (AIS) and its implications for innovation", *Journal of Maritime Science and Engineering*, Vol. 7, (2019) pp. 287–304.
- [10] Hareide O.S., Jøsok Ø., Lund M.S, Ostnes R., Helkala, K., "Enhancing Navigator Competence by Demonstrating Maritime Cyber Security", *Journal of Navigation*, Vol. 71, (2018), pp. 1025-1039.
- [11] Lee Y.C., Park S.K., Lee W.K., Kang J., "Improving cyber security awareness in maritime transport: A way forward", *Journal of the Korean Society of Marine Engineering*, Vol. 41, (2017), pp. 738-745.
- [12] Tam K., Jones K., "MaCRA: a model-based framework for maritime cyber-risk assessment", *WMU Journal of Maritime Affairs*, Vol. 18, (2019), pp. 129-163.
- [13] Kessler G.C., Craiger J.P., Haass J.C., "A taxonomy framework for maritime cybersecurity: a demonstration using the automatic identification system", *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 12, (2018), pp. 429–437.
- [14] International Maritime Organization, "Guidelines on maritime cyber risk management", MSC-FAL.1/ Circ.3, (2017).
- [15] International Maritime Organization, "Maritime Cyber Risk Management in Safety Management Systems", MSC 98/23/Add.1, (2017).
- [16] Brčić D., Žuškin S., "Towards paperless vessels: a Master's perspective", *Pomorski zbornik*, Vol. 55, (2018), pp. 183-199.
- [17] Weintrit A., "Clarification, systematization and general classification of electronic chart systems and electronic navigational charts used in marine navigation. Part 1 - electronic chart systems", *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 12, (2018) pp. 471–482.

- [18] BIMCO, "The guidelines on cyber security onboard ships", (2017).
- [19] DNV-GL "Cyber security resilience management for ships and mobile offshore units in operation", DNVGL-RP-0496, (2016).
- [20] Nessus, "Tenable Products: Nessus Professional", <https://www.tenable.com/products/nessus/nessus-professional>, (2022).
- [21] Microsoft, "Microsoft Security Bulletin MS17-010 – Critical", <https://technet.microsoft.com/library/security/MS17-010>, (2022).
- [22] United States Computer Emergency Readiness Team, "Alert (TA17-181A) Petya Ransomware", <https://www.us-cert.gov/ncas/alerts/TA17-181A>, (2020).
- [23] Swiss Government Computer Emergency Response Team, "Notes About the NotPetya Ransomware" <https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware#>, (2020).
- [24] Microsoft, "Microsoft: Search product lifecycle", <https://support.microsoft.com/en-us/lifecycle>, (2022).
- [25] Apache, "The Apache Software Foundation", <https://www.apache.org/foundation/>, (2022).
- [26] Python, "The Python Community", <https://www.python.org>, (2022).

Appendix

Appendix: Deliverable (Conference Abstract)

Abstract presented at the *International Association of Maritime Universities Conference 2021* (Alexandria, Egypt) and published in the *International Association of Maritime Universities Conference Book 2021* (ISSN: 2706-6738), pages 80-81.

Shipboard ECDIS: Cyber Security Challenges

Boris Svilicic^a, Sam Pecota^b, Jeric Bacasdoon^c, Ahmed K. Tawfik^d

^a Faculty of Maritime Studies University of Rijeka, Studentska ulica 2, HR-51000, Rijeka, Croatia

^b California State University Maritime Academy, USA

^c Maritime Academy of Asia and the Pacific, Philippines

^d Arab Academy for Science, Technology and Maritime Transport, Egypt
e-mail: svilicic@pfri.hr

Keywords: navigation safety, ECDIS, maritime cyber security, cyber-physical system

The Electronic Chart Display and Information System (ECDIS) has strongly influenced how ships are navigated. The ECDIS meets the International Maritime Organization (IMO) requirement for the nautical charts carriage and the IMO mandatory ECDIS carriage requirement is currently in force for all SOLAS vessels [1]. The paper charts workload reduction and real-time navigational information provided by the ECDIS have allowed the ship's command to focus on the actual traffic situation, and thus the safety of ship navigation is improved [2]. The ECDIS has been improved for nearly three decades, primarily on the basis of integration and networking, which resulted in development of a complex cyber-physical system.

The IMO has recognised security risks rising from the usage of cyber technologies and published the Guidelines on maritime cyber risk management, which offers general guidelines for safeguarding the ship navigation from cyber threats and risks [3]. In addition, IMO has imposed that cyber security risks are to be adequately implemented in the International Safety Management (ISM) code and the periodical audit of ships for ISM code by 1st January 2021 [4].

In this work, we present an analysis of cyber security challenges in ECDIS system implemented on board of a ship. The analysis is based on experimental cyber security testing of a shipboard ECDIS with a vulnerability scanning software tool [5-7]. The tested ECDIS is implemented on the training ship *Kraljica mora* of the Faculty of Maritime Studies Rijeka, University of Rijeka, Croatia (Figure 1). Technical specification of the ECDIS and details of the experiment will be presented. On the basis of the cyber security testing (Figure 2), cyber security challenges are identified and analyzed regarding the ECDIS working conditions. The cyber security challenges together with possible solving solutions will be presented.

References:

- [1] International Maritime Organization, "ECDIS—Guidance for Good Practice", MSC-FAL.1/Circ.3, 2017.
- [2] D. Brčić, S. Žuškin, S. Valčić, I. Rudan, "ECDIS transitional period completion: analyses, observations and findings", *WMU Journal of Maritime Affairs*, vol. 18, pp. 359-377, 2019.
- [3] International Maritime Organization, "Guidelines on Maritime Cyber Risk Management", MSC-FAL.1/Circ.3, 2017.
- [4] International Maritime Organization, "Maritime Cyber Risk Management in Safety Management Systems", MSC.428(98), 2017.
- [5] B. Svilicic, J. Kamahara, M. Rooks, Y. Yano, "Maritime Cyber Risk Management: An Experimental Ship Assessment", *Journal of Navigation*, vol. 72, pp. 1108-1120, 2019.
- [6] B. Svilicic, I. Rudan, V. Frančić, D. Mohović, "Towards a Cyber Secure Shipboard Radar", *Journal of Navigation*, vol. 73, pp. 547-558, 2020.
- [7] B. Svilicic, I. Rudan, A. Jugović, D. Zec, "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System", *Journal of Maritime Science and Engineering*, vol. 7, pp. 364-375, 2019.



Figure 1. The training ship *Kraljica mora*.

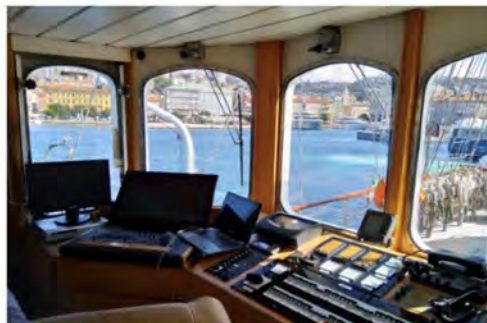



Figure 2. Cyber security testing of the shipboard ECDIS.

Acknowledgements

The materials and data in this publication have been obtained through the support of the International Association of Maritime Universities (IAMU) and The Nippon Foundation in Japan.

Appendix: Deliverable (Conference Paper)

Paper accepted for presentation at the *International Association of Maritime Universities Conference 2022* (Batumi, Georgia) and publication in the Proceedings of the *International Association of Maritime Universities Conference 2022* (ISSN: 2706-6754).



The 22nd IAMUC

Proceedings of the
International Association of Maritime Universities Conference



Batumi, 21-22 Oct 2022

Towards a Cyber Secure Shipboard ECDIS

Boris Svilicic^{1,*}, Jeric Bacasdoon², Ahmed K. Tawfik³ and Sam Pecota⁴

¹ Faculty of Maritime Studies University of Rijeka, Croatia
² Maritime Academy of Asia and the Pacific, Philippines
³ Arab Academy for Science, Technology and Maritime Transport, Egypt
⁴ California State University Maritime Academy, USA

^{*} Corresponding author: boris.svilicic@pfri.uniri.hr; Tel.: +385-98-529-550.

Abstract: A comparative study of cyber security vulnerabilities in ECDIS systems that are implemented on board of three training ships is presented. The cyber security vulnerabilities have been detected by performing computational testing of the ECDIS systems using a widely used vulnerability scanning software tool. The tested ECDIS systems were chosen from different manufacturers and different underlying operating systems. The results obtained suggest that the selection of the underlying operating system plays an important role in securing the ECDIS systems. In addition, the results point that the cyber security of ECDIS systems could be significantly violated by exploitation of vulnerabilities in the third-party components of ECDIS software.


Keywords: navigation safety, ECDIS, maritime cyber security, cyber-physical system

1. Introduction

The Electronic Chart Display and Information System (ECDIS) has become a major aid for safe navigation of ships. The ECDIS brings the combination of the paper charts workload reduction and real-time navigational information provision, so the ship's navigational officers can focus on the actual traffic situation, improving the safety of ship navigation (Brčić 2019). The International Maritime Organization (IMO) has setup the requirement for the mandatory ECDIS carriage requirement for all SOLAS vessels (IMO 2017a). With the improvement for nearly three decades, mainly by the integration and networking, ECDIS has developed in a complex cyber-physical system.

The security risks rising from the application of cyber technologies in ECDIS systems has been recognized by the IMO, and therefore the general cyber security guidelines for safeguarding the ship navigation are recently published (IMO 2017b). In addition, the cyber security risks must be adequately implemented in the International Safety Management (ISM) code and periodically audited for ISM code from the beginning of the year 2021 (IMO 2017c).

In this work, we present a comparative study of cyber security threats in ECDIS systems that are implemented on board of three ships, *Kraljica mora*, *Aida IV*, and *Kapitan Gregorio Oca* (Figure 1). In order to perform the comparative study, a computational vulnerability scanning of the ECDIS systems was conducted



(a) (b) (c)

Figure 1. The training ships: (a) *Kraljica mora*, (b) *AIDA IV*, and (c) *Kapitan Gregorio Oca*.

www.iamu-edu.org

using an industry leading software tool (Svilicic 2020, Svilicic 2019a, Svilicic 2019b, Svilicic 2019c) and by applying the same scanning model. The detected cyber security vulnerabilities are studied and solutions for the risks mitigation are discussed.

2. The Shipboard ECDIS systems

The cyber security vulnerabilities in the current deployment of three ECDIS systems have been studied. The ECDIS systems are implemented on the training ships: (i) *Kraljica mora* (IMO: 9569358), provided by the University of Rijeka Faculty of Maritime Studies (Croatia), (ii) *Aida IV* (IMO: 9018775) provided by the Arab Academy for Science, Technology and Maritime Transport (Egypt), and (iii) *Kapitan Gregorio Oca* (IMO: 9859959) provided by the Maritime Academy of Asia and the Pacific (Philippines). The shipboard ECDIS systems are IMO compliant and meets IMO performance standards. The technical specifications of the ECDIS systems are given in Table 1.

Table 1. Technical specification of the tested ECDIS systems.

ECDIS	<i>Kraljica mora</i>	<i>AIDA IV</i>	<i>Kapitan Gregorio Oca</i>
Manufacturer	Wärtsilä Transas	Transas	Furuno
Model	Navi Sailor 4000	Navi Sailor 4000	FMD-3200
Software version	3.02.350	2.00.012	2450074-03.17
Approval date	2016	2009	2017
Installation date	2019	2010	2020

While the ECDIS system of the training ship *AIDA IV* is implemented in the stand-alone mode, ECDIS systems of the two other ships are internetworked in a local area network together with a sensor switch. Data from the Global Positioning System (GPS) and Automatic Identification System (AIS) are gathered via serial interfaces. The sensor switch is used for gathering data from radar, gyrocompass, Navtex and other sensors.

3. Cyber Security Testing

The testing of the ECDIS systems was performed by computational scanning for cyber vulnerabilities using a software tool that is most widely used in the industry. The testing software tool used is Nessus Professional, version 8.15.2. (Nessus 2022). The ECDIS systems were tested individually, by connecting a laptop with preinstalled testing software tool to the ships' local area network (Fig. 3).



Figure 2. Cyber security testing of the ECDIS systems implemented on the training ships:
(a) *Kraljica mora*, (b) *AIDA IV*, and (c) *Kapitan Gregorio Oca*.

The main objective of the testing is identification of all cyber security vulnerabilities that are known not only to the software developers, but also to potential attackers. The used software tool provides comprehensive database of all known cyber security vulnerabilities, allowing to understand the vulnerability level of the tested ECDIS systems. As the ships are engaged in regular voyage, the tests were conducted in a passive manner, with no disturbance of the ECDIS systems operation, while the ships were docked in a port. The same scanning model was applied for the testing all the ECDIS systems.

4. Results and Discussion

The summary report of the cyber vulnerabilities scanning of the ships *Kraljica mora* and *Kapitan Gregorio Oca* are shown on Figure 3. The results obtained indicate high security level of ECDIS systems implemented on the ships *Kapitan Gregorio Oca* and *AIDA IV*, while the results show significant vulnerabilities detected on the ECDIS system of the ship *Kraljica mora*.

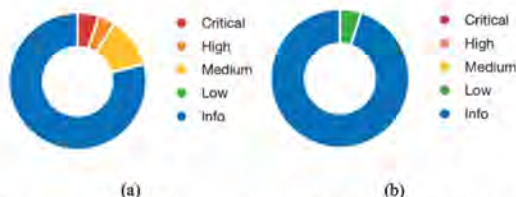


Figure 3. Cyber security vulnerabilities detected: (a) *Kraljica mora*, and (b) *Kapitan Gregorio Oca*.

The ECDIS system on the ship *AIDA IV* was not tested because the ECDIS software (Table 1) is running on the stand-alone workstation with no hardware for internetworking implemented. However, the ECDIS software is running on the Microsoft Windows XP operating system, which is unsupported by the manufacturer from the year 2014 (Microsoft 2022). The unsupported operating system implies that no new cyber security patches have been released by the manufacturer for about 8 years now. While the ECDIS software is running on the highly vulnerable operating system, the stand-alone implementation with no internetworking ability, provides high level of the cyber security.

The results detected on the ship *Kraljica mora* (Figure 3a) indicate 3 critical, 2 high and 7 medium cyber vulnerabilities. Exploitation of vulnerabilities with the critical severity is usually straightforward, meaning that attackers do not need any special knowledge about target systems, and likely results in root-level compromise of target systems. The most critical vulnerability of the ECDIS system is that the ECDIS software is running on the operating system that is unsupported by its manufacturer. In particular, Microsoft Windows 7 Professional operating system has been used, which is not supported by the manufacturer from January 2020 (Microsoft 2022). The remaining critical and high severity cyber security vulnerabilities are related to the vulnerable web server and unsupported version of a system software. In particular, Apache web server version 2.4.49 (Apache 2022) and Python interpreter version 2.7.15 (Python 2022) are running on the ECDIS system. For the both critical vulnerabilities, the support is based on help from members of the communities (Apache and Python communities) who work as enthusiastic volunteers. In addition, the results point out that the significant cyber vulnerabilities exist not only in the software components developed by the manufacturers of the ECDIS software (Wärtsilä Transas) or the underlying operating system (Microsoft), but also in the third-party software components (Apache web server and Python interpreter).

The ECDIS system implemented on the training ship *Kapitan Gregorio Oca* has been shown with low level of cyber security vulnerabilities, having very little impact on the ECDIS operation (Figure 3b). The only vulnerability detected, classified as the low-level, is related to an X11 server running on the ECDIS system. The basis for the excellent cyber security results is in usage of a Linux operating system, which makes the ECDIS system less susceptible to potential cyber security threats. In addition, adequate setup and maintenance of the operating system enhance the level of the ECDIS system cyber security.

5. Conclusions

The cyber security vulnerabilities in the deployment of three shipboard ECDIS systems have been presented. The cyber security testing of the ECDIS system have been done using the industry leading vulnerability scanner. The results obtained show that the highest cyber security level is achieved on the ECDIS system that is based on the Linux operating system, suggesting that the selection of the underlying operating system can play important role to mitigate cyber security risks. In addition, the results point out that the cyber security of ECDIS system could be significantly threaten not only by exploiting vulnerabilities in the

unmaintained ECDIS software and the underlying operating systems, but also by exploiting vulnerabilities in the third-party components of ECDIS software.

Acknowledgements

The materials and data in this publication have been obtained through the support of the International Association of Maritime Universities (IAMU) and The Nippon Foundation in Japan.

References

- Apache (2019) The Apache Software Foundation. <https://www.apache.org/foundation/>. Accessed 25 May 2022.
- Brčić D, Žuškin S, Valčić S, Rudan I (2019) ECDIS transitional period completion: analyses, observations and findings. *WMU J Marit Affairs* 18: 359-377. <https://doi.org/10.1007/s13437-019-00173-z>.
- International Maritime Organization (IMO) (2017a) ECDIS—Guidance for Good Practice. https://iho.int/uploads/user/About_IHO/International_Organisations/ECDIS-ENC/English/MSC.1-Circ.1503-Rev.1 - Ecdis - Guidance For Good Practice.pdf Accessed 25 May 2022.
- International Maritime Organization (IMO) (2017b) Guidelines on maritime cyber risk management. <https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf>. Accessed 25 May 2022
- International Maritime Organization (IMO) (2017c) Maritime cyber risk management in safety management systems. [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf). Accessed 25 May 2022
- Microsoft (2022) Microsoft Lifecycle Policy. <https://docs.microsoft.com/en-us/lifecycle>. Accessed 25 May 2022.
- Nessus (2022) Tenable products: Nessus Professional version 8. <https://www.tenable.com/products/nessus/nessus-professional>. Accessed 25 May 2022.
- Python (2022) The Python Community. <https://www.python.org>. Accessed 25 May 2022.
- Svilicic B, Kamahara J, Rooks M, Yano Y (2019a) Maritime cyber risk management: an experimental ship assessment. *J Navig* 72:1108–1120. <https://doi.org/10.1017/S0373463318001157>.
- Svilicic B, Kamahara J, Celic J, Bolmsten J (2019b) Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU J Marit Affairs* 18:509–520. <https://doi.org/10.1007/s13437-019-00183-x>.
- Svilicic B, Rudan I, Jugović A, Zec D (2019c) A study on cyber security threats in a shipboard integrated navigational system. *J Mar Sci Eng* 7:364–375. <https://doi.org/10.3390/jmse7100364>.
- Svilicic B, Rudan I, Frančić V, Mohović Đ (2020) Towards a cyber secure shipboard radar. *J Navig*. 73:547-558. <https://doi.org/10.1017/S0373463319000808>.



International Association of Maritime Universities

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

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

ISBN No. 978-4-907408-39-8