WMU Journal of Maritime Affairs
https://doi.org/10.1007/s13437-019-00183-x

IAMU SECTION ARTICLE

Assessing ship cyber risks: a framework and case study of ECDIS security

Boris Svilicic[1] · Junzo Kamahara[2] · Jasmin Celic[1] · Johan Bolmsten[3]

Received: 7 December 2018 / Accepted: 9 October 2019/Published online: 25 October 2019

Abstract

The growing reliance of the shipping industry on information and communication technologies places a high premium on cyber risk management. The International Maritime Organization has imposed improvement of the approved safety management system of ships by incorporating the cyber risk management no later than the first annual verification of a shipping company's document of compliance following 1 January 2021. In this paper, we present a framework for assessing cyber risks that affect safe operation of ships. The framework relies on an on-board survey to identify existing safeguards, cyber security testing to detect vulnerabilities and threats, and determination of the cyber risk level. The cyber security testing of the ship's critical systems and assets, as the specific part of the framework, is introduced and studied. The cyber security testing method is based on computational vulnerability scanning and penetration testing techniques, which is aligned with the upcoming maritime standard IEC 63154. For a case study, the testing of a shipboard Electronic Chart Display and Information System cyber security was performed using an industry vulnerability scanning tool.

Keywords Maritime cyber risk management · Ship security assessment · Ship cyber critical systems · Cyber risk assessment · Assessment framework · Cyber security testing

1 Introduction

In the maritime transport industry, with the growing reliance on information and communication technologies, there is a compelling necessity to develop mechanisms and measures that allow not only data protection, but also safe ship operations (Tam and Jones

✉ Boris Svilicic
svilicic@pfri.hr

[1] Faculty of Maritime Studies, University of Rijeka, Studentska ulica 2, 51000 Rijeka, Croatia

[2] Graduate School of Maritime Sciences, Kobe University, 5-1-1 Fukaeminami-machi, Higashinada-ku, Kobe, Japan

[3] World Maritime University, Fiskehamnsgatan 1, 211 18, PO Box 500, SE-201 24 Malmö, Sweden

2019; Polatid 2018; Hareide 2018; Shapiro 2018; Botunac and Gržan 2017; Lee 2017; Hassani 2017; Burton 2016; Balduzzi 2014; Svilicic and Kras 2005). The International Maritime Organization (IMO) has recently published the guidelines on high-level recommendations for maritime cyber risk management (IMO 2017). IMO has also imposed to include maritime cyber risk assessment in the implementation of the International Safety Management (ISM) Code safety management system on ships by 1 January 2021 (IMO 2017). In addition, jointly with the International Electrotechnical Commission (IEC), IMO is developing a new maritime standard IEC 63154 with target publication date of April 2021 (IEC 2019). The standard is intended for maritime navigation and radiocommunication equipment and systems, with emphasis on general cyber security requirements, testing methods, and required test results.

In this work, we present a general and comprehensive framework for conducting cyber risk assessment of ships to offer guidance for improving security level of cyber systems on-board ships. The proposed framework provides a method to balance cyber security protection mechanisms and measures by assessing ship critical cyber systems and assets, and is aligned with the upcoming maritime standard IEC 63154. The assessment is based on the combination of existing safeguard controls identification, cyber threats and vulnerabilities computational detection, and risk level determination. While existing safeguards identification relies on an on-board survey method, the cyber threats and vulnerabilities detection is based on the cyber security testing of a ship critical system. For a case study, a shipboard Electronic Chart Display and Information System (ECDIS) was tested using an industry leading vulnerability scanner software tool.

2 Assessment framework

The framework for assessing ship cyber risks represents a complex set of related and interdependent actions that intersect to provide safeguards that are effective and corresponding to challenges presented by ship critical systems specifics, information and communication technologies evolution, and human resource capabilities. Cyber risk assessment relies upon determination of a ship's specific cyber risk factors to be assessed and relations among those factors. Results should provide identification of threats and vulnerabilities in the current deployment of a ship's critical systems and determination of 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 framework relies on guidelines and practices (IMO 2017; NIST 2018; IET 2018; BIMCO 2017; DVN-GL 2016), and is shown on Fig. 1. The framework consists of four main phases: (i) preparation operations including ship critical systems identification, (ii) assessment conduction and cyber risk determination, (iii) results communication activities necessary for cyber security level improvement, and (iv) maintenance activities for ensuring efficiency. Details about the assessment phases are given in the following chapters.

The specific element of the proposed assessment framework, compared with IMO International Ship and Port Facility Security (ISPS) ship security assessment (IMO 2013), and other types of ship assessments (OCIMF VIQ 2019; Ernstsen and Nazir 2018), is conduction of the cyber security testing, which should be based on

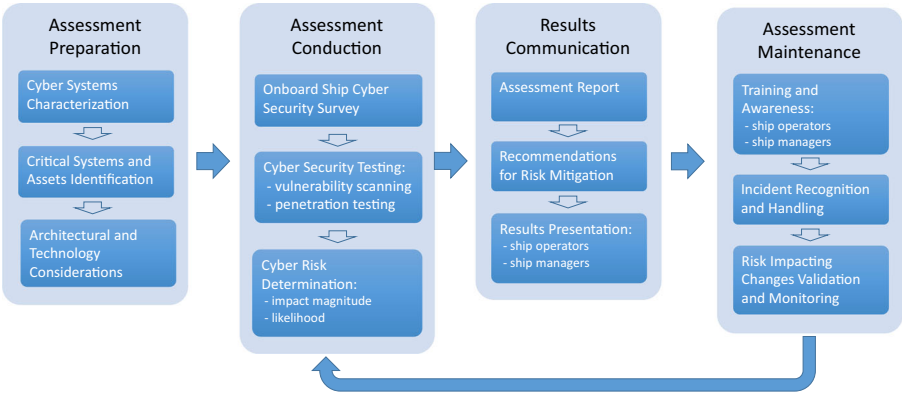

Fig. 1 Proposed framework for cyber risk assessment of ships

computational vulnerability scanning and penetration testing techniques (analyzed in detail in the following chapters). The proposed framework is not only intended for initial assessment, but also for periodic implementation to respond to rapid technological changes in the ship's environment, as well as rapidly changing of the cyber security situation. In addition, because of the rapidly changing nature of the cyber security landscape, the cyber security risk assessment should be undertaken by qualified individuals with expertise in the maritime cyber security and performed more frequently than the ISPS ship security assessment.

3 Assessment preparation

In the assessment process, the first phase to be performed is characterization of the ship's cyber systems by gathering information about the ship's general technical specifications (type, layout of the ship, stowage arrangements plan), identifying critical operations (cargo operations, crew/passenger exchange, bunkering), identifying critical arears and personnel that may be targeted in cyber security incidents, and identifying possible types of motives for cyber security incidents (economical, political, symbolic, terroristic). The outputs from the system characterization are the basis for identification of the ship's cyber risk critical systems and assets (the second step of the assessment phase). Figure 2 shows general overview of ships' critical systems and assets.

As ships are becoming increasingly complex, a comprehensive identification of the ship's critical systems and assets strongly depends on key shipboard operations being performed on a particular ship, such as navigation in high-density traffic area, navigation in restricted visibility, heavy water operation, and people accessing the ship. The last step of this assessment phase is to consider the technological and architectural implications of the identified critical systems and assets on the cyber security, e.g., implemented network connections, operating systems, services, and applications. This step is to be conducted on the basis of the ship's technical specification documentation for each asset of the ship's critical system.

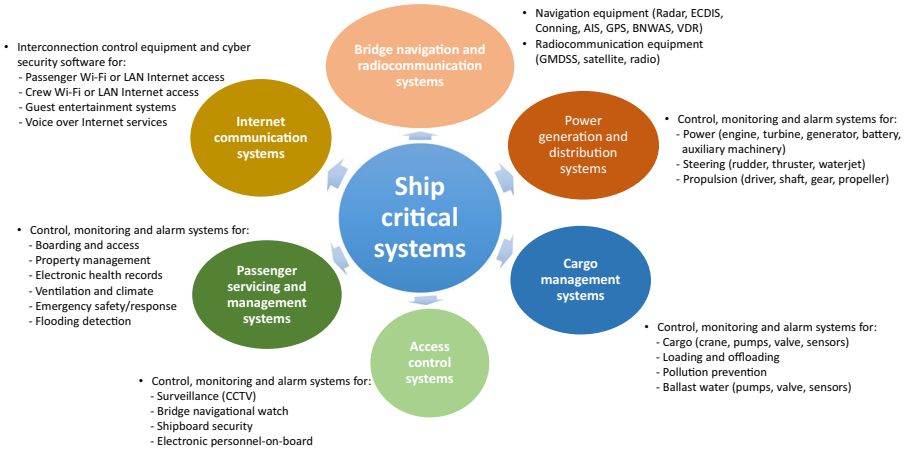

Fig. 2 Ship critical systems and assets

4 On-board survey

The conduction (second) phase of the ship cyber security assessment consists of three main activities: on-board ship cyber security survey, cyber security testing, and determination of the cyber risk level (Fig. 1). The goal of the first activity, the on-board ship cyber security survey, is confirmation that implemented safeguard mechanisms and measures are in place, and identification of omitted and/or inadequate safeguard mechanisms and measures. Collection of the relevant information is to be conducted by interviewing the ship crew with a questionnaire developed on the basis of the identified ship's critical systems and assets. Results of the evaluation of the current safeguard mechanisms and measures implemented should provide identification of potential cyber threats and vulnerabilities to the ship's critical systems and assets. An example of a questionnaire for conducting the survey by interviewing the ship's crew is given in Table 1. While the given table represents an overview of common cyber threats and vulnerabilities related to the ship critical systems/assets, a practical form for conducting the survey should be extended with columns regarding existence of safeguard measures and mechanisms, corrective actions required, and cyber risk estimation (impact magnitude and likelihood).

5 Cyber security testing

Compared with the ISPS ship security assessment and other types of ship assessments (IMO 2013; OCIMF VIQ 2019; Ernstsen and Nazir 2018), the most specific element of the cyber security assessment is conduction of the cyber security testing based on computational vulnerability scanning and penetration testing techniques. The vulnerability scanning is a process of reviewing critical systems and assets to locate and identify known weaknesses. As a step beyond, penetration testing is a systematic employment of legal and authorized attempts to exploit the target system/asset in order to prove that a cyber risk exists. Therefore, in this work, vulnerability assessment is considered as a phase utilized to

Table 1 Example of the on-board survey

Critical system	Assets	Threats	Vulnerabilities
Bridge navigation and radiocommunication systems	- Radar - ECDIS - Conning - AIS - GPS - VDR - GMDSS	- Internetworking security - Software security - Cyber incident handling procedures - Access controls are in place - Handling of portable devices	- Connection to the Internet is established - Operating system and applications are up to date - Incident detection, analysis, respond - Enforcement of security status of USB media
Power generation and distribution systems	- Control systems - Monitoring systems - Alarm systems	- Physical and logical access controls - Authentication controls - Audit and logs - Procedure for authorized access	- All accesses are provided to authorized personnel only - All control mechanisms are enforced - Security-relevant events are recorded - Log-out obligation is enforced
Cargo management systems	- Control systems - Monitoring systems - Alarm systems	- Remote authentication controls - Physical access for authorized personnel only - Policies and procedures are reviewed periodically - Training before actual use of a program	- Remote authentication by using cryptographic only - All default passwords have been changed - Incident detection, analysis and response - Physical and environmental protection
Access control systems	- Control systems - Monitoring systems - Alarm systems	- Remote authentication controls are in place - Physical access is provided to authorized personnel only - Policies and procedures are reviewed periodically - Training before actual use of a program	- Remote authentication by using cryptographic only - All default passwords have been changed - Incident detection, analysis and response - Physical and environmental protection
Passenger servicing and management systems	- Control systems - Monitoring systems - Alarm systems	- Access control policy - Fail-over procedures - Policy for authorized access - Training on security safeguards	- Documentation of authorized users and privileges - Redundant architecture and backup systems - Password sharing and common accounts are forbidden - Incident recognition and handling
Internet communication systems	- Interconnection control equipment - Cyber security software	- Network privacy protection - Latest patches or new releases update - Malicious code protection mechanisms - Latest virus definitions or new releases implementation	- Routers and firewall designs, rules and policies - Central management and reporting - Malicious software infections - Central management and reporting

complete a process of penetration testing. The process for conducting the vulnerability scanning and penetration testing (Fig. 3) starts with gathering all relevant information about the target system. This phase relies on the data collected by the survey, which should be enhanced with technical documentation of the target system. The second phase of the process begins by breaking the model preparation for effective scanning and testing into three distinct steps: (i) determining turned-on and communicable target systems, (ii) identifying active ports and services on the target system, and (iii) obtaining appropriate credential to gain access to the targeted system.

The computational vulnerability scanning and penetration testing (Fig. 3, the third and fourth phases) in information systems generally is mainly conducted using commercial tools. Table 2 shows a list of today's mostly used software tools together with a type of a tool (some of the tools allow the both functionalities), license (commercial proprietary and free general public license, GPL), and supporting operating system.

The main advantage of this tool usage is the ability to scan a large number of systems for common vulnerabilities and exposures. However, the process is limited to only detecting vulnerabilities and exposures for which the vendor of the tool used has released plugins. In addition, as the tool vendor has no knowledge of a ship critical systems and assets specifics, the results could incorrectly reflect the real risk.

5.1 Experimental case study

As an experiment for the case study, we had performed vulnerability scanning of a shipboard ECDIS. ECDIS is a critical ship operational technology asset that relies on the information technology, i.e., it is basically a software package installed on a conventional computer with a conventional operating system pre-installed. The vulnerability scanning of the Transas Navi-Sailor 4000 ECDIS was performed (Transas 2018). The tested ECDIS is the type approved and is implemented recently on-board

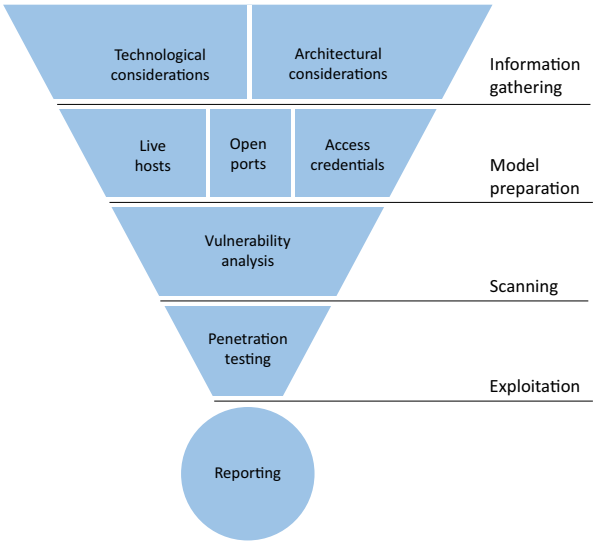

Fig. 3 Process for conducting vulnerability scanning and penetration testing

Table 2 Vulnerability scanner (VS) and penetration (PT) test software tools

Name	Type	License	Operating system
Nessus	VS & PT	Proprietary	Cross-platform
Kali	VS & PT	GPL	Linux
ImmuniWeb	VS & PT	Proprietary	MS Windows
Netsparker	VS & PT	Proprietary	MS Windows
Acunetix	VS	Proprietary	Cross-platform
Nexpose	VS & PT	GPL	Cross-platform
Core Impact	VS & PT	Proprietary	MS Windows
OpenVAS	VS	GPL	Linux
Retina	VS	GPL	MS Windows

of a ship. Data from ECDIS mandatory sensors (GPS, gyrocompass and speed log) and additional sensors (AIS, radar data, and NAVTEX) are gathered directly via serial interfaces. The electronic navigational charts are updated with a USB storage device provided by the manufacturer. The ECDIS specification is given in Table 3.

The vulnerability scan was performed using the most widely deployed solution for application vulnerability detection, Nessus Professional version 8.0.1 (Cybersecurity 2019; Nessus 2018). The ECDIS was tested by connecting a laptop with the vulnerability scanner via an Ethernet cross cable. Even if the vulnerability scanning is a passive process, the testing was conducted while the ship was docked in a port. The testing setup is shown on Fig. 4.

The scan resulted in 9 risky vulnerabilities detected and 35 information identified. The vulnerability scan summary report is shown on Fig. 5.

The vulnerabilities detected together with descriptions are given in Table 4. The detected high severity vulnerabilities are related to a web server running on the ECDIS

Table 3 The shipboard ECDIS specification

ECDIS	Manufacturer	Wärtsilä Transas
	Model	Navi Sailor 4000
	Software version	3.00.340
	USCG approval	165.123/33/0
	Approval date	July 2016
	Installation date	March 2019
Charts	IHO ENC	IHO S-57
	IHO RNC	IHO S-61
	IHO chart content	IHO S-52
	IHO data protection	IHO S-63
Interfaces	Serial NMEA	IEC61162-1
	Serial high speed	IEC61162-2
	Network	IEC61162-450
	Chart update	USB

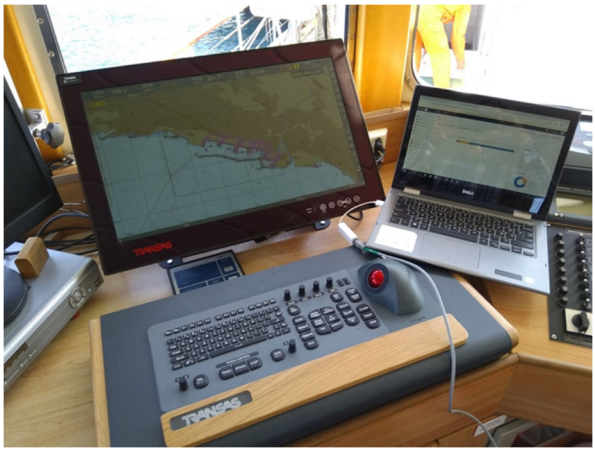

Fig. 4 Testing setup for the vulnerability scanning of the shipboard ECDIS

(Table 4, vulnerabilities 1 and 2). The version of the Apache web server is 2.2, which is obsolete by its provider since December 2017 (Apache 2019). For the obsolete software, no support is given by the provider, allowing an attacker to exploit newly discovered and well-known vulnerabilities using widely available tutorials. The recommended solution by the provider for the detected vulnerabilities is an upgrade to the currently supported version of the web server. However, it is worth noting that web server features are not necessary for the regulated ECDIS software functionality.

Most of the seven medium severity vulnerabilities detected are also related to the web server running on the ECDIS (Table 4, vulnerabilities 3–9). One of the medium severity vulnerabilities detected is related to Server Message Block (SMB) version 1. The SMB server, which is a standard component of Microsoft Windows operating systems, provides the file/printer sharing service. While the active service is updated with the latest security patches released by the provider (Microsoft), the provider's recommendation is discontinuation of SMB version 1 usage due to lack of security features implemented (Microsoft 2018). As in the case of the web server, the file/printer sharing service is not necessary for the ECDIS software functionality, especially in the case of ECDIS operation in the stand-alone configuration. The key information obtained with the vulnerability scanning is that the ECDIS software is running on Microsoft Windows 7 Professional (Service Pack 1) operating system. The provider of the underlying operating system will end the support for this version of operating system before the end of the current 2019 year (Microsoft 2019). It is very important to point out that the upgrades of the obsolete web server and, in the close future, the underlying operating system could significantly impact the ECDIS software functionality and therefore should be only conducted by the ECDIS manufacturer authorized personnel.

Fig. 5 Vulnerability scan summary report

Table 4 The shipboard ECDIS cyber vulnerabilities detected

	Service	Vulnerability description	Severity
1–2	Apache web server	The web server running on the ECDIS is obsolete and no longer maintained by its provider.	High
		The version of the web server running on the ECDIS is affected by multiple vulnerabilities. An attacker could cause a denial of service condition, gain unauthorized access or cause the ECDIS to crash.	
3–9	File/printer sharing	Signing is not required on the ECDIS's Server Message Block (SMB) service version 1. An unauthenticated, remote attacker can conduct man-in-the-middle attacks against the ECDIS.	Medium
	Apache web server	The version of the web server running on the ECDIS is affected by multiple vulnerabilities. An attacker could cause a denial of service condition, execute code, obtain sensitive information, execute cross-site scripting attacks or cause the ECDIS to crash.	
1–35	Underlying operating system	The ECDIS is running Microsoft Windows 7 Professional version of the underlying operating system.	Info
		A file/print sharing service based on Server Message Block version 1 protocol is running on the ECDIS.	
		Identification of services running on the ECDIS is possible.	

6 Cyber risk determination

On the basis of the results of the on-board survey and cyber security testing, the cyber risk analysis is to be performed to identify and categorize cyber threats to which the ship is exposed. The qualitative risk analysis is performed by evaluating the impact magnitude and likelihood of various threats determined that could exploit vulnerabilities to harm cyber security of critical systems and assets. The method provides a relatively simple, but satisfactory basis for the cyber risk analysis. The threat likelihood is a rating of the probability that a vulnerability is exploited. The likelihood levels are given as low, medium, and high with given values of 0.1, 0.5, and 1, respectively (Fig. 6). The impact refers to the magnitude of a harm resulting from successful exploitation of a vulnerability. The impact magnitude rates are high, medium, and low with given values of 100, 50, and 10, respectively.

The cyber risk level is to be calculated by multiplying the threat likelihood ratings with the impact magnitude of the vulnerability exploited. The given result indicates qualitative risk level: (i) critical-risk level requiring immediate action, (ii) high-risk level requiring remediation implementation plan, (iii) medium-risk level which may be acceptable over the short period of time, and (iv) acceptable low-risk level.

7 Results communication and assessment maintenance

The final steps in the cyber risk assessment process are the results communication and assessment maintenance. The assessment results communication phase produces assessment reports that describe cyber threats and vulnerabilities, qualitative risk level determined, and recommendations for implementation of safeguard controls to mitigate

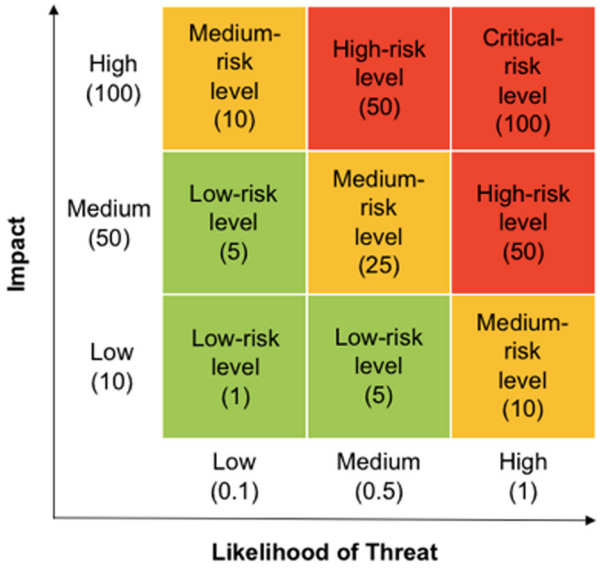

Fig. 6 Example of the risk-level matrix for qualitative risk analysis of cyber threats

the cyber risks. The report is to ensure that each recommendation is addressed with specific, realistic, and tangible actions. The recommendations should contain information to support appropriate decisions on ship policies, procedures, operational impact, and feasibility. Because a cyber risk can never be completely eliminated, recommendations for the risk mitigation must be acceptable by a cost–benefit analysis, resulting in a least-cost solution with minimal adverse impact on the ship's critical systems and assets. The assessment report is to be presented to the ship's managers and operators to improve the cyber security level.

The awareness and training of the whole ship's crew have a significant impact on detecting cyber security incidents and preventing cyber security compromises in general, and therefore should be considered as a part of the assessment maintenance phase. The whole ship's crew has the obligation to be aware of their responsibilities in protecting the critical systems and assets from compromise. In addition, the ship's crew training is also a tool that can increase ship's crew awareness and capabilities in recognition and handling of cyber security incidents. Incident prioritization is very important for successful response process and is conducted on the basis of the determined risk-level matrix (Fig. 6). During the incident handling, communication with external parties is required (vendors, law enforcement, media), so communication guidelines are predetermined to share only appropriate information with the right parties.

Once the cyber security risk assessment of the ship is completed and recommendations for the risk mitigation are initiated, the achieved risk impacting changes are to be validated and monitored. The validation and monitoring processes basically include the activities covered with the assessment conduction phase (the on-board survey, cyber security testing, and risk determination) resulting in updated recommendations for the risk mitigation. Therefore, the cyber security management requires continuous commitment, evaluation, and improvement of the safeguard controls to mitigate the cyber risks.

8 Conclusions

The general and comprehensive framework for assessing cyber risks of ships is presented. The framework consists of four main processes: the preparation, conduction, results communication, and maintenance. The framework relies on the on-board survey to identify existing safeguards, specific cyber security testing to detect vulnerabilities and threats, and the following determination of the cyber risk levels. The cyber security testing method, which is based on the vulnerability scanning and penetration testing techniques, is studied. For the case study, the cyber security testing of the shipboard Wärtsilä NaviSailor 4000 ECDIS is presented. The cyber security testing results indicate that the ECDIS is affected by a vulnerable version of services running on the underlying operating system, which could result in the destruction of the ECDIS functionality.

The obtained test results point out the usefulness of the cyber security testing and importance of its conduction as a part of the ship cyber risk assessment. The presented cyber security testing method together with the obtained results supports the development of the upcoming related maritime standard, IEC 63154. The proposed framework is general and provides the foundation for cyber security assessment of all types of ships.

Funding information The research was financially supported by the University of Rijeka under the research project Cyber Security of Maritime ICT-Based Systems (grant number: uniri-tehnic-18-68).

References

Balduzzi M, Pasta A, Wilhoit K (2014) A security evaluation of AIS automated identification system. Proceedings of the 30th Annual Computer Security Applications Conference, pp 436-445, New Orleans, USA. https://doi.org/10.1145/2664243.2664257

Baltic and International Maritime Council (BIMCO) (2017) The guidelines on cyber security on-board ships. http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-on-board-ships.pdf?sfvrsn=16. Accessed 25 November 2018

Botunac I, Gržan M (2017) Analysis of software threats to the automatic identification system. Brodogradnja 68:97–105. https://doi.org/10.21278/brod68106

Burton J (2016) Cyber attacks and maritime situational awareness: evidence from Japan and Taiwan. Proceedings of the 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, London, UK. https://doi.org/10.1109/CyberSA.2016.7503295

Cybersecurity Insiders (2019) Application security report. https://www.cybersecurity-insiders.com/portfolio/application-security-report. Accessed 1 June 2019

DNV-GL (2016) Cyber security resilience management for ships and mobile offshore units in operation. http://www.gard.no/Content/21865536/DNVGL-RP-0496.pdf. Accessed 25 November 2018

Ernstsen J, Nazir S (2018) Consistency in the development of performance assessment methods in the maritime domain. WMU J Marit Aff 17:71–90. https://doi.org/10.1007/s13437-018-0136-5

Hareide OS, Jøsok Ø, Lund MS, Ostnes R, Helkala K (2018) Enhancing navigator competence by demonstrating maritime cyber security. J Navig 71:1025–1039. https://doi.org/10.1017/S0373463318000164

Hassani V, Crasta N, Pascoal AM (2017) Cyber security issues in navigation systems of marine vessels from a control perspective. Proceedings of the International Conference on Ocean, Offshore Mechanics and Arctic Engineering, Trondheim, Norway. https://doi.org/10.1115/OMAE2017-61771

Institution of Engineering and Technology (IET) (2018) Code of Practice: Cyber Security for Ships. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf. Accessed 25 November 2018

International Electrotechnical Commission (IEC) (2019) IEC 63154 Maritime navigation and radiocommunication equipment and systems - cybersecurity - general requirements, methods of testing

and required test results. https://www.cybersecurity-insiders.com/portfolio/application-security-report. Accessed 1 June 2019
International Maritime Organization (IMO) (2013) International Ship and Port Facility Security (ISPS) code. SOLAS/CONF.5/34
International Maritime Organization (IMO) (2017) Guidelines on maritime cyber risk management. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3 - Guidelines On Maritime Cyber Risk Management (Secretariat).pdf. Accessed 25 November 2018
International Maritime Organization (IMO-MSC) (2017) Maritime cyber risk management in safety management systems. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution MSC.428(98).pdf. Accessed 25 November 2018
Lee YC, Park SK, Lee WK, Kang J (2017) Improving cyber security awareness in maritime transport: a way forward. J Kor Soc Mar Eng 41:738–745. https://doi.org/10.5916/jkosme.2017.41.8.738
Microsoft (2018) Microsoft Security Bulletin MS17-010 - Critical. https://technet.microsoft.com/library/security/MS17-010. Accessed 25 November 2018
Microsoft (2019) Microsoft: search product lifecycle. https://support.microsoft.com/en-us/lifecycle. Accessed 1 June 2019
National Institute of Standards and Technology (NIST) (2018) Framework for improving critical infrastructure cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed 25 November 2018
Nessus (2018) Tenable products: Nessus Professional version 8. https://www.tenable.com/products/nessus/nessus-professional. Accessed 1 June 2019
Oil Companies International Marine Forum (OCIMF) (2019). Ship Inspection Report (SIRE) programme - vessel inspection questionnaires for oil tankers, combination carriers, shuttle tankers, chemical tankers and gas tankers, Seventh Edition (VIQ 7). https://www.ocimf.org/media/127546/SIRE-Vessel-Inspection-Questionnaire-VIQ-Ver-7007.pdf. Accessed 1 June 2019
Polatid N, Pavlidis M, Mouratidis H (2018) Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Comp Stand Interfaces 59:74–82. https://doi.org/10.1016/j.csi.2017.09.006
Shapiro LR, Maras MH, Velotti L, Pickman S, Wei HL, Till R (2018) Trojan horse risks in the maritime transportation systems sector. J Transp Secur 8:1–19. https://doi.org/10.1007/s12198-018-0191-3
Svilicic B, Kras A (2005) Computer systems privacy protection. Pomorstvo Sci J Marit Res 19(1):275–284
Tam K, Jones K (2019) MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J Marit Aff 18:129–163
The Apache Software Foundation (2019) Apache Web Server 2.2 vulnerabilities. https://httpd.apache.org/security/vulnerabilities_22.html. Accessed 1 June 2019
Transas (2018) Navi-Sailor 4000 ECDIS. http://wwwtransascom/products/navigation/ecdis/ECDIS. Accessed 25 November