Journal of
*Marine Science
and Engineering*

Article

A Study on Cyber Security Threats in a Shipboard Integrated Navigational System

Boris Svilicic *, Igor Rudan, Alen Jugović and Damir Zec

Faculty of Maritime Studies, University of Rijeka, Studentska ulica 2, 51000 Rijeka, Croatia; rudan@pfri.hr (I.R.); ajugovic@pfri.hr (A.J.); zec@pfri.hr (D.Z.)

* Correspondence: svilicic@pfri.hr; Tel.: +38-5(0)-9852-9550

Received: 17 September 2019; Accepted: 11 October 2019; Published: 12 October 2019

Abstract: The integrated navigational system (INS) enhances the effectiveness and safety of ship navigation by providing multifunctional display on the basis of integration of at least two navigational functions, the voyage route monitoring with Electronic Chart Display and Information System (ECDIS) and collision avoidance with radar. The INS is essentially a software platform for fusion of data from the major ECDIS and radar systems with sensors for the additional navigation functions of route planning, status and data display, and alert management. This paper presents a study on cyber security resilience examination of a shipboard INS installed on a RoPax ship engaged in international trade. The study was based on a mixed-method approach, combining an interview of the ship's navigational ranks and cyber security testing of the INS using an industry vulnerability scanner. The identified threats were analyzed qualitatively to study the source of cyber risks threatening the INS. The results obtained point out cyber threats related to weaknesses of the INS underlying operating system, suggesting a need for occasional preventive maintenance in addition to the regulatory compliance required.

Keywords: navigation safety; maritime cyber security; integrated navigational system; cyber security testing

1. Introduction

Ship navigation systems have been increasingly relying on cyber technologies to improve the effectiveness and safety of navigation, which has consequently resulted in a need for safeguarding the shipping from cyber threats [1–21]. Therefore, the International Maritime Organization (IMO) has published the guidelines on maritime cyber risk management [22], and has also included cyber security assessment in the International Safety Management (ISM) code to be introduced on ships by the beginning of the year 2021 [23]. In addition, the IMO is preparing in collaboration with the International Electrotechnical Commission (IEC), a new standard for maritime navigation and radio-communication equipment and systems, IEC 63154 "Cybersecurity—General Requirements, Methods of Testing and Required Test Results" [24].

The integrated navigational system (INS) is a composite system, whose purpose is to enhance the effectiveness and safety of ship navigation by providing the multifunctional display on the basis of integration of at least two navigational functions [25]—collision avoidance using a radar sensor and voyage route monitoring using the Electronic Chart Display and Information System (ECDIS) [26]. The INS is essentially a software platform for fusion of data from the major radar and ECDIS systems with sensors for the additional navigation functions of route planning, status and data display, and alert management. The INS is recognized as the one type of equipment by IMO and its functionality is standardized with the performance standards [26].

Recently, cybersecurity assessments of a shipboard ECDIS and a shipboard radar have been presented [1,21]. Although both the ECDIS and radar are IMO type approved and computer-based systems, they are installed as an individual equipment, providing their basic functionality. This paper reports on an examination of the cyber security resilience of a shipboard INS. The examined INS is installed on a roll-on/roll-off ship for freight vehicle transport with passenger accommodation (RoPax), which is engaged in international trade (Figure 1). The examination is based on a mixed-method approach, combining an interview of the ship's navigational ranks to identify implemented safeguards and cybersecurity testing of the INS to detect existing vulnerabilities. The threats identified were qualitatively analyzed to determine the level of cyber risks threatening the INS.

Figure 1. The RoPax ship engaged in international trade.

2. The Integrated Navigational System

The INS examined is the NACOS MULTIPILOT Platinum 2017 of the manufacture Wärtsilä SAM Electronics GmbH. Navigational tools integrated are ECDIS, radar, and conning. The INS is IMO compliant, and the technical specification is given in Table 1.

Table 1. The shipboard integrated navigational system (INS) specification.

INS's Elements	Parameter	Specification
General	Manufacturer	Wärtsilä SAM Electronics GmbH
	Model	NACOS MULTIPILOT Platinum 2017
	Software version	2.1.02.10
	International Maritime Organization (IMO) compliant	Yes
Navigation tools	Electronic Chart Display and Information System (ECDIS)	NACOS ECDISPILOT Platinum
	Radar	NACOS RADARPILOT Platinum
	Conning	NACOS CONNINGPILOT Platinum
Charts	IHO electronic navigation chart (ENC)	IHO S-57 (Edition 3.1.1)
	IHO RNC	IHO S-61 (Edition 1.0)
	IHO chart content	IHO S-52 (Edition 6.1.1)
	IHO data protection	IHO S-63 (Edition 1.2.0)
Interfaces	Serial NMEA	IEC61162-1
	Serial high speed	IEC61162-2
	Network	Ethernet local area network (LAN)
	Chart update	USB
	Remote maintenance	Possible

The examined INS architecture configuration is shown on Figure 2. The integration is based on the sensor adapter, which acts as a central medium for gathering all of the sensors data via serial interfaces that collectively feed to the INS via the high speed local area network (LAN). Sensors integrated include ECDIS mandatory sensors (position DGPS, heading gyrocompass, and speed log), radar x-band scanner and additional sensors, AIS, Navtex, EPFS, echo sounder, and anemometer. The INS software, including ECDIS and radar software, meets IMO performance standards for each of the individual navigation equipment [26–28].

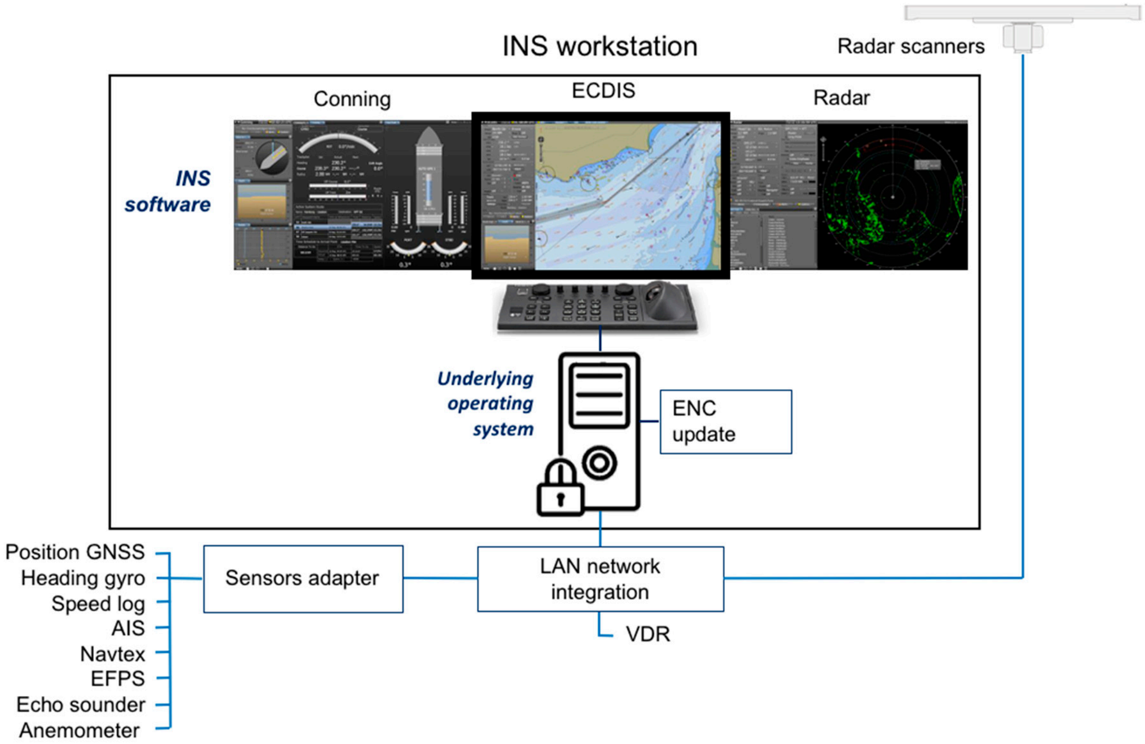

Figure 2. The shipboard INS architecture configuration. LAN: Local area network.

3. Implemented Safeguards

The implemented safeguard measures and mechanisms were identified by interviewing the ship navigational ranks, in particular the ship's master, and first and second officers. During the interview, we focused on three elements of the safeguard regarding the INS's operating environment: the ship's security management system, INS navigation tools, and integration network system. For each of the elements, the identified safeguard measures and mechanisms, together with the description, are given in Table 2.

The results regarding the cyber security management system showed that the cyber security was implemented only partially in the ship's security policies and procedures. However, the policies and procedures were well communicated and reviewed regularly. The ship navigational ranks training was conducted by the INS vendor, and cyber security awareness was at quite a high level. The shipboard INS navigation tools were not connected to the Internet. Strong physical protection policy was in place for unauthorized personnel, and INS hardware interfaces were kept in a locked case. The electronic navigation chart (ENC) update portable storage device was strictly controlled, the device provided by the INS vendor was used, and the ship navigational ranks cyber hygiene was at a high level. A confidentiality agreement with the vendor was in place. The LAN network for integration was also disconnected from the Internet, and strong physical protection and logical authentication policies were in place.

Table 2. Implemented safeguards.

Safeguard Elements	Measures and Mechanisms	Description
Security management system	Policies and procedures	–Developed but cyber security partially dedicated –Well-communicated –Periodic review is in place
	Training and awareness	–Ship navigational ranks training is provided by the integrated navigational system (INS) vendor –Quite a high level of awareness
	Incident handling	–Incident reporting is in place –The procedures are adhered to
INS navigation tools	Internet access	–Internet connection is not established
	Physical protection	–Access controls are in place and enforced –Physical access allowed for authorized personnel –Hardware interfaces are kept in a locked case –Portable storage device handling is controlled
	Confidentiality agreement	–Confidentiality agreement with the vendor is in place
Network for integration	Internet communication	–Internet connection is not established
	Physical protection policy	–Access controls are in place and enforced –Physical access allowed for authorized personnel –Hardware interfaces are kept in a locked case
	Authentication policy	–Authentication controls are in place and enforced –Default passwords are changed

4. Cybersecurity Testing

The cybersecurity testing of the INS was conducted with the world's most widely deployed industry vulnerability scanner, Nessus Professional version 8.0.1 [29]. Vulnerability scanning is a passive method of reviewing the INS to gain comprehensive insight into all vulnerabilities that are already known to the cybersecurity community, attackers, and software developers [6,30]. A laptop with the installed vulnerability scanner was connected directly to the INS with a crossover Ethernet cable. The INS software was running with administrative rights, whereas the remote scanning was conducted without administrative permission. Figure 3 shows the testing setup. During the testing, the ship was docked in a port. The INS was activated to use the ECDIS as the base display layer, together with the radar and conning data (Figure 3).

The scanning report summary is shown on Figure 4. In total, 4 vulnerabilities and 27 pieces of information were detected. According to the severity level, the report showed that 1, 1, and 2 vulnerabilities were assigned under the critical, high, and medium severity, respectively.

Table 3 shows descriptions and possible solutions of the INS cyber-vulnerabilities detected. The critical vulnerability detected (Table 3, vulnerability 1) alerts that a vulnerable version of the Server Message Block (SMB) service is running on the INS. Namely, the underlying operating system of the INS software is Microsoft Windows 7 Professional (Service Pack 1), and the SMB is its default service for file and printer sharing. By following the manufacturer's recommendation, immediate implementation of a security update for the INS underlying operating system is required [31]. This vulnerability is particularly interesting because of one of the most recognized maritime cyber security incidents, the NotPetya attack on Maersk container shipping company [32]. NotPetya is a malicious ransomware program that was rapidly spreading worldwide by utilizing the SMB version 1 vulnerabilities [33]. Although the INS underlying operating system update recommended by the manufacturer is relatively complex to implement in a ship environment, it offers reactive protection, such as is provided with anti-malicious code security programs. A proactive solution would be secure setup of the INS underlying operating system by blocking or disabling the SMB service version 1. However, it is very important to point out that the update of the underlying operating system could significantly impact the INS software functionality [26] and should be only conducted by INS vendor authorized personnel.

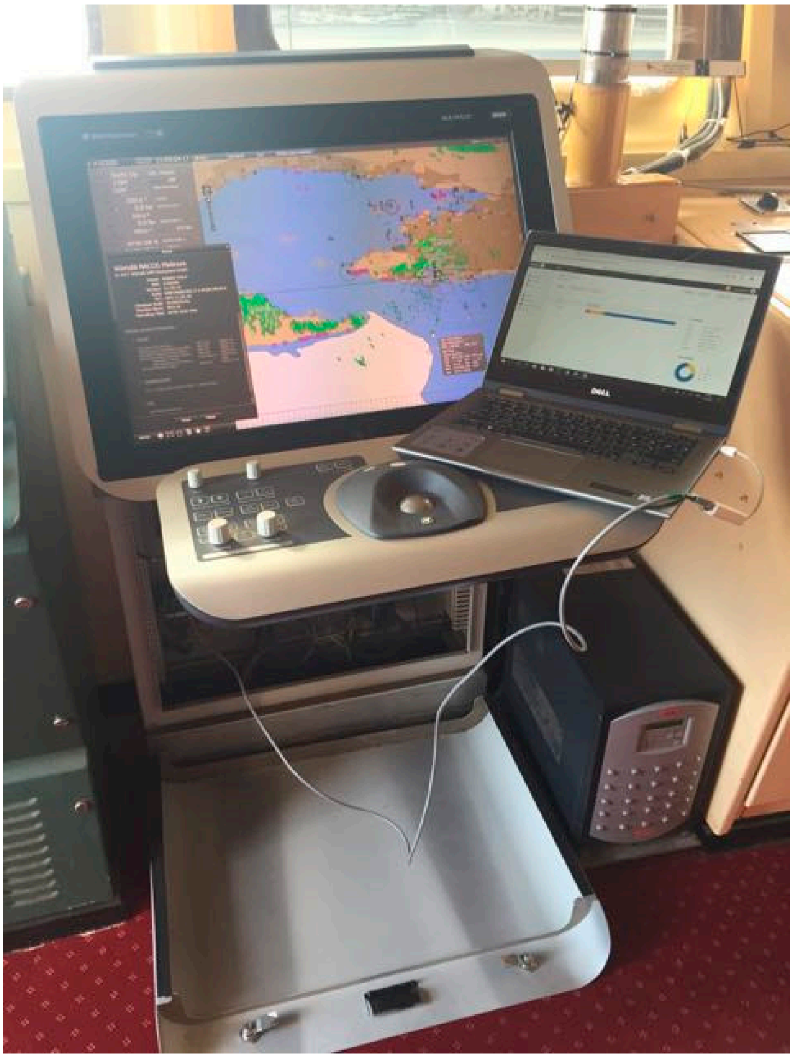

Figure 3. Testing setup for the INS cyber-vulnerability scanning.

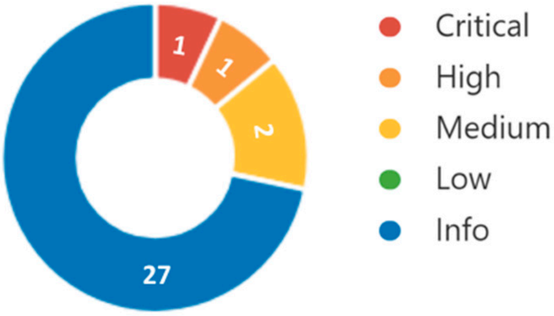

Figure 4. The vulnerability scanning summary report.

The vulnerabilities with high and medium severities detected (Table 3, vulnerabilities 2–4) are related to weaknesses of services running on the INS underlying operating system, allowing possible remote code execution and unauthorized access gaining. As in the case of the critical vulnerability detected, the vulnerable services are not necessary for the INS operational functionality. The solution includes underlying operating system update with a security patch released by the manufacturer and secure setup by disabling or blocking the vulnerable services and forcing strong cryptography. These activities are also to be conducted by the INS vendor authorized personnel.

Table 3. Results of the vulnerability scan.

	Name	Description	Solution	Severity
1.	Server Message Block (SMB) service	The INS is affected by following vulnerabilities: → Remote code execution vulnerabilities exist in the SMB service version 1.0. The vulnerabilities can be exploited by a remote attacker to execute arbitrary code without authentication. → Information disclosure vulnerability exists in the SMB service version 1.0. The vulnerability can be exploited by a remote attacker to disclose sensitive information.	– Update the operating system with a security patch released by the manufacturer. – Operating system secure setup by blocking the service.	Critical
2.	Remote Desktop service	Arbitrary remote code vulnerability exists in the Remote Desktop service running on the INS. The vulnerability can be exploited by a remote attacker to execute arbitrary code.	Update the operating system with a security patch released by the manufacturer.	High
3.	Terminal Service	Remote Desktop Protocol Server (Terminal Service) running on the INS is vulnerable to a man-in-the-middle attack due to low encryption level used. The vulnerability can be exploited by a remote attacker to gain access to the INS.	Operating system secure setup by forcing strong cryptography.	Medium
4.	Remote protocols	Remote Desktop Protocol Server (Terminal Service) running on the INS is vulnerable to a man-in-the-middle attack due to low encryption level used. The vulnerability can be exploited by a remote attacker to get access to the INS.	Operating system secure setup by forcing strong cryptography.	Medium

5. Risk Level Determination

The INS cyber risk determination was conducted on the basis of a qualitative analysis of cyber threats identified by the interview and vulnerability scanning conducted. Whereas the vulnerabilities scan is used to detect all known vulnerabilities existing in the INS, the used vulnerability scanner is a general industry tool, and the results could inaccurately reflect the actual severity of threats due to specifics of the ship environment. Therefore, the scan results were studied in the context of the INS's operating environment and implemented safeguards on the ship. On the basis of the interview and vulnerability scan results, we conducted the identification of cyber threats. Table 4 shows the list of the identified cyber threats together with our estimation of the threats' impact magnitude and likelihood. The impact magnitude represented a damage resulting from a threat execution, and was given with a value from 0 (no impact) to 100 (total impact). The threat likelihood represented a probability that a threat was executed, and the likelihood rate was given with a value from 0 up to 1.

Table 4. The identified INS cyber threats.

	Threat	Description	Impact Magnitude	Likelihood
1.	INS underlying operating system out of date	Allows exploitation of well-known vulnerabilities of the INS underlying operating system	100	0.4
2.	INS underlying operating system insecure setup	Backdoors are open for possible intrusions and performance is reduced	100	0.4
3.	Navigational ranks training	Ship navigational ranks are not able to perform their duties and responsibilities	50	0.2
4.	Navigational ranks awareness	Ship navigational ranks are not able to adhere to policies and procedures	50	0.2
5.	Internet connection establishment	Remote attacker is provided with access to the INS's navigational tools	100	0.1
6.	Unauthorized access	Attacker is provided with physical or logical access to the INS's navigational tools	100	0.1
7.	Cyber security policies and procedures	Ship navigational ranks are not aware of their roles and responsibilities	20	0.5
8.	Continuous assessment and improvement	Lack of ability to respond to rapid technological development	20	0.2

Four of the eight determined cyber threats were assigned with the highest impact magnitude (Table 4, threats 1, 2, 5, 6). The threats were related to the INS underlying operating system being out of date and setup insecurely, as well as establishment of the Internet connection and unauthorized access. The middle impact magnitude was assigned to two threats (Table 4, threats 3 and 4) that were related to the ship training and awareness. The low impact magnitude was assigned to the threats raised from lack of cyber security-dedicated policies and procedures, and continuous assessment and improvement (Table 4, threats 7 and 8). Five of the eight determined cyber threats were assigned with the low likelihood level (Table 4, threats 3–6, 8). The threats assigned with middle likelihood level (Table 4, threats 1, 2, 7) were related to the INS underlying operating system being out of date and having insecure setup, as well as lack of cyber security dedicated policies and procedures. The given values of the impact magnitude and likelihood are discussed with the risk level analysis in the following part of the chapter.

The INS cyber risk levels were calculated by multiplying the impact magnitude value with the likelihood value. The given result represented the qualitative cyber risk level: (i) acceptable low risk (product of the multiplication was lower than 25), (ii) medium risk that is acceptable for a short time (product of the multiplication was between 25 and 50), (iii) high risk demanding a risk mitigation plan (product of the multiplication was between 50 and 75), and (iv) critical risk demanding instant action (product of the multiplication was higher than 75). Figure 5 shows the cyber risk-level radar graph of the results obtained with the qualitative risk analysis.

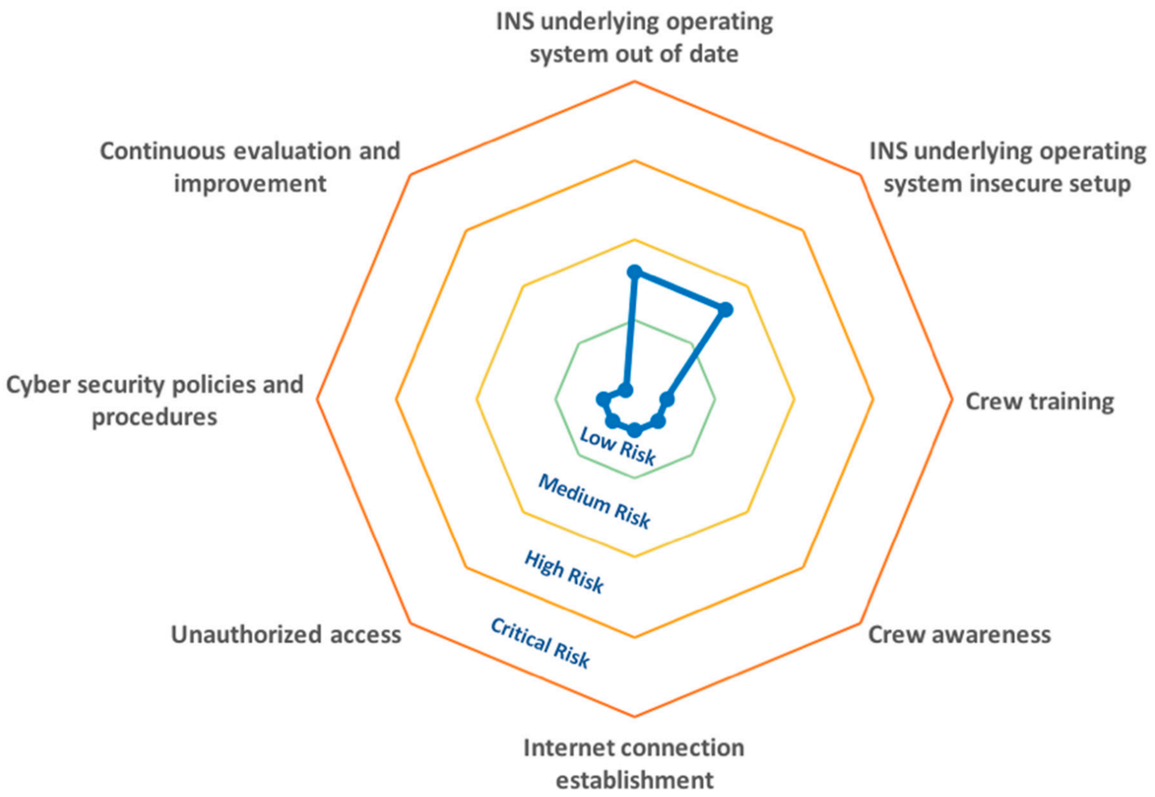

Figure 5. Risk level radar graph of the cyber threats determined for the INS.

The risk level radar graph (Figure 5) indicated that two cyber threats that were determined were classified as medium risk (the highest risk level assigned) for the ship INS cyber security. The threats were related to the INS underlying operating system, in particular to the operating system update and secure setup. The out-of-date INS underlying operating system implied that an attacker can exploit a known vulnerability using publicly available instructions without significant expertise in ship navigation and computing technologies (analyzed in detail in Chapter 4). Securing the underlying operating system by disabling unnecessary services provides proactive protection from from unknown vulnerabilities and threats, and also could improve the performance of the INS because of additional resources released. On the other hand, relying on reactive protection solution and having out-of-date supporting software, cyber risk level over time will probably increase. In the case of the tested INS, the manufacturer of the underlying operating system will discontinue support and strongly recommend moving to next generation before the end of the current year (2019) [34]. The identified cyber threats corresponded to the previous findings with shipboard ECDIS and radar systems, indicating the same cyber risk threatening each of the navigation systems that are from different manufacturers and are installed on different types of ships [1,21].

The low (acceptable) risk level was assigned to most of the threats determined (six of eight), which are shown in Figure 5. The cyber threats were related to the ship navigational ranks training and awareness, physical protection controls, the cyber security-dedicated policy and procedure development, and periodic assessment and improvements. One of the threats assigned with the lowest risk level was related to the establishment of the Internet connection (Table 4, threat 5). The tested INS was not connected to the Internet and operated in the environment with strong physical protection and logical authentication control policies; thus, the Internet connection by installation of a network device was very unlikely to happen. Although disconnection from the Internet prevents outside threats, the vulnerabilities rising from the unmaintained operating system (its update and secure setup) could be triggered by inside actors (the ship's crew), either unintentionally or maliciously. However, it should be noted that with the INS connection to the Internet, risk level of all of the cyber threats determined would raise to the critical level, demanding instant action.

6. Conclusions

The comprehensive cyber security resilience examination of the INS installed on the RoPax ship engaged in international trade was presented. The examination was based on the mixed-method approach, combining an interview of the ship's navigational ranks and the following cyber security testing of the INS. The test was conducted using the industry vulnerability scanner, and the results were studied in the context of the INS's operating environment and implemented safeguards on the ship. While six determined threats were classified with acceptable risk level, the two medium risk level threats are related to the maintenance of the INS's underlying operating system, in particular its update and secure setup. The satisfactory risk level was attributed not only to maritime traditionally strong physical protection controls, navigational ranks' training, and adherence to security policies and procedures, but also to the INS's disconnection from the Internet.

The results from this study advance understanding of the source of cyber risks threatening the INS, and are applicable to any shipboard integrated system or type of ship. The results indicate the importance of the cyber security test performing as well as the analysis of the detected vulnerabilities regarding the ship operating environment. The cyber vulnerabilities detected with the passive scanning method suggest significance of the cyber security testing for the proactive protection by disabling unnecessary services. In addition, the findings contribute to the development of the new testing standard IEC 63154 and suggest the testing results that should be targeted. The study implies the need for occasional preventive maintenance of the underlying operating system to address weaknesses, despite the care taken for the purpose of regulatory compliance.

Author Contributions: B.S. developed the methodology; B.S. and I.R. performed the investigation; B.S., A.J., and D.Z. provided the resources; B.S. and A.J. ensured funding acquisition; B.S. wrote the original draft; B.S., I.R., A.J., and D.Z. wrote and edited the paper.

Funding: This research was financially supported by the University of Rijeka, grant number uniri-tehnic-18-68.

Acknowledgments: 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).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Svilicic, B.; Kamahara, J.; Rooks, M.; Yano, Y. Maritime Cyber Risk Management: An Experimental Ship Assessment. *J. Navig.* **2019**, *72*, 1108–1120. [CrossRef]
2. Kaleem Awan, M.S.; Al Ghamdi, M.A. Understanding the Vulnerabilities in Digital Components of An Integrated Bridge System (IBS). *J. Mar. Sci. Eng.* **2019**, *7*, 350. [CrossRef]
3. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Mar. Affairs.* **2019**, *18*, 129–163. [CrossRef]
4. Chybowski, L.; Gawdzinska, K.; Laskowski, R. Assessing the Unreliability of Systems during the Early Operation Period of a Ship—A Case Study. *J. Mar. Sci. Eng.* **2019**, *7*, 213. [CrossRef]
5. Tsimplis, M.; Papadas, S. Information Technology in Navigation: Problems in Legal Implementation and Liability. *J. Navig.* **2019**, *72*, 833–849. [CrossRef]
6. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security. *WMU J. Mar. Affairs* **2019**, in press. [CrossRef]
7. Chen, Y.; Liu, Q.; Wan, C.; Li, Q.; Yuan, P. Identification and Analysis of Vulnerability in Traffic-Intensive Areas of Water Transportation Systems. *J. Mar. Sci. Eng.* **2019**, *7*, 174. [CrossRef]
8. Svilicic, B.; Brčić, D.; Žuškin, S.; Kalebić, D. Raising Awareness on Cyber Security of ECDIS. *TransNav Int. J. Mar. Navig. Safety Sea Trans.* **2019**, *13*, 231–236. [CrossRef]
9. Lee, E.; Mokashi, A.J.; Moon, S.Y.; Kim, G. The Maturity of Automatic Identification Systems (AIS) and Its Implications for Innovation. *J. Mar. Sci. Eng.* **2019**, *7*, 287. [CrossRef]

10. Hareide, O.S.; Jøsok, Ø.; Lund, M.S.; Ostnes, R.; Helkala, K. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *J. Navig.* **2018**, *71*, 1025–1039. [CrossRef]
11. Zăgan, R.; Raicu, G.; Pazara, R.H.; Enache, S. Realities in Maritime Domain Regarding Cyber Security Concept. *Adv. Eng. Forum* **2018**, *27*, 221–228. [CrossRef]
12. Dobryakova, L.A.; Lemieszewski, L.S.; Ochin, E.F. GNSS spoofing detection using static or rotating single-antenna of a static or moving victim. *IEEE Access* **2018**, *6*, 79074–79081. [CrossRef]
13. Polatidis, N.; Pavlidis, M.; Mouratidis, H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Comput. Stand. Interfaces* **2018**, *56*, 74–82. [CrossRef]
14. Kalogeraki, E.; Apostolou, D.; Polemi, N.; Papastergiou, S. Knowledge management methodology for identifying threats in maritime/ logistics supply chains. *Knowl. Manag. Res. Pract.* **2018**, *16*, 508–524. [CrossRef]
15. Lund, M.S.; Gulland, J.E.; Hareide, O.S.; Jøsok, O.; Carlsson Weum, K.O. Integrity of Integrated Navigation Systems. In Proceedings of the IEEE International Workshop on Cyber-Physical Systems Security, Beijing, China, 30 May–1 June 2018.
16. Lewis, S.; Maynard, L.; Chow, C.E.; Akos, D. Secure GPS Data for Critical Infrastructure and Key Resources: Cross-Layered Integrity Processing and Alerting Service. *Navig. J. Inst. Navig.* **2018**, *65*, 389–403. [CrossRef]
17. Shapiro, L.R.; Maras, M.-H.; Velotti, L.; Pickman, S.; Wei, H.-L.; Till, R. Trojan horse risks in the maritime transportation systems sector. *J. Trans. Secur.* **2018**, *8*, 1–19. [CrossRef]
18. Kessler, G.C.; Craiger, J.P.; Haass, J.C. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *Trans. Nav. Int. J. Mar. Navig. Safety Sea Trans.* **2018**, *12*, 429–437. [CrossRef]
19. Lee, Y.C.; Park, S.K.; Lee, W.K.; Kang, J. Improving cyber security awareness in maritime transport: A way forward. *J. Korean Soc. Mar. Eng.* **2017**, *41*, 738–745. [CrossRef]
20. Borkowski, P. Presentation algorithm of possible collision solutions in a navigational decision support system. *Sci. J. Marit. Univ. Szczec.* **2014**, *38*, 20–26.
21. Svilicic, B.; Rudan, I.; Frančić, V.; Mohović, Đ. Towards a Cyber Secure Shipboard Radar. *J. Navig.* **2019**, in press. [CrossRef]
22. International Maritime Organization. *Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3*; IMO: London, UK, 2017.
23. International Maritime Organization. *Maritime Cyber Risk Management in Safety Management Systems, MSC 98/23/Add.1*; IMO: London, UK, 2017.
24. International Electrotechnical Commission. *Maritime Navigation and Radiocommunication Equipment and Systems-Cybersecurity-General Requirements, Methods of Testing and Required Test Results. IEC 63154 ED1*; IEC: Geneva, Switzerland, 2019.
25. Vu, V.D.; Lützhöft, M.; Emad, G.R. Frequency of use—the First Step Toward Human-Centred Interfaces for Marine Navigation Systems. *J. Navig.* **2019**, *72*, 1089–1107. [CrossRef]
26. International Maritime Organization. *Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS), Resolution MSC.252(83)*; IMO: London, UK, 2007.
27. International Maritime Organization. *ECDIS—Guidance for Good Practice, Resolution MSC.1/Circ.1503/Rev.1*; IMO: London, UK, 2017.
28. International Maritime Organization. *Adoption of the Revised Performance Standards for Radar Equipment, Resolution MSC.192(79)*; IMO: London, UK, 2004.
29. Tenable, Tenable Products: Nessus Professional. Available online: https://www.tenable.com/products/nessus/nessus-professional (accessed on 1 September 2019).
30. Svilicic, B.; Celic, J.; Kamahara, J.; Bolmsten, J. A Framework for Cyber Security Risk Assessment of Ships. In Proceedings of the 19th International Association of Maritime Universities (IAMU) Conference, Barcelona, Spain, 17–19 October 2018; pp. 21–28.
31. Microsoft, Microsoft Security Bulletin MS17-010 -Critical. Available online: https://technet.microsoft.com/library/security/MS17-010 (accessed on 1 September 2019).
32. Swiss Government Computer Emergency Response Team, Notes About the NotPetya Ransomware. Available online: https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware# (accessed on 1 September 2019).

33. United States Computer Emergency Readiness Team, Alert (TA17-181A) Petya Ransomware. Available online: https://www.us-cert.gov/ncas/alerts/TA17-181A (accessed on 1 September 2019).
34. Microsoft, Microsoft: Search Product Lifecycle. Available online: https://support.microsoft.com/en-us/lifecycle (accessed on 1 September 2019).