2021

Cyber security training strategy: dealing with maritime SCADA risks

Dimitrios Dalaklis
World Maritime University

Nikitas Nikitakos
University of the Aegean

Razali Yaacob
Netherland Maritime Institute of Technology

Recommended Citation

Dalaklis, D., Nikitakos, N. & Yaacob, R. (2021). Cyber security training strategy: dealing with maritime SCADA risks. In Pazaver, A., Manuel, M. E., Bolmsten, J., Kitada, M., Bartuseviciene, I. (Eds.), Proceedings of the International Maritime Lecturers' Association. Seas of transition: setting a course for the future (pp. 53-61). World Maritime University. http://dx.doi.org/10.21677/imla2021.05

http://dx.doi.org/10.21677/imla2021.05

Cyber security training strategy: Dealing with maritime SCADA risks

Dimitrios Dalaklis
Associate Professor, *World Maritime University, Malmo, Sweden,* dd@wmu.se

Nikitas Nikitakos
Professor, *University of the Aegean, Chios, Greece*, nnik@aegean.gr

Razali Yaacob
Captain, *Netherland Maritime Institute of Technology, Johor Darul Takzim, Malaysia*, razaliy@nmit.edu.my

Abstract: Control systems on board ships collect sensor measurements and data from various operational activities and display all the relevant information; they also facilitate relaying of control commands to local or remote equipment. Distributed control systems (DCS) are typically used within a single process or generating plant; supervisory control and data acquisition (SCADA) systems are used for larger-scale environments. The SCADA system communications infrastructure tends to be slower and less reliable, and so the remote terminal unit in a SCADA system has local control schemes to handle that eventuality. Security in general and cyber security specifically were not the major concerns of early standalone maritime SCADA systems. Security was primarily achieved by controlling physical access to system components, which were unique and used proprietary communication protocols. For years, security in SCADA systems was viewed as just an implication of safety. Over the last decade, however, the situation has changed, and numerous standards/directives dealing with the cyber security of SCADA systems have emerged. Characteristics of maritime SCADA cyber security are discussed; related training needs are identified next. The pedagogical approaches are also presented in order to train seafarers in risk assessment, prevention and mitigation strategies related with maritime SCADA cyber security risks.

Keywords: Cyber Security; Training Needs; Maritime Supervisory Control and Data Acquisition (SCADA) Systems.

Introduction

Ships today are quite complex systems to design, build and maintain throughout their life-cycle. Contemporary sea-going vessels are equipped with a wide variety of technologically advanced systems and are associated with an extremely high level of automation. It is a rather self-explanatory fact that the continuous improvement and integration/interconnection of electronic systems (most commonly termed as the "network-centric" approach), have created a rather different operating environment for the shipping industry, when compared with the prevailing model of just two decades ago. At that time, the exploitation of data exchange between interconnected equipment and systems on vessels engaged with maritime transport tasks, was relying mainly on stove-piped architectures and applications. However nowadays, the issues of connectivity and interconnection are clearly standing out when examining the prevailing trends in ships' design and equipment. Furthermore, easy access to various computer systems, and quite often in the so-called "remote mode", is holding a pivotal role during the conduct of operations -both on board a modern ship, as well as in relation to an extended number of related

activities ashore, with indicative examples in this domain being provided by various remote sensing and maintenance tasks (Dalaklis et all, 2020).

The seas and oceans of our planet are now well integrated into the Internet (most often via satellite support); this global coverage has provided the opportunity for shipping companies to reduce costs across supply/demand chains, improve customer services, and even redefine their way of conducting operations. Modern ships are being transformed into "remote offices at sea"; applications like voice over IP (Internet Protocol), email and instant messaging are now used on-board contemporary sea-going vessels on a daily basis. However, this new and "interconnected world" that is also strongly associated with an on-going digitalisation trend within the maritime industry itself is simultaneously associated with very significant risks, which in case they are not effectively and timely addressed, can result into really devastative outcomes. On the positive side and with a quite forward looking approach, during July 2017, the International Maritime Organization (IMO) already approved Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) in order to provide high-level recommendations on maritime cyber risk management, to safeguard shipping from current and emerging cyber threats and vulnerabilities. The adoption of Resolution MSC.428(98), which brought the importance of Cyber Security to the forward of attention, is also clearly standing out.

The European Union's Agency for Cybersecurity has already pointed out that the contemporary heavily industrialised world is constantly changing, including the introduction and/or further modification of technologies and associated business models that are needed to adapt towards "new" and evolving market requirements (ENISA, 2014). One of the most transcendental adaptations that the maritime transport industry is currently experiencing is the convergence between Operations Technology (OT), the operations needed to carry out the industrial processes, and Information Technology (IT), the use of computers to manage data needed by the organisation's enterprise processes. This convergence has many advantages (optimisation of operations, better use of resources, cost savings, etc.), but on the other hand it increases the need for cyber security of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. Initially, SCADA systems were used mainly in power transmission, gas pipeline and water distribution control systems. However, in recent year their use has expanded significantly and nowadays they are found extensively on-board ships. SCADA systems stand out among other ICSs, as systems that (1) monitor and control assets distributed over large geographical areas, and (2) use specific control equipment such as a Master Terminal Unit (MTU) and (various) Remote Terminal Units (RTUs) and are therefore exposed to cyber security risks (Cherdantseva et all, 2015). The Control Systems framework and the technical components of the basic SCADA structure are presented in Figure 1.

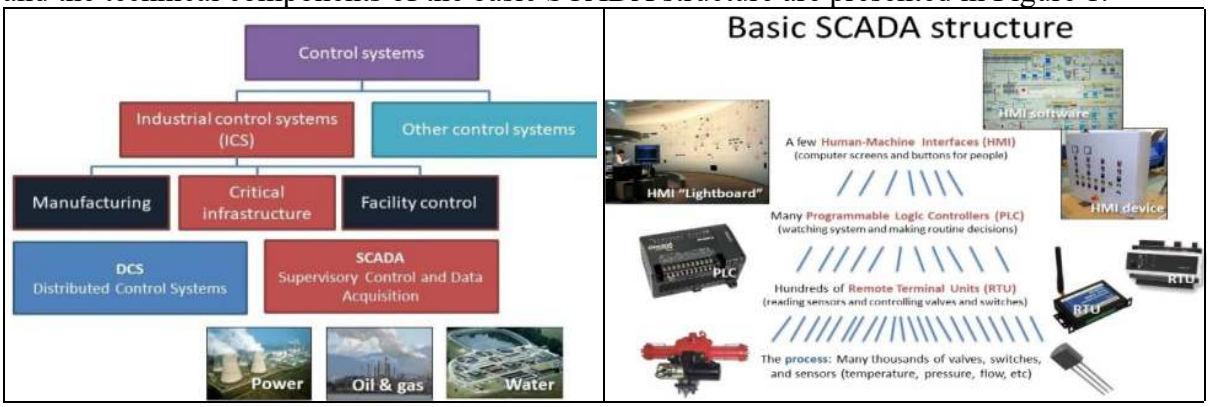

Figure 1. Use and technical components of a SCADA system.

Created by the authors, via adaption of certain slides from the presentation: Woudenberg, B. (2012). SCADA Right Now, Retrieved from https://slideplayer.com/slide/5703843/ June 2021

Control systems on board ships collect sensor measurements and data from various operational activities and display all the relevant information; they also facilitate relaying of control commands to local or remote equipment. Distributed control systems (DCS) are typically used within a single process or generating plant; SCADA systems are most often used for larger-scale environments. Security in general and cyber security specifically were not the major concerns of early standalone maritime SCADA systems. Security was primarily achieved by controlling physical access to system components, which were unique and used proprietary communication protocols (Cherdantseva et all, 2015). For many years, security in SCADA systems was viewed as just an implication of safety. Over the last decade, however, the situation has changed, and that paradigm is not valid in the contemporary "well interconnected world". It is indicative of the fact that numerous standards/directives dealing with the cyber security of SCADA systems have emerged, as an initial response to the specific need. In any case, this aforementioned convergence between OT and IT, which affects hundreds of thousands of industrial systems worldwide, implies that professionals with knowledge of cyber security for ICS/SCADA will be needed. However, currently, there are very few professionals with the proven skills available to do this work. Following a rather simplistic qualitative approach, characteristics of maritime SCADA cyber security are discussed first and related training needs are identified next. The main aim is to identify the "right" pedagogical approaches which can be deployed in order to train seafarers in risk assessment, prevention and mitigation strategies related with maritime SCADA cyber security risks.

Importance of Cyber Security

The contemporary era is very frequently referred to as "the information age"; cyber-attacks on the wider maritime industry (and especially on the relevant port IT systems) should no longer be considered hypothetical or simply the stuff of over-exaggerating analysts, resembling a fictional narrative. Probably a very strong "wake up" message was sent in June 2017, when the Maersk shipping company was hit by a cyber-attack from the purely destructive NotPetya virus (Boyes et all, 2020). The virus entered Maersk's systems through a widely used piece of tax accounting software in Ukraine. Maersk was not the intended target for the attack, but the consequences for the company were very real. The virus spread through the company globally and made all their applications and data unavailable for several days. Real world operations, including its extremely important Rotterdam terminal, were seriously affected, or even completely crippled, with relevant financial losses being estimated at the level of $200-300 million. The Maersk story testifies how a system that fails in key ways becomes unusable, even if certain parts of it remain unaffected: Maersk's shipboard systems were fine, but there was no way to distribute their loads or take on new cargo (Dalaklis and Schröder-Hinrichs, 2019).

It is a self-explanatory fact that the NotPetya virus could attack the Maersk global network because it was loaded onto one unpatched computer operating in a single local office, which in turn was connected to the company's global network. This incident shows the vulnerability of everyone to cyber-attacks: you do not even have to be the intended victim. On a positive note, Maersk could recover relatively quickly because it had already recognised that resilience and recovery processes are as important in terms of the wider Cyber Security framework as trying to prevent an attack. Being able to recover all your systems and data from secure backups within a very short timeframe of a successful cyber-attack will protect your business from potentially serious financial and the more important reputational damage. Spreading of viruses

through the computer systems that are serving the wider needs of the maritime industry is just a small part of the complex equation. In other cyber security incidents, IT assets have been quite often infected with malware and in numerous occasions it has been recorded unintentional jamming or interference with wireless networks (Boyes et all, 2020).

In order to bring forward a widely accepted definition, "Cyber Security" can be described as "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets*" (International Telecommunications Union (ITU), 2008). Within this definition, the "cyber environment" comprises the standalone computers and interconnected networks of both information and operational technology that use electronic, computer-based and wireless systems, including information, services, social and business functions that exist only in cyberspace. At the same time, the "organisation and user's assets" includes connected and standalone computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted, processed or stored data in the cyber environment. Cyber security is not just about preventing hackers gaining access to systems and information. It also addresses the maintenance, integrity, confidentiality and availability of information and systems, ensuring business continuity and the continuing utility of cyber assets. Before moving to a different direction, it is worth clearly highlighting the fact that on board a modern ship there are numerous SCADA systems. With the help of Figure 2, an attempt to summarize all ICS that can be found on a modern vessel is taking place; a few indicative examples of interest are also listed next: Alarm and Monitoring System; Auxiliary Control System; Power Management System; Cargo Control System; Propulsion Control System; Ballast Automation System; Air Conditioning System; Anti–Heeling; Reefer Monitoring; Fire System; Main Engine Monitoring System. Furthermore, a representation of the IT environment supporting the conduct of a shipping company's business and other activities, as well as how the use of these computers relates to maritime SCADA is provided.

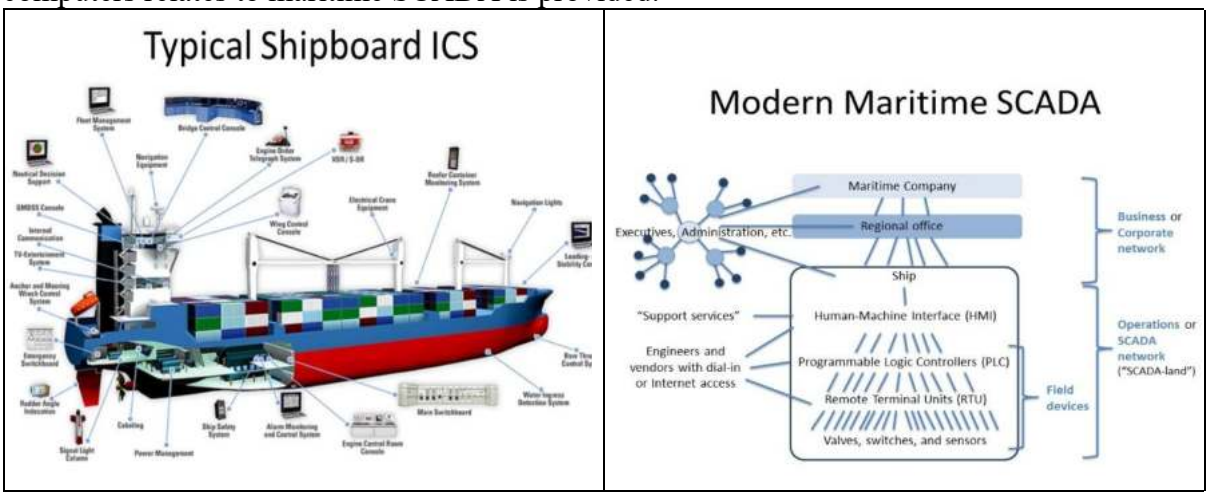

Figure 2 ICS on-board a vessel and the wider framework of maritime SCADA.
Created by the authors, via adaption of certain slides from the presentation: Woudenberg, B. (2012). SCADA Right Now, Retrieved from https://slideplayer.com/slide/5703843/ June 2021

The main vulnerabilities that are related to SCADA systems are (Woudenberg, 2012; Nikitakos 2017): The adoption of standardized technologies with known vulnerabilities; The connectivity of many control systems via, through, within, or exposed to unsecured networks, networked portals, or mechanisms connected to unsecured networks (which includes the Internet); Implementation constraints of existing security technologies and practices within the existing

control systems infrastructure (and its architectures); The connectivity of insecure remote devices in their connections to control systems; The widespread availability of technical information about control systems, most notably via publicly available and/or shared networked resources such as the Internet; Disrupt the operations of control systems by delaying or blocking the flow of information through the networks supporting the control systems, thereby denying availability of the networks to control systems' operators and production control managers; Attempt, or succeed, at making unauthorized changes to programmed instructions within PLC, RTU, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control station equipment; Send falsified information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions; Modify or alter control system software or firmware such that the net effect produces unpredictable results (such as introducing a computer "time bomb"); Interfere with the operation and processing of safety systems; Many control systems are vulnerable to attacks of varying degrees. These attack attempts range from telephone line sweeps (a.k.a. "wardialing"), to wireless network sniffing (a.k.a. "wardriving"), to physical network port scanning, and to physical monitoring and intrusion (Nikitakos, 2017)

It is also necessary to mention that there are several types of exploiting maritime ICS/SCADA. A limited number of them is discussed next: **Direct physical damage to affected equipment and systems.** By exploiting an ICS, the controlled mechanism can fail with catastrophic results, damaging a single piece of equipment, interrupting a larger system, or disabling or destroying an entire ship; **Small-scale, local disruptions.** They can damage or interrupt individual systems or single ships within a single organization, without widespread impact beyond the affected function or service; **Injury or death to operators, passengers or the general public**. An incident can affect a single operator or a larger number of crewmembers or bystanders. Targeted attacks on a critical for safety equipment can result into a fire, or explosion that could injure or kill hundreds of people; **Catastrophic disruptions to the transportation system.** A vessel sunk in a shipping channel, an explosion at an oil or LNG facility, sabotage to canal locks, or a series of mishaps involving cargo container cranes in critical ports can have long-term impacts to the safety, stability and reliability of very crucial elements of the wider transportation system (Nikitakos, 2017; Boyes et al, 2020).

Knowledge areas

The most important knowledge areas for concerned professionals have been identified, by taking into account the existing ICS/SCADA Cyber Security Certification schemes and other relevant studies. The following uses as reference the work done under the ERNCIP (European Reference Network for Critical Infrastructure). One of its subgroups has focused on defining the competences, qualifications and experience needed by ICS Cyber Security Professionals. The result is a high level overview of the knowledge areas that need to be developed; they are summarized with the help of Figure 3. Of very specific interest are the following (ENISA, 2014): **General Information Technology.** This domain includes an introduction to IT architecture to Networking and Communications, systems development and software, data management and finally an overview of standards and processes. It is considered as the basic step for any certification related to Maritime SCADA taking into account the complexity that the trainee will face in the next steps; **Cyber Security & Information Risk Management.** The vulnerabilities and the complexity of several attacks makes risk management very essential for the Maritime SCADA Knowledge area. Risk management includes several methods for risk identification, (PHA/HAZOP usage), methodologies and procedures for risk acceptance, application of possible risk control options and finally risk/mitigation plan); **Industrial**

Automation Control and Safeguarding. This is the main area given the variety of several maritime SCADA on board of ships. It includes topics such as maritime networking and Architecture, embedded device and control for maritime SCADA, Operating environment and hazards particularly on board of a ship. Maritime process Safety management, relevant standards and procedures from other sectors.

Figure 3 Knowledge areas relating to education and training activities for maritime SCADA. Created by the Authors, via adaptation from European Union Agency for Cybersecurity. (2014). Certification of Cyber Security skills of ICS/SCADA professionals: Good practices and recommendations for developing harmonized certification schemes. Retrieved from https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals

Proposed curriculum development

Benjamin Bloom was one of the first scientists who systematically categorized the educational objectives and the related educational goals. The so-called "Bloom's taxonomy" is one of the main principles of the educational sciences, which has been revised and updated in the last years (Bloom, 1956; Bloom 1969). In general, the taxonomy forms a hierarchical model for the classification of educational learning objectives into levels of specificity and complexity. The overall method tries to enhance the communication between educators on the design of curricula, exercises, and examinations. It has been adopted by related teaching philosophies that lean more on skills rather than on content. It consists of 6 layers, with the 3 bottom levels (remembering, understanding, and applying) denoting the basic understanding of the examined topic, while the coverage of the 3 top ones (analyzing, evaluating, and creating) reveals that the trainee has achieved a higher-order of thinking. The first three layers assess the trainee's knowledge about the teaching content while skill development is promoted with "higher-order thinking". This also forms the final aim of the Bloom's taxonomy—building a culture of thinking. The Blooms taxonomy was chosen for the scope of our study, but since the topic of cyber security in relation to maritime SCADA systems is also associated with a very practical

element in terms of training requirements, it was combined with so called Work Based Learning (WBL), which is an educational strategy that provides students with real-life work experiences where they can apply academic and technical skills and develop their employability.
The discussion revolves around a series of educational courses which will integrate the theoretical curriculum with the workplace to create a different learning paradigm. It has already been pointed out that: "Work-based learning deliberately merges theory with practice and acknowledges the intersection of explicit and tacit forms of knowing" (Raelin, 1997). Most WBL programs are generally university accredited courses, aiming at a win-win situation where the learner's needs and the industry requirement for skilled and talented employees are both met. WBL programs are targeted to bridge the gap between the learning and the doing. Work-based learning strategies provide career awareness, career exploration opportunities, career planning activities and help students attain competencies such as positive work attitudes and other employable skills (Hamilton, S.F. & Hamilton, M.A. 1998; Stasz & Brewer, 1998). WBL encompasses a diversity of formal, non-formal and informal arrangements including apprenticeships, work placement and informal learning on the job. The key driver is the need for active policies to secure learning that meets the need of the workplace.

Indicative WBL strategies could include the following (Hamilton, S.F. & Hamilton, M.A., 1998; Stasz & Brewer, 1998; Axcelerate, 2020): **Apprenticeship or internship or mentorship.** An apprenticeship involves the student working for an employer where he or she is taught and supervised by an experienced employee of the chosen organization. The student is periodically evaluated for progress as per the skills and knowledge acquired, and maybe granted wages accordingly. At the end of the course, the student receives a certificate of service. The student learns in a realistic environment and gets the opportunity to apply his or her knowledge in real-world scenarios; **Job shadowing.** Job Shadowing is a short term opportunity that introduces the student to a particular job or career by pairing the student with an employee of the workplace. By following or 'shadowing' the employee, the student gets familiar with the duties and responsibilities associated with that job; **Business/industry field trip.** Field trips offer the students an insight in the latest technical advancements and business strategies of an enterprise. Students also gain awareness of the various career opportunities available and understand the driving forces of the community's economy; **Entrepreneurial experience.** This includes setting up of specific business, right from the planning, organizing and managing stage to the risk control and management aspects of a business; **Cooperative education.** In cooperative education, the work experience is planned in conjunction with the technical classroom instruction. This method is used by universities that do not have access to state-of-art equipment required to transact the technical course practically; **School-based enterprise.** A school-based enterprise is a simulated or actual business run by the school. It offers students a learning experience by letting them manage the various aspects of a business; **Service learning.** This strategy combines community service with career, where students provide volunteer service to public and non-profit agencies, civic and government offices etc.

Summary and Conclusion

During recent years, the wider maritime industry (ports included) has been undergoing a digital transformation in order to effectively meet emerging business challenges, optimise existing business and operational processes, as well as introducing new capabilities, such as automation and real-time monitoring of operations. Especially in the maritime sector, a large volume of data is produced from a very extended pool of relevant sources (i.e. systems supporting the conduct of navigation and/or ship's machinery, as well as related marine fleet management

systems etc.), on a daily basis. This digitalisation trend has been based on the interconnectivity of Information Technology (IT) and Operation Technology (OT) assets and the introduction of new technological enablers, such as cloud computing, big data and Internet of Things (IoT). However, this phenomenon is also creating numerous challenges, since in an "interconnected world" the whole security chain is as strong as its weakest link. On the positive side, the various implications of Cyber Security have been discussed at the International Maritime Organization (IMO) and as a very timely response, the adoption of Resolution MSC.428(98), which aims to address cyber risks in the shipping industry, is pushing forward with the first initial step: raising awareness thought all involved stakeholders. Furthermore, this IMO resolution is creating a framework of effectively addressing cyber risks as a part of the already existing safety management systems, within the ISM Code. It clearly establishes the obligation of Maritime Administrations and concerned shipping companies to ensure that the existing safety management systems appropriately address cyber risks and cyber security for ships by their 2021 annual verification.

The field of risk assessment related to cyber security and especially with ICS/SCADA is a new and quite complex domain; concerned maritime personnel, most often receive "random" training offerings by several different manufacturers and are then expected to effectively deal with an extended portfolio of security incidents. In this paper, targeted knowledge areas that were considered as essential for certification were identified first; then, by using Bloom's taxonomy and in combination with a work-based learning (WBL) approach, relevant training strategies were discussed and their advantages and drawbacks were also highlighted. Cutting a long way short, WBL is an educational method that immerses students in the workplace, prompting them to learn about the environment in which they'll be working, and to complete typical tasks for the company. The WBL approach is relatively new in the maritime sector, but it looks like it fits with the particular complexities for security risks related with maritime SCADA. As it was already very clearly explained, WBL encompasses a wide portfolio of formal, non-formal and informal arrangements including apprenticeships, work placement and informal learning on the job. Needless to mention: the maritime industry is already relying on the job training and mentoring to create and further improve competencies in relation to the maritime profession; this transition towards WBL will not require a significant paradigm shift. Last, but not least, the "hot to implement" these particular training strategies should be included as a future research topic; examining more carefully the adoption of the "right" methods and tools for the concerned instructors and facilitating the easy understanding of the trainees must also be included into the portfolio of future investigations.

References

Axcelerate Inc. (2020). What is Work-Based Learning (WBL)?,
Retrieved from https://www.axcelerate.com.au/post/what-is-work-based-learning-wbl

Bloom, B.S. (1956). *Taxonomy of Educational Objectives, Handbook: The Cognitive Domain*. New York, NY: David McKay Company.

Bloom, B.S. (1969). *Taxonomy of Educational Objectives: The Classification of Educational Goals.* New York, NY: David McKay Company.

Boyes, H., Roy Isbell, R. & Luck, A. (2020). Good Practice Guide Cyber Security for Ports and Port Systems. Retrieved from

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsbyc, H. & Stoddart, K. (2015). A Review of Cyber Security Risk Assessment Methods for SCADA Systems, *Computers & Security*, 56, 1–27.

Dalaklis, D. & Schröder-Hinrichs, J.U. (2019). The Cyber-Security Element of Hybrid Warfare: Is there a Need to "Formalise" Training Requirements? *10th NMIOTC Annual Conference* ("*Countering Hybrid Threats: An Emerging Maritime Security Challenge")*, Chania-Greece, 4 June 2019. Retrieved from https://www.researchgate.net/publication/333631928_The_Cyber-Security_Element_of_Hybrid_Warfare_Is_there_a_Need_to_Formalize_Training_Requirements

Dalaklis, D., Katsoulis, G., Kitada, M., Schröder-Hinrichs J. U. & Ölcer, A. I. (2020). A "Net-Centric" Conduct of Navigation and Ship Management, *Maritime Technology and Research*, 2(2), 90-107.

European Union Agency for Cybersecurity. (2014). Certification of Cyber Security skills of ICS/SCADA professionals: Good practices and recommendations for developing harmonized certification schemes. Retrieved from https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals

Hamilton, S.F. & Hamilton, M.A. (1998). When is Learning Work-Based?, *The Phi Delta Kappan*, 78(9), 677.

International Telecommunications Union (2008). Overview of cyber security. ITU-T X.1250, Geneva, Switzerland.

Nikitakos, N. (2017). Maritime SCADA cyber resilience, *3rd ShipIT Conference: Aligning Maritime Business with* IT, Athens-Greece, 27 September 2017. Retrieved from http://globalsustain.org/en/story/12430

Raelin, J.A. (1997). A Model of Work-Based Learning, *Organization Science*, 8(6), 563–578.

Stasz, C. & Brewer, D.J. (1998). Work-Based Learning: Student Perspectives on Quality and Links to School, *Educational Evaluation and Policy Analysis*, 20(1), 31–46.

Woudenberg, B. (2012). SCADA Right Now,
Retrieved from https://slideplayer.com/slide/5703843/ June 2021