Cyber Security: Supply Chain Risk Management and Defense-in-Depth requirements for Maritime Systems

W. Johnson, B. Wisniewski, Rockwell Automation*

* Corresponding Authors Email: wajohnson@ra.rockwell.com, bdwisnie@ra.rockwell.com

Synopsis

Cybersecurity for maritime operations requires a robust defense-in-depth approach from the initial sourcing of components, software, and systems; continuing through robust security engineering during the design, implementation, and deployment processes of those systems; and extending to proactive defensive measures of not only traditional information communications technology (ICT) systems but operational technology (OT) systems as well.

Global connectivity has extended the risk of network attack even while a vessel is underway. Additionally, the long lifecycle of many maritime systems contributes to the challenge of defending outdated or no longer supported components and systems, (which are difficult to patch or totally unpatchable in many cases). Emerging standards and regulatory guidance are pushing the maritime industry toward compliance. These initiatives provide an opportunity to achieve improved operational practices and eliminate the underlying cyber security vulnerability as well.

International bodies such as BIMCO, the Oil Companies International Marine Forum (OCIMF), and the International Maritime Organization's (IMO) extension of the International Safety Management (ISM) Code and the International Ship and Port Facility Security Code (ISPS) are excellent resources to address cyber security risk. The new IMO guidance, adopted by the Maritime Safety Committee on June 16, 2017, as Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems, encourages organizations "to ensure that cyber risks are appropriately addressed in existing safety management systems."[1]

Many experts recommend adopting one of several international security standards or frameworks already developed to help identify, assess, and mitigate cyber security risk; these include the International Standards Organization (ISO)/ International Electrotechnical Commission (IEC) 27000 Information Security Management Systems (ISMS) family of standards, the Center for Internet Security (CIS) Top 20 Controls, and the United States National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework. Another family of standards, the IEC 62443 Industrial Networks and Systems Security series of standards, have a direct application to shipboard automation and control systems typically found throughout a vessel's propulsion, stabilization, electrical control, and deck machinery systems. Organizations can leverage a growing number of IEC 62443 compliant components, systems, and processes to help streamline the steps required for overall compliance and help address their underlying cyber security risk overall. This paper will focus on addressing supply chain cyber risk management for maritime operations and effective cyber security defense-in-depth practices for the vessel's hull, mechanical, and electrical shipboard systems.

Keywords: Cybersecurity, Supply Chain Risk Management, Defense-in-Depth, IEC 62443

[1] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

1. Introduction

A common challenge faced by all different organizations in the shipping industry is their dependence on receipt of critical goods and services through vendors and suppliers. When establishing a cyber risk management program, an integral part within the many facets of that encompassing program is management and mitigation of the security vulnerabilities and cyber threats that could occur due to the procurement of materials from an organization's suppliers. The NIST Risk Management Framework (RMF), IMO's Guidelines on Maritime Cyber Risk Management under MSC-FAL.1/Circ 3, and the BIMCO Cybersecurity Guidelines have all delineated the same five

 https://doi.org/10.24868/issn.2515-818X.2020.051

functional elements of a Risk Management Program which are Identify, Protect, Detect, Respond, and Recover. These are illustrated in Table 1 below.

NIST	IMO	BIMCO	Examples
Identify	Identify	Identify Threats Identify Vulnerabilities Assess Risks	Threat Intelligence Feeds Vulnerability Scanning Vulnerability Assessment Penetration Testing Risk Assessment
Protect	Protect	Develop Protective Controls	Firewalls, Endpoint Protections, File Encryption, Mobile Device Management (MDM)
Detect	Detect	Develop Protective Controls	Intrusion Detection, Log Monitoring, Network Traffic Sensors, SIEM
Respond	Respond	Respond	Malware Recovery Tools, Live Malware Analysis
Recover	Recover	Recover	Reimaging Process, Restore from Backups, Confirm System Integrity

Table 1: Identify, Protect, Detect, Respond, Recover[i]

In the Identify function, companies are to identify not only organizational roles and personnel responsibilities involved with cyber security, but also identify systems and equipment, which if compromised, would impact the safety and security of their operations, personnel, and vessels. The second function, to Protect, companies leverage the risk assessments and threat modeling undertaken as part of the Identify function and implement controls and mitigations designed to protect critical assets within the infrastructure It also requires that components possess the security capabilities required to support integration into a broader cybersecurity infrastructure. The third function, to Detect, means to develop and implement practices to detect events in a timely manner. Subcategories of activities within those three functions involve Supply Chain Risk Management (SCRM) and they contribute to an organization's overall cybersecurity posture. Organizations are looking for help from their suppliers to assist them in enforcing their cyber security policies and practices. To that end, suppliers that have implemented secure product development and lifecycle protections as well as engineered their components and products with configurable features to fulfill security controls within those functional elements help address areas for a company's Supply Chain Risk Management effort and help a company deploy a defense-in-depth approach against cyber security vulnerabilities and threats.

2. Supply Chain Risk Management

Focused Supply Chain attacks pose a unique challenge for organizations. Identifying, detecting, and mitigating this type of issue requires vigilance throughout an organization. Everyone from the Procurement Department, through Supplier Quality, and Integration must operate with a clear focus to prevent malicious or counterfeit components or software from entering into the development lifecycle.

A prime example of this type of threat is the Zombie Zero attack that impacted global shipping and manufacturing in 2014. "Zombie Zero is a suspected nation-state sponsored Zero Day attack on targeted logistics and shipping industries. Variants of this Advanced Persistent Malware have recently been seen in manufacturing sectors as well. Weaponized malware was delivered into customer environments from the Chinese factory responsible for selling a proprietary hardware/software scanner application used in many shipping and logistic companies around the world. The same hardware product with a variant of this malware was sold and delivered to a manufacturing company as well as to seven other identified customers. The malware was embedded in a version of Windows XP installed on hardware at manufacturer's location in China. Malware also

 https://doi.org/10.24868/issn.2515-818X.2020.051

persisted in the Windows XP embedded version located at the Chinese manufacturer's support website hosted in China."[ii]

"Zombie Zero is an attack method discovered by TrapX labs in 2014. The discovery showed that at least eight companies were compromised beginning in May 2013. Zombie Zero is highly unusual in that the entry point is based on malware that has been "weaponized" through its placement within hardware developed by an original manufacturer, then sold to unsuspecting customers. [TrapX] believe that the Zombie Zero malware was preloaded into newly manufactured scanners by a manufacturer in China. The scanners were sold on the open market to global shipping-and-logistics companies. The targets included some of the largest manufacturing companies in the world. Once the scanners were installed and in use, the secretly embedded malware had instant access inside the perimeter protections. The attacker tools were thus available to compromise networks from the inside and, once remotely updated with additional functionality by the attackers in China, exfiltrate proprietary financial and shipping information."[iii]

Beyond traditional piracy, criminal organizations are also becoming more interested in attacking the support systems behind maritime operations. Given that the vast majority of global trade occurs over the world's oceans, it should be no surprise that illicit materials are a not insignificant portion of that total. The attack against the Port of Antwerp illustrates this point. The attack began when hackers started a phishing campaign against port staff in 2011. "A criminal group gained access to data remotely which they then used to identify and intercept containers with drugs smuggled onboard. The compromise was discovered after entire containers disappeared from the port with no apparent explanation. Once the software had been discovered and neutralized, the attackers then broke into offices at the port, deploying computers concealed in everyday objects to intercept data from systems, including the staff's keyboard inputs and screenshots from their workstations. The complex and sustained attack has led to warnings from security experts that attacks on shipping and port infrastructure will continue to evolve, and protecting the supply chain is of utmost importance."[iv]

Additionally, the United States Coast Guard (USCG) recently issued a warning that cyber adversaries, likely nation states, are targeting the shipping industry not only by trying to send phishing emails, but also by creating malware designed specifically to attack ship-based systems.[v]

The complexity of SCRM cannot be overstated. A recent report responding to Executive Order 13806 in the United States echoes this concern around SCRM overall. "The defense manufacturing supply chain flows goods and critical supporting information through multiple organizations of varying size and sophistication to transform raw materials into components, subassemblies, and ultimately finished products and systems that meet [Department of Defense] DoD performance specifications and requirements. These supply chain operations rely on an infinite number of touch points where digital and physical information flows through multiple networks – both within and across many manufacturers' systems. In today's digitized world, every one of these supply chain touch points represents a potential product security risk."[vi]

As noted in NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, "supply chain risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed. They are also associated with the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services." Echoing the requirements set forth in IEC 62443-4-1, NIST SP 800-161 lays out a number of key steps required for a formal supply chain risk management (SCRM) capability. These include the following:

1. Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39, Managing Information Security Risk [NIST SP 800-39]) including an organization-wide risk assessment process (in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments [NIST SP 800-30 Rev. 1]);
2. Establish an organization governance structure that integrates ICT SCRM requirements and incorporates these requirements into the organizational policies;
3. Establish consistent, well-documented, repeatable processes for determining [FIPS 199]impact levels;
4. Use risk assessment processes after the [FIPS 199] impact level has been defined, including criticality analysis, threat analysis, and vulnerability analysis;

 https://doi.org/10.24868/issn.2515-818X.2020.051

5. Implement a quality and reliability program that includes quality assurance and quality control process and practices;
6. Establish a set of roles and responsibilities for ICT SCRM that ensures that the broad set of appropriate stakeholders are involved in decision making, including who has the required authority to take action, who has accountability for an action or result, and who should be consulted and/or informed (e.g., Legal, Risk Executive, HR, Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/procurement, supply chain logistics, etc.);
7. Ensure that adequate resources are allocated to information security and ICT SCRM to ensure proper implementation of guidance and controls;
8. Implement consistent, well-documented, repeatable processes for system engineering, ICT security practices, and acquisition;
9. Implement an appropriate and tailored set of baseline information security controls in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [NIST SP 800-53 Rev. 4];
10. Establish internal checks and balances to assure compliance with security and quality requirements;
11. Establish a supplier management program including, for example, guidelines for purchasing directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers;
12. Implement a tested and repeatable contingency plan that integrates ICT supply chain risk considerations to ensure the integrity and reliability of the supply chain including during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor strikes); and
13. Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying causes of security incidents, including those originating from the ICT supply chain.

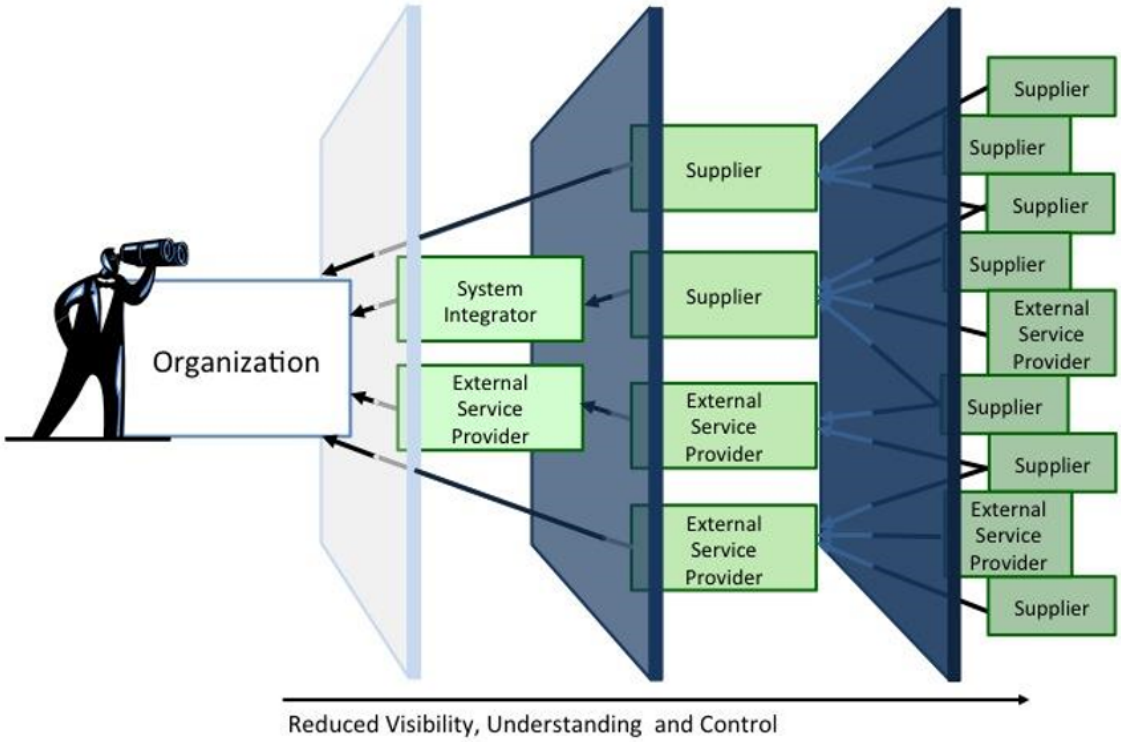

Figure 1: Challenges of Supply Chain Visibility[vii]

 https://doi.org/10.24868/issn.2515-818X.2020.051

3. Supply Chain Visibility Challenge

Understanding the full scope and scale of the challenge of SCRM within the maritime domain is further illustrated in the Center for Strategic and Budgetary Assessments Report, Strengthening the U.S. Defense Maritime Industrial Base, A Plan to Improve Maritime Industry's Contribution to National Security, "The modern shipbuilding and repair industry draws equipment and parts from a web of U.S. and foreign suppliers. The complexity of the supplier base, particularly two or three tiers below the shipbuilder, sometimes obscures that one or two manufacturers are the only sources for key components that are being used by all shipbuilding and repair yards."[viii] Figure 1, above, highlights the challenge of maintaining visibility over multiple layers of the supply chain.

Over time, emerging threats have led policy makers and standards bodies to extend the scale and scope of security requirements across a variety of fields. One example is the NIST Risk Management Framework (RMF). RMF is an overarching framework to approach cyber security and within that framework various NIST publications offer instructional guidelines to implement security controls for information systems and operational systems deployed by an organization. NIST SP 800-53 provides an overarching catalog of security controls for technology systems in general while NIST SP 800-82 provide a targeted subset of controls focused on operational technology (OT) environments. Within both of those publications, organizations have an objective to assess and define gaps in their existing cyber posture for the acquisition of products and services followed by implementing the security controls under the Security Control Family "System and Services Acquisition". All 22 security controls in that security family are identified by the two-letter designation, SA, followed by its number. For example, the security control labeled SA-1 is the System and Services Acquisition Policy and Procedures security control. Once an organization has created and established their acquisition policies and procedures, the other security controls in that security family follow. For SA-12, Supply Chain Risk Management, an organization will need to address the cyber related risks associated with procuring systems, system components, and services from their individual suppliers. Those cyber risks include counterfeit products, product software vulnerabilities, and a supplier's product design and development quality controls to reduce or eliminate functional and design security weaknesses in the product. How does an organization begin to assess or vet their suppliers for such cyber risks? With constrained budgets and limited time, an organization needs an efficient and effective way to accomplish this activity for the supply of OT systems such as industrial automation and control systems.

With that in mind, the International Electrotechnical Committee developed the IEC 62443-4-1 Standard which encompasses secure product development lifecycle requirements for OT systems and components. Those suppliers which have implemented product development policies and practices that conform with IEC 62443-4-1 and have been audited and attained the IEC 62443-4-1 Certification have demonstrated mature cyber protections and mitigations against those threats in their products' development and design. Supplier's that can show they have IEC 62443-4-1 Certified product development and lifecycle requirements enforced, demonstrate two significant security objectives to manage those aforementioned supply chain cyber risks.

- Objective #1: Provide a product development framework that addresses a secure by design, defense in depth approach to designing, building, maintaining and retiring products used in industrial automation and control products and systems
- Objective #2: Align their development process with the elevated security needs of product users, i.e. organizations and companies, of Industrial Automation and Control Systems

 https://doi.org/10.24868/issn.2515-818X.2020.051

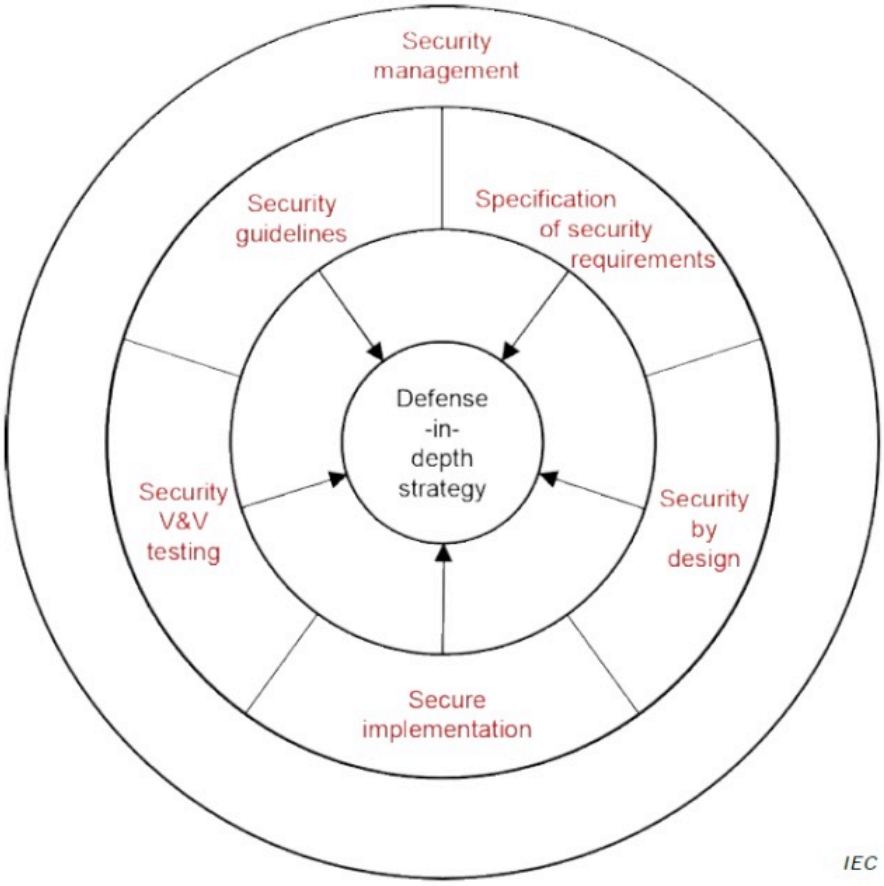

Figure 2: Security Management and Defense-in-Depth

Both of those objectives are accomplished through the processes and procedures a supplier has established that perform the eight Practices in that IEC Standard. Those Practices, shown above in Figure 2, are:

- Security Management
- Specification of Security Requirements
- Secure By Design
- Secure Implementation
- Security Verification and Validation Testing
- Management of Security Related Issues
- Security Update Management
- Security Guidelines

Specifically, the requirements spelled out in the Security Management section, SM-9: Security requirements for externally provided components and SM-10: Custom developed components from third-party, highlight the importance of establishing a process to "ensure that supply chain security is addressed for equivalent security practices, latest security updates, security deployment guides and the supplier's ability to respond if a vulnerability is discovered. Supply chain security applies to components which are included within the product and are provided external to the development team responsible for a given product, but do not meet the definition described in [SM-10: Custom developed components from third-party]. The security provided by such third-party components is directly related to their role in the product's secure design and defense in depth strategy."[ix] These, along with the other 45 requirements in IEC 62443-4-1, help provide a measure of assurance in the steps taken to securely design, develop, implement, and test components as part of a formal secure development lifecycle.

 https://doi.org/10.24868/issn.2515-818X.2020.051

By ensuring compliance with these requirements and demonstrating that compliance to a 3rd party conformance assessment organization, an audited supplier that attains the IEC 62443-4-1 Certification has shown it has structured security management activities for the entire lifecycle of a product from its first development stage to its final obsolescence and disposal. A supplier which annually maintains this IEC 62443-4-1 certification has defined and disciplined processes for development and documentation of their products' security capabilities and the context of their products' use against security attacks and other threats as they are intended when integrated within IT and OT systems. That supplier has demonstrated it can take the planning and development stage ideas of security capabilities forward into a sound engineered design and implementation of those security capabilities within their products. Each product has a process for its security capabilities to be thoroughly verified and validated. After a product has been released to the market, the supplier continues to provide updates and communications to those users about any discovered vulnerabilities and the supplier documents and provides recommended corrective actions for their products to mitigate those threats. Finally, at the end of the product's service life, the supplier has documented guidelines and effective communication to those users about their products disposal methods and activities to remove or erase memory and proper destruction of their products. These all stem from the first practice of Security Management which ensures that the security activities throughout a product's lifecycle are sufficiently planned, documented, and executed.

Adherence to the requirements within IEC 62443-4-1 demonstrate the supplier must have well-defined and proven product development processes in place which can meet security requirements. It has identified organizational roles and personnel that are responsible for the security processes and identified which appropriate controls and requirements for each product based on up-to-date threat modeling. Compliance with the IEC 62443 standard also means that suppliers must ensure personnel assigned to those key roles which have responsibility for the design, development, implementation, and testing of security requirements throughout the product development process undertake regular security training and assessment programs to ensure they have the latest knowledge of the emerging threats and overall security requirements. Leveraging this knowledge, those individuals, typically identified formally as Subject Matter Experts within their fields, and based upon a formal threat model and risk assessment, shall determine which security controls, technologies, and processes are necessary and of sufficient applicability for the product type. For any software scripts and executables within a product such as firmware, the supplier will need to deploy cyber security hash and encryption signing methods to provide integrity and authenticity verification mechanisms of their products. These give product users the ability to determine whether the provided product's files have not been altered. For any externally provided components used in the final assembled product, a supplier with this IEC Certification verifies that these same security requirements are enforced on their sub-tier suppliers. The supplier must have a process in-place that assesses, addresses, and verifies that all security related issues in a product or patch have been mitigated and corrected before release and that such processes must be verifiable and documented before a product or patch is released. Once all of this has been established, a supplier then must develop and enforce a process for continual improvement of their product's secure development lifecycle and include an analysis of Quality Assurance / Quality Control (QA/QC) issues of security defects that were discovered in the field.

What all this means for an asset owner and maritime organization, is that they can have a high degree of certainty and confidence that they are addressing those cyber related risks to their company from components and products received by their suppliers when they procure components and systems from suppliers who are maintaining an IEC 62443-4-1 certification for their products' development lifecycle. Using suppliers with an IEC 62443-4-1 certification is an effective and efficient way to implement integral activities for supply chain risk management. For an organization working toward an ATO within the NIST Risk Management Framework engaging those suppliers with the IEC 62443-4-1 Certification is a method to reference accomplishment of the SA-12 security control for Supply Chain Management. Ultimately, SCRM serves as a key component of a broader Defense-in-Depth approach to cybersecurity.

 https://doi.org/10.24868/issn.2515-818X.2020.051

4. Defense-in-Depth

Defense-in-Depth is a fundamental philosophy within security. The goal is to create a series of overlapping systems designed to provide security even if one of them fails. Defense-in-Depth within the maritime domain hinges on many of the same best practices found in other realms. The Center for Internet Security (CIS) Top 20 Security Controls and Resources outlines essential elements of this approach. As illustrated in Table 2 below, these form the core for a comprehensive Defense-in-Depth strategy.

Basic CIS Controls
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs
Foundational CIS Controls
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
Organizational CIS Controls
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises[x]

Table 2: CIS Top 20 Security Controls & Resources

Supply chain security stands as a cornerstone in a broader cybersecurity Defense-in-Depth program. The first 3 Basic CIS Controls noted above, 1. Inventory and Control of Hardware Assets, 2. Inventory and Control of Software Assets, and 3. Continuous Vulnerability Management require that vendors ensure all hardware and software components are vetted and verified to be authentic and free of vulnerabilities. Continuous Vulnerability Management operates under the assumption that no system can ever be without errors and vendors, systems integrators, and operators must remain vigilant in watching for potential issues as they are discovered.

In much the same way naval formations are used to defend key assets, as illustrated in Figure 3 below, a cybersecurity approach to Defense-in-Depth should be designed to detect any potential attack as early as possible, frustrate potential attackers and raise the potential cost of an attack beyond a reasonable threshold.

 https://doi.org/10.24868/issn.2515-818X.2020.051

Figure 3: Example of a Defense-in-Depth Approach[xi]

IEC 62443-4-1 aligns well with not only NIST guidance, but also the recent IMO and BIMCO guidelines as outlined below. Leveraging suppliers certified against IEC 62443 provide end users and organizations with a solid framework to assess their risk and make informed decisions on the next steps to address and mitigate any potential residual risks if necessary. Table 3 below helps show the relationship between IEC 62443-4-1 and the emerging maritime cybersecurity requirements.

NIST	IMO	BIMCO	62443-4-1
Identify	Identify	Identify Threats Identify Vulnerabilities Assess Risks	SM-2: Identification of responsibilities SM-3: Identification of applicability SM-9: Security requirements for externally provided components SM-10: Custom developed components from third-party SM-11: Assessing and addressing security-related issues SM-12: Process verification SR-2: Threat model SR-3: Product security requirements
Protect	Protect	Develop Protective Controls	SM-1: Development process SM-4: Security expertise SM-5: Process scoping SM-6: File integrity SM-7: Development environment security SM-8: Controls for private keys SR-3: Product security requirements SR-4: Product security requirements content SR-5: Security requirements review SD-1: Secure design principles SD-2: Defense in depth design SD-3: Security design review SD-4: Secure design best practices SI-1: Security implementation review SI-2: Secure coding standards SVV-1: Security requirements testing SVV-2: Threat mitigation testing SVV-3: Vulnerability testing SVV-4: Penetration testing SVV-5: Independence of testers

 https://doi.org/10.24868/issn.2515-818X.2020.051

			SG-1: Product defense in depth SG-2: Defense in depth measures expected in the environment SG-3: Security hardening guidelines SG-5: Secure operation guidelines SG-6: Account management guidelines SG-7: Documentation review
Detect	Detect	Develop Protective Controls	DM-1: Receiving notifications of security-related issues DM-2: Reviewing security-related issues DM-3: Assessing security-related issues DM-4: Addressing security-related issues DM-5: Disclosing security-related issues DM-6: Periodic review of security defect management practice
Respond	Respond	Respond	SUM-1: Security update qualification SUM-2: Security update documentation SUM-3: Dependent component or operating system security update documentation SUM-4: Security update delivery SUM-5: Timely delivery of security patches
Recover	Recover	Recover	SM-13: Continuous improvement SG-4: Secure disposal guidelines

Table 3: NIST CSF, IMO, BIMCO and IEC 62443-4-1

IEC 62443-4-2 provides additional configurable features and security capabilities from the 7 Foundational Requirements that allow systems integrators and asset owners to further implement security controls identified as necessary during the risk assessment and threat modeling. These features and capabilities allow further integration within the overall Defense-in-Depth strategy. An example of how these configurable features and security capabilities map to NIST 800-53 controls is shown below in Table 4.

Security Controls of NIST SP 800-53 Rev5	**Foundation Requirements (FRs) of IEC 62443-4-2** **FR1 - Identification & Authentication Control**
A-2 Identification and Authentication, CE(5) Individual Authentication, CE(10) Single Sign-On.	CR1.1 Human user Identification & Authentication
AC-3 Access Enforcement. CE(3) Mandatory Access Control. CE(4) Discretionary Access Control. CE(7) Role-Based Access Control. CE(8) Revocation of Access Authorizations. CE(9) Controlled Release. CE(11) Restrict Access to Specific Information. CE(12) Assert and Enforce Application Access. CE(13) Attribute-Based Access Control. IA-3 Device Identification and Authentication. CE(1) Cryptographic Bidirectional Authentication. CE(4) Device Attestation.	CR1.2 Software Process and Device Identification and Authentication
AC-2 Account Management. CE(1) Automated System Account Management. CE(7) Role-Based Schemes. CE(9) Restrictions on use of Shared and Group Accounts. CE(10) Shared and Group Account Credential Change. CE(13) Disable Accounts for High-Risk Individuals. CE(14) Prohibit Specific Account Types. CE(15) Attribute-Based Schemes.	CR1.3 Account Management

Table 4: Example of NIST 800-53 and IEC 62443-4-1 Mapping

 https://doi.org/10.24868/issn.2515-818X.2020.051

5. Conclusion

Cybersecurity risks are growing and the threats facing the maritime domain continue to evolve and become ever more sophisticated. The cornerstone to a broader Defense-in-Depth strategy is establishing a formal Supply Chain Risk Management program. As noted in the CIS Top 20 Controls and Resources, identifying and controlling the hardware and software within an infrastructure while monitoring it for vulnerabilities will comprise most of the various electronics and electrical equipment used for propulsion, electric plant, navigation, life safety, and other primary systems deployed in modern vessels and maritime infrastructure today. Leveraging suppliers who adhere to the IEC/ISO 62443-4-1 Standard and who maintain that standard through 3rd party certification audits allows vessel owners and supporting organizations to address their cybersecurity risks effectively and in a disciplined way. Working from the component level up through to the fully functional shipboard system, if the individual components or products have been developed and sourced following IEC/ISO 62443-4-1 product security development lifecycle requirements and combined with those configurable products that have been certified under IEC/ISO 62443-4-2 meeting the required security levels identified during the security formal risk assessment process, then the cybersecurity posture of the overall shipboard control architecture, be it a commercial vessel or naval ship, will be significantly improved.

Acknowledgements

The views expressed in this paper are that of the authors and do not necessarily represent the views and opinions of Rockwell Automation.

References

[i] Based off the Cyprus Shipping Chamber City Chambers, Limassol, Cyprus, www.csc-cy.org, Version 2.0 – May 2018, p. 10.

[ii] https://trapx.com/anatomy-of-an-attack-1/

[iii] Anatomy of an Attack, Zombie Zero, Weaponized Malware Targets ERP Systems, TrapX Research Labs March 1, 2017

[iv] https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk

[v] https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_004_19.pdf

[vi] Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, September 2018, p. 51.

[vii] NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Jon Boyens, Celia Paulsen, Rama Moorthy, Nadya Bartol, April 2015, p. 7

[viii] Center for Strategic and Budgetary Assessments Report, Strengthening the U.S. Defense Maritime Industrial Base, A Plan to Improve Maritime Industry's Contribution to National Security, Bryan Clark, Timothy A. Walton, Adam Lemon, 2020, p. 58.

[ix] IEC 62443-4-1:2018 © IEC 2018, p. 24.

[x] https://www.cisecurity.org/controls/cis-controls-list/

[xi] Source: https://www.navsea.navy.mil/Home/RMC/SRFJRMC/JapanTours/WhyJapan/SEVENTHFleet/

 https://doi.org/10.24868/issn.2515-818X.2020.051