WHITE PAPER

A Practical Approach to Adopting the IEC 62443 Standards

Felipe Sabino Costa
International Society of Automation (ISA)
Moxa Americas
São Paulo, Brazil
felipe.costa@moxa.com

MOXA®

Abstract

From cybersecurity strategy to technical projects, many companies struggle with how to put theory into practice for industrial control systems (ICS). Although it is difficult to completely cover the full range of the IEC 62443 standards and the related literature, this paper summarizes the key points for the IEC 62443 standards and provides some practical recommendations for Cyber Security Management System (CSMS) development. This paper will also consider the importance of product and company certifications to support asset owners in their journey towards IEC 62443 compliance.

Keywords— Supply Chain Management, Device Security, Defense in Depth, Industrial Intrusion Detection System (IDS), Industrial Intrusion Prevention System (IPS)

Executive Summary

This article will consider different aspects of how the IEC 62443 standard provides a holistic and wide ranging approach to securing industrial control systems. The first step before creating a CSMS is to have the management team's support to ensure the CSMS will have sufficient financial and organizational support to implement necessary actions. Afterwards, a risk assessment should be performed to understand the company risks, respective security levels (SL), and critical assets.

Once the risk and security factors are defined, it is necessary to develop countermeasures to bring the SuC to a level of risk that the company is willing to accept. This comprises different steps and techniques, such as defense in depth and the creation of zones and conduits to provide different levels of protection.

A further step is security monitoring for enhancing network visibility and planning how to respond to incidents. Finally, the human factor and supply chain management aspects should also be considered throughout the CSMS development process.

Released on July 16, 2021

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 71 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA

INTRODUCTION

In general, many companies struggle with how to transform theory into practical actions. These challenges range from 'how to gain the executives' buy-in' for cybersecurity strategy, to 'which technology will better fit their needs', and 'what are the most relevant risks' for technical projects. This article provides guidance on how to perform some key actions recommended by the IEC 62443 standards. Although we are just scratching the surface of this extensive undertaking, this article may help technicians and executives to improve their understanding of the recommendations included in the standard.[5][6]

The series of IEC 62443 standards provide a holistic and wide-ranging approach to securing industrial control systems (ICS). These standards are holistic because they embrace the different structural aspects of security strategy, defined by the International Electrotechnical Commission (IEC) as 'People', 'Processes', and 'Technologies'. In addition, these standards cover a lot of ground because they provide internal and external recommendations to asset owners, supply chain management, and product development teams. For asset owners, the IEC 62443 standard recommends the creation of a Cyber Security Management System (CSMS) that includes analyzing, addressing, monitoring, and improving the system against risks, according to the company's risk appetite. For supply chain management, the specifications recommend security development throughout the product lifecycle. It starts from aspects that include the secure-by-design approach and extends right the way to product manufacturing. The goal is to develop and maintain a reasonable level of security in the products and systems the solution provider offers.[1][2][3][4]

The cyber security management system (CSMS) proposed by the IEC 62443 standards have six main elements:

- Initiating the CSMS program (to provide the information that is required to get support from management).
- High-level risk assessment (identifying and assessing the priority of risks).
- Detailed risk assessment (detailed technical assessment of vulnerabilities).
- Establishing security, organization, and awareness policies.
- Selecting and implementing countermeasures (to lower risk to the organization).
- Maintaining the CSMS (to ensure the CSMS remains effective and supports the organization's goals).[4]

This paper is structured to summarize key takeaways from these elements.

MANAGEMENT SUPPORT

Before starting to consider technical aspects, the first important recommendation from the IEC 62443 standard is to consider the business rational and obtain support from management. In order to obtain support, the company needs to have a clear understanding of the systems, subsystems, and respective components that are essential or critical to operation and safety. Once this has been established, it will be easier to communicate to management the possible consequences if any component is impacted.[4]

Critical Assets

Critical assets include any device that once compromised may generate a high financial, health, safety, or environmental impact to an organization. The list of the company's critical assets forms the basis of the risk management analysis, and will be used to guide further decisions.[18]

Business Rationale

Once the company has identified the critical assets, it is necessary to engage management and get them to commit to invest in the cybersecurity plan that will be developed. Without this support, the plan has a very low chance of success. High-level management should approve and participate in defining the business rationale to ensure the CSMS will have enough resources and support to deploy the necessary changes to the system and throughout the entire organization. In some cases, it is necessary to create a business case or business rationale, as suggested by the IEC 62443 standards to present to the management team. The business case or business rational contains a list of the potential threats and the possible consequences to the business with an estimation of the costs annually, as well as the cost of any countermeasures. This will provide a clear overview of the risks and costs for mitigation to acceptable levels, increasing the chances of obtaining support from management.[4][7][8]

RISK ASSESSMENT

Once the management team is engaged and committed to supporting the CSMS, it is important to perform a risk assessment. Risk assessment is part of the overall risk management strategy of every company and it is a mandatory step in order to create a solid and efficient cybersecurity strategy. It requires correlation and collaboration between many different groups of people within the company. These levels have been defined by the NIST (National Institute of Standards and Technology) as the organization, mission/business processes, and information system (IT and ICS) levels.[11][13]

Risk management aims to assess and understand the different types of risks the company is susceptible to in different areas such as investment, budgeting, legal liability, safety, inventory, and supply chain risks. The focus of this paper will be on the risks to the ICS, which is generally agreed to be one of the greatest potential areas of risk for an organization.[9][10][12]

In order to perform a risk assessment of the ICS, it is necessary to define the scope and boundaries of the system that will be assessed, also known as the System under Consideration (SuC). Once the SuC is defined, it is necessary to systematically identify, analyze the threats and vulnerabilities, and prioritize the risks based on their potential consequences. At the same time, it is also important to define asset criticality and dependencies to the operation.[9]

The risk formula is as follows:[1][2][4]

$Likelihood_{\ Event\_Occurring} = Likelihood_{\ Threat\_Realized} \times Likelihood_{\ Vulnerability\_Exploited}$ [1]

$Risk = Likelihood_{\ Event\_Occurring} \times Consequence$ [2]

There are two different types of risk assessments applicable to ICS: high level and detailed risk assessments. As their names suggest, one approach deals primarily with high-level concepts and the other involves a detailed look at the different types of risk. It is common to perform a high-level risk assessment to support the business rationale and business case, with the latter performing a detailed risk assessment to ensure the system has specific countermeasures included in the design.[4][9][10][13][14]

An expected outcome from this step is to be able to form a comprehensive list of critical assets and determine where connectivity is taking place. The assessment should also be able to identify dependencies, determine what are the critical risks to the operation/safety of these processes and the appropriate responses to these risks, which include the partition of the system into zones and conduits to mitigate risks to levels the company can accept.[15]

DEFENSE IN DEPTH

One of the most common security weaknesses in an ICS is the use of flat networks where there are no internal layers of protection and segregation, allowing all the devices to communicate with each other, even if it is not necessary. This is an undesirable scenario due to different internal and external factors, such as the facilitation of threat propagation (external factor) and communication degradation (internal factor), which both result from a lack of control of the information on the network.[30]

To address this type of problem, upon completing the high-level cybersecurity risk assessment, it is necessary to begin the initial partitioning of the SuC. Each partition is called a zone. The concept of zones is detailed in the next section, but it also forms an important part of the broader concept of the defense-in-depth approach.[18]

Defense in depth is a military concept that provides different levels or layers of protection against a potential attacker or intruder trying to hack the SuC. In the context of a network, the result is different tailored cybersecurity countermeasures deployed throughout the system. Although it is closely linked to technology, defense in depth should also consider other aspects, such as people and processes, as part of its deployment. Some important aspects of defense in depth include, but are not limited to, physical security, ICS network architecture (zones and conduits), ICS network perimeter security (firewalls and jump servers), host or device security, security monitoring, the human element, and vendor management.[10][19]

Establishment of Zones and Conduits

A zone, as part of the defense-in-depth strategy, is a subset of the network communication system where all the communication devices share the same security requirement and consequently are equally critical. It is possible to have a zone inside another zone with different security requirements.

Conduits provide inspection and protection of the communications shared by different zones. Zones and conduits can be established in the physical or logical sense. Lastly, conduits include the concept of a channel, which is a specific link within the conduit that respects the security level of the conduits where it is inserted. All these concepts are intended to achieve uniformity in protection. It should be remembered that each zone is only as secure as its weakest link, therefore, it is highly recommended to isolate the high-risk assets into specific zones.[17]

Security Levels

An important part of the defense-in-depth strategy is to consider countermeasures for zones and internal products. Accordingly, the IEC 62443 standard introduces the concept of security levels (SL) that can be applied to zones, conduits, channels, and products. The security level is defined by researching a particular device, and then determining what level of security it should have, depending on its place in the system. The security levels may be classified into four distinct levels 1 to 4, (although the standard also mentions an "open" level 0 that is rarely used):

- Level 1 is a casual exposure
- Level 2 is an intentional attack with low resources
- Level 3 is an intentional attack with moderate resources
- Level 4 is an intentional attack with extensive resources

Once the security level target of a zone is defined, it is necessary to analyze if the devices inside the zone can meet the corresponding security level. If they do not, it is necessary to plan which countermeasures can help reach the SL target. These countermeasures can be technical (e.g., firewall), administrative (e.g., policies and procedures), or physical (e.g., locked doors).[17]

Protection of Critical Assets

As we discussed earlier, critical assets are essential to the correct operation of the ICS. Any impact on those assets may have a high financial, health, safety, or environmental impact on an organization. Those assets should always have a high priority in the risk assessment and in the company security strategy.

The criticality assessment is one input for the definition of scope and zone protection. This assessment identifies the level of impact that assets have on the organization. Other assessments, such as CARVER (Criticality, Accessibility, Recuperability), from the U.S. Department of Defense (DoD), aim to identify, from an attacker's perspective, which targets could cause the largest impact to businesses. Regardless, it is expected that critical assets have higher security levels with proportional countermeasures that adhere to levels the company can accept. This is one of the reasons why the IEC 62443 standard foresees the use of zones inside zones with different security levels.[9][24][35]

Device Security

The same concept of security levels (SL) is also applied to products. The IEC 62443-4-2 defines the security requirements for four types of components: software application requirements (SAR), embedded device requirements (EDR), host device requirements (HDR), and network device requirements (NDR). There are also seven different perspectives, defined as foundational requirements (FR) for each type of component, including identification and authentication control (IAC), use control (UC), system integrity (SI), data confidentiality (DC), restricted data flow (RDF), timely response to events (TRE), and resource availability (RA). These definitions help asset owners simplify technical specifications and the product selection process ensuring the expected security level is applied to their application, as each security level (SL) has distinct foundational requirements and details that can be tangibly measured and compared.[20]

In order to support organizations audit whether all of above foundational requirements were really deployed on the devices, there are different laboratories, such as ISA Secure, that can certify products that satisfy the requirements of IEC 62443-4-2. These laboratories simplify the selection process for the asset owner, as all they need to do is determine the level of security required and select a certified product that meets that requirement. Consequently, all security features that the organization needs to satisfy the security requirements for the defined SL will be available.[21]

This component level security assurance adds another layer of protection to the system as part of a defense-in-depth strategy, it is known as hardening and facilitates security level zone protection.[22][23]

SECURITY MONITORING FOR ENHANCING VISIBILITY

According to the U.S. Department of Homeland Security, in 2016, the most common threat was ‘unknown’. As it was only possible to manage what is visible, most incidents could not be investigated due a lack of visibility, making it difficult to identify threats, understand how threats pass through defenses, and determine the steps taken to identify the origin of the attack. This is known as forensic analysis and provides important information to asset owners so they can understand how the incident happened and help avoid similar incidents in the future.[36][37][38]

Enhancing visibility requires a proper cybersecurity strategy to continuously monitor the system in order to identify potential threats that passed any defenses that were implemented.[4][24][25][26][27]

The most common solution for monitoring a network is a network intrusion detection system (NIDS), or simply, Intrusion Detection System (IDS). It enhances network visibility through the monitoring of anomalies in network traffic or malicious signatures. Adoption of an IDS facilitates forensic analysis and a response to the incident. To enhance efficiency, any forensic data collected from the IDS and other devices should be synchronized, as this will facilitate proper correlation analysis among the different types of data collected.[10]

It is also necessary to have a proper understanding how to calculate the number of sensors needed, define where to install them, and determine whether a passive or active topology is most suited to each application. Each one of these aspects has advantages and disadvantages that should be evaluated when selecting a monitoring solution.[39][40]

RESPONSE TO INCIDENTS

Although network visibility is important, it is more important to respond to the cybersecurity incidents detected, which requires a cybersecurity incident response plan. In short, cybersecurity incident response planning is the preparation for any negative events that may affect the ICS and how to get back to normal as quickly as possible after the incident occurs. Its main elements include planning, incident prevention, detection, containment, remediation, recovery and restoration, and post incident analysis/forensics. It also requires proper communication paths and to assign respective owners who will conduct forensic analysis for each response.[4][24][25][26][27][41]

One current discussion revolves around whether to use an intrusion prevention system (IPS) inside the ICS to respond to certain types of incidents. An IPS may use different types of technologies, such as signature-based detection (monitors specific events and threats) or anomaly-based detection (monitors changes in trends) to identify a threat and execute pre-approved responses. Although it may vary case by case, a general recommendation for increasing its effectiveness and minimizing false positives if the IPS uses anomaly-based detection is to train the IPS and its algorithm offline first (passively). In this manner, the IPS will learn the network patterns and provide some potential answers that can be validated by the security analyst first, increasing its effectiveness. For example, one of the most common types of attack is denial of service (DoS) that affects the network traffic flow pattern. Due to the deterministic nature of an ICS, these attacks are easily detected and are a good starting point to calibrate the effectiveness of an IPS.[10][31][32]

HUMAN FACTORS, TRAINING, AND SECURITY AWARENESS

When it comes to cybersecurity, the human factor should also be considered. This is a wide and complex topic because humans can insert different vulnerabilities into a system. Social engineering and misconfiguration are common examples, independent of the motivation (intentional and unintentional) and their causes (e.g., fatigue or lack of expertise). It is necessary to implement countermeasures to minimize these risks.[28][29]

For this reason, the IEC 62443 standards specifically recommend all employees receive trainings including about security awareness, which provides them with the information they need to perform their responsibilities in a more secure way, and minimize any risks that can be caused by human error.[4]

SUPPLY CHAIN MANAGEMENT AND SUPPORT

Another important element that spreads across all previously discussed items is the security of the supply chain and solution providers. Suppliers should provide security throughout the product lifecycle, including support, quality control, validation of performance, and vulnerability responses, among other aspects. To support conformity with those aspects, the IEC 62443 standards have a specific subsection, IEC 62443-4-1, to specify the requirements for ensuring 'secure by design' throughout the product lifecycle (i.e., building, maintaining, and discontinuing devices). These requirements are generally associated with the support needed for patch management, policies, procedures, and security communications about known vulnerabilities. Similar to the IEC 62443-4-2 standard for product certification, it is possible to certify that a solution provider is following good security management practices and adheres to tangible criteria in the IEC 62443-4-1 standard simplifying the asset owner's decision-making process.[10][33][34]

CONCLUSION

Although it is now possible to become certified for devices and supply chain management according to the IEC 62443 recommendations, asset owners should still consider to holistically implement the IEC 62443 standards. The IEC 62443 standard brings together several important aspects widely discussed by a global community of subject matter experts (SME). Even though this article considered some important aspects that were presented in a progressive and actionable manner, it is difficult to simplify such an extensive body of information such as the IEC 62443. As a result, it is highly recommended that companies looking to adopt the recommendations of the IEC 62443 standard into their own applications, should consult certified partners and experts as they embark on their IEC 62443 journey.

REFERENCES

[1] IEC "IEC Cyber security Brochure overview," 2018.

[2] R.S.H. Piggin "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security",2013

[3] C.M. Portella, M. Hoeve, F. Hwa., H. Slootweg "Implementing An Isa/Iec-62443 And ISO/IEC-27001 OT Cyber Security Management System At Dutch DSO Enexis", 2019

[4] ANSI/ISA-62443-2-1 "Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program", 2009

[5] M. Doan "Companies Need to Rethink What Cybersecurity Leadership Is", 2019 accessed on May 17th https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is

[6] T. J. Parenty and J. J. Domet "Sizing Up Your Cyberrisks", 2019, accessed on May 17th https://hbr.org/2019/11/sizing-up-your-cyberrisks

[7] H. Elkhannoubi and M. Belaissaoui "Fundamental pillars for an effective cybersecurity strategy", 2015

[8] https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html

[9] ISA/IEC-62443-3-2 "Security for Industrial Automation and Control Systems: Security Risk Assessment and System Design", 2015

[10] U.S. Homeland Security “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”,2016

[11] NIST SP 800-82 Rev. 2 “Guide to Industrial Control Systems (ICS) Security”

[12] FIPS PUB 200 “Minimum Security Requirements for Federal Information and Information Systems”

[13] NIST SP 800-39 “Managing Information Security Risk Organization, Mission, and Information System View”, 2011

[14] A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler and D. Marchese “Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management”, 2017

[15] Office of the Secretary of Defense “Handbook for Self-Assessing Security Vulnerabilities and Risk of Industrial Control Systems on DOD Installations”,2014

[16] NISTIR 8179 “Criticality Analysis Process Model”, 2018

[17] “IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models” 2009

[18] N. Papakonstantinou, J. Linnosmaa, A. Z. Bashir, T. Malm and D. L. V. Bossuyt, "Early Combined Safety - Security Defense in Depth Assessment of Complex Systems," 2020

[19] Idaho National Laboratory “Control Systems Cyber Security: Defense in Depth Strategies”, 2006

[20] ISA/ANSI-62443-4-2 “Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components”, 2018

[21] https://www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification

[22] P. Kwan “Ironshield Best Practices Hardening Foundry Routers & Switches”, 2003

[23] A. Laszka, W. Abbas, Y. Vorobeychik, X. Koutsoukos “Synergistic Security for the Industrial Internet of Things: Integrating Redundancy, Diversity, and Hardening”, 2018

[24] ANSI/ISA-62443-3-3 “Security for industrial automation and control systems Part 3-3: System security requirements and security levels”, 2013

[25] ISO/IEC 27001 “Information technology — Security techniques — Information security management systems — Requirements”, 2013

[26] NIST SP 800-53 Rev 4 “Security and Privacy Controls for Federal Information Systems and Organizations”

[27] CIS Controls, 2019

[28] S. Dekker “The Field Guide to Understanding 'Human Error', 2011

[29] M. Adams, M. Makramalla “Cybersecurity Skills Training: An AttackerCentric Gamified Approach,”, 2015

[30] U.S Homeland Security “Common Cybersecurity Vulnerabilities in Industrial Control Systems”, 2011

[31] E. Nurcan Y., S. Gönen “Attack detection/prevention system against cyber attack in industrial control systems” ,2018

[32] R. Das, V. Menon and T. H. Morris “On the Edge Realtime Intrusion Prevention System for DoS Attack”, 2018

[33] https://www.isasecure.org/en-US/Certification/IEC-62443-SDLA-Certification-(1)

[34] IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements,2018

[35] A. Cook, R. Smith, L. Maglaras and H. Janicke “Measuring the Risk of Cyber Attack in Industrial Control Systems”, 2016

[36] CISA “Incident Response Pie Charts (YIR 2016 Addendum)”, 2016

[37] T. Spyridopoulos, T. Tryfonas, J. May “Incident Analysis & Digital Forensics in SCADA and Industrial Control Systems”, 2013

[38] G. A. P. Rodrigues,R. O. Albuquerque, F. E. G. Deus 1, R. T. Sousa Jr., G. A. Oliveira Júnior, L. J. G. Villalba and T.-H. Kim "Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection", 2017

[39] A. S. Ashoor and Prof. S. Gore "Importance of Intrusion Detection System (IDS)", 2011

[40] U.S Homeland Security "Recommended Practice: Creating Cyber Forensics Plans for Control Systems", 2008

[41] U.S Homeland Security "Developing an Industrial Control Systems Cybersecurity Incident Response Capability", 2009

Disclaimer

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.