IoT Security Maturity Model: 62443
Mappings for Asset Owners and Product Suppliers

An Industry IoT Consortium and ISA Whitepaper

2022-05-05

Authors

Eric Cosman (OIT Concepts), Jim Gilsinn (Dragos), Frederick Hirsch (Upham Security), Pierre Kobes (Kobes Consulting), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft).

Contents

1 Key Concepts 9
1.1 Security Maturity 9
1.1.1 Security Maturity vs. Security Level 10
1.2 SMM Approach Toward Organizing Security Understanding 11
1.2.1 SMM Domains, Subdomains & Practices 11
1.2.2 SMM Comprehensiveness Levels 13
1.2.3 Scope Levels 14
1.3 62443 Standards Series Framework 14
1.3.1 Principal Roles in 62443 16

2 General Mapping Considerations 17
2.1 Ecosystem Participants 17
2.2 Meaning Versus Keywords 18
2.3 System and Operational Integrity 18
2.4 Primary Purposes of Requirements 19
2.5 Trustworthiness 19
2.6 Example of How to Use Mappings 19

3 62443 Standard Mapping Considerations 21
3.1 62443-2-1 Requirements Mapping 21
3.2 62443-2-4 Requirements Mapping 23
3.3 62443-3-3 and 62443-4-2 Requirements Mapping 24
3.4 62443-4-1 Requirements Mapping 26

4 62443 SMM Practice Mappings 27
4.1 Mappings Common to Both Asset Owners and Product Suppliers 27
4.1.1 Security Program Management [Asset Owners and Product Suppliers] (SMM Practice 1) 27
4.1.2 Compliance Management [Asset Owners and Product Suppliers] (SMM Practice 2) 28
4.1.3 Threat Modeling [Asset Owners and Product Suppliers] (SMM Practice 3) 28
4.1.4 Threat Modeling [Asset Owners and Product Suppliers] (SMM Practice 4) 28
4.1.5 Product Supply Chain Risk Management [Asset Owners and Product Suppliers] (SMM Practice 5) 29
4.1.6 Services Third-Party Dependencies Management [Asset Owners and Product Suppliers] (SMM Practice 6) 29
4.1.7 Establishing and Maintaining Identities [Asset Owners and Product Suppliers] (SMM Practice 7) 29
4.1.8 Access Control [Asset Owners and Product Suppliers] (SMM Practice 8) 31
4.1.9 Access Control [Asset Owners and Product Suppliers] (SMM Practice 9) 33
4.1.10 Access Control [Asset Owners and Product Suppliers] (SMM Practice 10) 34
4.1.11 Protection Model and Policy for Data [Asset Owners and Product Suppliers] (SMM Practice 11) 35
4.1.12 Implementation of Data Protection Controls [Asset Owners and Product Suppliers] (SMM Practice 12) 35
4.1.13 Vulnerability Assessment [Asset Owners and Product Suppliers] (SMM Practice 13) 37
4.1.14 Patch Management [Asset Owners and Product Suppliers] (SMM Practice 14) 37

4.1.15 Monitoring Practice [Asset Owners and Product Suppliers] (SMM Practice 15) 38
4.1.16 Situation Awareness and Information Sharing [Asset Owners and Product Suppliers] (SMM Practice 16) 39
4.1.17 Event Detection and Response Plan [Asset Owners and Product Suppliers] (SMM Practice 17) 39
4.1.18 Remediation, Recovery and Continuity of Operations [Asset Owners and Product Suppliers] (SMM Practice 18) 40
4.2 Mappings Unique to Asset Owners 41
4.2.1 Security Program Management [Asset Owners Only] (SMM Practice 1) 41
4.2.2 Compliance Management [Asset Owners Only] (SMM Practice 2) 42
4.2.3 Threat Modeling [Asset Owners Only] (SMM Practice 3) 43
4.2.4 Risk Attitude [Asset Owners Only] (SMM Practice 4) 43
4.2.5 Product Supply Chain Risk Management [Asset Owners Only] (SMM Practice 5) 44
4.2.6 Services Third-Party Dependencies Management [Asset Owners Only] (SMM Practice 6) 45
4.2.7 Establishing and Maintaining Identities [Asset Owners Only] (SMM Practice 7) 47
4.2.8 Access Control [Asset Owners Only] (SMM Practice 8) 48
4.2.9 Asset, Change and Configuration Management [Asset Owners Only] (SMM Practice 9) 50
4.2.10 Physical Protection [Asset Owners Only] (SMM Practice 10) 51
4.2.11 Protection Model and Policy for Data [Asset Owners Only] (SMM Practice 11) 52
4.2.12 Implementation of Data Protection Controls [Asset Owners Only] (SMM Practice 12) 53
4.2.13 Vulnerability Assessment [Asset Owners Only] (SMM Practice 13) 54
4.2.14 Patch Management [Asset Owners Only] (SMM Practice 14) 55
4.2.15 Monitoring Practice [Asset Owners Only] (SMM Practice 15) 56
4.2.16 Situation Awareness and Information Sharing [Asset Owners Only] (SMM Practice 16) 56
4.2.17 Event Detection and Response Plan [Asset Owners Only] (SMM Practice 17) 57
4.2.18 Remediation, Recovery and Continuity of Operations [Asset Owners Only] (SMM Practice 18) 58
4.3 Mappings Unique to Product Suppliers 59
4.3.1 Security Program Management [Product Suppliers Only] (SMM Practice 1) 59
4.3.2 Compliance Management [Product Suppliers Only] (SMM Practice 2) 61
4.3.3 Threat Modeling [Product Suppliers Only] (SMM Practice 3) 61
4.3.4 Risk Attitude [Product Suppliers Only] (SMM Practice 4) 62
4.3.5 Product Supply Chain Risk Management [Product Suppliers Only] (SMM Practice 5) 63
4.3.6 Services Third-Party Dependencies Management [Product Suppliers Only] (SMM Practice 6) 63
4.3.7 Establishing and Maintaining Identities [Product Suppliers Only] (SMM Practice 7) 63
4.3.8 Access Control [Product Suppliers Only] (SMM Practice 8) 64
4.3.9 Asset, Change and Configuration Management [Product Suppliers Only] (SMM Practice 9) 64
4.3.10 Physical Protection [Product Suppliers Only] (SMM Practice 10) 64
4.3.11 Protection Model and Policy for Data [Product Suppliers Only] (SMM Practice 11) 65
4.3.12 Protection Model and Policy for Data [Product Suppliers Only] (SMM Practice 12) 65
4.3.13 Vulnerability Assessment [Product Suppliers Only] (SMM Practice 13) 65
4.3.14 Patch Management [Product Suppliers Only] (SMM Practice 14) 66
4.3.15 Monitoring Practice [Product Suppliers Only] (SMM Practice 15) 66

4.3.16 Situation Awareness and Information Sharing [Product Suppliers Only] (SMM Practice 16) 66
4.3.17 Event Detection and Response Plan [Product Suppliers Only] (SMM Practice 17) 67
4.3.18 Remediation, Recovery and Continuity of Operations [Product Suppliers Only] (SMM Practice 18) 67
Annex A Glossary 68
Annex B References 70
Authors & Legal Notice 71

FIGURES

Figure 1-1: IoT Security maturity model hierarchy. 12
Figure 1-2: ISA/IEC 62443 series of IACS standards and technical reports. 15
Figure 1-3: Principal roles in 62443. 17
Figure 2-1: Standards included in specific mappings for various ecosystem participants. 18
Figure 3-1: Graphical view of elements of a security program (cyber security management system). 22
Figure 3-2: Practices of IEC 62443-4-1. 26

TABLES

Table 4-1: Security program management mappings [asset owners and product suppliers]. 27
Table 4-2: Compliance management mappings [asset owners and product suppliers]. 28
Table 4-3: Threat modeling mappings [asset owners and product suppliers]. 28
Table 4-4: Risk attitude mappings [asset owners and product suppliers]. 28
Table 4-5: Product supply chain risk management mappings [asset owners and product suppliers]. 29
Table 4-6: Services third-party dependencies management mappings [asset owners and product suppliers]. 29
Table 4-7: Establishing and maintaining identities mappings [asset owners and product suppliers]. 30
Table 4-8: Access control mappings [asset owners and product suppliers]. 33
Table 4-9: Asset, change and configuration management mappings [asset owners and product suppliers]. 33
Table 4-10: Physical protection mappings [asset owners and product suppliers]. 34
Table 4-11: Protection model and policy for data mappings [asset owners and product suppliers]. 35

Table 4-12: Implementation of data protection controls mappings [asset owners and product suppliers]. 37
Table 4-13: Vulnerability assessment mappings [asset owners and product suppliers]. 37
Table 4-14: Patch management mappings [asset owners and product suppliers]. 38
Table 4-15: Monitoring practice mappings [asset owners and product suppliers]. 39
Table 4-16: Situation awareness and information sharing mappings [asset owners and product suppliers]. 39
Table 4-17: Event detection and response plan mappings [asset owners and product suppliers]. 40
Table 4-18: Remediation, recovery and continuity of operations mappings [asset owners and product suppliers]. 40
Table 4-19: Security program management mappings [asset owners only]. 42
Table 4-20: Compliance management mappings [asset owners only]. 42
Table 4-21: Threat modeling mappings [asset owners only]. 43
Table 4-22: Risk attitude mappings [asset owners only]. 44
Table 4-23: Product supply chain risk management mappings [asset owners only]. 45
Table 4-24: Services third-party dependencies management mappings [asset owners only]. 45
Table 4-25: Establishing and maintaining identities mappings [asset owners only]. 47
Table 4-26: Access control mappings [asset owners only]. 49
Table 4-27: Asset, change and configuration management mappings [asset owners only]. 51
Table 4-28: Physical protection mappings [asset owners only]. 52
Table 4-29: Protection model and policy for data mappings [asset owners only]. 52
Table 4-30: Implementation of data protection controls mappings [asset owners only]. 53
Table 4-31: Vulnerability assessment mappings [asset owners only]. 54
Table 4-32: Patch management mappings [asset owners only]. 55
Table 4-33: Monitoring practice mappings [asset owners only]. 56
Table 4-34: Situation awareness and information sharing mappings [asset owners only]. 57
Table 4-35: Event detection and response plan mappings [asset owners only]. 58
Table 4-36: Remediation, recovery and continuity of operations mappings [asset owners only]. 59
Table 4-37: Security program management mappings [product suppliers only]. 61
Table 4-38: Compliance management mappings [product suppliers only]. 61
Table 4-39: Threat modeling mappings [product suppliers only]. 62

Table 4-40: Risk attitude mappings [product suppliers only].....62
Table 4-41: Product supply chain risk management mappings [product suppliers only]. 63
Table 4-42: Services third-party dependencies management mappings [product suppliers only]. 63
Table 4-43: Establishing and maintaining identities mappings [product suppliers only]. 64
Table 4-44: Access control mappings [product suppliers only].....64
Table 4-45: Asset, change and configuration management mappings [product suppliers only]. 64
Table 4-46: Physical protection mappings [product suppliers only]. 64
Table 4-47: Protection model and policy for data mappings [product suppliers only]. 65
Table 4-48: Implementation of data protection controls mappings [product suppliers only]. 65
Table 4-49: Vulnerability assessment mappings [product suppliers only].....66
Table 4-50: Patch management mappings [product suppliers only]. 66
Table 4-51: Monitoring practice mappings [product suppliers only].....66
Table 4-52: Situation awareness and information sharing mappings [product suppliers only]. 67
Table 4-53: Event detection and response plan mappings [product suppliers only].....67
Table 4-54: Remediation, recovery and continuity of operations mappings [product suppliers only]. 67

This document is intended for asset owners and product suppliers who wish to improve the security maturity of their organization. The IoT Security Maturity Model (SMM)[1] provides a detailed model and approach for achieving a good fit of security governance, technology and operations to meet business needs.

For asset owners, the scope of the SMM is the organization responsible for the operational technology (OT) environment, especially industrial automation and control systems (IACS) in a variety of industries, including manufacturing, utilities such as electricity, water and gas, transportation systems and building systems. We provide a way to relate the detailed guidance in 62443-2-1,[2] 62443-3-3,[3] and 62443-4-2[4] with SMM practices and comprehensiveness levels. We provide guidance on relating 62443-2-4[5] with SMM, for support to be expected by service providers for integration and maintenance as well as relating 62443-4-1[6] with SMM for support to be expected by product suppliers, making it easier for asset owners to address gaps in their security maturity.

For product suppliers, the scope of the SMM is the organization responsible for the development of the products. We provide a way to relate the detailed guidance in 62443-3-3 and 62443-4-2 with SMM practices and comprehensiveness levels. We also provide guidance on relating the product development lifecycle process practices of 62443-4-1 with SMM, making it easier for product suppliers to address gaps in their security maturity.

This document is a joint effort between the Industry IoT Consortium (IIC) SMM authors, the ISA GCA and ISA99 Committee. Each requirement and requirement enhancement of the 62443-2-1, 3-3, 4-2, 2-4 and 4-1 standards was examined to relate it to the IIC Security Maturity Model. This document summarizes the results, enabling asset owners to relate these documents more easily.

This is one of a number of anticipated mapping documents to relate various 62443 requirements with SMM practices for various 62443 roles, such as asset owner, product supplier and service providers for integration or maintenance. Details about these roles are provided in section 1.5.

Different mapping tables will be provided for different roles since both the relevant 62443 standards and specific requirements from specific 62443 standards may differ for different role mappings.

There is no simple generic solution that can address security needs for every system. Organizations have differing needs, and different systems need different strengths of protection

[1] [IIC-SMMP2020]
[2] [IEC 62443-2-1]
[3] [IEC 62443-3-3]
[4] [IEC 62443-4-2]
[5] [IEC 62443-2-4]
[6] [IEC 62443-4-1]

mechanisms. The same technology can be applied in different ways and to different degrees, depending on needs. The SMM helps organizations determine priorities to drive their security enhancements. The security maturity reflects the proper fit of their choices to their needs.

The security maturity model fosters effective and productive collaboration among business and technical stakeholders. Business decision makers, business risk managers and owners of IoT systems, concerned about proper strategy for implementing security practices with the appropriate maturity, can collaborate with analysts, architects, developers, system integrators and other stakeholders who are responsible for the technical implementation.

To drive proper investment, the IoT Security Maturity Model includes both organizational and technological components. Organizations use the model to set their maturity target, understand their current maturity and determine what they need to do to move to a higher maturity state.

The mappings with the IoT SMM may be used in the following, probably non-exhaustive scenarios.

Security maturity target refinement: Assume we have the established security maturity target for the system under consideration. Using the mapping tables defined below, it is possible to set up more concrete requirements on the practice implementation (what needs to be done) and concrete indicators of achievement. To do so, the indicators of achievement for the SMM target comprehensiveness and lower levels should be compared side-by-side with the requirements mapped to these levels. The 62443 requirements refining the common requirements for the comprehensiveness should be documented in the security maturity target. The gap between the 62443 requirements to comprehensiveness must be also examined and the remaining requirements must be written down.

Using the IEC 62443 assessment or certification results as the additional factor for security maturity assessment: Though the security level assessed for the system does not represent the direct metric for security maturity, the separate 62443-3-3 and 62443-4-2 requirements may be used as indirect evidence for the assessment of comprehensiveness levels during security maturity assessment. To implement this scenario, one should consider the 62443 security level assigned to a system, note the associated 62443-3-3 and 62443-4-2 requirements, find them in the mapping tables, and assess the system for the appropriate comprehensiveness levels first.

Using the security maturity assessment results as input for assessment for IEC 62443: Similarly, assessment for security maturity may be used as input for 62443 assessments. To implement this scenario, one should consider the comprehensiveness levels assigned to the current security maturity state of a system, write down the 62443-3-3 and 62443-4-2 requirements associated with practices comprehensiveness levels in the mapping tables and assess whether the system implements these 62443-3-3 and 62443-4-2 requirements. This may be also used as an additional check for the validity of security maturity assessment results.

The requirements of 62443-2-4 and 62443-4-1 are not directly mapped to SMM comprehensiveness levels. The requirements of 62443-2-4 should be used by asset owners for assessing the expected support from service providers for the asset owner to achieve certain SMM comprehensiveness levels. In the same way, the requirements of 62443-4-1 should be used by asset owners for assessing the expected support from product suppliers.

1 KEY CONCEPTS

1.1 SECURITY MATURITY

Security maturity is about effectiveness, not the use of security mechanisms to achieve arbitrary security levels. The SMM aligns the comprehensiveness (degree of depth, consistency and assurance of security measures) and scope (degree of fit to the industry or system needs) of security needs with the investment in appropriate practices.

Not all systems require the same strength of security mechanisms and procedures to meet their security maturity targets. The organization's leadership determines the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementations of security mechanisms and processes are considered *mature* if they are expected to be effective in addressing those goals. It is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the maturity. The SMM defines *security maturity* as the degree of confidence that the current security state meets all organizational security needs and all organizational security-related requirements. Security maturity is a measure of the understanding of the overall current security approach including people, processes and technology including its necessity, benefits and cost to support. Contributing factors include the specific threats to an organization's industry vertical, safety, regulatory, ethical and compliance requirements, the organization's threat profile and the unique risks present in an environment.

The 62443 series of standards also have a concept of maturity, focused on the maturity of the security program and processes. The 62443 maturity levels are based on the Capability Maturity Model Integration (CMMI) for Development (CMMI-DEV)[7] and Services (CMMI-SVC)[8] standard. This maturity approach can be aligned with the SMM maturity model that includes technology and operations, rather than the processes alone.

[7] [IEC 62443-4-1]

[8] In particular [IEC 62443-2-4]

1.1.1 SECURITY MATURITY VS. SECURITY LEVEL

Security level,[9] such as the one used in the 62443 standard is a measure of the strength of a security measure (e.g. stronger cryptography) while security maturity is about the level of understanding of the need and confidence in appropriate corresponding implementation. Increasing security levels relate to increasing security threats and corresponding risk-reduction ability. The SMM does not say what the appropriate security level should be. Rather, it provides guidance and structure for organizations to select the maturity appropriate for their industry and system. The notion of security level must not be confused with security maturity. However, achieving an appropriate 62443 security level can contribute to achieving the needed system maturity.

The 62443 series is evolving to include the concept of *security protection rating,* which is a "security rating combining the evaluation of the technical security measures in the automation solution and process measures for operating and maintaining the automation solution." This is relevant to the IoT Security Maturity Model but is focused on the measure of the level of protection including operations and maintenance—a more detailed view of the quality of a control.

Organizations are interested in finding out if their IoT solutions are secure, and how to protect them to meet their needs. A maturity model helps organizations understand how to match their security investment with their goals and needs, while a security requirement framework identifies what mechanisms are available and can be applied to reach certain levels of security.

Mapping the SMM[10] with the 62443[11] requirement framework for industrial automation and control systems is useful to enable 62443 requirements to be related to SMM target setting and assessment. If you determine that you need to achieve an SMM comprehensiveness level 3 for your identity management capability, such a mapping then allows you to identify the appropriate security measures that you can apply to achieve this comprehensiveness level. Since you need to also apply the mechanisms of comprehensiveness levels 1 and 2 to reach level 3, this provides a clear roadmap of what investment in technologies and processes must be made, and which ones must work together to achieve the business requirements.

This document presents a high-level introduction to the IoT Security Maturity Model, the 62443 standard, a mapping between the IoT SMM practices and levels and the 62443 requirements.

[9] According to [IEC 62443-3-3]

[10] [IIC-SMMD2020], [IIC-SMMP2020], [IIC-SMMRP2020]

[11] All mentions of 62443 refer to the published IEC 62443 International Standards in this document.

1.2 SMM Approach Toward Organizing Security Understanding

The SMM provides a means to set maturity targets and perform assessments to manage security efforts better. The 62443 standards offer requirements that can be used to achieve specific SMM comprehensiveness levels for practices. Used together the two offer an approach toward achieving a suitable security approach.

1.2.1 SMM Domains, Subdomains & Practices

The domains of governance, enablement and hardening determine the priorities of security maturity enhancements at the strategic level.

Governance is the "establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization."[12] *Governance* influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation. The culture of the organization is reflected in the governance and the degree of importance placed on security.

Enablement is the implementation of security mechanisms and procedures needed to create a system meeting the policy and operational requirements. Enablement uses architectural design to address business risks and specific practices to enable operations.

Hardening is the use of security practices during system operation. This includes identifying ongoing risks through situational awareness, monitoring system operation and managing change of the system (e.g. patching).

When planning, different priorities can be placed on the different domains and subdomains based on risk analysis and other factors. Business stakeholder conversations and decisions can focus at this level without going into the details of the practices. Subsequent implementation will use the practices based on these priorities. The domains and subdomains also serve to organize the practices logically, making clear where different alternatives may be used to address requirements of a given domain or subdomain. Domains and subdomains make clear various perspectives. Figure 1-1 displays the hierarchy of domains and associated subdomains and practices.

The model has been designed to be extensible and provides the ability to add new domains, subdomains and practices in the future.

[12] [IIC-SMMP2020]

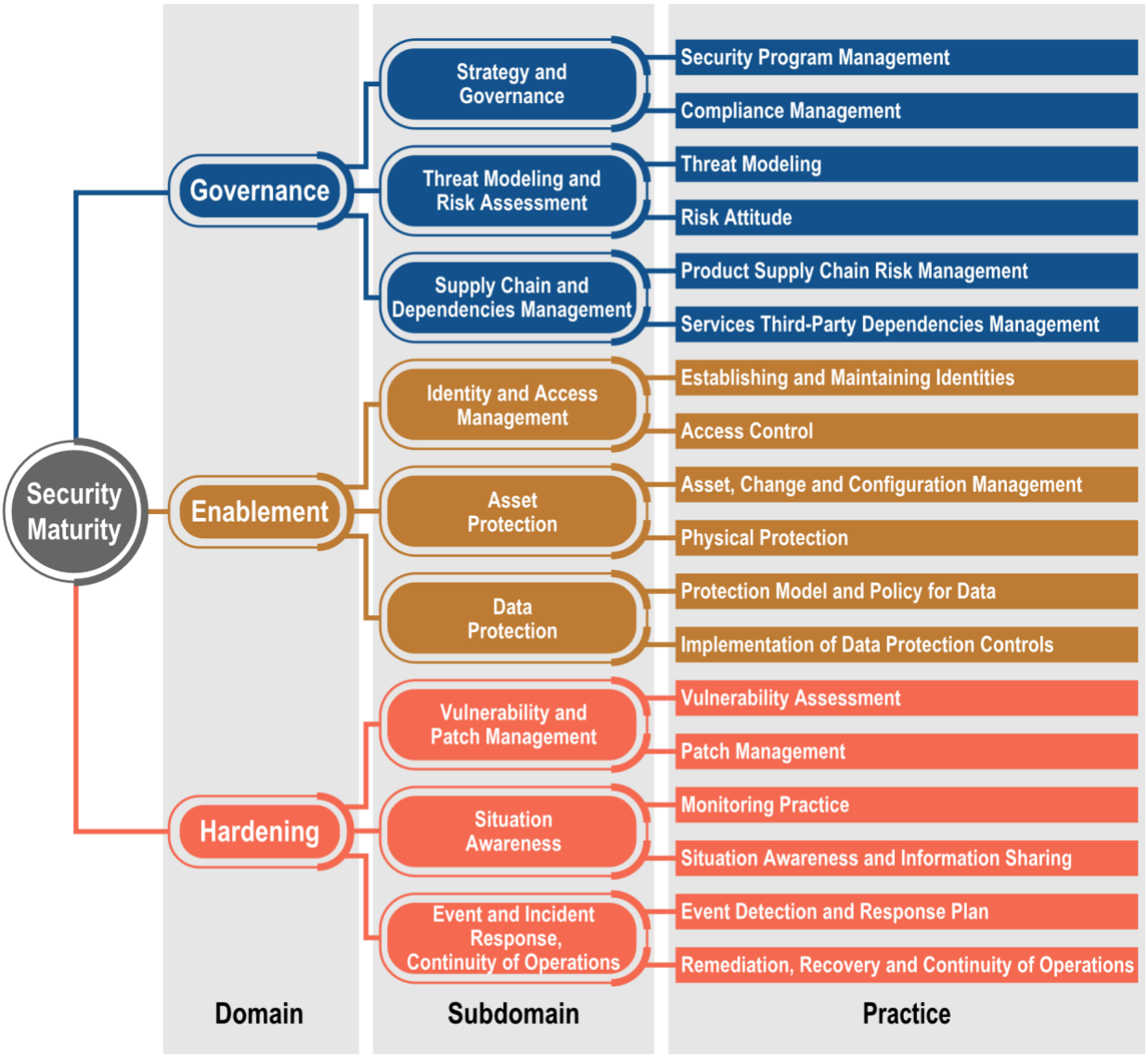

Figure 1-1: IoT Security maturity model hierarchy.

There are two orthogonal dimensions to the evaluation of the security maturity: comprehensiveness and scope. *Comprehensiveness* captures the degree of depth, consistency and assurance of security practices. Use of comprehensiveness in this model reduces complexity by considering different aspects together such as organizational security awareness, degree of implementation of practices, and assurance of the practices (and their evolution). For example, a higher level of comprehensiveness of threat modeling implies a more automated, systematic, and extensive approach.

Scope reflects the degree of fit to the industry or system needs. This captures the degree of customization of the security measures that support security maturity domains, sub domains or practices. Such customizations are typically required to address industry- or system-specific constraints of the IoT system.

Comprehensiveness and scope help manage and prioritize security maturity practices. Certain systems may not require certain practices at all, yet this can still reflect a high level of security maturity when that decision is appropriate. Avoiding unnecessary mechanisms reduces costs and lowers complexity, which will reduce risks. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

1.2.2 SMM Comprehensiveness Levels

There are five SMM comprehensiveness levels for every security domain, subdomain and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones. The overall maturity of an organization's approach to IoT security is based on how well the assessed comprehensiveness levels of the SMM practices match the SMM comprehensiveness level targets for those practices. An organization is not more mature with higher comprehensiveness levels since higher levels may not be appropriate to the need, but rather for the fit. Thus the concepts of achieving maturity by meeting requirements is similar to maturity levels in 62443, but higher comprehensiveness levels do not mean more maturity as is the case with maturity levels in 62443.[13]

Level 0, None: There is no common understanding of how the security practice is applied and no related requirements are implemented (as this level has no assurance or practices applied, we do not discuss it further).

Level 1, Minimum: The minimum requirements of the security practice are implemented. There are no assurance activities for the security practice implementation.

Level 2, Ad hoc: The requirements for the practice cover main use cases and well-known security incidents in similar environments. The requirements increase accuracy and level of granularity for the environment under consideration. The assurance measures support ad hoc reviews of the practice implementation to ensure baseline mitigations for known risks. For this assurance, one may apply measures learned through successful references.

Level 3, Consistent: The requirements consider best practices, standards, regulations, classifications, software and other tools. The tools establish a consistent approach to practice deployment. The assurance of the implementation validates the implementation against security patterns, design with security in mind from the beginning and known protection approaches and mechanisms. This includes creating a system with the security design considered in the architecture and design as well as definition defaults.

Level 4, Formalized: A well-established process forms the basis for practice implementation, providing continuous support and security enhancements. The assurance of the implementation

[13] [IEC 62443-4-1]

focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. This assurance uses semi-formal to formal methods.

1.2.3 SCOPE LEVELS

There are three levels of scope for every security domain, subdomain and practice, from Level 1 to Level 3, with higher numbers indicating a narrower and more specific scope.

Level 1, General: This is the broadest scope. The security practice is implemented in the computer systems and networks without any assessment of its relevance to the specific sector, equipment used, software or processes to be maintained. The security capabilities and techniques are applied as they were in the typical environment.

Level 2, Industry specific: The scope is narrowed from the general case to an industry-specific scenario. The security practice is implemented considering sector-specific issues, particularly those regarding components and processes that are prone to certain types of attacks and known vulnerabilities and incidents that have taken place.

Level 3, System specific: This is the narrowest scope. The security practice implementation is aligned with the specific organizational needs and risks of the system under consideration, identified trust boundaries, components, technologies, processes and usage scenarios.

As we mentioned previously, mappings enable aligning SMM practices with other frameworks and guidance for detailed understanding on addressing gaps discovered when performing an SMM assessment against an SMM target.

1.3 62443 STANDARDS SERIES FRAMEWORK

The 62443 standards are a series of standards that also provide structure to the security space, covering key concepts, security management systems and process, risk assessment, security program requirements, system security requirements, product life cycle requirements and more.

The 62443-3-3 standard notes: “The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. The IACS community audience for this standard is intended to be asset owners, service providers for integration or maintenance, product suppliers and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.”[14]

The translations of the standards from this series have been adopted in multiple countries as national standards. In some other countries the process of adoption is in progress.

[14] Quoted from [IEC 62443-3-3].

The wide-ranging structure of the 62443 series of standards and reports currently includes fourteen standards and technical reports, each addressing a specific aspect of the subject. Figure 1-2 below shows standards and technical reports that make up the current 62443 series.

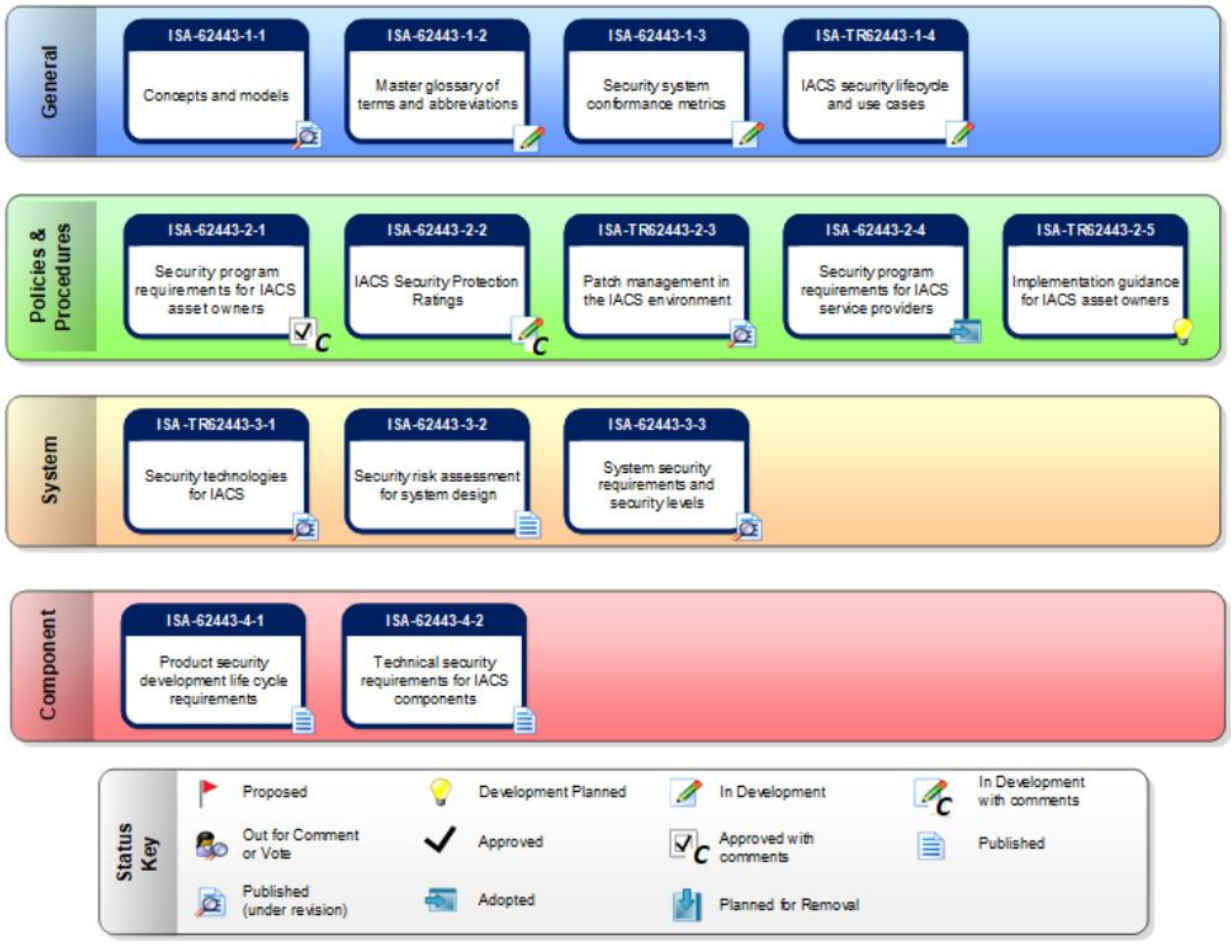

Figure 1-2: ISA/IEC 62443 series of IACS standards and technical reports[15].

The 62443 series of standards is a joint development by the ISA99 committee[16] and IEC Technical Committee 65 Working Group 10.[17] It is intended to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). Documents in this series of standards are named in the form ISA-62443-x-y for the ISA versions and IEC 62443-x-y (where x and y refer to a specific document, e.g. 62443-3-3). The ISA and IEC versions of each document are released as closely together as possible. For simplicity we typically refer to the series as "ISA/IEC 62443" or simply "62443". Here, we refer to each specification as "62443-x-y".

[15] Taken from *https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99* on February 2022

[16] Search for 62443 at International Society of Automation standards page: *https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order*

[17] *http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:2612,25*

1.3.1 PRINCIPAL ROLES IN 62443

To understand the processes that make up a cybersecurity management system fully it is necessary to understand the roles involved in executing them.

A role is responsible for fulfilling certain activities and is held accountable for doing so. A role may be executed by an individual or a legal entity, such as a company or government agency, or a subdivision of the legal entity, such as a department.

An organization can fulfill one or several roles. For example, it is not unusual that the same company is responsible for the operation of an IACS as well as for the design, implementation and validation of the solution. Alternatively, a role can be fulfilled by one or several organizations. For example, the maintenance activities can be performed by different organizations.

The development, operation and maintenance of a comprehensive protection scheme for an IACS in operation requires the contribution and collaboration of all involved actors according to their role. Figure 1-3 gives an overview of the roles defined in 62443.

The *asset owner* is accountable for the IACS including its cybersecurity posture and the associated risks throughout the life cycle. The asset owner also defines the acceptable residual cybersecurity risk as an input requirement for all activities along the IACS life cycle. While remaining accountable, the organization fulfilling this role may delegate specific responsibilities and the associated activities to organizations fulfilling other roles. The asset owner is also responsible for the operation of the IACS. In many cases the company that operates the IACS is also the legal owner and is accountable for the IACS. In this case the accountable role belongs to the business management and responsibility for operation is with the production department of the company.

The *integration service provider* for the IACS is responsible for the design, deployment, commissioning and validation of its security measures. The activities cover the development and validation of a security protection scheme for the IACS to match the acceptable residual cybersecurity risk. These include the development of technical measures of the automation solution and guidelines for organizational measures to be implemented during operation and maintenance. It is common for one organization to design and deploy parts of the automation solution while another is responsible for its commissioning and validation.

The *maintenance service provider* for the IACS is responsible for its maintenance and decommissioning. The maintenance activities are performed on a regular schedule of scheduled maintenance, and when needed due to changes of the operational requirements or the threat environment. This role also has the responsibility for decommissioning parts or the whole automation solution. Measures to match the acceptable residual cybersecurity risk during decommissioning typically include active purging of sensitive data.

The *product supplier* is responsible for the development and support of products used in the IACS. The activities include the development and deployment of security capabilities. The product

supplier is responsible for supplying integration and hardening guidelines and for establishing a process for incident handling and vulnerability management applied to its products.

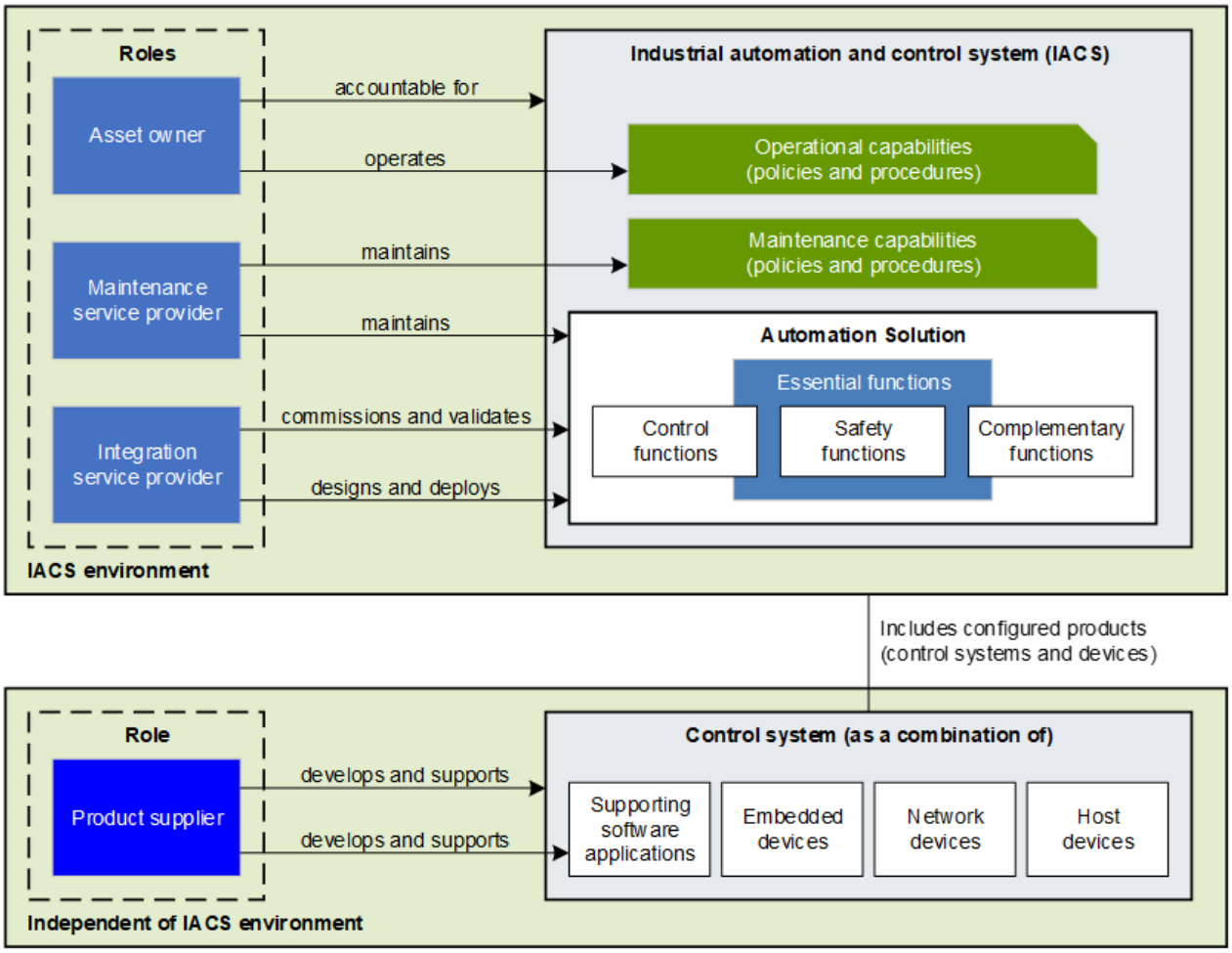

Figure 1-3: Principal roles in 62443.

2 General Mapping Considerations

2.1 Ecosystem Participants

The 62443 standards are designed to support participants in the IACS ecosystem to ensure that all aspects of the system are considered from a holistic security perspective. The asset owners who operate control systems have operational requirements (62443-2-1 Ed 1), the product suppliers have requirements for the security capabilities of system and component products (62443-3-3 and 62443-4-2) and the product development lifecycle process (62443-4-1). The system integrators have requirements for the development of solutions (62443-2-4, 62443-3-2) and the solution itself has requirements that all parties must consider (62443-3-3).

Given the importance of making the requirements and maturity analysis actionable for various ecosystem participants, it makes sense to orient the SMM 62443 mappings to the specific parties,

as shown in Figure 2-1. A mapping document for a product supplier, for example, will need to consider the mapping of 62443 requirements directly affecting the product development life cycle (62443-4-1) and those of the security capabilities of the products (62443-3-3 and 62443-4-2). The overall roadmap of 62443 SMM Mappings can be visualized as follows:

Ecosystem Participant / Mapped Specifications	62443-2-1	62443-2-4	62443-3-3	62443-4-1	62443-4-2
Asset Owner	X	#	X	#	X
Product Supplier			X	#	X

Figure 2-1: Standards included in specific mappings for various ecosystem participants.

This table has an X for 62443 standards that have requirements directly mapped to SMM comprehensiveness levels, and a # for items in 62443 standards that have requirements that should be considered to achieve certain SMM comprehensiveness levels but are not directly mapped (e.g. checklists that can aid in achieving SMM comprehensiveness levels). 62443-4-1 specifies process requirements for the secure development of products used in IACSs. This can contribute to the confidence that the asset owner has in those products and contribute to the SMM comprehensiveness levels the asset owner can achieve. Similarly, 62443-2-4 specifies integration or maintenance service provider requirements that can affect the asset owner.

2.2 Meaning Versus Keywords

The mapping of 62443 to the SMM comprises matching 62443 requirements with SMM comprehensiveness levels for security practices. A given 62443 requirement may map to more than one practice, or may map to none, as shown in the detailed tables below. All mappings are a judgment call based on interpretation of both the 62443 standards language and the SMM practice tables, specifically the purpose of the SMM practices, the actions needed, and the indicators of accomplishment.

Mappings are related by purpose and intent, not keywords in descriptions. For example, 62443-3-3 SR 1.13 “Access via untrusted networks” says “The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks”. Despite the use of the word “monitoring” this is not mapped to the SMM monitoring practice since the use of the word monitoring in the description of SR 1.13 relates to monitoring protocols to control access, not monitoring *per se*. That said, this information could be used to enhance monitoring and intrusion protection if implemented to do so, but this is not a direct mapping.

2.3 System and Operational Integrity

Integrity is important to IACS systems, including system integrity, data integrity and integrity of operations.

The SMM does not have a dedicated practice devoted to integrity since integrity is related to practices in the SMM governance, enablement and hardening domains. For example, system and operational integrity depends on policies, supply chain and third-party dependency management (governance domain), data protection, proper configuration (possibly including boot process integrity) and access control (enablement domain), and patch management with secure updates (hardening domain).

Mappings are placed in the appropriate SMM practice tables and may appear in more than one table. In some case mappings were placed in the data protection practice even though they could be generalized beyond data when their focus is on preserving integrity and they don't apply to other practices.

2.4 Primary Purposes of Requirements

The following example illustrates the mapping approach based on the primary purposes of the requirements. The mapping of 62443-3-3 SR 2.3 RE 1, "Enforcement of security status of portable and mobile devices" requires some discussion. We placed this as a level 2 Access Control mapping, since this requirement serves to control access from portable devices depending on their status. The need to check status and configuration before attempting to connect to system, e.g. for connecting a notebook, is important to avoid introducing malware into the system. The key purpose is access control. Despite this primary purpose, the requirement is also relevant to configuration management since devices must be configured properly to support access control. It can also be considered relevant to vulnerability management, since it serves to reduce vulnerabilities based on inadequate access control. We have recorded these as mappings in the access control table.

2.5 Trustworthiness

The SMM is focused on security and does not directly address other aspects of trustworthiness such as safety, reliability, resilience and privacy; the mapping of trustworthiness related 62443 requirements in this document is limited to how they relate to security. Despite this, a system assessment should consider trustworthiness characteristics and include verification and validation (V&V) considerations and general availability concerns (beyond the security denial-of-service concept).

2.6 Example of How to Use Mappings

One approach to using these mappings is to first determine the target comprehensiveness level required for an SMM practice for a specific 62443 role, such as an asset owner. This is done as discussed in the SMM practitioner's guide, with the role providing the context for the analysis. Once this SMM target is determined then the corresponding mapping tables in this document can be used to understand 62443 requirements that may be used to achieve that level.

As an example, consider using the SMM for the asset owner role. If the SMM target setting results in setting a target of comprehensiveness level 3 for the compliance management practice, then this mapping document can provide guidance on how to meet that target. Achieving comprehensiveness level 3 will require achieving comprehensiveness levels 1-3 since all lower levels must also be achieved to achieve a specific level.

Guidance in the 62443 requirements is provided in the mapping table *Compliance Management for Asset Owners and Product Suppliers* as well as the additional table *Compliance Management for Asset Owners,* which offers additional guidance specific to asset owners.

From the compliance mapping table applicable to both asset owners and product suppliers we see that to achieve level 3 the following requirements must be met (there are no level 2 mapped requirements in this mapping table):

- From Level 3 mapping: SR 3.3 RE 1 (62443-3-3) Automated mechanisms for security functionality verification.
- From Level 1 mapping: SR 3.3 (62443-3-3) Security functionality verification.
- From Level 1 mapping: CR 3.3 (62443-4-2) Security functionality verification.

From the additional compliance mapping table applicable only to asset owners we see that to achieve level 3 the following requirements must be met (there are no level 1 mapped requirements in this mapping table):

- From Level 3 mapping: 4.4.2.1 (62443-2-1 Ed 1) Specify the methodology of the audit process.
- From Level 3 mapping: 4.4.3.7 (62443-2-1 Ed 1) Monitor and evaluate applicable legislation relevant to cyber security.
- From Level 2 mapping: 4.3.2.6.4 (62443-2-1 Ed 1) Define cyber security policy and procedure compliance requirements.
- From Level 2 mapping: 4.4.2.4 (62443-2-1 Ed 1) Establish a document audit trail.
- From Level 2 mapping: 4.4.2.5 (62443-2-1 Ed 1) Define punitive measures for non-conformance.
- From Level 2 mapping: 4.4.2.6 (62443-2-1 Ed 1) Ensure auditors' competence.

We also see that there is a list of 62443-2-4 requirements that are relevant for an asset owner evaluating whether or not a specific service provider's security program includes the capabilities that the asset owner needs for this Security Maturity Model practice and whether they should be requested by the asset owner:

- SP.01.02 (62443-2-4) Solution staffing / Training / Security requirements - asset owner.

- SP.01.02 RE 1 (62443-2-4) Solution staffing / Training / Security requirements - asset owner.
- SP.01.03 (62443-2-4) Solution staffing / Training / Sensitive data.
- SP.01.03 RE 1 (62443-2-4) Solution staffing / Training / Sensitive data.

Thus to achieve compliance comprehensiveness level 3 the asset owner should consider the following 62443 requirements:

- 62443-2-1 Ed 1: 4.3.2.6.4, 4.4.2.1, 4.4.2.4, 4.4.2.5, 4.4.2.6, 4.4.3.7.
- 62443-3-3: SR 3.3, SR 3.3 RE 1.
- 62443-4-2: CR 3.3.

Capabilities of service providers, which are also relevant:

- 62443-2-4: SP.01.02, SP.01.02 RE 1, SP.01.03, SP.01.03 RE 1.

3 62443 Standard Mapping Considerations

The following tables add the industry and device scope to the general SMM considerations as appropriate.

3.1 62443-2-1 Requirements Mapping

For asset owners the SMM addresses organizations responsible for the OT environment, especially industrial automation and control systems (IACS). 62443-2-1 provides requirements on how the asset owner should manage processes, practices and personnel as part of the asset owner's security program, also known as "cybersecurity management system" (CSMS). 62443-2-1 is not mapped for the product supplier.

IEC 62443-2-1: 2010 defines the elements necessary to establish a security program for IACSs and provides guidance on how to develop them. The standard uses the broad definition and scope of what constitutes an IACS.

The elements of a security program are policy, procedure, practice and personnel related, describing what shall or should be included in the security program for the organization.

The 62443-2-1 guidance provided on how to develop a security program is an example. It is a general view on how an organization could go about developing the elements and may not work in all situations. The users of the standard will have to read the requirements carefully and apply the guidance appropriately to develop a fully functioning CSMS for an organization. The policies and procedures discussed in the standard should be tailored to fit within the organization.

The elements are presented in the following three main categories:

- risk analysis,
- addressing risk and
- monitoring and improving the security program.

Each of these categories is further divided into element groups or elements. Figure 3-1 depicts the relationship between the categories, element groups and elements.

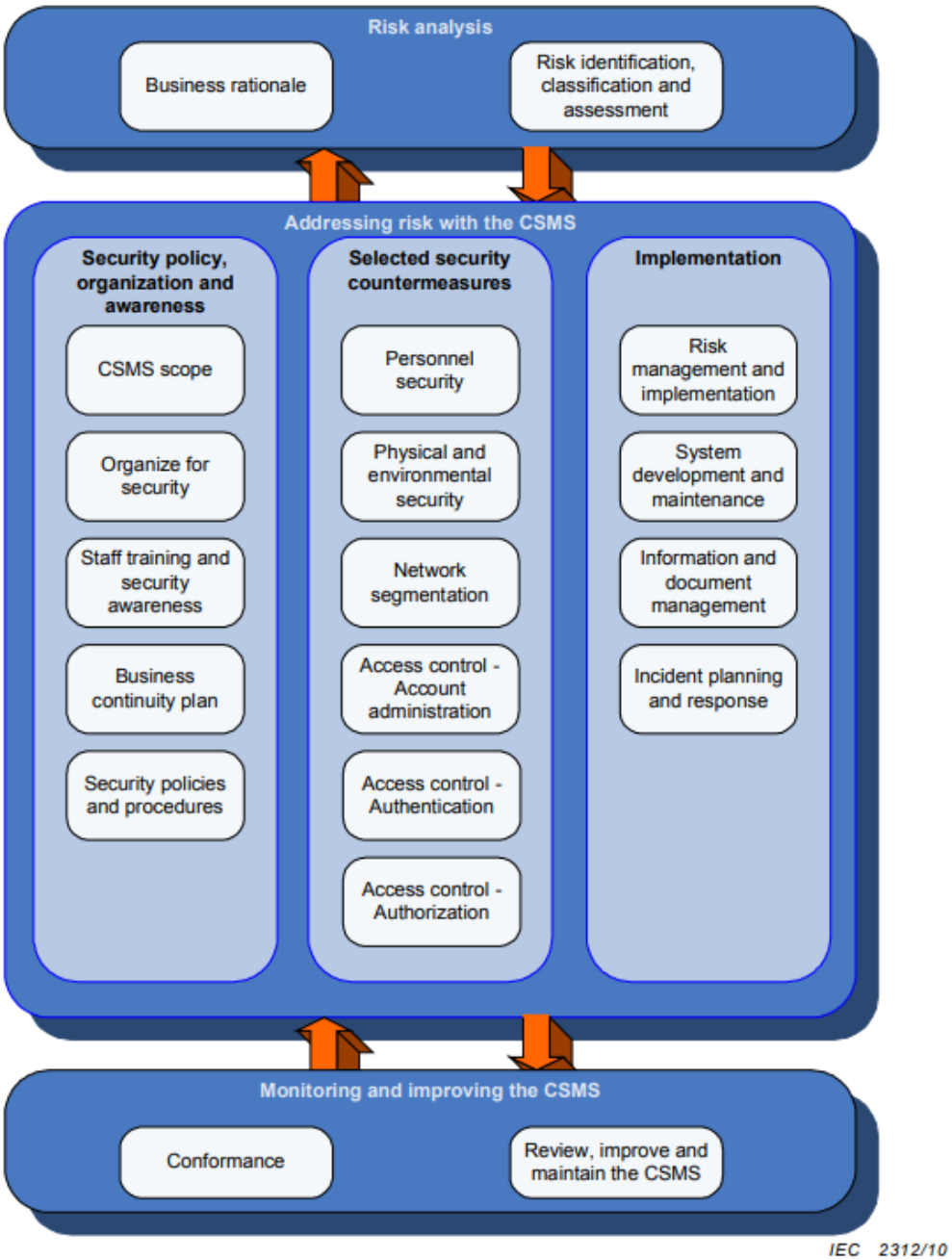

Figure 3-1: Graphical view of elements of a security program (cyber security management system).

The standard emphasizes the need for consistency between the practices to manage IACS cybersecurity with IT security. ISO/IEC 27001 are widely accepted standards that describe IT cybersecurity management. Much of the content in 27001 is applicable to IACS as well. The standard addresses some of the important differences between IACS and general business/information technology systems. It introduces the concept that cybersecurity risks with IACS may have implications for health, safety and the environment (HSE) and should be integrated with other existing risk management practices addressing these risks.

This document includes the mappings of the requirements of IEC 62443-2-1: 2010 to the SMM practices. The edition 2 of IEC 62443-2-1 is planned to be an international standard in 2023. IEC 62443-2-1 Ed.2 will rely on an established ISMS (typically based on 27001) and includes only OT specific requirements to the security program of IACS asset owners. Asset owners will combine 27001 and IEC 62443-2-1 for the establishment of IACS security programs. In future versions of this document, it is planned to map the requirements of IEC 62443-2-1 Ed.2 along with the security controls of 27001.

3.2 62443-2-4 Requirements Mapping

62443-2-4 is relevant for asset owners and addresses capabilities of service providers that may support or undermine the security maturity of asset owners. These capabilities are mapped to the appropriate SMM practices but are not assigned to comprehensiveness levels since they are relevant but are not directly asset owner requirements.

IEC 62443-2-4:2015 contains security requirements for providers of integration and maintenance services for IACSs. The standard specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an automation solution. Collectively, the security capabilities offered by an IACS service provider are referred to as its *security program*. It is related to IEC 62443-2-1, which describes requirements for the security management system of the asset owner.

62443-2-4[18] states: “62443-2-4 can be used by asset owners to request specific security capabilities from the service provider. More specifically, prior to such a request, 62443-2-4 can be used by asset owners to determine whether or not a specific service provider’s security program includes the capabilities that the asset owner needs.”

Figure 1-3 illustrates how the integration and maintenance roles relate to the IACS, the automation solution, and the products that are integrated into the automation solution. Service providers need to be aware of and support system security requirements defined in 62443-3-3. This may be achieved by the products themselves meeting the requirements or by addressing the requirements in the automation solution. Supporting these requirements means that the service provider can provide them to the asset owner upon request.

[18] Section 4.1.2, [IEC 62443-2-4]

Moreover, IACS service providers can use 62443-3-3 and 62443-4-2 in conjunction with 62443-2-4 to work with suppliers of control systems and components. This collaboration can assist the service provider in developing policies and procedures around a capability of a system or component, e.g. backup and restore based on the recommendations from the suppliers of the systems and components used.

The security programs implementing these requirements are expected to be independent of different releases of the products used in the automation solution. That is a new release of products does not necessarily require a change to the service provider's security program. However, changes to the security program will be required when changes to the underlying products create deficiencies in the security program with respect to 62443-2-4 requirements.

The requirements are defined in terms of the capabilities that these security programs are required to provide. The standard recognizes that security programs evolve and that capabilities go through a life cycle of their own, often starting as completely manual and evolving over time to become more formal, more consistent, and more effective. 62443-2-4 addresses this issue of evolving capabilities by defining a maturity model to be used with the application of this standard. As a result, the requirements are stated abstractly, allowing for a wide range of implementations. Service providers and asset owners should negotiate and agree on which of these required capabilities are to be provided and how.

The standard has been written to encourage service providers to implement the required capabilities so they can be adaptable to a wide variety of asset owners. The maturity model also allows asset owners to understand the maturity of a specific service provider's capabilities better.

When determining SMM practice comprehensiveness levels and implementing security programs for the protection of their operating facilities, asset owners can use 62443-2-4 to request specific security capabilities from the service provider. More specifically, prior to such a request, 62443-2-4 can be used by asset owners to determine whether or not a specific service provider's security program includes the capabilities that the asset owner needs.

3.3 62443-3-3 AND 62443-4-2 REQUIREMENTS MAPPING

IEC 62443-3-3:2013 provides detailed system security requirements (SRs) and requirement enhancements (REs). IEC 62443-4-2:2019 is derived from 62443-3-3 and provides technical security requirements (CRs) and requirement enhancements to IACS components. They are associated with the seven foundational requirements (FRs) described in 62443-1-1:

- 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).

62443-3-3 and 62443-4-2 provide requirements on how the security capabilities of products and solutions support asset owners and product suppliers in achieving security maturity. SMM mappings for these requirements are included as mappings in the SMM practice tables at the appropriate comprehensiveness levels.

The 62443 standard also defines security levels (SLs). These are used to differentiate the strength of the security capabilities of products or solutions to mitigate the threat of violation by attackers with increasing skills, motivation and resources. The SMM mapping is about relating 62443-3-3 and 62443-4-2 requirements to maturity comprehensiveness levels, which correspond to the need, including risks. Therefore the security levels are not directly related to the comprehensiveness levels.

The FRs themselves are not mapped since the associated 62443 requirements are often mapped to different SMM practices.

Not all SMM practices may be implemented using security capabilities of products or solutions. Some aspects are covered by other standards of this series, so some of the mapping tables don't include any 62443-3-3 or 62443-4-2 requirement. On the other hand, some requirements defined by 62443-3-3 or 62443-4-2 may support more than one SMM practice, so the same requirements may appear in more than one mapping table.

For the most part, 62443-4-2 requirements correspond to 62443-3-3 requirements, but not always. This is noted with footnotes in the tables to clarify that this is not an oversight.

Typically, the reason is that 62443-3-3 is focused on system requirements and 62443-4-2 is focused on component requirements. Some component level requirements, such as 62443-4-2 CR 3.12 on provisioning roots of trust in a component are not applicable to 62443-3-3 (Identity Management mapping). Similarly, some system requirements in 62443-3-3 are not appropriate for component enhancements in 62443-4-2, such as SR 2.1 RE 1 for "authorization enforcement for all users", which is system specific, not for a component (Access Control mapping).

There are also some cases where there is a differentiation in 62443-3-3 which is not relevant for components such as 62443-4-2 having an RE for "all interfaces" while 62443-3-3 has two REs, one for 'untrusted networks' and one for 'all networks' (Identity Management mapping).

Implementation of one or more requirements related to the comprehensiveness level of the SMM practice does not mean that this level is achieved for this practice. The rest of the indicators of achievement for this comprehensiveness level must be checked to confirm that.

3.4 62443-4-1 Requirements Mapping

IEC 62443-4-1:2018 specifies process requirements for the secure development of products used in IACSs. It defines a secure development life cycle for the purpose of developing and maintaining secure products. The life cycle includes the typical development phases from security requirements definition, design, implementation to verification and validation, as well as the support activities during commercialization with guidelines as well as vulnerability and update management. The requirements apply to the product supplier that develops and maintains the product.

The primary goal is to provide a framework to address a secure-by-design, defense-in-depth approach to designing, building, maintaining and retiring products used in IACSs. Application of the framework is intended to provide confidence that the product has security commensurate with its expected level of risk throughout the product's life cycle.

The secondary goal of these requirements is to align the development process with the elevated security needs of product users (for example, integration service providers and asset owners). This means the process needs to generate items such as well-documented security configurations and update management policies and procedures and to provide clear and succinct communications about security vulnerabilities uncovered in the product.

The requirements are grouped in 8 practices as shown in Figure 3-2 below.

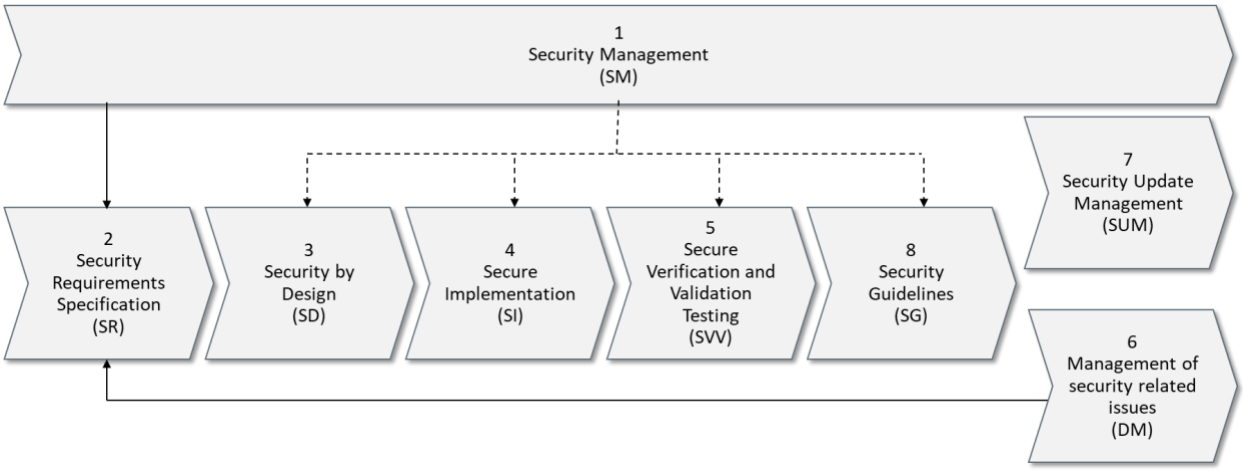

Figure 3-2: Practices of IEC 62443-4-1.

Practices 1 to 5 provide requirements for integrating security in the phases of the development process. A product supplier implementing these practices in its development organization will improve its posture regarding the security quality of its products. In the supply chain of asset owners, these suppliers will most probably be rated as being more trustworthy.

Practices 6 to 8 directly support users of the products, asset owners or service providers in the achievement of their security maturity by addressing the support to be expected from the product supplier. Management of security related issues and update management support asset

owners to better handle incidents when vulnerabilities are discovered in their IACSs during the operating phase. Guidelines support service providers and asset owners to optimize the use the security capabilities of the products for improving the security of solutions.

The 62443-4-1 requirements are mapped differently for asset owners and product suppliers.

For asset owners, 61443-4-1 include requirements to practices of product suppliers that may support or undermine the security maturity of asset owners, in the same way that 62443-2-4 addresses practices of service providers. Matching the requirements with SMM practices relevant to asset owners communicates how the practices of product supplier affect the SMM efforts of asset owners to reach their security maturity targets. We do not map 62443-4-1 requirements to comprehensiveness levels for the asset owner since they apply to the practices of organizations included in the supply chain of the asset owner.

Despite this, this document lists 62443-4-1 requirements relevant to each SMM practice table of product suppliers and notes the corresponding comprehensiveness level. This information should assist the asset owner in asking appropriate questions in the sense of having a checklist, useful in understanding aspects to consider in the components and services that impact the asset owner practice and comprehensiveness level.

4 62443 SMM PRACTICE[19] MAPPINGS

4.1 MAPPINGS COMMON TO BOTH ASSET OWNERS AND PRODUCT SUPPLIERS

4.1.1 SECURITY PROGRAM MANAGEMENT [ASSET OWNERS AND PRODUCT SUPPLIERS] (SMM PRACTICE 1)

Security Program Management			
This practice is critical for the planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-1: Security program management mappings [asset owners and product suppliers].

[19] We may wish to use industry and system/device scope in this mapping as well.

4.1.2 Compliance Management [Asset Owners and Product Suppliers] (SMM Practice 2)

Compliance Management			
This practice is necessary when strict requirements for compliance with evolving security standards is needed.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 3.3 (62443-3-3) Security functionality verification CR 3.3 (62443-4-2) Security functionality verification	*No mappings*	SR 3.3 RE 1 (62443-3-3) Automated mechanisms for security functionality verification[20]	SR 3.3 RE 2 (62443-3-3) Security functionality verification during normal operation CR 3.3 RE 1 (62443-4-2) Security functionality verification during normal operation

Table 4-2: Compliance management mappings [asset owners and product suppliers].

4.1.3 Threat Modeling [Asset Owners and Product Suppliers] (SMM Practice 3)

Threat Modeling			
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-3: Threat modeling mappings [asset owners and product suppliers].

4.1.4 Threat Modeling [Asset Owners and Product Suppliers] (SMM Practice 4)

Risk Attitude			
This practice enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-4: Risk attitude mappings [asset owners and product suppliers].

[20] Note that there is no 62443-4-2 requirement corresponding to SR 3.3 RE 1.

4.1.5 Product Supply Chain Risk Management [Asset Owners and Product Suppliers] (SMM Practice 5)

Product Supply Chain Risk Management			
This practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-5: Product supply chain risk management mappings [asset owners and product suppliers].

4.1.6 Services Third-Party Dependencies Management [Asset Owners and Product Suppliers] (SMM Practice 6)

Services Third-Party Dependencies Management			
This practice addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 1.13 (62443-3-3) Access via untrusted networks NDR 1.13 (62443-4-2) Access via untrusted networks (network devices)	SR 2.6 (62443-3-3) Remote session termination CR 2.6 (62443-4-2) Remote session termination	*No mappings*	*No mappings*

Table 4-6: Services third-party dependencies management mappings [asset owners and product suppliers].

4.1.7 Establishing and Maintaining Identities [Asset Owners and Product Suppliers] (SMM Practice 7)

Establishing And Maintaining Identities			
This practice helps to identify and constrain who may access the system and their privileges.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 1.1 (62443-3-3) Human user identification and authentication SR 1.3 (62443-3-3)	SR 1.1 RE 1 (62443-3-3) Unique identification and authentication SR 1.2 (62443-3-3) Software process and	SR 1.1 RE 2 (62443-3-3) Multifactor authentication for untrusted networks SR 1.1 RE 3 (62443-3-3)	SR 1.5 RE 1 (62443-3-3) Hardware security for software process identity credentials SR 1.8 (62443-3-3) Public key infrastructure (PKI) certificates

Account management SR 1.4 (62443-3-3) Identifier management SR 1.5 (62443-3-3) Authenticator management SR 1.6 (62443-3-3) Wireless access management SR 1.7 (62443-3-3) Strength of password-based authentication SR 1.10 (62443-3-3) Authenticator feedback CR 1.1 (62443-4-2) Human user identification and authentication CR 1.3 (62443-4-2) Account management CR 1.4 (62443-4-2) Identifier management CR 1.5 (62443-4-2) Authenticator management NDR 1.6 (62443-4-2) Wireless access management (network devices) CR 1.7 (62443-4-2) Strength of password-based authentication CR 1.10 (62443-4-2) Authenticator feedback	device identification and authentication SR 1.2 RE 1 (62443-3-3) Unique identification and authentication SR 1.6 RE 1 (62443-3-3) Unique identification and authentication SR 1.7 RE 1 (62443-3-3) Password generation and lifetime restrictions for human users CR 1.1 RE 1 (62443-4-2) Unique identification and authentication CR 1.2 (62443-4-2) Software process and device identification and authentication CR 1.2 RE 1 (62443-4-2) Unique identification and authentication NDR 1.6 RE 1 (62443-4-2) Unique identification and authentication (network devices) CR 1.7 RE 1 (62443-4-2) Password generation and lifetime restrictions for human users	Multifactor authentication for all networks SR 1.3 RE 1 (62443-3-3) Unified account management SR 1.7 RE 2 (62443-3-3) Password lifetime restrictions for all users CR 1.1 RE 2 (62443-4-2) Multifactor authentication for all interfaces CR 1.7 RE 2 (62443-4-2) Password lifetime restrictions for all users (human, software process, or device) EDR 3.12 (62443-4-2) Provisioning product supplier roots of trust (embedded devices) HDR 3.12 (62443-4-2) Provisioning product supplier roots of trust (host devices) NDR 3.12 (62443-4-2) Provisioning product supplier roots of trust (network devices) EDR 3.13 (62443-4-2) Provisioning asset owner roots of trust (embedded devices) HDR 3.13 (62443-4-2) Provisioning asset owner roots of trust (host devices) NDR 3.13 (62443-4-2) Provisioning asset owner roots of trust (network devices)	SR 1.9 (62443-3-3) Strength of public key authentication SR 1.9 RE 1 (62443-3-3) Hardware security for public key authentication CR 1.5 RE 1 (62443-4-2) Hardware security for authenticators CR 1.8 (62443-4-2) Public key infrastructure (PKI) certificates CR 1.9 (62443-4-2) Strength of public key authentication CR 1.9 RE 1 (62443-4-2) Hardware security for public key authentication CR 1.14 (62443-4-2) Strength of symmetric key-based authentication[21] CR 1.14 RE 1 (62443-4-2) Hardware security for symmetric key-based authentication

Table 4-7: Establishing and maintaining identities mappings [asset owners and product suppliers].

[21] 62443-3-3 has no corresponding requirement to 62443-4-2 CR 1.14 or CR 1.14 RE 1.

4.1.8 Access Control [Asset Owners and Product Suppliers] (SMM Practice 8)

Access Control			
This practice's policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 1.11 (62443-3-3) Unsuccessful login attempts CR 1.11 (62443-4-2) Unsuccessful login attempts SR 1.13 (62443-3-3) Access via untrusted networks[22] NDR 1.13 (62443-4-2) Access via untrusted networks (network devices) SR 2.1 (62443-3-3) Authorization enforcement[23] CR 2.1 (62443-4-2) Authorization enforcement SR 2.2 (62443-3-3) Wireless use control CR 2.2 (62443-4-2) Wireless use control SR 2.3 (62443-3-3) Use control for portable and mobile devices CR 2.3 (62443-4-2) Use control for portable and mobile devices SR 5.2 (62443-3-3) Zone boundary protection	SR 1.13 RE 1 (62443-3-3) Explicit access request approval NDR 1.13 RE1 (62443-4-2) Explicit access request approval (network devices) SR 2.1 RE 1 (62443-3-3) Authorization enforcement for all users CR 2.1 RE 1 (62443-4-2) Authorization enforcement for all users (humans, software processes and devices) SR 2.3 RE 1 (62443-3-3) Enforcement of security status of portable and mobile devices[27,28] SR 2.5 (62443-3-3) Session lock CR 2.5 (62443-4-2) Session lock SR 2.6 (62443-3-3) Remote session termination CR 2.6 (62443-4-2) Remote session termination	SR 2.1 RE 2 (62443-3-3) Permission mapping to roles CR 2.1 RE 2 (62443-4-2) Permission mapping to roles EDR 2.13 (62443-4-2) Use of physical diagnostic and test interfaces (embedded devices) [32] HDR 2.13 (62443-4-2) Use of physical diagnostic and test interfaces (host devices) NDR 2.13 (62443-4-2) Use of physical diagnostic and test interfaces (network devices) SR 2.1 RE 3 (62443-3-3) Supervisor override CR 2.1 RE 3 (62443-4-2) Supervisor override SR 5.1 RE 3 (62443-3-3) Logical and physical isolation of critical networks[33] SR 5.2 RE 2 (62443-3-3) Island mode	SR 2.1 RE 4 (62443-3-3) Dual approval CR 2.1 RE 4 (62443-4-2) Dual approval

[22] Intent is to control access, so this is not in the monitoring practice even though network traffic may be examined. That said, this information could also be used to contribute to intrusion detection systems.

[23] This is basic and goes along with authentication in SR 1.1 in Identity Management table.

[27] See discussion in text.

[28] There is no 62443-4-2 component level requirement associated with 62443-3-3 SR 2.3.

[32] 62443-3-3 has no corresponding requirement to 62443-4.2 EDR/HDR/NDR 2.13.

[33] No corresponding 62443-4-2 requirement.

NDR 5.2 (62443-4-2) Zone boundary protection (network devices) SR 5.2 RE 1 (62443-3-3) Deny by default, allow by exception[24] NDR 5.2 RE1 (62443-4-2) Deny all, permit by exception (network devices) SR 5.3 (62443-3-3) General purpose person-to-person communication restrictions[25] NDR 5.3 (62443-4-2) General purpose person-to-person communication restrictions (network devices) SR 5.4 (62443-3-3) Application partitioning[26] SR 7.7 (62443-3-3) Least functionality CR 7.7 (62443-4-2) Least functionality	SR 2.7 (62443-3-3) Concurrent session control CR 2.7 (62443-4-2) Concurrent session control SR 3.2 RE 1 (62443-3-3) Malicious code protection on entry and exit points HDR 3.2 RE1 (62443-4-2) Report version of code protection (host devices) SR 3.8 (62443-3-3) Session integrity[29] CR 3.8 (62443-4-2) Session integrity SR 3.8 RE 1 (62443-3-3) Invalidation of session IDs after session termination[30] SR 3.8 RE 2 (62443-3-3) Unique session ID generation SR 3.8 RE 3 (62443-3-3) Randomness of session IDs SR 5.1 (62443-3-3) Network segmentation CR 5.1 (62443-4-2) Network segmentation SR 5.1 RE 1 (62443-3-3) Physical network segmentation[31] SR 5.1 RE 2 (62443-3-3) Independence from non-control system	NDR 5.2 RE2 (62443-4-2) Island mode (network devices) SR 5.2 RE 3 (62443-3-3) Fail close NDR 5.2 RE3 (62443-4-2) Fail close (network devices) SR 5.3 RE 1 (62443-3-3) Prohibit all general purpose person-to-person communications[34]	

[24] Should be common practice at level 1, often found only at higher maturity levels such as 2.

[25] Do not allow external messages (e.g. email, text) into control network.

[26] This is common and basic to industrial control systems, hence SMM level 1 (e.g. emergency safety system is separate, human interface separate). There is no 62443-4-2 requirement associated with 62443-3-3 SR 5.4.

[29] This could be considered device specific and so part of SMM scope, but we keep it general here because it could also be considered general, for all parts of system that are appropriate.

[30] No 62443-4-2 requirement for 62443-3-3 SR 3.8 RE requirements.

[31] No 62443-4-2 requirement enhancements for CR 5.1 to correspond with 62443-3-3 SR 5.1 RE requirements.

[34] No corresponding 62443-4-2 requirement. At level 3 since across entire organization.

	networks		

Table 4-8: Access control mappings [asset owners and product suppliers].

4.1.9 Access Control [Asset Owners and Product Suppliers] (SMM Practice 9)

Asset, Change And Configuration Management			
This practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SR 7.6 (62443-3-3) Network and security configuration settings CR 7.6 (62443-4-2) Network and security configuration settings SR 7.8 (62443-3-3) Control system component inventory CR 7.8 (62443-4-2) Automation solution component inventory	EDR 3.14 (62443-4-2) Integrity of the boot process (embedded devices) [35] HDR 3.14 (62443-4-2) Integrity of the boot process (host devices) NDR 3.14 (62443-4-2) Integrity of the boot process (network devices) EDR 3.14 RE 1 (62443-4-2) Authenticity of the boot chain (embedded devices) HDR 3.14 RE 1 (62443-4-2) Authenticity of the boot process (host devices) NDR 3.14 RE 1 (62443-4-2) Authenticity of the boot process (network devices) SR 7.6 RE 1 (62443-3-3) Machine-readable reporting of current security settings CR 7.6 RE 1 (62443-4-2) Machine-readable reporting of current security settings	*No mappings*

Table 4-9: Asset, change and configuration management mappings [asset owners and product suppliers].

[35] No 62443-3-3 requirement corresponds to 62443-4-2 requirement 3.14 or 3.14 RE.

4.1.10 Access Control [Asset Owners and Product Suppliers] (SMM Practice 10)

Physical Protection			
This practice's policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	EDR 2.13 (62443-4-2) Use of physical diagnostic and test interfaces (embedded devices) [36] HDR 2.13 (62443-4-2) Use of physical diagnostic and test interfaces (host devices) NDR 2.13 (62443-4-2) Use of physical diagnostic and test interfaces (network devices) EDR 3.11 (62443-4-2) Physical tamper resistance and detection (embedded devices) [37] HDR 3.11 (62443-4-2) Physical tamper resistance and detection (host devices) NDR 3.11 (62443-4-2) Physical tamper resistance and detection (network devices)	*No mappings*

Table 4-10: Physical protection mappings [asset owners and product suppliers].

[36] No 62443-3-3 requirement corresponds to 62443-4-2 requirements 2.13.

[37] No 62443-3-3 requirement corresponds to 62443-4-2 requirements 3.11.

4.1.11 Protection Model and Policy for Data [Asset Owners and Product Suppliers] (SMM Practice 11)

Protection Model and Policy For Data			
This practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SR 2.4 (62443-3-3) Mobile code SAR 2.4 (62443-4-2) Mobile code (Software applications) EDR 2.4 (62443-4-2) Mobile code (embedded devices) HDR 2.4 (62443-4-2) Mobile code (host devices) NDR 2.4 (62443-4-2) Mobile code (network devices)	*No mappings*	*No mappings*

Table 4-11: Protection model and policy for data mappings [asset owners and product suppliers].

4.1.12 Implementation of Data Protection Controls [Asset Owners and Product Suppliers] (SMM Practice 12)

Implementation of Data Protection Controls			
This practice describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 2.2 (62443-3-3) Wireless use control CR 2.2 (62443-4-2) Wireless use control SR 2.3 (62443-3-3) Use control for portable and mobile devices CR 2.3 (62443-4-2) Use control for portable and mobile devices SR 3.1 (62443-3-3) Communication	SR 2.4 (62443-3-3) Mobile code SAR 2.4 (62443-4-2) Mobile code (Software applications) EDR 2.4 (62443-4-2) Mobile code (embedded devices) HDR 2.4 (62443-4-2) Mobile code (host devices) NDR 2.4 (62443-4-2)	SR 3.2 RE 2 (62443-3-3) Central management and reporting for malicious code protection SR 3.4 (62443-3-3) Software and information integrity CR 3.4 (62443-4-2) Software and information integrity CR 3.4 RE 1 (62443-4-2)	SR 3.9 RE 1 (62443-3-3) Audit records on write-once media CR 3.9 RE 1 (62443-4-2) Audit records on write-once media SR 4.2 RE 1 (62443-3-3) Purging of shared memory resources CR 4.2 RE 1 (62443-4-2) Erase of shared memory resources CR 4.2 RE 2 (62443-4-2) Erase verification SR 4.3 (62443-3-3) Use of cryptography

integrity CR 3.1 (62443-4-2) Communication integrity SR 3.1 RE 1 (62443-3-3) Cryptographic integrity protection CR 3.1 RE 1 (62443-4-2) Communication authentication SR 4.1 (62443-3-3) Information confidentiality CR 4.1 (62443-4-2) Information confidentiality SR 4.1 RE 1 (62443-3-3) Protection of confidentiality at rest or in transit via untrusted networks[38] SR 5.2 (62443-3-3) Zone boundary protection NDR 5.2 (62443-4-2) Zone boundary protection (network devices) SR 5.2 RE 1 (62443-3-3) Deny by default, allow by exception NDR 5.2 RE1 (62443-4-2) Deny all, permit by exception (network devices) SR 5.3 (62443-3-3) General purpose person-to-person communication restrictions NDR 5.3 (62443-4-2) General purpose person-to-person communication restrictions (network devices)	Mobile code (network devices) SR 3.2 (62443-3-3) Malicious code protection SAR 3.2 (62443-4-2) Malicious code protection (Software applications) EDR 3.2 (62443-4-2) Malicious code protection (embedded devices) HDR 3.2 (62443-4-2) Malicious code protection (host devices) NDR 3.2 (62443-4-2) Malicious code protection (network devices) SR 3.2 RE 1 (62443-3-3) Malicious code protection on entry and exit points HDR 3.2 RE1 (62443-4-2) Report version of code protection (host devices) SR 3.5 (62443-3-3) Input validation CR 3.5 (62443-4-2) Input validation SR 3.7 (62443-3-3) Error handling CR 3.7 (62443-4-2) Error handling SR 3.9 (62443-3-3) Protection of audit information CR 3.9 (62443-4-2) Protection of audit information SR 4.1 RE 2 (62443-3-3) Protection of confidentiality across	Authenticity of software and information SR 3.6 (62443-3-3) Deterministic output CR 3.6 (62443-4-2) Deterministic output SR 4.2 (62443-3-3) Information persistence CR 4.2 (62443-4-2) Information persistence SR 5.1 RE 3 (62443-3-3) Logical and physical isolation of critical networks SR 5.2 RE 2 (62443-3-3) Island mode NDR 5.2 RE2 (62443-4-2) Island mode (network devices) SR 5.2 RE 3 (62443-3-3) Fail close NDR 5.2 RE3 (62443-4-2) Fail close (network devices) SR 5.3 RE 1 (62443-3-3) Prohibit all general purpose person-to-person communications	CR 4.3 (62443-4-2) Use of cryptography

[38] No 62443-4-2 requirements to correspond to 62443-3-3 SR 4.1 RE 1.

SR 5.4 (62443-3-3) Application partitioning	zone boundaries[39] SR 5.1 (62443-3-3) Network segmentation CR 5.1 (62443-4-2) Network segmentation SR 5.1 RE 1 (62443-3-3) Physical network segmentation SR 5.1 RE 2 (62443-3-3) Independence from non-control system networks		

Table 4-12: Implementation of data protection controls mappings [asset owners and product suppliers].

4.1.13 Vulnerability Assessment [Asset Owners and Product Suppliers] (SMM Practice 13)

Vulnerability Assessment			
This practice helps identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-13: Vulnerability assessment mappings [asset owners and product suppliers].

4.1.14 Patch Management [Asset Owners and Product Suppliers] (SMM Practice 14)

Patch Management			
This practice clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
EDR 3.10 (62443-4-2) Support for updates (embedded devices) [40] HDR 3.10 (62443-4-2) Support for updates (host devices) NDR 3.10 (62443-4-2)	*No mappings*	EDR 3.10 RE 1 (62443-4-2) Update authenticity and integrity (embedded devices) HDR 3.10 RE 1 (62443-4-2) Update authenticity and	*No mappings*

[39] No 62443-4-2 requirements to correspond to 621443-3-3 SR 4-1 RE 2.

[40] No 62443-3-3 requirements to correspond to 62443-4-2 requirements 3.10.

Support for updates (network devices)		integrity (host devices) NDR 3.10 RE 1 (62443-4-2) Update authenticity and integrity (network devices)	

Table 4-14: Patch management mappings [asset owners and product suppliers].

4.1.15 MONITORING PRACTICE [ASSET OWNERS AND PRODUCT SUPPLIERS] (SMM PRACTICE 15)

Monitoring Practice			
This practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 2.11 (62443-3-3) Timestamps CR 2.11 (62443-4-2) Timestamps SR 6.1 (62443-3-3) Audit log accessibility CR 6.1 (62443-4-2) Audit log accessibility	SR 2.2 RE 1 (62443-3-3) Identify and report unauthorized wireless devices[41] SR 2.4 RE 1 (62443-3-3) Mobile code integrity check SAR 2.4 RE 1 (62443-4-2) Mobile code integrity check (Software applications) EDR 2.4 RE 1 (62443-4-2) Mobile code integrity check (embedded devices) HDR 2.4 RE 1 (62443-4-2) Mobile code integrity check (host devices) NDR 2.4 RE 1 (62443-4-2) Mobile code integrity check (network devices) SR 2.8 (62443-3-3) Auditable events CR 2.8 (62443-4-2) Auditable events	SR 2.8 RE 1 (62443-3-3) Centrally managed, system-wide audit trail[42] SR 2.11 RE 1 (62443-3-3) Internal time synchronization CR 2.11 RE 1 (62443-4-2) Time synchronization SR 2.11 RE 2 (62443-3-3) Protection of time source integrity CR 2.11 RE 2 (62443-4-2) Protection of time source integrity SR 2.12 (62443-3-3) Non-repudiation CR 2.12 (62443-4-2) Non-repudiation SR 2.12 RE 1 (62443-3-3) Non-repudiation for all users CR 2.12 RE 1 (62443-4-2) Non-repudiation for all users SR 3.2 RE 2 (62443-3-3)	EDR 2.13 RE 1 (62443-4-2) Active monitoring (embedded devices) [44] HDR 2.13 RE 1 (62443-4-2) Active monitoring (host devices) NDR 2.13 RE 1 (62443-4-2) Active monitoring (network devices) CR 3.4 RE 2 (62443-4-2) Automated notification about integrity violations[45] EDR 3.11 RE 1 (62443-4-2) Notification of a tampering attempt (embedded devices) HDR 3.11 RE 1 (62443-4-2) Notification of a tampering attempt (host devices) NDR 3.11 RE 1 (62443-4-2) Notification of a tampering attempt (network devices) SR 6.2 (62443-3-3) Continuous monitoring CR 6.2 (62443-4-2) Continuous monitoring

[41] No 62443-4-2 requirements to correspond to 62443-3-3 SR 2.2 RE 1.
[42] No 62443-4-2 requirements to correspond to 62443-3-3 SR 2.8 RE 1.
[44] No 62443-3-3 requirements to correspond to 62443-4-1 2.13 RE requirements.
[45] No 62443-3-3 requirements to correspond to 62443-4-2 3.4 RE 2 since this is component specific about integrity reporting.

	SR 2.9 (62443-3-3) Audit storage capacity CR 2.9 (62443-4-2) Audit storage capacity SR 2.9 RE 1 (62443-3-3) Warn when audit record storage capacity threshold reached CR 2.9 RE 1 (62443-4-2) Warn when audit record storage capacity threshold reached SR 2.10 (62443-3-3) Response to audit processing failures CR 2.10 (62443-4-2) Response to audit processing failures	Central management and reporting for malicious code protection[43] CR 3.4 RE 1 (62443-4-2) Authenticity of software and information SR 3.4 RE 1 (62443-3-3) Automated notification about integrity violations SR 6.1 RE 1 (62443-3-3) Programmatic access to audit logs CR 6.1 RE 1 (62443-4-2) Programmatic access to audit logs	

Table 4-15: Monitoring practice mappings [asset owners and product suppliers].

4.1.16 Situation Awareness and Information Sharing [Asset Owners and Product Suppliers] (SMM Practice 16)

Situation Awareness And Information Sharing			
This practice helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-16: Situation awareness and information sharing mappings [asset owners and product suppliers].

4.1.17 Event Detection and Response Plan [Asset Owners and Product Suppliers] (SMM Practice 17)

Event Detection And Response Plan			
This practice defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)

[43] Level 3 since holistic. No corresponding 3.2 RE requirement in 62443-4-2 since this is a system requirement.

No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-17: Event detection and response plan mappings [asset owners and product suppliers].

4.1.18 Remediation, Recovery and Continuity of Operations [Asset Owners and Product Suppliers] (SMM Practice 18)

Remediation, Recovery and Continuity Of Operations			
This practice is a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SR 1.12 (62443-3-3) System use notification CR 1.12 (62443-4-2) System use notification	SR 7.2 (62443-3-3) Resource management CR 7.2 (62443-4-2) Resource management SR 7.3 (62443-3-3) Control system backup CR 7.3 (62443-4-2) Automation solution backup SR 7.3 RE 1 (62443-3-3) Backup verification CR 7.3 RE 1 (62443-4-2) Backup integrity verification SR 7.4 (62443-3-3) Control system recovery and reconstitution CR 7.4 (62443-4-2) Automation solution recovery and reconstitution	SR 7.1 (62443-3-3) Denial of service protection CR 7.1 (62443-4-2) Denial of service protection SR 7.1 RE 1 (62443-3-3) Manage communication loads CR 7.1 RE 1 (62443-4-2) Manage communication load from component SR 7.1 RE 2 (62443-3-3) Limit DoS effects to other systems or networks[46] SR 7.3 RE 2 (62443-3-3) Backup automation[47] SR 7.5 (62443-3-3) Emergency power[48]	*No mappings*

Table 4-18: Remediation, recovery and continuity of operations mappings [asset owners and product suppliers].

[46] No 62443-4-2 requirements to correspond to 62443-3-3 SR 7.1 RE 2 since this is a system requirement.
[47] No 62443-4-2 requirements to correspond to 62443-3-3 SR 7.3 RE 2 since this is a system requirement.
[48] No 62443-4-2 requirements to correspond to 62443-3-3 SR 7.5 since this is a system requirement.

4.2 MAPPINGS UNIQUE TO ASSET OWNERS

4.2.1 SECURITY PROGRAM MANAGEMENT [ASSET OWNERS ONLY] (SMM PRACTICE 1)

Security Program Management			
This practice is critical for the planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
4.2.2.1 (62443-2-1[49]) Develop a business rationale 4.3.2.2.1 (62443-2-1 Ed 1) Define the scope of the CSMS 4.3.2.2.2 (62443-2-1 Ed 1) Define the scope content 4.3.2.3.1 (62443-2-1 Ed 1) Obtain senior management support 4.3.2.3.2 (62443-2-1 Ed 1) Establish the security organization(s) 4.3.2.3.3 (62443-2-1 Ed 1) Define the organizational responsibilities 4.3.2.6.1 (62443-2-1 Ed 1) Develop security policies 4.3.3.2.6 (62443-2-1 Ed 1) State cyber security terms and conditions of employment clearly	4.2.3.5 (62443-2-1 Ed 1) Develop simple network diagrams 4.3.2.3.4 (62443-2-1 Ed 1) Define the stakeholder team makeup 4.3.2.4.1 (62443-2-1 Ed 1) Develop a training program 4.3.2.4.2 (62443-2-1 Ed 1) Provide procedure and facility training [2 +] 4.3.2.4.3 (62443-2-1 Ed 1) Provide training for support personnel 4.3.2.6.2 (62443-2-1 Ed 1) Develop security procedures 4.3.2.6.6 (62443-2-1 Ed 1) Communicate the policies and procedures to the organization [2 +] 4.3.2.6.8 (62443-2-1 Ed 1) Demonstrate senior leadership support for cyber security 4.3.3.2.1 (62443-2-1 Ed 1) Establish a personnel security policy [2+] 4.3.3.2.5 (62443-2-1 Ed 1) Document and	4.3.3.2.2 (62443-2-1 Ed 1) Screen personnel initially 4.3.3.2.3 (62443-2-1 Ed 1) Screen personnel on an ongoing basis 4.3.3.2.4 (62443-2-1 Ed 1) Address security responsibilities 4.4.3.3 (62443-2-1 Ed 1) Establish triggers to evaluate CSMS 4.4.3.7 (62443-2-1 Ed 1) Monitor and evaluate applicable legislation relevant to cyber security	4.3.2.4.4 (62443-2-1 Ed 1) Validate the training program 4.3.2.4.5 (62443-2-1 Ed 1) Revise the training program over time 4.3.2.4.6 (62443-2-1 Ed 1) Maintain employee training records 4.3.2.6.7 (62443-2-1 Ed 1) Review and update the cyber security policies and procedures 4.3.4.4.7 (62443-2-1 Ed 1) Audit the information and document management process 4.4.3.1 (62443-2-1 Ed 1) Assign an organization to manage and implement changes to the CSMS 4.4.3.2 (62443-2-1 Ed 1) Evaluate the CSMS periodically 4.4.3.4 (62443-2-1 Ed 1) Identify and implement corrective and preventive actions 4.4.3.8 (62443-2-1 Ed 1) Request and report employee feedback on security suggestions

[49] 62443-2-1 refers to Edition 1 of 62443 2-1.

	communicate security expectations and responsibilities 4.3.3.2.7 (62443-2-1 Ed 1) Segregate duties to maintain appropriate checks and balances		

Table 4-19: Security program management mappings [asset owners only].

4.2.2 COMPLIANCE MANAGEMENT [ASSET OWNERS ONLY] (SMM PRACTICE 2)

Compliance Management			
This practice is necessary when strict requirements for compliance with evolving security standards is needed.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.2.6.4 (62443-2-1 Ed 1) Define cyber security policy and procedure compliance requirements 4.4.2.4 (62443-2-1 Ed 1) Establish a document audit trail 4.4.2.5 (62443-2-1 Ed 1) Define punitive measures for non-conformance 4.4.2.6 (62443-2-1 Ed 1) Ensure auditors' competence	4.4.2.1 (62443-2-1 Ed 1) Specify the methodology of the audit process 4.4.3.7 (62443-2-1 Ed 1) Monitor and evaluate applicable legislation relevant to cyber security	4.4.2.2 (62443-2-1 Ed 1) Conduct periodic IACS audits 4.4.2.3 (62443-2-1 Ed 1) Establish conformance metrics

Table 4-20: Compliance management mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether or not a specific service provider's security program includes the capabilities that the asset owner needs for this Security Maturity Model practice and whether they should be requested by the asset owner:

- SP.01.02 (62443-2-4) Solution staffing / Training / Security Requirements - Asset Owner
- SP.01.02 RE 1 (62443-2-4) Solution staffing / Training / Security Requirements - Asset Owner
- SP.01.03 (62443-2-4) Solution staffing / Training / Sensitive Data
- SP.01.03 RE 1 (62443-2-4) Solution staffing / Training / Sensitive Data

4.2.3 Threat Modeling [Asset Owners Only] (SMM Practice 3)

Threat Modeling			
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.2.3.7 (62443-2-1 Ed 1) Perform a detailed vulnerability assessment	*No mappings*	*No mappings*

Table 4-21: Threat modeling mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.02.01 (62443-2-4) Assurance / Testing / 3rd Party

4.2.4 Risk Attitude [Asset Owners Only] (SMM Practice 4)

Risk Attitude			
This practice enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
4.2.3.3 (62443-2-1 Ed 1) Conduct a high-level risk assessment	4.2.3.9 (62443-2-1 Ed 1) Conduct a detailed risk assessment 4.2.3.13 (62443-2-1 Ed 1) Document the risk assessment 4.3.2.6.5 (62443-2-1 Ed 1) Determine the organization's tolerance for risk	4.2.3.1 (62443-2-1 Ed 1) Select a risk assessment methodology 4.2.3.2 (62443-2-1 Ed 1) Provide risk assessment background information 4.2.3.4 (62443-2-1 Ed 1) Identify the IACS 4.2.3.5 (62443-2-1 Ed 1) Develop simple network diagrams 4.2.3.6 (62443-2-1 Ed 1) Prioritize systems 4.2.3.8 (62443-2-1 Ed 1) Identify a detailed risk assessment methodology	4.2.3.10 (62443-2-1 Ed 1) Identify the reassessment frequency and triggering criteria 4.2.3.12 (62443-2-1 Ed 1) Conduct risk assessments throughout the life cycle of the IACS 4.3.4.2.1 (62443-2-1 Ed 1) Manage IACS risk on an ongoing basis 4.4.3.5 (62443-2-1 Ed 1) Review risk tolerance

		4.2.3.11 (62443-2-1 Ed 1) Integrate physical, HSE and cyber security risk assessment results 4.2.3.14 (62443-2-1 Ed 1) Maintain vulnerability assessment records 4.3.2.6.3 (62443-2-1 Ed 1) Maintain consistency between risk management systems 4.3.4.2.2 (62443-2-1 Ed 1) Employ a common set of countermeasures 4.4.3.6 (62443-2-1 Ed 1) Monitor and evaluate industry CSMS strategies	

Table 4-22: Risk attitude mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.03.01 (62443-2-4) Architecture / Risk Assessment / Usage
- SP.03.01 RE 1 (62443-2-4) Architecture / Risk Assessment / Usage
- SP.03.01 RE 2 (62443-2-4) Architecture / Risk Assessment / 3rd Party
- SP.05.01 (62443-2-4) SIS / Risk Assessment / Verification
- SP.11.01 RE 1 (62443-2-4) Patch Management / Manual Process / Patch Qualification

4.2.5 PRODUCT SUPPLY CHAIN RISK MANAGEMENT [ASSET OWNERS ONLY] (SMM PRACTICE 5)

Product Supply Chain Risk Management			
This practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.2.4.2 (62443-2-1 Ed 1) Provide procedure and facility training 4.3.3.2.1 (62443-2-1 Ed 1) Establish a personnel security policy	*No mappings*	*No mappings*

Table 4-23: Product supply chain risk management mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.02.01 (62443-2-4) Assurance / Testing / 3rd party
- SP.02.03 (62443-2-4) Assurance / Hardening Guidelines / Usage
- SP.02.03 RE 1 (62443-2-4) Assurance / Hardening Guidelines / Verification

The following considerations are relevant for an asset owner evaluating comprehensiveness level 2 for this Product Supply Chain Risk Management practice. This list of 62443-4-1 requirements relates to the SMM level 2 indicator of accomplishment "Document templates for the identified typical cases (e.g., inspection checklists and return forms)".

- SM-1 (62443-4-1) Development process
- SM-2 (62443-4-1) Identification of responsibilities
- SM-3 (62443-4-1) Identification of applicability
- SM-4 (62443-4-1) Security expertise
- SM-5 (62443-4-1) Process scoping
- SM-12 (62443-4-1) Process verification
- SM-13 (62443-4-1) Continuous improvement
- DM-6 (62443-4-1) Periodic review of security defect management practice
- SG-1 (62443-4-1) Product defense-in-depth
- SG-2 (62443-4-1) Defense-in-depth measures expected in the environment
- SG-5 (62443-4-1) Secure operation guidelines
- SG-7 (62443-4-1) Documentation review

4.2.6 Services Third-Party Dependencies Management [Asset Owners Only] (SMM Practice 6)

Services Third-Party Dependencies Management			
This practice addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-24: Services third-party dependencies management mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.01.01 (62443-2-4) Solution Staffing / Training / Security Requirements - IEC 62443-2-4
- SP.01.01 RE 1 (62443-2-4) Solution Staffing / Training / Security Requirements - IEC 62443-2-4
- SP.01.02 (62443-2-4) Solution Staffing / Training / Security Requirements - Asset Owner
- SP.01.02 RE 1 (62443-2-4) Solution Staffing / Training / Security Requirements - Asset Owner
- SP.01.03 (62443-2-4) Solution Staffing / Training / Sensitive Data
- SP.01.03 RE 1 (62443-2-4) Solution Staffing / Training / Sensitive Data
- SP.01.04 (62443-2-4) Solution Staffing / Background Checks / Service Provider
- SP.01.04 RE 1 (62443-2-4) Solution Staffing / Background Checks / Subcontractor
- SP.01.05 (62443-2-4) Solution Staffing / Personnel - Assignments / Security Contact
- SP.01.06 (62443-2-4) Solution Staffing / Personnel - Assignments / Security Lead
- SP.01.07 (62443-2-4) Solution Staffing / Personnel - Changes / Access Control
- SP.10.05 RE 1 (62443-2-4) Malware Protection / Portable Media / Usage
- SP.10.05 RE 2 (62443-2-4) Malware Protection / Portable Media / Sanitizing

The following 62443-4-1 considerations are relevant for an asset owner evaluating comprehensiveness level 2 for this Services Third-Party Dependencies Management practice. This list of 62443-4-1 requirements supports establishing quality of service and progress metrics, measurable outcomes and compliance.

- SM-6 (62443-4-1) File integrity
- SM-7 (62443-4-1) Development environment security
- SM-8 (62443-4-1) Controls for private keys
- SM-9 (62443-4-1) Security requirements for externally provided components
- SM-10 (62443-4-1) Custom developed components from third-party suppliers
- SM-11 (62443-4-1) Assessing and addressing security-related issues
- SR-1 (62443-4-1) Product security context
- SR-2 (62443-4-1) Threat model
- SR-3 (62443-4-1) Product security requirements
- SR-4 (62443-4-1) Product security requirements content
- SR-5 (62443-4-1) Security requirements review
- SD-1 (62443-4-1) Secure design principles
- SD-2 (62443-4-1) Defense in depth design
- SD-3 (62443-4-1) Security design review
- SD-4 (62443-4-1) Secure design best practices
- SI-1 (62443-4-1) Security implementation review
- SI-2 (62443-4-1) Secure coding standards
- SVV-1 (62443-4-1) Security requirements testing
- SVV-2 (62443-4-1) Threat mitigation testing

- SVV-3 (62443-4-1) Vulnerability testing
- SVV-4 (62443-4-1) Penetration testing
- SVV-5 (62443-4-1) Independence of testers
- DM-1 (62443-4-1) Receiving notifications of security-related issues
- DM-2 (62443-4-1) Reviewing security-related issues
- DM-3 (62443-4-1) Assessing security-related issues
- DM-4 (62443-4-1) Addressing security-related issues

4.2.7 Establishing and Maintaining Identities [Asset Owners Only] (SMM Practice 7)

Establishing and Maintaining Identities			
This practice helps to identify and constrain who may access the system and their privileges.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
4.3.3.5.7 (62443-2-1 Ed 1) Change default passwords 4.3.3.6.5 (62443-2-1 Ed 1) Authenticate all remote users at the appropriate level Wireless access management (network devices)	4.3.3.5.2 (62443-2-1 Ed 1) Identify individuals 4.3.3.6.1 (62443-2-1 Ed 1) Develop an authentication strategy 4.3.3.6.3 (62443-2-1 Ed 1) Require strong authentication methods for system administration and application configuration 4.3.3.7.1 (62443-2-1 Ed 1) Define an authorization security policy 4.3.3.7.2 (62443-2-1 Ed 1) Establish appropriate logical and physical permission methods to access IACS devices 4.3.3.7.3 (62443-2-1 Ed 1) Control access to information or systems via role-based access accounts	4.3.3.5.4 (62443-2-1 Ed 1) Record access accounts 4.3.3.7.4 (62443-2-1 Ed 1) Employ multiple authorization methods for critical IACS	4.3.3.5.5 (62443-2-1 Ed 1) Suspend or remove unneeded accounts 4.3.3.5.6 (62443-2-1 Ed 1) Review account permissions 4.3.3.5.8 (62443-2-1 Ed 1) Audit account administration

Table 4-25: Establishing and maintaining identities mappings [asset owners only].

The following 62443-2-4 and 62443-4-1 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities

that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.03.07 RE 1 (62443-2-4) Architecture / Devices - Workstations / Access Control
- SP.03.08 RE 3 (62443-2-4) Architecture / Devices - Network / Access Control
- SP.04.02 (62443-2-4) Wireless / Network Design / Access Control
- SP.04.03 RE 1 (62443-2-4) Wireless / Network Design / Wireless Network Identifiers
- SP.04.03 RE 2 (62443-2-4) Wireless / Network Design / Connectivity
- SP.09.01 (62443-2-4) Account Management / Accounts - User and Service Accounts / Administration
- SP.09.02 (62443-2-4) Account Management / Accounts - User and Service Accounts / Administration
- SP.09.02 RE 1 (62443-2-4) Account Management / Accounts - User and Service Accounts / Administration
- SP.09.02 RE 2 (62443-2-4) Account Management / Accounts - User and Service Accounts / Administration
- SP.09.02 RE 3 (62443-2-4) Account Management / Accounts - User and Service Accounts / Expiration
- SP.09.02 RE 4 (62443-2-4) Account Management / Accounts - Administrator / Least Functionality
- SP.09.03 (62443-2-4) Account Management / Accounts - Default / Least Functionality
- SP.09.04 (62443-2-4) Account Management / Accounts - User / Least Functionality
- SP.09.04 RE 1 (62443-2-4) Account Management / Accounts - User / Logging
- SP.09.05 (62443-2-4) Account Management / Passwords / Composition
- SP.09.06 (62443-2-4) Account Management / Passwords / Expiration
- SP.09.06 RE 1 (62443-2-4) Account Management / Passwords / Expiration
- SP.09.07 (62443-2-4) Account Management / Passwords / Change
- SP.09.08 (62443-2-4) Account Management / Passwords / Reuse
- SP.09.08 RE 1 (62443-2-4) Account Management / Passwords / Change
- SP.09.09 (62443-2-4) Account Management / Passwords / Shared
- SP.09.09 RE 1 (62443-2-4) Account Management / Passwords / Shared
- SG-6 (62443-4-1) Account Management Guidelines

4.2.8 Access Control [Asset Owners Only] (SMM Practice 8)

Access Control			
This practice's policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)

4.3.3.5.3 (62443-2-1 Ed 1) Authorize account access 4.3.3.6.2 (62443-2-1 Ed 1) Authenticate all users before system use	4.3.3.5.1 (62443-2-1 Ed 1) Access accounts implement authorization security policy 4.3.3.5.2 (62443-2-1 Ed 1) Identify individuals 4.3.3.6.4 (62443-2-1 Ed 1) Log and review all access attempts to critical systems 4.3.3.6.6 (62443-2-1 Ed 1) Develop a policy for remote login and connections 4.3.3.6.7 (62443-2-1 Ed 1) Disable access account after failed remote login attempts 4.3.3.6.8 (62443-2-1 Ed 1) Require re-authentication after remote system inactivity 4.3.3.7.3 (62443-2-1 Ed 1) Control access to information or systems via role-based access accounts	4.3.3.5.4 (62443-2-1 Ed 1) Record access accounts 4.3.3.6.9 (62443-2-1 Ed 1) Employ authentication for task-to-task communication 4.3.3.7.4 (62443-2-1 Ed 1) Employ multiple authorization methods for critical IACS	4.3.3.5.6 (62443-2-1 Ed 1) Review account permissions

Table 4-26: Access control mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether or not a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.03.02 (62443-2-4) Architecture / Network Design / Connectivity
- SP.03.02 RE 1 (62443-2-4) Architecture / Network Design / Connectivity
- SP.03.02 RE 2 (62443-2-4) Architecture / Network Design / Connectivity
- SP.03.06 (62443-2-4) Architecture / Devices - Workstations / Session Lock
- SP.03.07 (62443-2-4) Architecture / Devices - Workstations / Access Control
- SP.03.07 RE 1 (62443-2-4) Architecture / Devices - Workstations / Access Control
- SP.03.08 (62443-2-4) Architecture / Devices - Network / Least Functionality
- SP.03.08 RE 1 (62443-2-4) Architecture / Devices - Network / Administration
- SP.03.08 RE 3 (62443-2-4) Architecture / Devices - Network / Access control
- SP.04.01 (62443-2-4) Wireless / Network Design / Verification

- SP.04.02 (62443-2-4) Wireless / Network Design / Access Control
- SP.05.01 (62443-2-4) SIS / Risk Assessment / Verification
- SP.05.02 (62443-2-4) SIS / Network Design / Communications
- SP.05.03 (62443-2-4) SIS / Network Design / Communications
- SP.05.04 (62443-2-4) SIS / Network Design / Communications
- SP.05.05 (62443-2-4) SIS / Devices - Workstations / Communications
- SP.05.05 RE 1 (62443-2-4) SIS / Devices - Workstations / Communications
- SP.05.06 (62443-2-4) SIS / Devices - Workstations / Connectivity
- SP.05.08 (62443-2-4) SIS / Devices - Wireless / Connectivity
- SP.07.01 (62443-2-4) Remote Access / Security Tools and Software / Usage
- SP.07.02 (62443-2-4) Remote Access / Security Tools and Software / Usage
- SP.07.03 (62443-2-4) Remote Access / Security Tools and Software / Usage
- SP.07.04 (62443-2-4) Remote Access / Security Tools and Software / Approval
- SP.07.04 RE 1 (62443-2-4) Remote Access / Data Protection / Cryptography
- SP.09.01 (62443-2-4) Account Management / Accounts - User and Service Accounts / Administration

The following consideration is relevant for an Asset Owner evaluating comprehensiveness level 2 or higher for this access control practice. For example, comprehensiveness level 3 is appropriate when considering IT and together in terms of a policy supporting access permissions as well as default accounts (e.g. as appropriate for OT).

- SG-6 (62443-4-1) Account management guidelines

4.2.9 Asset, Change and Configuration Management [Asset Owners Only] (SMM Practice 9)

Asset, Change and Configuration Management			
This practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.3.3.7 (62443-2-1 Ed 1) Maintain equipment assets 4.3.4.3.1 (62443-2-1 Ed 1) Define and test security functions and capabilities 4.3.4.3.3 (62443-2-1 Ed 1) Assess all the risks of changing the IACS 4.3.4.3.4 (62443-2-1 Ed	4.3.3.3.1 (62443-2-1 Ed 1) Establish complementary physical and cyber security policies 4.3.4.3.2 (62443-2-1 Ed 1) Develop and implement a change management system 4.3.4.3.5 (62443-2-1 Ed 1) Integrate cyber	4.3.3.3.9 (62443-2-1 Ed 1) Establish procedures for the addition, removal, and disposal of assets 4.3.4.4.4 (62443-2-1 Ed 1) Ensure appropriate records control

	1) Require security policies for system development or maintenance changes	security and process safety management (PSM) change management procedures 4.3.4.3.6 (62443-2-1 Ed 1) Review and maintain policies and procedures	

Table 4-27: Asset, change and configuration management mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether or not a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.02.03 (62443-2-4) Assurance / Hardening Guidelines / Usage
- SP.02.03 RE 1 (62443-2-4) Assurance / Hardening Guidelines / Verification
- SP.03.05 (62443-2-4) Architecture / Devices - All / Least Functionality
- SP.03.05 RE 1 (62443-2-4) Architecture / Devices - All / Least Functionality
- SP.05.07 (62443-2-4) SIS / Devices - Workstations / Least Functionality
- SP.06.01 (62443-2-4) Configuration Management / Network Design / Connectivity
- SP.06.01 RE 1 (62443-2-4) Configuration Management / Network design / Connectivity
- SP.06.02 (62443-2-4) Configuration Management / Devices - All / Inventory Register
- SP.06.03 (62443-2-4) Configuration Management / Devices - Control and Instrumentation / Verification
- SP.10.04 (62443-2-4) Malware Protection / Manual Process / Malware Definition Files
- SP.10.05 (62443-2-4) Malware Protection / Devices - All / Sanitizing
- SP.11.02 RE 2 (62443-2-4) Patch Management / Patch List / Approval
- SP.11.06 RE 1 (62443-2-4) Patch Management / Security Patch / Installation
- SP.11.06 RE 3 (62443-2-4) Patch Management / Security Patch / Installation

The following consideration is relevant for an asset owner evaluating comprehensiveness level 2 for this Asset, Change and Configuration Management practice:

- SG-3 (62443-4-1) Security hardening guidelines

4.2.10 Physical Protection [Asset Owners Only] (SMM Practice 10)

Physical Protection			
This practice's policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)

4.3.3.3.3 (62443-2-1 Ed 1) Provide entry controls 4.3.3.3.4 (62443-2-1 Ed 1) Protect assets against environmental damage 4.3.3.3.5 (62443-2-1 Ed 1) Require employees to follow security procedures	4.3.3.3.1 (62443-2-1 Ed 1) Establish complementary physical and cyber security policies 4.3.3.3.2 (62443-2-1 Ed 1) Establish physical security perimeter(s) 4.3.3.3.6 (62443-2-1 Ed 1) Protect connections 4.3.3.4.1 (62443-2-1 Ed 1) Develop the network segmentation architecture 4.3.4.3.4 (62443-2-1 Ed 1) Require security policies for system development or maintenance changes	4.3.3.3.8 (62443-2-1 Ed 1) Establish procedures for monitoring and alarming	4.3.3.3.10 (62443-2-1 Ed 1) Establish procedures for the interim protection of critical assets

Table 4-28: Physical protection mappings [asset owners only].

4.2.11 Protection Model and Policy for Data [Asset Owners Only] (SMM Practice 11)

Protection Model and Policy for Data			
This practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.3.3.1 (62443-2-1 Ed 1) Establish complementary physical and cyber security policies 4.3.4.4.2 (62443-2-1 Ed 1) Define information classification levels 4.3.4.4.3 (62443-2-1 Ed 1) Classify all CSMS information assets	*No mappings*	4.3.4.4.1 (62443-2-1 Ed 1) Develop life cycle management processes for IACS information 4.3.4.4.4 (62443-2-1 Ed 1) Ensure appropriate records control 4.3.4.4.6 (62443-2-1 Ed 1) Maintain information classifications

Table 4-29: Protection model and policy for data mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether or not a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.01.03 RE 1 (62443-2-4) Solution Staffing / Training / Sensitive Data

- SP.03.10 (62443-2-4) Architecture / Data Protection / Sensitive Data
- SP.03.10 RE 2 (62443-2-4) Architecture / Data Protection / Data/Event Retention
- SP.03.10 RE 3 (62443-2-4) Architecture / Data Protection / Cryptography
- SP.04.02 RE 1 (62443-2-4) Wireless / Network Design / Communications
- SP.04.03 (62443-2-4) Wireless / Network Design / Communications
- SP.05.09 (62443-2-4) SIS / User Interface / Configuration Mode
- SP.05.09 RE 1 (62443-2-4) SIS / User Interface / Configuration Mode
- SP.05.09 RE 2 (62443-2-4) SIS / User Interface / Configuration Mode

The following consideration is relevant for an asset owner evaluating comprehensiveness level 2 for this Protection Model and Policy for Data practice. SMM level 2 provides for the policy to support various means to protect data according to security and business requirements and explicitly notes an indicator of accomplishment that the "policy specifies storage life and destruction policies for data". Note that this 4-1 requirement includes data protection but goes further since it also refers to the product as a whole.

- SG-4 (62443-4-1) Secure disposal guidelines

4.2.12 Implementation of Data Protection Controls [Asset Owners Only] (SMM Practice 12)

Implementation of Data Protection Controls[50]			
This practice describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.3.4.1 (62443-2-1 Ed 1) Develop the network segmentation architecture 4.3.3.4.2 (62443-2-1 Ed 1) Employ isolation or segmentation on high risk IACS	4.3.3.4.3 (62443-2-1 Ed 1) Block non-essential communications with barrier devices	4.3.4.4.5 (62443-2-1 Ed 1) Ensure long-term records retrieval

Table 4-30: Implementation of data protection controls mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.03.08 RE 2 (62443-2-4) Architecture / Devices - Network / Administration
- SP.03.09 (62443-2-4) Architecture / Data Protection / Communications

[50] See discussion in Section 2: *General Mapping Considerations.*

- SP.03.10 RE 1 (62443-2-4) Architecture / Data Protection / Sensitive Data
- SP.03.10 RE 2 (62443-2-4) Architecture / Data Protection / Data/event Retention
- SP.03.10 RE 3 (62443-2-4) Architecture / Data Protection / Cryptography
- SP.03.10 RE 4 (62443-2-4) Architecture / Data Protection / Sanitizing
- SP.04.01 (62443-2-4) Wireless / Network Design / Verification
- SP.04.02 RE 1 (62443-2-4) Wireless / Network Design / Communications
- SP.05.09 (62443-2-4) SIS / User Interface / Configuration Mode
- SP.05.09 RE 1 (62443-2-4) SIS / User Interface / Configuration Mode
- SP.05.09 RE 2 (62443-2-4) SIS / User Interface / Configuration Mode
- SP.07.04 RE 1 (62443-2-4) Remote Access / Data Protection / Cryptography
- SP.11.06 RE 2 (62443-2-4) Patch Management / Security Patch / Installation

4.2.13 Vulnerability Assessment [Asset Owners Only] (SMM Practice 13)

Vulnerability Assessment			
This practice helps identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.2.3.7 (62443-2-1 Ed 1) Perform a detailed vulnerability assessment 4.2.3.9 (62443-2-1 Ed 1) Conduct a detailed risk assessment	4.2.3.8 (62443-2-1 Ed 1) Identify a detailed risk assessment methodology 4.2.3.14 (62443-2-1 Ed 1) Maintain vulnerability assessment records	4.2.3.10 (62443-2-1 Ed 1) Identify the reassessment frequency and triggering criteria

Table 4-31: Vulnerability assessment mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether or not a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.02.01 (62443-2-4) Assurance / Testing / 3rd Party
- SP.02.02 (62443-2-4) Assurance / Security Tools and Software / Usage
- SP.02.02 RE 1 (62443-2-4) Assurance / Security Tools and Software / Approval
- SP.02.02 RE 2 (62443-2-4) Assurance / Security Tools and Software / Detection
- SP.02.02 RE 3 (62443-2-4) Assurance / Security Tools and Software / Robustness
- SP.03.03 (62443-2-4) Architecture / Solution Components / Vulnerabilities
- SP.03.03 RE 1 (62443-2-4) Architecture / Network Design / Vulnerabilities
- SP.08.01 RE 2 (62443-2-4) Event Management / Events - Security Compromises / Responding

- SP.10.05 (62443-2-4) Malware Protection / Devices - All / Sanitizing
- SP.10.05 RE 2 (62443-2-4) Malware Protection / Portable Media / Sanitizing

4.2.14 Patch Management [Asset Owners Only] (SMM Practice 14)

Patch Management			
This practice clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
4.3.4.3.7 (62443-2-1 Ed 1) Establish and document a patch management procedure	*No mappings*	*No mappings*	*No mappings*

Table 4-32: Patch management mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.11.01 (62443-2-4) Patch Management / Manual Process / Patch Qualification
- SP.11.01 RE 1 (62443-2-4) Patch Management / Manual Process / Patch Qualification
- SP.11.02 (62443-2-4) Patch Management / Patch List / Patch Qualification
- SP.11.02 RE 1 (62443-2-4) Patch Management / Patch List / Patch Qualification
- SP.11.02 RE 2 (62443-2-4) Patch Management / Patch List / Approval
- SP.11.03 (62443-2-4) Patch Management / Security Patch / Delivery
- SP.11.04 (62443-2-4) Patch Management / Security Patch / Installation
- SP.11.05 (62443-2-4) Patch Management / Security Patch / Approval
- SP.11.06 (62443-2-4) Patch Management / Security Patch / Installation
- SP.11.06 RE 1 (62443-2-4) Patch Management / Security Patch / Installation
- SP.11.06 RE 3 (62443-2-4) Patch Management / Security Patch / Installation

The following considerations are relevant for an asset owner evaluating comprehensiveness levels. For example, SMM Level 1 requires installing patches based on vendor advisories, while SMM level 2 provides for a "standard process" for patch management.

- SUM-1 (62443-4-1) Security update qualification
- SUM-2 (62443-4-1) Security update documentation
- SUM-3 (62443-4-1) Dependent component or operating system security update documentation
- SUM-4 (62443-4-1) Security update delivery

- SUM-5 (62443-4-1) Timely delivery of security patches

4.2.15 Monitoring Practice [Asset Owners Only] (SMM Practice 15)

Monitoring Practice			
This practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.4.3.8 (62443-2-1 Ed 1) Establish and document antivirus/malware management procedure	*No mappings*	*No mappings*

Table 4-33: Monitoring practice mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.03.04 (62443-2-4) Architecture / Network Design / Network Time
- SP.10.01 (62443-2-4) Malware Protection / Manual Process / Malware Protection mechanism
- SP.10.02 (62443-2-4) Malware Protection / Security tools and Software / Installation
- SP.10.02 RE 1 (62443-2-4) Malware Protection / Security Tools and Software / Installation
- SP.10.03 (62443-2-4) Malware Protection / Security Tools and Software / Detection
- SP.10.04 (62443-2-4) Malware Protection / Manual Process / Malware Definition Files

The following consideration is relevant for an asset owner evaluating comprehensiveness levels for this Monitoring practice because they need to determine how they will disclose security related information.

- DM-5 (62443-4-1) Disclosing security-related issues

4.2.16 Situation Awareness and Information Sharing [Asset Owners Only] (SMM Practice 16)

Situation Awareness and Information Sharing			
This practice helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)

4.3.4.5.2 (62443-2-1 Ed 1) Communicate the incident response plan 4.3.4.5.5 (62443-2-1 Ed 1) Report cyber security incidents in a timely manner	4.3.4.5.8 (62443-2-1 Ed 1) Document the details of incidents	*No mappings*	4.3.4.5.10 (62443-2-1 Ed 1) Address and correct issues discovered

Table 4-34: Situation awareness and information sharing mappings [asset owners only].

4.2.17 Event Detection and Response Plan [Asset Owners Only] (SMM Practice 17)

Event Detection and Response Plan			
This practice defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
4.3.4.5.5 (62443-2-1 Ed 1) Report cyber security incidents in a timely manner 4.3.4.5.7 (62443-2-1 Ed 1) Identify failed and successful cyber security breaches	4.3.3.3.10 (62443-2-1 Ed 1) Establish procedures for the interim protection of critical assets 4.3.4.5.1 (62443-2-1 Ed 1) Implement an incident response plan 4.3.4.5.2 (62443-2-1 Ed 1) Communicate the incident response plan 4.3.4.5.3 (62443-2-1 Ed 1) Establish a reporting procedure for unusual activities and events 4.3.4.5.4 (62443-2-1 Ed 1) Educate employees on reporting cyber security incidents 4.3.4.5.6 (62443-2-1 Ed 1) Identify and respond to incidents 4.3.4.5.8 (62443-2-1 Ed 1) Document the details of incidents 4.3.4.5.9 (62443-2-1 Ed 1) Communicate the incident details 4.3.4.5.10 (62443-2-1	*No mappings*	4.3.4.5.11 (62443-2-1 Ed 1) Conduct drills

	Ed 1) Address and correct issues discovered		

Table 4-35: Event detection and response plan mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.08.01 (62443-2-4) Event Management / Events - Security Compromises / Responding
- SP.08.01 RE 1 (62443-2-4) Event Management / Events - Security Compromises / Reporting
- SP.08.02 (62443-2-4) Event Management / Events - Security-Related / Logging
- SP.08.02 RE 1 (62443-2-4) Event Management / Events - Security-Related / Reporting
- SP.08.02 RE 2 (62443-2-4) Event Management / Events - Security-Related / Logging
- SP.08.03 (62443-2-4) Event Management / Events - Alarms & Events / Logging
- SP.08.03 RE 1 (62443-2-4) Event Management / Events - Alarms & Events / Reporting
- SP.08.04 (62443-2-4) Event Management / Events - Alarms & Events / Robustness

4.2.18 Remediation, Recovery and Continuity of Operations [Asset Owners Only] (SMM Practice 18)

Remediation, Recovery and Continuity of Operations			
This practice is a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad-Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	4.3.2.5.1 (62443-2-1 Ed 1) Specify recovery objectives 4.3.2.5.2 (62443-2-1 Ed 1) Determine the impact and consequences to each system 4.3.2.5.3 (62443-2-1 Ed 1) Develop and implement business continuity plans 4.3.2.5.4 (62443-2-1 Ed 1) Form a business continuity team 4.3.4.5.10 (62443-2-1 Ed 1) Address and	4.3.2.5.5 (62443-2-1 Ed 1) Define and communicate specific roles and responsibilities 4.3.2.5.6 (62443-2-1 Ed 1) Create backup procedures that support business continuity plan 4.3.3.3.10 (62443-2-1 Ed 1) Establish procedures for the interim protection of critical assets 4.3.4.3.9 (62443-2-1 Ed	4.3.2.5.7 (62443-2-1 Ed 1) Test and update the business continuity plan

	correct issues discovered	1) Establish backup and restoration procedure	

Table 4-36: Remediation, recovery and continuity of operations mappings [asset owners only].

The following 62443-2-4 requirements are relevant for an asset owner evaluating whether a specific service provider's security program includes the capabilities that the asset owner needs for this SMM practice and whether they should be requested by the asset owner:

- SP.12.01 (62443-2-4) Backup/Restore / Manual Process / Backup Process
- SP.12.02 (62443-2-4) Backup/Restore / Manual Process / Restore Process
- SP.12.03 (62443-2-4) Backup/Restore / Portable Media / Administration
- SP.12.04 (62443-2-4) Backup/Restore / Backup / Verification
- SP.12.05 (62443-2-4) Backup/Restore / Restore / Verification
- SP.12.06 (62443-2-4) Backup/Restore / Backup / Usage
- SP.12.07 (62443-2-4) Backup/Restore / Backup / Robustness
- SP.12.08 (62443-2-4) Backup/Restore / Manual Process / Logging
- SP.12.09 (62443-2-4) Backup/Restore / Manual Process / Disaster Recovery

4.3 Mappings Unique to Product Suppliers

4.3.1 Security Program Management [Product Suppliers Only] (SMM Practice 1)

Security Program Management			
This practice is critical for the planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
SM-1 (62443-4-1) Development process SM-2 (62443-4-1) Identification of responsibilities SM-3 (62443-4-1) Identification of applicability SM-11 (62443-4-1) Assessing and addressing security-related issues SR-1 (62443-4-1) Product security context SD-1 (62443-4-1)	SM-4 (62443-4-1) Security expertise SM-5 (62443-4-1) Process scoping SM-12 (62443-4-1) Process verification SR-3 (62443-4-1) Product security requirements SR-4 (62443-4-1) Product security requirements content SR-5 (62443-4-1) Security requirements review SD-3 (62443-4-1)	SVV-5 (62443-4-1) Independence of testers	SM-13 (62443-4-1) Continuous improvement DM-6 (62443-4-1) Periodic review of security defect management practice

Secure design principles SD-4 (62443-4-1) Secure design best practices SI-1 (62443-4-1) Security implementation review	Security design review SI-2 (62443-4-1) Secure coding standards SVV-1 (62443-4-1) Security requirements testing SVV-2 (62443-4-1) Threat mitigation testing SVV-3 (62443-4-1) Vulnerability testing SVV-4 (62443-4-1) Penetration testing DM-2 (62443-4-1) Reviewing security-related issues DM-3 (62443-4-1) Assessing security-related issues DM-4 (62443-4-1) Addressing security-related issues DM-5 (62443-4-1) Disclosing security-related issues SUM-1 (62443-4-1) Security update qualification SUM-2 (62443-4-1) Security update documentation SUM-3 (62443-4-1) Dependent component or operating system security update documentation SUM-4 (62443-4-1) Security update delivery SUM-5 (62443-4-1) Timely delivery of security patches SG-1 (62443-4-1) Product defense-in-depth SG-2 (62443-4-1) Defense-in-depth measures expected in		

	the environment SG-3 (62443-4-1) Security hardening guidelines SG-4 (62443-4-1) Secure disposal guidelines SG-5 (62443-4-1) Secure operation guidelines SG-6 (62443-4-1) Account management guidelines SG-7 (62443-4-1) Documentation review		

Table 4-37: Security program management mappings [product suppliers only].

4.3.2 Compliance Management [Product Suppliers Only] (SMM Practice 2)

Compliance Management			
This practice is necessary when strict requirements for compliance with evolving security standards is needed.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-38: Compliance management mappings [product suppliers only].

4.3.3 Threat Modeling [Product Suppliers Only] (SMM Practice 3)

Threat Modeling			
This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describing these factors.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SR-1 (62443-4-1) Product security context SR-2 (62443-4-1) Threat model SD-3 (62443-4-1) Security design review SD-4 (62443-4-1) Secure design best	SD-1 (62443-4-1) Secure design principles	*No mappings*

	practices SI-1 (62443-4-1) Security implementation review DM-3 (62443-4-1) Assessing security-related issues		

Table 4-39: Threat modeling mappings [product suppliers only].

4.3.4 Risk Attitude [Product Suppliers Only] (SMM Practice 4)

Risk Attitude			
This practice enables an organization to establish a strategy for dealing with risks according to risk management policy, including conditions for acceptance, avoidance, evaluation, mitigation and transference.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SR-3 (62443-4-1) Product security requirements SR-4 (62443-4-1) Product security requirements content SR-5 (62443-4-1) Security requirements review SD-2 (62443-4-1) Defense in depth design SVV-2 (62443-4-1) Threat mitigation testing SVV-3 (62443-4-1) Vulnerability testing SVV-4 (62443-4-1) Penetration testing DM-2 (62443-4-1) Reviewing security-related issues DM-3 (62443-4-1) Assessing security-related issues DM-4 (62443-4-1) Addressing security-related issues	*No mappings*	*No mappings*

Table 4-40: Risk attitude mappings [product suppliers only].

4.3.5 Product Supply Chain Risk Management [Product Suppliers Only] (SMM Practice 5)

Product Supply Chain Risk Management			
This practice addresses the need to enable trust for contractors or suppliers and to ascertain the absence of hidden threat sources, ensuring the integrity of the supply chain.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-9 (62443-4-1) Security requirements for externally provided components SM-10 (62443-4-1) Custom developed components from third-party suppliers	*No mappings*	*No mappings*

Table 4-41: Product supply chain risk management mappings [product suppliers only].

4.3.6 Services Third-Party Dependencies Management [Product Suppliers Only] (SMM Practice 6)

Services Third-Party Dependencies Management			
This practice addresses the need to enable trust for partners and other third parties. The ability to have assurance of the trust of third parties requires understanding of the business and trust infrastructure and possible hidden threat sources.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-9 (62443-4-1) Security requirements for externally provided components SD-1 (62443-4-1) Secure design principles	*No mappings*	*No mappings*

Table 4-42: Services third-party dependencies management mappings [product suppliers only].

4.3.7 Establishing and Maintaining Identities [Product Suppliers Only] (SMM Practice 7)

Establishing And Maintaining Identities			
This practice helps to identify and constrain who may access the system and their privileges.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-2 (62443-4-1) Identification of responsibilities	SM-8 (62443-4-1) Controls for private keys	*No mappings*

	SD-1 (62443-4-1) Secure design principles		

Table 4-43: Establishing and maintaining identities mappings [product suppliers only].

4.3.8 Access Control [Product Suppliers Only] (SMM Practice 8)

Access Control			
This practice's policy and implementation allow a business to limit access to resources to only the specific identities that require access and only at the specific level needed to meet organizational requirements.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SD-1 (62443-4-1) Secure design principles	*No mappings*	SVV-4 (62443-4-1) Penetration testing

Table 4-44: Access control mappings [product suppliers only].

4.3.9 Asset, Change and Configuration Management [Product Suppliers Only] (SMM Practice 9)

Asset, Change And Configuration Management			
This practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-7 (62443-4-1) Development environment security SD-1 (62443-4-1) Secure design principles	*No mappings*	*No mappings*

Table 4-45: Asset, change and configuration management mappings [product suppliers only].

4.3.10 Physical Protection [Product Suppliers Only] (SMM Practice 10)

Physical Protection			
This practice's policies address the physical security and safety of the premises, its people and its systems to prevent theft and ensure the ongoing safe operation of equipment.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-7 (62443-4-1) Development environment security	*No mappings*	*No mappings*

Table 4-46: Physical protection mappings [product suppliers only].

4.3.11 Protection Model and Policy for Data [Product Suppliers Only] (SMM Practice 11)

Protection Model And Policy For Data			
This practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-6 (62443-4-1) File integrity	*No mappings*	*No mappings*

Table 4-47: Protection model and policy for data mappings [product suppliers only].

4.3.12 Protection Model and Policy for Data [Product Suppliers Only] (SMM Practice 12)

Implementation Of Data Protection Controls			
This practice describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-6 (62443-4-1) File integrity SM-7 (62443-4-1) Development environment security SM-8 (62443-4-1) Controls for private keys SD-1 (62443-4-1) Secure design principles	*No mappings*	*No mappings*

Table 4-48: Implementation of data protection controls mappings [product suppliers only].

4.3.13 Vulnerability Assessment [Product Suppliers Only] (SMM Practice 13)

Vulnerability Assessment			
This practice helps identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SM-11 (62443-4-1) Assessing and addressing security-related issues DM-3 (62443-4-1)	SD-1 (62443-4-1) Secure design principles SVV-3 (62443-4-1) Vulnerability testing SVV-4 (62443-4-1) Penetration testing	*No mappings*

	Assessing security-related issues		

Table 4-49: Vulnerability assessment mappings [product suppliers only].

4.3.14 Patch Management [Product Suppliers Only] (SMM Practice 14)

Patch Management			
This practice clarifies when and how frequently to apply the software patches, sets up procedures for emergency patches and proposes additional mitigations in the instance of constrained access to the system or other issues involved with patching.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	SD-1 (62443-4-1) Secure design principles DM-4 (62443-4-1) Addressing security-related issues	SUM-1 (62443-4-1) Security update qualification SUM-2 (62443-4-1) Security update documentation SUM-3 (62443-4-1) Dependent component or operating system security update documentation SUM-4 (62443-4-1) Security update delivery SUM-5 (62443-4-1) Timely delivery of security patches	*No mappings*

Table 4-50: Patch management mappings [product suppliers only].

4.3.15 Monitoring Practice [Product Suppliers Only] (SMM Practice 15)

Monitoring Practice			
This practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	*No mappings*	*No mappings*	*No mappings*

Table 4-51: Monitoring practice mappings [product suppliers only].

4.3.16 Situation Awareness and Information Sharing [Product Suppliers Only] (SMM Practice 16)

Situation Awareness And Information Sharing

This practice helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	DM-5 (62443-4-1) Disclosing security-related issues	DM-1 (62443-4-1) Receiving notifications of security-related issues	*No mappings*

Table 4-52: Situation awareness and information sharing mappings [product suppliers only].

4.3.17 Event Detection and Response Plan [Product Suppliers Only] (SMM Practice 17)

Event Detection And Response Plan			
This practice defines what a security event is and how to detect and assign events for investigation, escalate them as needed and respond appropriately. It should also include a communications plan for sharing information appropriately and in a timely manner with stakeholders.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	DM-2 (62443-4-1) Reviewing security-related issues DM-4 (62443-4-1) Addressing security-related issues	*No mappings*	*No mappings*

Table 4-53: Event detection and response plan mappings [product suppliers only].

4.3.18 Remediation, Recovery and Continuity of Operations [Product Suppliers Only] (SMM Practice 18)

Remediation, Recovery And Continuity Of Operations			
This practice is a combination of technical redundancies whereby trained staff and business continuity policy help an organization recover quickly from an event to expedite returning to business as usual.			
Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
No mappings	DM-4 (62443-4-1) Addressing security-related issues	*No mappings*	*No mappings*

Table 4-54: Remediation, recovery and continuity of operations mappings [product suppliers only].

Annex A GLOSSARY

The terms and their definitions in this section are specific to this document and may not be applicable to other IIC documents including the Industry IoT Vocabulary Technical Report.

Asset Owner is an individual or organization responsible for one or more IACSs.[51]

Automation Solution is a control system and any complementary hardware and software components that have been installed and configured to operate in an IACS.[51]

Comprehensiveness is a measure of the completeness, consistency and assurance of the implementation of measures supporting the security maturity domain, subdomain or practice.

Control System is the hardware and software components used in the design and implementation of an IACS.[51]

The maturity *current state* represents the maturity as captured by an assessment of the organization.

Domains are the strategic priorities for security maturity. In the SMM, there are three domains: governance, enablement, and hardening.

Enablement is the implementation of security controls and practices needed to create an operational system meeting the policy and operational requirements.

Governance is the "establishment of policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization."[52]

Hardening is the use of security practices during system operation.

Industrial Automation and Control System (IACS) is the collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation.[51]

Industry IoT Consortium (IIC) is an open membership, international not-for-profit consortium that is setting the architectural framework and direction for the Industrial Internet. Founded by AT&T, Cisco, GE, IBM and Intel in March 2014, the consortium's mission is to coordinate vast ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards.

Industrial Internet of Things (IIoT) describes systems that connects and integrates industrial control systems with enterprise systems, business processes, and analytics.

[51] [IEC 62443-2-4]
[52] [IIC-SMMP2020]

Integration Service Provider is a service provider that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover[51].

Maintenance Service Provider is a service provider that provides support activities for an Automation Solution after handover.[51]

A *Practice* comprises the typical activities performed for a given subdomain; they provide the deeper detail necessary for planning. Each sub domain has a set of practices.

A *Product Supplier* is a manufacturer of hardware and/or software product.[51]

Scope is a measure of the applicability to a specific vertical or system.

Security Level (SL) is a measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner.[53]

Security maturity is a measure of an understanding of the current security level, its necessity, benefits, and cost of its support. Maturity is captured by two dimensions, comprehensiveness and scope.

The *security maturity profile* is a typical security maturity target for a specific type of device, organization or system. Using security maturity target profiles simplifies the process of establishing the target for common use cases. Establishing a library of security maturity target profiles for common IoT scenarios is a subject for further development.

A *Security Program* is a portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the IACS.[51] Also known as a *Cyber Security Management System* (CSMS).

Security Verification and Validation Testing (V&V) is testing performed to assess the overall security of a component, product or system when used in its intended product security context and to determine if a component, product or system satisfies the product security requirements and satisfies its designed security purpose.[54]

A *Service Provider* is an individual or organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner.[51]

A *Subdomain* is the basic means to address a domain at the planning level. Each domain currently defines three subdomains.

[53] [IEC 62443-3-3]
[54] [IEC 62443-4-1]

System is comprised of interacting, interrelated, or interdependent elements forming a complex whole.[51]

Target state is the desired "end state" security maturity for an organization or system. The security maturity target can apply to a new system under development or an existing brownfield system. The security maturity target is determined based upon the business objectives of the organization or group.

Annex B REFERENCES

[IEC 62443-2-1] IEC 62443-2-1:2009, Security for Industrial Automation and Control Systems, Part 2-1: Establishing an Industrial Automation and Control Systems Security Program, 13 January 2009, https://webstore.iec.ch/publication/7330

[IEC 62443-2-4] IEC 62443-2-4:2015, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT), 13 July 2018, https://webstore.iec.ch/publication/61335

[IEC 62443-3-3] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels, 2013, https://webstore.iec.ch/publication/7033

[IEC 62443-4-1] IEC 62443-4-1:2018 2nd Printing 2020, Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements, 4 December 2020, https://webstore.iec.ch/publication/33615

[IEC 62443-4-2] IEC 62443-4-2:2019 2nd Printing 2020, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, 28 August 2019, https://webstore.iec.ch/publication/34421

[IIC-IIRA2019] Industry IoT Consortium: The Industrial Internet, Volume G1: Reference Architecture Technical Report, version 1.9, 2019-06-19, retrieved 2020-04-29 *https://www.iiconsortium.org/IIRA.htm*

[IIC-IISF2016] Industry IoT Consortium: Industrial Internet of Things Volume G4: Security Framework, 2016-09-26, retrieved 2019-01-24 *https://www.iiconsortium.org/IISF.htm*

[IIC-IIV2019] Industry IoT Consortium: The Industrial Internet, Volume G8: Vocabulary Technical Report, version 2.2, 2019-11-06, retrieved 2020-01-24 *https://www.iiconsortium.org/vocab/index.htm*

[IIC-SMMD2020] Industry IoT Consortium: IoT Security Maturity Model: Description and Intended Use, version 1.2, 2020-05-05, retrieved 2020-05-05 *https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf*

[IIC-SMMP2020] Industry IoT Consortium: IoT Security Maturity Model: Practitioner's Guide, Version 1.2, 2020-05-05, retrieved 2020-05-05 *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

[IIC-SMMRP2020] Industry IoT Consortium: IoT SMM: Retail Profile for Point-of-Sale Devices, 2020-08-01, retrieved 2020-11-18 *https://www.iiconsortium.org/pdf/SMM-Retail-Profile.pdf*

AUTHORS & LEGAL NOTICE

This document is a work product of the Industry IoT Consortium (IIC) and the ISA99 committee of the International Society for Automation (ISA).

In the IIC, it is a product of the IIC Contributing Group, chaired by Jim Gilsinn *(*Dragos), Frederick Hirsch (Upham Security), Ron Zahavi (Microsoft) in conjunction with the IIC Security Working Group, co-chaired by Keao Caindec (Farallon Technology Group) and Viacheslav Zolotnikov (Kaspersky).

Authors: The following persons contributed substantial written content to this document: Eric Cosman (OIT Concepts), Jim Gilsinn (Dragos), Frederick Hirsch (Upham Security), Pierre Kobes (Kobes Consulting), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft)..

Contributors: The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document: Tom Alrich (Red Alert Labs).

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors and Contributors into an integrated document.