IoT Security Maturity Model
Digital Twin Profile

An Industry IoT Consortium and Digital Twin Consortium Whitepaper

2022-06-20

Authors

Jon Geater (Jitsuin), Frederick Hirsch (Upham Security), Detlev Richter (TÜV SÜD), Michael Robkin (Six By Six), Ron Zahavi (Microsoft).

Contents

FIGURES

TABLES

According to the Digital Twin Consortium (DTC),[1] "a digital twin is a virtual representation of real-world entities and processes, synchronized at a specified frequency and fidelity". They:

- transform business by accelerating holistic understanding, optimal decision-making and effective action,
- use real-time and historical data to represent the past and present and simulate predicted futures and
- are motivated by outcomes, tailored to use cases, powered by integration, built on data, guided by domain knowledge, and implemented in Information Technology (IT) and Operational Technology (OT) systems.

Given the importance of digital twins to business and digital transformation of business, security is an important consideration. Risks must be considered to all aspects of the system, including various technologies, governance and operations. The Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM) helps organize and manage these concerns, enabling various stakeholders to communicate and determine appropriate maturity targets, assess the current status and create action plans to address gaps.

The SMM defines general considerations to form a foundation from which communities can consider their specific needs and concerns and extend the SMM by creating profiles that consider industry and device specific concerns. This document is a profile for the Digital Twin community. The SMM allows for extensibility, which means that Digital Twin communities can use this profile and extend it as necessary to meet the needs of their vertical industry or needs.

This document, the "IoT Security Maturity Model (SMM) Digital Twin Profile," is an industry profile extension to the "IoT Security Maturity Model: Practitioners Guide"[2] that provides details on the SMM. This profile draws on the detailed analysis conducted through collaboration of the IIC security, IIC digital twin and DTC security groups.

1 THE IOT SECURITY MATURITY MODEL

The goal of an SMM is to provide a path for Internet of Things (IoT) providers to know where they need to be, and how to invest in security mechanisms that meet their requirements without over-investing in unnecessary security mechanisms. It seeks to help organizations identify the appropriate approach for effective enhancement of these practices where needed. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape.

[1] *https://www.digitaltwinconsortium.org/initiatives/the-definition-of-a-digital-twin.htm*
[2] [IIC-SMMP2020]

As an informed understanding of the risks and threats an organization faces is the foundation of choosing and implementing appropriate security controls, the model provides a conceptual framework to organize the myriad considerations. The framework helps an organization decide what their security target state should be and what their current state is. Repeatedly comparing the target and current states identifies where further improvement can be made.

Not all IoT systems require the same strength of protection mechanisms and the same procedures to be deemed "secure enough". The organization 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 implementation 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. Hence, *security maturity* is the degree of confidence that the current security state meets all organizational needs and security-related requirements. Security maturity is a measure of the understanding of the current security level, its necessity, benefits and cost of its support. Factors to weigh in such an analysis include the specific threats to an organization's industry vertical, regulatory and compliance requirements, the unique risks present in an environment and the organization's threat profile.

Security level,[3] on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner. The SMM does not say what the appropriate security level should be; it provides guidance and structure for organizations to identify considerations for different maturity levels appropriate for their industry and system. It provides guidance for defining and accounting for different levels of comprehensiveness and alignment with industry sector and system, including non-industrial systems. Some users of the model will apply its guidance to create industry- and system-specific profiles, which can then be used by a broader audience, in concert with the model, to help assess maturity in a specific vertical or use case.

The audience for this document includes owners of IoT systems, decision makers, security leaders in various verticals, business risk managers, system integrators, architects, security assessors, analysts, policy and regulatory authorities, and other stakeholders concerned about the proper strategy for the implementation of mature security practices tailored to the needs and constraints of the specific IoT system.

Those using this SMM should be able to determine and clearly communicate to management the answers to the following questions:

- Given the organizational requirements[4] and threat landscape, what is my solution's target maturity state?

[3] According to [IEC-62443-33]

[4] Namely, business or mission needs, requirements from regulatory authorities, and other similar factors.

- What is my solution's current maturity state?
- What are the mechanisms and processes that will take my solution's maturity from its current state to its target state?

1.1 THE SMM PROCESS

Organizational business stakeholders define goals for the security posture of the organization and the systems it owns or operates. These systems may be brand new or brownfield. These goals should be mapped to objectives that tie to the risks. Technical teams within the organization, or third-party assessment vendors, map these objectives into tangible security techniques and capabilities, identifying the appropriate target security maturity state. Establishing a target maturity state, while accounting for industry and system-specific considerations, facilitates generation of security profiles. These profiles capture target security maturity states of systems and can act as templates for evaluating security maturity of a specific area of use, common use-case or system of interest.

1.2 UNDERSTANDING THE MODEL

Figure 1-1 illustrates the structure of the SMM and the breakdown of security maturity domains. *Domains* are the high-level views that capture the key aspects of security maturity: governance, enablement and hardening. Each of the domains has different key aspects to it, called *subdomains*. For example, the hardening domain includes subdomains vulnerability and patch management, situational awareness and event and incident response. Each domain may use a variety of practices, both technical and organizational, to achieve results related to that domain.

This hierarchical approach enables the maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.

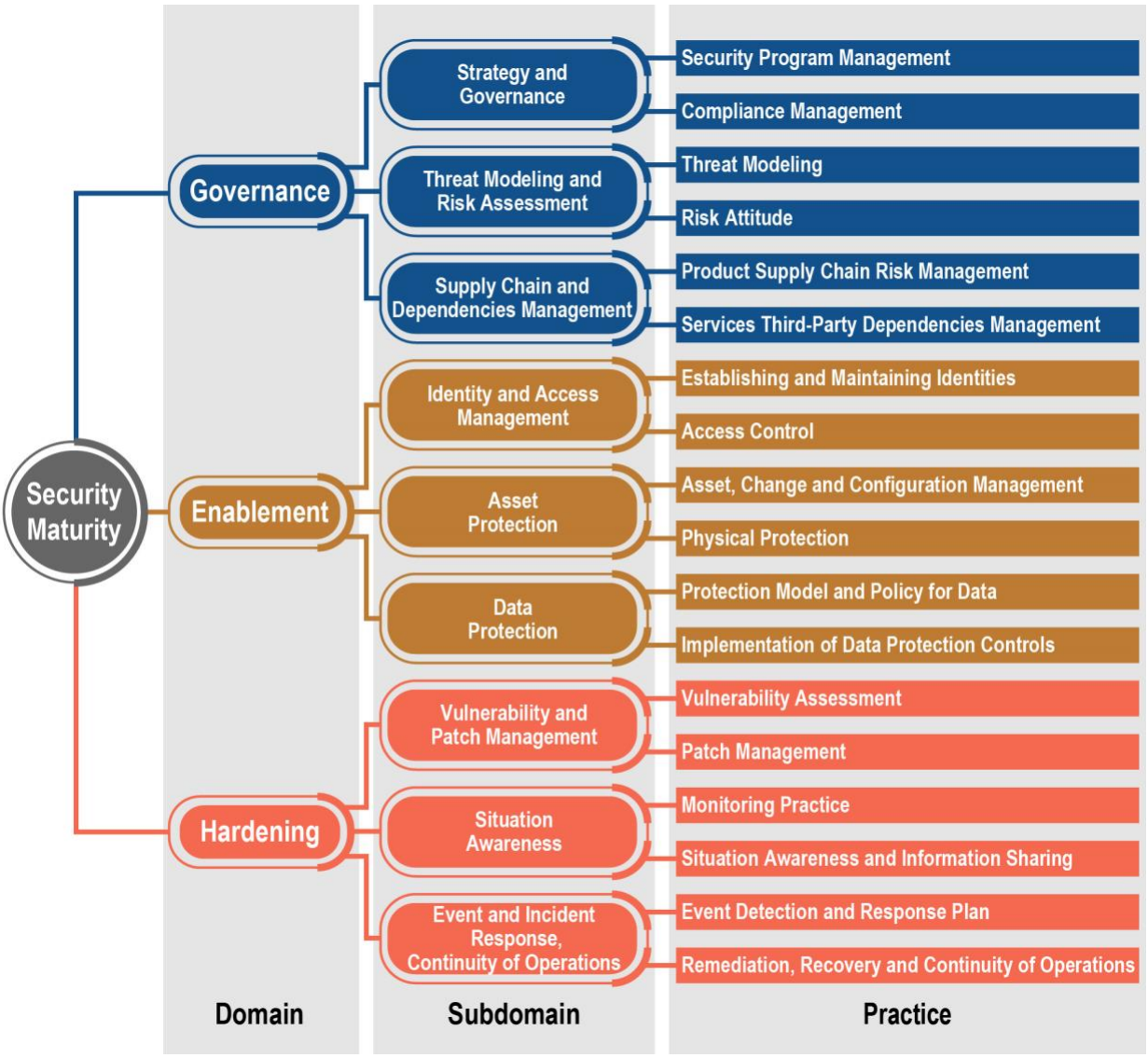

Figure 1-1: SMM hierarchy.

Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level.

At the domains level, the stakeholder determines the priorities of the direction in improving security.

Subdomains reflect the basic means of obtaining these priorities at the planning level.

At the subdomains level, the stakeholder identifies the typical needs for addressing security concerns.

Practices define typical activities associated with subdomains and identified at the tactical level.

At the practices level, the stakeholder considers the purpose of specific security activities.

1.2.1 SECURITY GOVERNANCE

Figure 1-2 below describes the elements of the governance domain of the SMM.

The security governance domain is the heart of security. It influences and informs every security practice including business processes, legal and operational issues, reputation protection and revenue generation.

Security strategy and the governance subdomain facilitates organizational drivers along with providing security, compliance with regulations, laws and contractual obligations. This also can relate to customer expectations and reputation management.

Security program management practice is vital to the clear planning and timely provision of security activities, control over the process and results and optimal decision-making procedure for fulfillment of security related demands.	**Compliance management practice** is necessary when strict requirements for compliance with evolving security standards is needed.

Threat modeling and the risk assessment subdomain identifies gaps in specific configurations, products, scenarios and technologies and prioritize countermeasures accordingly.

Threat modeling 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.	**Risk attitude 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.

Supply chain and the external dependencies management subdomain aims at controlling and minimizing a system's exposure to attacks from third parties that have privileged access and can conceal attacks.

Product Supply chain risk management 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.	**Services Third-Party dependencies management 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.

Figure 1-2: Security governance.

1.2.2 SECURITY ENABLEMENT

Figure 1-3 below describes the elements of the enablement domain of the SMM.

The security enablement domain is based on established security policy and addresses the business risks using the best available means. Security policy and controls are subject to periodic review and assessment.	
Identity and access management subdomain aims to protect the organization and control the use of resources by the identified agents to reduce the risk of information leakage, tampering, theft or destruction.	
Establishing and maintaining identities practice helps to identify and constrain who may access the system and their privileges.	**Access control practice** 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.
The asset management subdomain is put in place to protect both physical and digital assets. This is an area of strong collaboration between IT and physical security teams.	
Asset, Change and Configuration Management practice constrains the types of changes allowed, when those changes can be made, approval processes and how to handle emergency change scenarios.	**Physical protection practice** 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.
The data protection subdomain prevents unauthorized data disclosure or manipulation of data, both for data at rest, in transit and in use. This is important for security, privacy, regulatory compliance, legal and intellectual property protection.	
The security model and policy for data practice identifies whether different categories of data exist and considers the specific objectives and rules for data protection.	**The implementation of data protection controls practice** describes the preferred application of data protection mechanisms to address confidentiality, integrity and availability.

Figure 1-3: Security enablement.

1.2.3 SECURITY HARDENING

Figure 1-4 below describes the elements of the security hardening domain of the SMM.

The security hardening domain practices support trustworthiness objectives through the assessment, recognition and remediation of risks with both organizational and technical countermeasures.	
Vulnerability and the patch management subdomain policies and procedures keep systems up to date and less prone to attacks.	
Vulnerability assessment practice helps to identify vulnerabilities, determine the risk that each vulnerability places on the organization and develop a prioritized remediation plan.	**Patch management practice** policy 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.
The situational awareness subdomain aims at understanding the current security state enabling an organization to prioritize and manage threats more effectively.	
Monitoring practice is used to monitor the state of the system, identify anomalies and aid in dispute resolution.	**Situational Awareness and Information sharing practice** helps organizations be better prepared to respond to threats. Sharing threat information keeps systems up to date.
Event and incident response, continuity of operations subdomain implemented in a combination of policy and technical preparation allows an organization to respond to incidents swiftly and minimize disruption to the rest of the system.	
An event detection and response plan define 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.	**Remediation, recovery, and continuity of operations** represent 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.

Figure 1-4: Security hardening.

1.3 APPLYING THE MODEL

Two aspects are essential for measuring the maturation progress of IoT systems and prioritizing associated security practices: comprehensiveness and scope. These are considered within the context of the target and assessment, namely the system of interest, whether end-to-end, a component or a sub-system under consideration.

Comprehensiveness captures the degree of depth, consistency and assurance of security measures that support security maturity domains, subdomains or practices. 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, subdomains or practices. Such customizations are typically required to address industry-specific or system-specific constraints of the IoT system.

1.3.1 SCORING AND PRIORITIZATION

Any rigorous security self-assessment procedure, including the SMM, needs a scoring and prioritization method to enable evaluation of the current state and the development of a metrics-based security strategy.

Comprehensiveness and scope, which are orthogonal, help score and prioritize security maturity practices. Certain IoT systems may not require the highly sophisticated or narrowly scoped implementation of all security practices. Such implementation may be over-engineered, given the particular system and the threats that it faces. The security maturity of the system should be determined against the requirements that best meet its purpose and intended use.

1.3.2 COMPREHENSIVENESS LEVELS

There are five comprehensiveness levels for every security domain, subdomain and practice, from Level 0 to Level 4, with larger numbers indicating a higher degree of comprehensiveness of security controls. Every comprehensiveness level covers all the requirements set by the lower levels, augmenting them with additional ones.

- *Level 0, None:* There is no common understanding of how the security practice is applied and no related requirements are implemented. (As this is null, we shall 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, application of measures learned through successful references may be applied.

- *Level 3, Consistent:* The requirements consider best practices, standards, regulations, classifications, software and other tools. Using such tools helps to 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 on the implementation focuses on the coverage of security needs and timely addressing of issues that appear to threaten the system of interest. For this assurance, a more complex approach is applied that uses semi-formal to formal methods.

1.3.3 SCOPE

The scope measurement captures the extent to which the specifics of an application, network or system of interest is taken into account during the implementation of the security facet.

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 IoT 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. Combining the general and domain specific objectives in a unique manner sets the requirements of this implementation.

1.3.4 SMM TEMPLATE

All IoT devices, networks and systems do not require the highest comprehensiveness and scope for all security domains, sub-domains or practices. The security maturity target for the system of interest is defined as the set of all desirable values of comprehensiveness and scope characteristics for every security maturity domain, sub-domain and practice.

In case of insufficient details about the system-security needs the stakeholders may initially determine the target levels of comprehensiveness and scope just for domains. These levels determine the relative priorities of security governance, enablement and hardening. The levels set for the domains will be inherited by the appropriate sub-domains and then by the practices according to the hierarchy. The stakeholders may modify the levels to match the risks more closely. This is helpful for the step-by-step recognition of an uncertain security maturity target.

The security maturity target by default is defined when referring to the comprehensiveness and scope for security maturity practices as seen in The Security Maturity Model Practitioner's Guide.[5] Each practice table has four columns, one for each comprehensiveness level. The objective in each level describes the general considerations that should be met. Guidance is provided in the form of general considerations.

	Comprehensiveness Level 1 (Minimum)	Comprehensiveness Level 2 (Ad Hoc)	Comprehensiveness Level 3 (Consistent)	Comprehensiveness Level 4 (Formalized)
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>

Table 1-1: SMM template.

1.4 SECURITY MATURITY PROFILES

The SMM is designed to be extensible across a wide array of industries and systems. It addresses the general scope, which looks at common security maturity best practices in the industry. There is an opportunity to add industry-specific and system-specific scope to any or all of the practices.

The IIC will collaborate with a wide range of industry groups to encourage development of profiles—practice tables that go beyond general scope and include industry- and system-specific requirements for different comprehensiveness levels. For example, a retail group may create profiles of some or all practices that include best practices and regulatory requirements specific

[5] [IIC-SMMP2020]

to the retail industry; they may also create system specific profiles for commonly used devices such as card readers or security cameras. A health care profile may include specific guidance related to *HIPAA*, while a system-specific profile could address considerations for, say, *FDA* pre- and post-market guidance for implanted medical devices.

Industry and system profiles need not be created for every practice in the model. An industry may decide that the general scope is sufficient for most of the governance-related practices but that a few of the enablement practices necessitate an industry-level point of view. When extending for industry or system-specific considerations, the practice table as seen in Table 1-2 expands to include two additional rows.

<Practice Name>				
<Practice Description>				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Industry-specific considerations	<List of Level 1 industry specific considerations>	<List of Level 2 industry specific considerations>	<List of Level 3 industry specific considerations>	<List of Level 4 industry specific considerations>
System-specific considerations	<List of Level 1 system specific considerations>	<List of Level 2 system specific considerations>	<List of Level 3 system specific considerations>	<List of Level 4 system specific considerations>

Table 1-2: Template with industry and system specific considerations.

Industry-specific considerations include the sector-specific issues, particularly components and processes that are prone to certain types of attacks, known vulnerabilities, incidents that took place in similar systems and possible harm to this kind of operational technology as well as sector specific priorities including legal and regulatory guidance.

While the general row in the table included headings for achieving the level and indicators of accomplishment, the industry row should include a general description of the industry-specific issues as noted above and for a comprehensiveness level with industry-specific considerations:

- what needs to be done to achieve that level and
- relevant industry guidelines for that level.

System-specific considerations include the specific security-relevant business needs and risks for the system under consideration, identified trust boundaries, components, technologies, processes, and usage scenarios that combine the general and domain-specific objectives in a unique manner. This digital twin profile provides considerations at the system-specific scope. Digital twins may be applicable to a variety of industries, yet in each case the concerns about the digital twin system are applicable, since they are system-specific. An industry profile may reference this profile without repeating the system-specific digital twin concerns while elaborating the industry scope considerations.

As the general and industry rows in the table included headings and structure described above, the system row should include a description of the system and how it is used in the larger IoT infrastructure and for a comprehensiveness level with industry-specific considerations:

- what needs to be done to achieve that level and
- indicators of accomplishment that can assist assessors in identifying if the organization has met the requirements of the level.

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)**
System-Specific Scope Considerations	Threat models are static. Twins and assets have different threat modeling.	Threat models incorporate the impact of twin on asset, and vice versa.	Threat models incorporate both physical and virtual at the same time. That is, they include threat models that attack vulnerabilities that cross the physical and virtual.	Threat models include multiple industries (i.e., from both physical and virtual), or from other industries using virtual twin systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Critical infrastructure, or mission critical components have appropriate (if siloed) threat models.	Threat modeling scenarios consider threats to the asset posed by breach through a digital twin, and digital twin threats posed by a compromised asset.	Threat models include scenarios that span the entire digital twin system from asset to twin.	Twin vendors share information and cooperate on building threat models and share vulnerabilities in such a way that cross twin impact can be analyzed.
		Threat modeling standards used are not twin aware.	Static threat models incorporate the impact on critical infrastructure. Threat modeling standards used incorporate twins.	Federated twins across industries and organizations are using threat modeling standards and best practices.
		Understanding and inventory of third-party software, open-source software used in twin and general understanding of threats.	Threat modeling of third-party software, open source in twin.	
			Twin vendors share information on their own domain with corresponding twins and customers in a way that is actionable and useful by the other parties.	
			Threat modeling and testing of digital twin simulation	

			component reflecting understanding of algorithms and simulation.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Threat modeling exists but found in separate asset-related and digital related documents. Digital twin threat modeling documents consider general IT security threats only.	Asset and digital twin threat modeling documents and approach reference each other and consider threats across both and from both to each other. Documented digital twin threats go beyond IT threats and consider asset posed threats.	Threat modeling documents and standards consider digital twins and interactions between assets, twins, and vice versa, as well as threats posed by third-party components. Threat modeling documents consider threats posed by simulations and algorithms.	Threat modeling includes threats from other vendors and industries.

Table 1-3: Threat modeling practice example.

Establishing a target maturity state, while accounting for industry and system-specific considerations, facilitates generation of security profiles. These profiles capture systems' target security maturity and can act as templates for evaluating security maturity of a specific area of use, common use-case or system of interest.

2 DIGITAL TWIN SECURITY CONSIDERATIONS

2.1 DIGITAL TWIN ARCHITECTURE CONSIDERATIONS

Digital twin architecture can be fairly complex since assets and twins must have corresponding information models to the required degree of fidelity and must maintain synchronization with each other at an appropriate frequency. In addition, a system may include multiple twins and assets interacting with other systems as well. These include a data model, AI and simulation components, synchronization mechanisms, application interfaces, a networking and software platform and support for security and trustworthiness as shown in Figure 2-1:

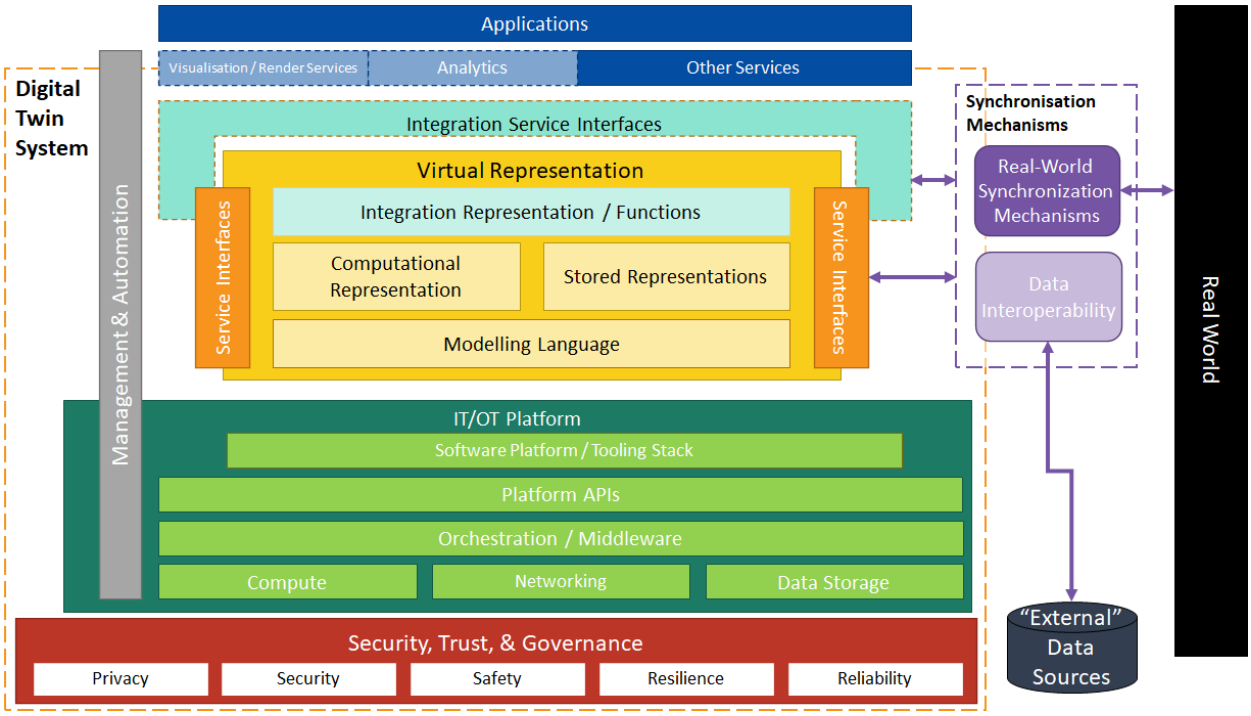

Figure 2-1: Digital twin architecture.

In addition to the architecture of a single digital twin, multiple digital twins may be deployed as part of a solution, as federated digital twins. These digital twins may span organizations and administrative boundaries and may or may not have originally been constructed with intent to be a digital twin. Connections among digital twins may need to reflect and possible enforce policy constraints (e.g. security access control) similar to the corresponding real assets.

Physical assets may also have physical twins such as testbeds or redundant hardware implementations. These should be understood and managed in the context of assets but are not addressed directly in this document. In the tables in this document the term “twin” refers to a digital twin.

In a more complicated scenario involving more than one twin, it may be the case that many of the components of the system will be developed in isolation from each other and with different design assumptions. This can become an issue when they have to work together, and problems may arise ranging from basic interoperability to the semantics of data and the approach toward security. Data from different sources may describe the same things in different ways so work may be required to align data and models. In addition, since these systems may be under different organizational control they may evolve at different rates and with different goals, so the lifecycle needs to be considered across the entire system.

The DTC definition of a digital twin highlights two essential aspects of a digital twin architecture that must be considered when evaluating security maturity:

- The appropriate fidelity of the virtual representation to the real-world entities.
- The ability to synchronize the virtual twin at a specified frequency with the asset, maintaining integrity of the representation over time.

Fidelity of digital twins is a bi-directional concern. There should be confidence on the part of creators and users of the digital twin model that it reflects assets, but there should also be confidence on the part of the asset owners that the model is reasonable and useful. This has implications for change management, for example.

The requirements for synchronization can vary. The time can vary, and it can be real-time or intermittent or manual depending on the context. Data loss and latency are considerations. Synchronization is also bi-directional and the digital and the physical twin may have different requirements.

The consequences of security risks associated with twins includes safety concerns related to OT, since assets associated with twins can affect people and cause loss of life, injury or harmful effects on the environment. Twins take these concerns further since an inadequate or attacked model can lead to unanticipated consequences.

Twins can be considered a system of systems, whether as a single twin and asset or several interconnected twins and corresponding assets, a federation of twins. With twins, especially with multiple interacting twins (systems of twins, including their associated assets), data sovereignty may play a role when twins are in different countries or even if they fall under the regulatory scope of different industries. The role of local laws and regulations can be of especial concern when physical assets are involved, bringing into consideration safety and other concerns. This means assets and twins may be subject to laws and regulations of the countries in which they are located, and this can have an impact on the security maturity targets and the corresponding assessments of how well such requirements are considered. Data residency, requirements on where data is stored, may also play a role for the virtual twin itself, perhaps affecting the use of cloud solutions, for example.

The issues of multiple organizations, different administrative boundaries, variation in governance, and different technologies may also play a role in evaluating security maturity when multiple organization twins are used together. The differences of risks and risk tolerance in different locales may also matter, highlighting the need to carefully consider the context of the security maturity evaluation.

A major challenge with relying on laws and regulations for trustworthiness is that they are often written after a technology emerges and is adopted. The understanding needed to develop the laws and regulations occurs once the technical impacts are understood. For example, in the manufacturing domain machines and systems are being or are already interconnected while regulations and laws remain to be established. Thus, one cannot achieve safety and security simply by following rules and regulations but must understand the systems holistically, including

hazards, risks and consequences. In addition, one must understand the assumptions and possible influences that require changing these basic assumptions. This always true even when there are rules and regulations but is especially true when new technical approaches emerge. This highlights the importance of different parties involved with security, safety, reliability, resilience, privacy and production to collaborate across organizational boundaries to achieve trustworthiness.

In this integrated architecture it is clear that an organized approach to security that includes the entire implementation lifecycle, governance and operations is required. Understanding the context (e.g. the proper model for a given scenario such as cars vs. transportation system in an intersection) and the organizations involved is necessary. The SMM offers an approach toward prioritization and understanding requirements. SMM Mappings can offer linkage to detailed controls such as those offered in 62443, the NIST Cybersecurity Framework, the IIC Security Framework and others.

2.2 COMMON DIGITAL TWIN SMM COMPREHENSIVENESS LEVEL CONSIDERATIONS

There are some common themes of how digital twin considerations relate to the SMM comprehensiveness levels. This is not repeated in every table but is summarized here and can be used as a starting point for which comprehensiveness level is considered in each table.

For example, if the intent is to have complex federated digital twin implementations for mission critical applications, then the SMM Level 4 comprehensiveness level is likely a good starting point when considering each of the eighteen practice tables. Note that having a federation of twins does not make a system have higher security maturity but understanding and being able to work effectively with a federation may do so, depending on the common comprehensiveness level considerations as well as the considerations of specific practices.

When using this common table or the specific practice tables if one characteristic, such as the digital twin solution complexity suggests a comprehensiveness level (e.g. 3) as a target but another characteristic such as digital twin fidelity suggests a lower level (e.g. 1), the higher target level should be used, not an average.

Similarly, in an assessment, the lower assessed value should be used. The SMM practitioners guide notes that a + notation may be used to indicate that there are some indicators associated with a higher level, but not all criteria of the higher level have been met.

Common Digital Twin Comprehensiveness Level Considerations (All Practices) The contents of this table should be considered part of all the SMM Practice tables in this Digital Twin Profile.				
	Comprehensiveness Level 1 (Minimum)	**Comprehensiveness Level 2 (Ad Hoc)**	**Comprehensiveness Level 3 (Consistent)**	**Comprehensiveness Level 4 (Formalized)**
System-Specific Scope Considerations	Digital twin model used only for organization's low impact non-critical use cases.	Digital twin model used only for organization's low and moderate impact use cases.	Digital twin model used for use cases having higher organizational impact	Federated interaction among different twins understood and considered in analysis.
	Simple Digital Twin implementation with both twin and assets in one organization.	Slightly complex digital twin implementation with multiple digital twins of a uniform type and multiple assets within one organization.	More complex digital twin implementation with multiple digital twins of different types.	Complex digital twin implementation with variety of federated digital twins across organizations.
	Fidelity of digital twin with respect to assets can be low, not critical concern. Frequency of digital twin synchronization with assets need not be high.	Fidelity of digital twin with respect to assets should be good but may not require frequent update.	Fidelity of digital twin with respect to assets should be good and reasonably frequent.	Fidelity of digital twin with respect to assets should be high as a critical aspect. Frequency and variation of frequency of digital twin synchronization across federated digital twins is understood and managed.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Organization uses off-the-shelf security practices, not customized for its own needs, systems, or organization.	Organization considers its own risks in using digital twin models and considered asset OT and digital twin IT security but separately.	Organization considers data risk to other organizations when using their data and manages access control across organizations. Organizations consider the interrelationships of different twins, and different vendor implementations.	Organization continually considers impact on other organizations' security compliance when designing their policies and procedures. Organization continually updates security compliance with regard to environment. Organization regularly reviews security policy and procedures with regard to own assets, other organizations, and their environments.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	IT practices are documented and used and applied to asset and digital twin separately.	Static system level security requirements are implemented. Asset physical security is managed separately from cyber security.	Static cross-organizational security requirements are implemented. Organizations have separate security plans for different types of twins.	Pro-actively evolving or changing Cross-organizational security requirements and their implementation in policies and procedures.

Table 2-1: Digital twin comprehensiveness level considerations for all SMM practices.

The separation between the levels is designed to reflect the fundamental reality that digital twins are connected systems of systems. This means that higher levels represent:

- a higher level of control of flow of data between systems and across system boundaries,

- a higher capability to deal with unexpected changes in the system, particularly those coming from external (e.g. supply chain borne) components and
- a higher capability to ensure that the virtual data matches the physical reality, and vice versa.

3 PROFILE TABLES

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

3.1 SECURITY PROGRAM MANAGEMENT

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)**
System-Specific Scope Considerations	Security program management scope is siloed and does not consider digital twins.	Security program management scope considers digital twins but separately from assets.	Security program management scope considers digital twins and corresponding assets holistically.	Security program management scope considers digital twins and assets on a continuous basis.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Assets and digital twins are managed separately. Digital twin security is managed as part of IT security.	Security program management documents reference digital twins. Systems are compliant as stand-alone, or within only the scope of the system (Not within the scope of	The scope of security program management includes functions impacted by interactions between twins and assets.	Twins (virtual and physical) are regulated. Security program management considers regulatory impact across various regulatory domains. Security program management considers the

		multiple interacting physical or virtual systems). digital twins are considered.		impact of twins from different regulatory regimes operating together in a single system of systems.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
		Security program management documents reference twins.	Security program management documents consider the bi-directional impact of twins and assets.	Security program management documents consider regulatory impact. Security program management documents consider the entire digital twin lifecycle and management over time. Security program management considers required interactions between the organization and external organizations such as digital twin vendors of different types of digital twins and digital twins that span or interact with business partners.

Table 3-1: Security program management.

3.2 COMPLIANCE MANAGEMENT PRACTICE

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)**
System-Specific Scope Considerations	Formal or informal compliance with a set of general or generic practices.	Compliance documents reference digital twins.	Compliance of twins and assets take impact of the other into account. Scope of compliance includes the impact and risk of multiple regulatory regimes interacting in a single digital twin system.	Scope of compliance includes the impact and risk across multiple digital twin systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Compliance program for assets does not consider other systems, nor does it consider digital twins. Digital twins do not take into account industry or asset compliance requirements.	Consideration of interactions of virtual asset representations and physical assets. Compliance considers asset compliance and virtual representation compliance but separately.	Scope of compliance includes the entire system of twins. Scope of compliance includes functions impacted by interactions between assets and twins. Digital twins consider industry compliance and regulations.	Compliance deliverables for digital twin systems is considered across multiple systems. Fidelity of simulation is taken into account for physical system compliance, and for federated virtual system.

	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment
	Compliance documents exist for assets and do not reference their digital twin counterparts.	Systems are compliant as stand-alone, or within only the scope of the system. (Not the digital twin or the federation.) Scope of compliance includes interactions between twins and assets.	Compliance documents of assets take into account digital twins and vice versa. Compliance between twins and assets is synchronized. Fidelity of simulation taken into account for virtual system compliance.	Compliance documents take into account regulatory impact across multiple systems and different types of digital twins. Simulation component regulatory compliance is considered and synchronized with asset and digital twin regulations.

Table 3-2: Compliance management.

3.3 Threat Modeling Practice

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)**
System-Specific Scope Considerations	Threat models are static. Twins and assets have different threat modeling.	Threat models incorporate the impact of twin on asset, and vice versa.	Threat models incorporate both physical and virtual at the same time. That is, they include threat models that attack vulnerabilities that cross the physical and virtual.	Threat models include multiple industries (i.e., from both physical and virtual), or from other industries using virtual twin systems.

	What needs to be done to achieve this level	What needs to be done to achieve this level	What needs to be done to achieve this level	What needs to be done to achieve this level
	Critical infrastructure, or mission critical components have appropriate (if siloed) threat models.	Threat modeling scenarios consider threats to the asset posed by breach through a digital twin, and digital twin threats posed by a compromised asset.	Threat models include scenarios that span the entire digital twin system from asset to twin.	Twin vendors share information and cooperate on building threat models and share vulnerabilities in such a way that cross twin impact can be analyzed.
		Threat modeling standards used are not twin aware.	Static threat models incorporate the impact on critical infrastructure. Threat modeling standards used incorporate twins.	Federated twins across industries and organizations are using threat modeling standards and best practices.
		Understanding and inventory of third-party software, open-source software used in twin and general understanding of threats.	Threat modeling of third-party software, open source in twin.	Enhanced threat modeling based on bill of material (BOM) and provenance proofs available for third-party and open source software in twin.
			Twin vendors share information on their own domain with corresponding twins and customers in a way that is actionable and useful by the other parties.	

			Threat modeling and testing of digital twin simulation component reflecting understanding of algorithms and simulation.	
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Threat modeling exists but found in separate asset-related and digital related documents. Digital twin threat modeling documents consider general IT security threats only.	Asset and digital twin threat modeling documents and approach reference each other and consider threats across both and from both to each other. Documented digital twin threats go beyond IT threats and consider asset posed threats.	Threat modeling documents and standards consider digital twins and interactions between assets, twins, and vice versa, as well as threats posed by third-party components. Threat modeling documents consider threats posed by simulations and algorithms.	Threat modeling includes threats from other vendors and industries.

Table 3-3: Threat modeling.

3.4 Risk Attitude Practice

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)**

System-Specific Scope Considerations	Risk management is appropriate to criticality of systems and industry.	Risk management includes twin functions as part of a larger system of systems.	Risk management includes impact on the other part of the twin (e.g. the impact of twin on asset).	Risk management includes comprehensive and holistic risk of entire twin system of systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Risk management does not incorporate twin concepts. Twins are managed separately and without impact on each other taken into consideration or impact of the twin on an asset.	Risk management incorporates twin concepts. Twins are managed together with documented impact on each other but separately managed from assets.	Risk management incorporates twin concepts and documented impact of twins on assets and assets on twins.	Risk management incorporates risk posed by twin systems to other internal twin systems and across organizational boundaries. Risks of the same type of twins created by different vendors as well as twins of different types are included.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
		Risk management documents reference digital twins and general risk posed to systems and related assets.	Risk management documents reference the impact a twin has on its related asset and vice versa.	Risk management documents include risk posed by twins to other twins, to entire twin systems, and across organizations.

Table 3-4: Risk attitude.

3.5 Product Supply Chain Risk Management Practice

Product Supply Chain Risk Management				
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)**
System-Specific Scope Considerations	Physical and virtual supply chains are independent.	Physical and virtual supply chains are coordinated but may not be synchronized.	Physical and virtual supply chains are synchronized.	Physical and virtual supply chains are synchronized across multiple systems and partners and throughout the lifecycle.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
		Customer's supply chain functions take into account use of acquired systems and data in a digital twin but may not take into account the implications of the data exchanged between systems.	Supply chain considerations include data to and from both physical and virtual, and between twins. Acquired components and data are cross-referenced to their physical and virtual counterparts to maintain config-uration manage-ment. However, impact and risks may not be consistently or pro-actively incorpor-ated into supply chain functions.	Customer organization supply chain policies (acquisition, risk analysis) take into account implications for twins, virtual and physical asset counterparts. This includes functions, functionality, and data.

	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment
		Updates and changes to a twin triggers ad-hoc analysis in its asset counterpart.	Traceability documents exist to and from physical and virtual for security considerations.	Traceability documents to and from physical and virtual for security considerations are triggered by a process when a change in one, or the other occurs.

Table 3-5: Product supply chain risk management.

3.6 Services Third-Party Dependencies Management Practice

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)**
System-Specific Scope Considerations	Physical and virtual supply chains are managed independently.	Physical and virtual supply chains are coordinated but may not be synchronized. Vendors are not aware of their product's use or relationships.	Physical and virtual supply chains are synchronized. Vendors are aware of their product's use and of other vendors	Physical and virtual supply chains are synchronized across multiple systems and partners and throughout the lifecycle. Vendors are involved with the organization and their product and interacting with other vendors.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

		The organization manages digital twin implications with sufficient asset vendor information, but vendor is not necessarily aware of the organization using digital twins. The organization may derive data implication from system information, or vice-versa.	Vendor supplies sufficient information for the organization to manage digital twin implications, this includes systems and data. Vendor is aware that the organization is using digital twin and that the vendor is providing data for the digital twin. Differences in virtual and physical delivery times/frequency/scope are managed by the organization.	Vendor is active partner in the organization's digital twin effort. Regulatory licensing and certification approvals for a system include both digital twin and physical aspects of system.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
		Architecture and operations policies exist by the organization that demonstrate the relationship between the digital twin and the asset.	Supplier/contract includes DT specific information: fidelity, frequency, and operational requirements (training, skills, environment, support).	Vendor actively manages or is full partner with the organization and jointly manages twin implications.

Table 3-6: Services third-party dependencies management.

3.7 Establishing and Maintaining Identities Practice

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)**

System-Specific Scope Considerations	Identity management is separate for twins and assets. No coordination between virtual and physical**.**	Identity management of twins and assets is unified.	Identity management of twins and assets is automated.	Identity Management is coordinated across federated twins and organizations.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
		Systems have identity that is managed. Twins have roles, tied to the asset, but coordination is managed manually.	Identity management capabilities (roles, authentication) are managed and automatically synced across twins. Each role in the twin is managed with consideration of the different functional boundaries between corresponding twin roles.	Provenance of data is traced through twins. Identity management is automatically managed and synchronized across different types of twins and organizations.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
		Identify management manual processes and documents exist and cover identity management of assets and their twins.	Identify management automated tools support processes and documents exist and cover identity management of assets and their twins.	Identify management automated tools support processes and documents cover identity management across federated twin systems and organizations.

Table 3-7: Establishing and maintaining identities.

3.8 Access Control Practice

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)**
System-Specific Scope Considerations	No coordination of physical and virtual aspects – assets and twins are not aware of each other.	Access control is coordinated physical and virtual but is manually and independently managed.	Access control for assets and twins is managed holistically.	Access control for assets and twins is managed across systems of systems of twins and organizations.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
		There is communication of access control management information across different parts of system, but it is ad hoc and not necessarily consistent. The asset and virtual copy are different and may have different roles assigned to them. They have different levels of security and different types of security (e.g. hardware, power, physical feeds).	Access control to both virtual digital twin resources and physical asset resources is managed from one single administrative organization with understanding of relationship of twin to asset. Access control across multiple twins is managed from one place, with automated coordination between physical and virtual system access	Access and functionality are analyzed between physical and virtual, and the risk and impact of all access is controlled within and across all components of the system Access to physical and virtual components is managed across the lifecycle of the asset and its twin.

		Having access to one does not automatically imply having access to the other.		
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
		Access control policy development explicitly takes digital twins into account. Possible for twin administrator to determine who has access to asset aspect and also for asset administrator to determine who has access to corresponding twin aspect. The policies are then managed separately within each domain.	Single access control policy for digital twin takes into account both physical and virtual. Access is mapped between physical and virtual.	Access policy and implementation are managed continuously and coordinated.

Table 3-8: Access control.

3.9 Asset, Change and Configuration Management Practice

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)**

System-Specific Scope Considerations	Assets are updated independently, according to individual standards or best practices. No consideration between assets and twins and they are managed by OT and IT separately.	Assets and twins are considered together without impact.	Assets and twins are considered together with impact.	Assets and twins are automatically considered together with impact.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
		Updates are synchronized between twin and asset but may not consider impact.	Updates to twin or asset take into account the impact on the corresponding twin or asset.	Updates to twin or asset are automatic and take into account the impact on the corresponding twin or asset.
		Regression testing's impact on the other twin handled manually, or case-by-case.	Regression testing includes functions relevant to the other twin.	Regression Testing is continuous and automatic and includes impact on the other corresponding twin asset.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
		Standard operating procedures ensure that updates to an asset are reflected in the twin and vice versa.	Standard operating procedures ensure that updates to an asset are reflected in the twin and vice versa and that their impact on each other is considered.	Standard operating procedures include the use of automated tools and testing to ensure the relationship of the asset and twin is maintained.

Table 3-9: Asset, change and configuration management.

3.10 PHYSICAL PROTECTION PRACTICE

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)**
System-Specific Scope Considerations	Physical protection needs of an asset and its twin are considered completely separately.	Physical protection needs of an asset and its twin are coordinated.	Physical protection standards are applied and the impact of physical environments of the asset on twin and vice versa is considered.	Physical protection is understood and applied across a twin federation.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Physical protection of an asset and its twin are completely separate.	Physical security may encompass the asset and twin infrastructure together, or at least considered as part of a complete system. Physical security measures take into account the criticality of the asset.	Physical access to digital twin servers has same level of protection as access to assets.	One single, complete physical protection practice covers both assets and digital twins in a twin federation.
		Impact on digital twin of security breach on asset is considered, for example impact of simulated sensor, and vice versa.	Protect against sensor spoofing or false data being provided to twin.	

	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment	Indicators of accomplishment
	Documents and processes exist but are separate.	Physical security implementation and associated processes are coordinated across the asset and digital twin. Physical security measures match the criticality of the asset or severity of impact of a breach to the asset or twin.	Physical protection documents specific standards applied to physical assets as well as digital systems and the impact of a breach in the physical security of each is understood on the counterpart.	Physical access policies, processes and mechanisms recognize the asset criticality level and ensure both asset and twin are equally protected.

Table 3-10: Physical protection.

3.11 Protection Model and Policy for Data Practice

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)**
System-Specific Scope Considerations	Digital twin model does not consider data protection.	Digital twin model considers organizational data concerns.	Digital twin model adheres to data protection and data residency regulations.	Digital twin model considers data sharing concerns across organizations.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Enterprise policies do not address Digital Twins specifically. Security of information is a one-size-fits-all	Enterprise policies include some general aspects and references to digital twins such as:	Enterprise policies include specific static requirements for digital twins such as:	Enterprise policies include dynamic digital twin.

	approach: all data and processes are regarded equally. Policy limited to single-party digital twin systems and simulations. Only IT data protection mechanisms are applied.	• Data and their sources are classified according to its business and security impacts taking into the distinctions between general IT data and OT/digital twin data. • Risk assessments are performed over data sources, data outputs, and business criticality, specifically taking into account impacts on physical assets. • Data sharing, transfer, communication, etc. are distinguished between OT systems and IT systems, components, systems, systems of systems, and externally to the enterprise. (e.g. establish various security zones or perimeters to enforce different levels of security.) • Technical mechanisms and practices exist to	• Maintain an inventory of physical and virtual digital twins and their inter-dependencies. • Take into account physical and digital twin inter-dependencies. Digital twin inter-dependencies include shared data, interfaces, integration, synchronization, data sources, and data destinations. • Enable data traceability. • Provide static assurance cases.	

		lock down and isolate channels that pose the highest risk. Specific considerations are giving to isolate digital twins and their respective physical assets from the rest of the IT system. • Mechanisms exist to identify critical assets and sources of data inside and outside the local twin.		
		Policies address single-party or low complexity multi-party digital twin systems, but only for relatively static twin models. Physical assets and virtual twins are treated separately.	Policies address multi-party digital or more complex twin systems, but likely only for relatively static Twin models.	Policies address multi-party digital twin systems, even in a complex and dynamic use cases.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Enterprise policies exist but do not address digital twins.	Catalog of data sources and data exists. Risk assessment reports exist.	Understand data relationships of digital and physical assets.	Automatic and dynamic policy management.
			Review responses and corrective actions following specific breaches.	Regular analysis of collected information on breaches and responses and

			A process and documentation exist for post-mortem of breaches.	coordinated corrective actions.
		Enforce different levels of security for digital twins and assets and their communication		
		Quality of data is considered in use of the data.		

Table 3-11: Protection model and policy for data.

3.12 Implementation of Data Protection Practices Practice

Implementation of Data Protection Practices				
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)**
System-Specific Scope Considerations	Data protection implementation for asset and twin do not consider each other.	Data protection implementation considers asset and twin communication.	Data protection implementation uses standards and static assurance cases.	Data protection considers dynamic and real time cases as well as federated twins.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Few safeguards exist to prevent untrusted data from entering the control plane for critical assets, or for sensitive data from	Technology is applied to identify assets and secure communication channels.	Put policy management in place and enforce it technically to enable known trusted systems to communicate and exchange critical data (*AKA 'static*	Achieve support for dynamic, auditable and timely data protection compliance (e.g. *'dynamic assurance cases'*). This may be achieved by

	leaving the system unprotected. Policy limited to single-party Digital Twin systems and simulations. Only IT data protection mechanisms are applied.		*assurance case'*). This may be achieved by implementing the following actions: • Identify and document risks of missing or late data in critical areas of the system. • Verify data quality capabilities of components against twin system design before deployment.	implementing the following actions: • Data from all sources is considered throughout its entire lifecycle and in accordance with change • Implements lifecycle traceability of data and HW data sources for legal-standard traceability. • Implements automatic validation of data quality (including 'fidelity and frequency') and implemented automated V&V for data quality against use cases. • Implements redundancy and safeguards against data loss, missing readings in both virtual and physical. *(Deal with unexpected loss or late receipt of data)* • Implements protections and verification that dataflows in the Twin precisely match the connections in the

				physical world. *(Deal with unintended leakage/data flow.)*
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Only IT data protection mechanisms exist.	Channels of communications between asset and twin including data at rest are secure.	Data is traceable between multiple twins and multiple vendors.	Data is traceable through its lifecycle. Automatic data validation is in place.
			Policy management is in place supporting static assurance cases.	Dynamic assurance cases are supported.
			Audit compliance reports match system logs.	Audit compliance verification is based on the running system directly.

Table 3-12: Implementation of data protection practices.

3.13 VULNERABILITY ASSESSMENT PRACTICE

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)**
System-Specific Scope Considerations	Consider IT vulnerability analysis of twins and assets separately.	Consider vulnerabilities due to the relationship of twin and asset.	Consider vulnerabilities related to models within twin and relationship to physical assets and consequences.	Consider vulnerabilities related to systems of systems concerns and over system lifecycle.

	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Vulnerability assessments are performed, but separately for assets and digital twins.	Assessment includes vulnerabilities related to the fidelity and frequency of twin synchronization with assets.	Assessment includes the impact of geographical distribution and movements of assets in vulnerability analysis (e.g. physical protection may be less for remote assets than on premises assets).	Assessments include potential vulnerability introduced by models (e.g. appropriateness and fit of model including level of abstraction, and training, potential of inadvertent model changes, need for proper model evolution, adequate testing of model) such as patches). Coordinate vulnerability analysis across different twin administrative boundaries.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Assessment documents exist but do not take into consideration the twin and asset counterpart.	Vulnerability assessments are performed and consider both the asset and digital twin.	Vulnerability assessments are performed and also consider simulations, models and geographic implications of assets.	Vulnerability assessments consider vulnerabilities across federated twins and across organizations.

Table 3-13: Vulnerability assessment.

3.14 PATCH MANAGEMENT PRACTICE

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)**
System-Specific Scope Considerations	Understanding of relationship of patches to twin and asset is limited.	Basic understanding of the relationship of a patch to an asset and to a twin.	Understanding of relationship of twin models to patches of asset and or twin.	Understanding, agreement and coordination of patches with the system of systems as a whole is achieved.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Assets and virtual twins have individual siloed patch management.	Patches are communicated and coordinated between assets and twins.	Functions, systems, or capabilities that are impacted by patches in the corresponding asset or twin known and analyzed before implementation.	Patches to a twin and an asset are understood, agreed and coordinated, including an understanding of possible undesirable consequences of patching.
				Changes caused by patches are known ahead of time, or regression testing in complete.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Patch management policies and procedures are documented but	Patch management policies and procedures are documented, and	Patch management policies and procedures are documented with a	Patch management policies and procedures are documented and

	found in separate documents for assets and digital twins.	their deployment is coordinated, and impact understood, however, they may still be in separate documents.	single document and their impact on asset and twin are well understood.	understood across a federated system of twins and assets and across organizations.

Table 3-14: Patch management.

3.15 MONITORING PRACTICE

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)**
System-Specific Scope Considerations	Asset and twin monitoring are separate and have no awareness of each other.	Asset and twin monitoring are separate but awareness between them exists.	Asset and twin are monitored together, and impact of events is considered holistically.	Monitoring of multiple assets and twins across systems of systems.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**

	Siloed monitoring. Asset and twins have no awareness of each other, nor take any requirements from each other.	Relevant events are shared in a timely manner with corresponding assets or twins. Awareness of expected inputs from, and outputs to, the corresponding asset or twin. Alerts and monitoring may not take into consideration the effects on, or requirements of, the other systems. Awareness of relationship of attacks on twin and asset (e.g. are they coordinated or not, impact of timing)	Monitoring requirements for asset and twin take into account corresponding requirements. Monitoring reflects updates to assets and twins and includes alerts appropriate for inconsistent patching. Monitoring includes synchronization rate between the asset and twin and scope of what is being synchronized.	Events and monitoring capability of the asset take into account the current needs of the twin, and vise-versa. System-wide consolidation and understanding and prioritization of alerts. Monitoring approach addresses concern of alert overload appropriately, for example by having an intelligent automated alert manager that shows salient information.
			Manage alert overloads appropriately. May have intelligent alert interpretation and handling function.	Monitoring may provide automatic parsing and management of alerts.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Monitoring of digital twins and assets exists but are performed separately. Logs and other	Monitoring of assets and digital twins may still be performed separately or jointly.	An automated alerting system is used to monitor anticipated and unanticipated changes to the asset or twin, or both.	Intelligent alerting and events are implemented across a federated set of twins.

	records of one does not reflect any events related to the other.	In either case, logs and other records are compared manually to determine if there is any correlation.		

Table 3-15: Monitoring practice.

3.16 Situational Awareness and Information Sharing Practice

Situational 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)**
System-Specific Scope Considerations	Information sharing related to assets and twins is separate.	Information sharing for assets and twins together as a system.	Information sharing includes external sources.	One comprehensive information sharing plan across systems of twins and assets and other organizations.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	No information sharing plan relevant to twins	Information is shared in a timely manner with the corresponding assets or twins.	Content, timeliness, and requirements for sharing information incorporates both the assets and the twin's regulatory regime, safety requirements, and industry practices.	Formalized and standardized sharing of information within entire twin ecosystem (e.g. different twins across administrative boundaries).
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Information sharing policies and procedures may, or	Information sharing policies and procedures require	Information sharing policies and procedures include	Information sharing policies and procedures include

	may not exist, and do not take into considerations digital twins.	sharing of information when an event of interest occurs at the asset, twin, or both.	regulatory requirements and best practices.	sharing with partners and across federated twins and organizations.

Table 3-16: Situational awareness and information sharing practice.

3.17 Event Detection and Response Plan Practice

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)**
System-Specific Scope Considerations	Events and response plans of assets and twins are managed separately.	Events and response plans of assets and twins are managed separately but coordinated.	Events and response plans of assets and their twins are managed as a single system.	An automated event detection system is used for all assets and twins. Response plans are updated continuously.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Separate plans for each twin or asset.	Events are communicated to corresponding twin or asset. Assets and twins may have documentation of each other's plans.	Event plans are formulated and executed as one whole encompassing both asset and twins. Event detection is communicated in accordance with the integrated plan.	Understand twin federation events by having the ability to understand the relationship and possibly correlation of events across twins. There is one single comprehensive event detection capability, it is updated

				continuously, and the plan incorporates both asset and twins. Event detection and response plan includes synchronization issues, distributed assets or twins, and is continuously updated based on the state or configuration of the asset or twins.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Policies and procedures exist but are separate for assets and twins.	Policies and procedures exist, and if separate for assets and twins, take into consideration each other.	A single policies and procedures approach and document exists for both assets and twins.	A single automated system is deployed across assets and twins.

Table 3-17: Event detection and response plan.

3.18 Remediation, Recovery and Continuity of Operations Practice

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)**
System-Specific Scope Considerations	Remediation and recovery planning is managed separately for assets and twins.	Remediation and recovery planning is managed separately for assets and twins but coordinated.	One single coordinated plan for remediation and recovery is provided for assets and	There is one comprehensive plan for remediation and recovery of assets and twins that is

			twins.	updated continuously.
	What needs to be done to achieve this level	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**	**What needs to be done to achieve this level**
	Siloed recovery. Asset and twin do not take each other into account.	State of asset or twin is restored to previously known good state, including synchronization state. Corresponding asset changes may not be fully reflected in the twin and restoring to default states may result in loss of data.	Recovery and restored state are correct for both synchronized twin and asset. Synchronization data is incorporated in business continuity plans and operations. Recovery meets business objectives and for faithful operations (need to assess scope of impact of changes and recovery effort)	Continuous update of synchronized state of asset and twin. Continuity and recovery constantly updated for the state of the corresponding asset or twin.
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	Policies and procedures exist but are separate for assets and twins.	Evidence of backups, restore procedures, logs, and testing and ability to return to a previous good state. These exist separately for the asset and twin.	Fidelity and synchronization exist in a moment in time that allows restoration of asset and twin to a specific consistent state (such as checkpoint).	Evidence of continuous verification and restoration of state and data of both twins and assets bi-directionally.

Table 3-18: Remediation, recovery and continuity of operations.

Annex A ACRONYMS

CAPEC	Common Attack Pattern Enumeration and Classification
IIC	Industry IoT Consortium
IIRA	Industrial Internet Reference Architecture
IISF	Industrial Internet Security Framework
IoT	Internet of Things
IT	Information Technology
OT	Operational Technology
OWASP	Open Web Application Security Project
Twin	Digital twin or physical twin corresponding to an asset

Annex B DEFINITIONS

The following terms, specific to the context of the SMM, are defined here:

Security level is a measure of confidence that the system is free of vulnerabilities and functions in an intended manner.

Security maturity is a measure of an understanding of the current Security Level, its necessity, benefits, and cost of its support.

Domains are the strategic-level priorities for security maturity. In the SMM, there are three domains: Governance, Enablement, and Hardening.

Subdomains refer to the basic means to address a domain at the planning level. Each domain currently defines three subdomains.

Security practices are the typical activities performed for a given subdomain; they provide the deeper detail necessary for planning. Each subdomain has a set of practices.

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

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

Security maturity target is the desired “end state” 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 by the business objectives of the organization or group.

Annex C REFERENCES

[IEC-62443-33] 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

[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-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-IISF2016] Industry IoT Consortium: The Industrial Internet of Things Volume G4: Security Framework Version 1.0, 2016-September-26
http://www.iiconsortium.org/IISF.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 202-05-05
https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf

[RFC 2119] S. Brander. IETF. "Key Words for Use in RFCs To Indicate Requirement Levels." March 1997. Best Current Practice. *https://ietf.org/rfc/rfc2119.txt*

AUTHORS & LEGAL NOTICE

Copyright © 2022, Industry IoT Consortium® and Digital Twin Consortium®, programs of the Object Management Group, Inc. ("OMG®"). All other trademarks in this document are the properties of their respective owners.

This document is a work product of the Industry IoT Consortium IIC-DTC SMM Profile Contributing Group, chaired by Ron Zahavi (Microsoft). The group is a sub-group of the IIC's Security Working Group, chaired by Keao Caindec (Farallon Technology Group).

Authors: The following persons contributed substantial written content to this document: Jon Geater (Jitsuin), Frederick Hirsch (Upham Security), Detlev Richter (TÜV SÜD), Michael Robkin (Six By Six), Ron Zahavi (Microsoft).

Contributors: The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document: Shi-Wan Lin (Yo-i Information Technologies, Ltd.).

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