Guidance for Creating IoT Security Maturity Model Profiles

An Industry IoT Consortium® Whitepaper

2024-02-29

Authors

Frederick Hirsch (Upham Security), Ron Zahavi (Auron Technologies), Lehlogonolo Ledwaba (Mandela Mining Precinct)

Contents

TABLES

1 OVERVIEW

1.1 INTRODUCTION

The IoT Security Maturity Model (SMM) is guidance developed for the assessment and improvement of security for industries deploying IoT solutions[1]. The goal is to provide a unified path towards cyber-physical security for IoT applications by demystifying the where's and how's needed to implement necessary security measures without under investing or over-investing unnecessarily.

The SMM is non-prescriptive and is designed to be used in combination with existing standards and other Industry IoT Consortium (IIC) security guidelines such as the IIC Security Framework[2], the IIC Reference Architecture[3] and the Trustworthiness Framework Foundations[4] guidance. The SMM provides a means of assessment against the effectiveness of security mechanisms implemented in IoT applications and looks at comprehensiveness (degree of depth of security measures) combined with scope (degree of fit to industry/system needs). Security Maturity is then assessed within the governance, enablement, and hardening domains.

Generally, the commonly used process of introducing security into IoT application domains starts with identifying security mechanisms to include into solutions and then identifying the threats and vulnerabilities that those mechanisms cover at a later stage. This process leads to expensive, over-engineering of security without full breadth and depth coverage of the threat landscape identified in that domain. This differs from the SMM approach of involving stakeholders early on to determine comprehensiveness targets, assessing to find gaps, and then determining technical and non-technical approaches to address the gaps.

The IoT Security Maturity Model Practitioner's guide[5] provides general considerations for using the maturity approach which can be further extended to industry or system requirements through SMM Profiles such as the Retail Profile for Point-of-Sale Devices[6], the Digital Twin Profile[7] and the Mining Extraction Profile[8]. This guidance document is intended to allow industry and system experts to better understand how to create an IoT Security Maturity Model (SMM) profile

[1] [IIC-SMMD2020], [IIC-SMMP2020]
[2] [IIC-IISF2-2023]
[3] [IIC-IIRA-2022]
[4] [IIC-TFF-2021]
[5] [IIC-SMMP2020]
[6] [IIC-SMM-RP2022]
[7] [IIC-SMM-DTP2022]
[8] [IIC-SMM-MEP2023]

for their industry or system in an easy and efficient manner and is based on experience in developing the currently available SMM profiles.

1.2 AUDIENCE

This document is oriented toward readers with a general familiarity with the IoT Security Maturity Model and with an understanding of their industry domain. It is intended to allow them to better understand how to extend the SMM to enable target setting and assessment in their respective industry.

1.3 RELATIONSHIP WITH OTHER IIC DOCUMENTS

An SMM profile document extends the general IoT Security Maturity Model by providing industry specific guidance that goes beyond the core guidance. This means that all the guidance in the IoT Security Maturity Model Practitioner's Guide[9] and IIC SMM Training[10] is relevant and should be used by practitioners alongside this industry profile that adds to this guidance. Other SMM documentation is also relevant as discussed in this document. Various SMM profiles may be used in conjunction with each other, for example the SMM Digital Twin Profile could be used along with this Mining Extraction Profile, for example. SMM mappings documents such as the 62443 SMM mappings can also be used to obtain guidance related to requirements and controls.

2 PROVIDING DOMAIN-RELEVANT INFORMATION

2.1 DEFINE THE SCOPE OF THE PROFILE

The first step in developing a new profile is to determine whether the profile will be at the industry or system scope (system scope may be taken to mean specific technology components as well). For example, the Retail profile is an example of the former SMM scope, the industry scope, while the Digital Twin Profile is an example of the latter SMM scope representing a system or a technology applicable to many industries.

All profiles are structured to follow the same basic organization:

1. Summary of key SMM concepts
2. Summary of profile domain system of interest and context, concepts, and scenarios.
3. A comprehensiveness level table with maturity information relevant to all practices if this is relevant.
4. SMM practice tables with summary of information about the domain relevant to the practice and the various comprehensiveness levels. The details in the table extend and do not repeat the SMM table information provided in the SMM practitioner's guide.
5. References to domain documentation.

[9] [IIC-SMMP2020]

[10] https://www.iiconsortium.org/smm-fundamentals-training

The first section (IoT Security Maturity Model) introduces the SMM and is already pre-written and included in a template that profile authors can use. It is thus consistent across SMM profiles. It defines the SMM process, the SMM terms and concepts that are used throughout the document and guidance on how to apply the model.

The second section (Domain Security Considerations) defines the system of interest, the SMM scope, and information about the scenarios, context, and concerns that are specific to the industry and/or system being described. In the Mining Extraction profile, an example of this would be the section "Mining Extraction Security Considerations". The subject matter experts of the working group are expected to add this section.

The threat landscape of the domain or technology is described in this section by identifying the IoT devices, data and processes that may be vulnerable to security threats. As part of this, the security risks, threat actors, possible attacks and consequences of failure associated with the domain/technology are given alongside the challenges associated with implementing cybersecurity in the domain/technology. The identified challenges may also include environmental conditions in which these technologies operate.

The remaining sections (SMM Profile Tables) include the common SMM table applicable to all practices as well as the 18 individual SMM practice tables. This is where the new guidance will be added. Only new material and considerations specific to the industry or system should be added. The existing SMM tables should not be repeated to avoid versioning issues moving forward when the SMM baseline may change, and for clarity of what is specific to the profile domain.

Understanding and documenting scenarios can help with understanding how the practices and maturity levels relate to the domain.

2.2 Define the Boundaries of Interest

It is important to start by defining the scenario under consideration such that the boundaries of the SMM profile are known. This does not mean that other areas of the domain are unimportant but rather that the focus of the analysis is within the areas in which the profile will be useful and relevant and in which the creators have expertise and have control over improving maturity. When defining the boundaries for the SMM analysis, consider the devices, processes, infrastructure, protocols, and equipment making up the IoT network in the various sub-systems of the system or industry under consideration. This will form the trust boundary for which the SMM is applicable.

There are two acceptable methods for picking and defining the scenario for the SMM profile. The choice of which method is used depends on the expertise of the participants and their preferences.

In the first method, the profile working group could start with defining a narrow scenario for the deployment of the solution, focusing on a specific system or process within the application

domain. As an example, in the Retail Profile[11], the first step was to understand that the system under consideration for the SMM was the Retail Point of Sale, thereby limiting the security analysis to this aspect of retail.

In the second method, the profile working group may decide to consider a more generic, wider approach that is applicable to many scenarios in that domain. An example of this is in the Mining Extraction Profile[12], where the first step was to limit the boundary of analysis to the Ore Extraction process but without distinction between open and closed pit mining, or between the ore extraction processes for the various mined commodities. In general, mining includes many additional aspects, such as ore processing, but, owing to the high safety critical aspect of IoT in the extraction process, irrespective of commodity, this was chosen as the focus.

The specific needs of the project and experience of the working group will guide the selection of narrow, wide, or perhaps an intermediate approach.

2.3 Determine the Context and SMM Scope

Once the boundaries of the SMM analysis are defined, the next step is to define the context of the system and the SMM scope. Some of the questions that can be considered include:

- What are the IoT devices that comprise the system and how are they related?
- Can they be abstracted into meaningful groups, to reduce the complexity of the analysis?
- Which similar security or regulatory concerns relate to the various groups?

For example, in the retail point-of-sale profile, despite the numerous devices that comprise the point-of-sale implementation, there were four categories of devices found in the environment. Those that relate to financial transactions, or privacy, are of more concern and require more security, while others (such as lighting) are at a lower category of importance. In some profiles it is important to capture such differences if they require different maturity and level of investment.

The SMM scope, whether industry or system/devices (or both) is related to understanding the boundaries of the analysis.

2.4 Understand and Document Differences from Generic Information Technology Situations

It is important to understand and document in general terms what sets the system of interest and the context apart from generic information technology and IoT situations. Are there unique regulatory concerns related to privacy, safety or security that should be generally considered? In

[11] [IIC-SMM-RP2022]
[12] [IIC-SMM-MEP2023]

the retail application there are financial regulations, in mining there are mining standards and safety concerns, to give some examples.

A good resource to consider during this process are regulation or licensing documents (and their associated guidelines on how to achieve compliance), insurance and liability considerations, as well as the main standards and laws that govern safe operation within the application domain. These documents may not be explicitly related to security, but cybersecurity would come under their umbrella.

The next step is to review each of the SMM tables in the Practitioner's Guide to understand the general guidance and to determine what might need to be added or clarified in the profile. If the general considerations cover what is needed, then nothing needs to be added. If more guidance can be added to clarify what is already in the practitioner's guide, in terms of the new scope and context, then such clarifications can be added. If something is missing, or completely new, it should be added.

2.5 Worked Example: Extracting Considerations from Industry Feedback

The following example is based on real feedback that was captured through an industry survey conducted in the development of the SMM Mining Profile. In it, we show how to identify and extract information relevant to the SMM tables based on current industry practices as well as showing how the current practices are used to evolve the industry in maturity. This example is only a small part of the survey and detail that was included in the mining extraction profile.

As part of a survey, mining industry experts were asked the following questions:

- What is done to mitigate the cybersecurity risk on introducing new vendor devices in the mine?
- What is the process for introducing new equipment into the mines?

The survey results on these questions established that currently there is no formal third-party risk management procedure implemented for mining equipment. The current focus of existing procedures is on IT systems from IT vendors.

Mining engineers are responsible for the selection of new mining equipment with occasional review from the head office cyber security team for the compulsory minimum security standard checks prior to connection into the mining network. However, this forms a vulnerability as the involvement from the head office is occasional and mining engineers lack the IT and cybersecurity skillset to be able to review procured devices thoroughly and accurately prior to introducing them into the mine environment.

This scenario deals with third-party vendor devices that are integral to the operation of the ecosystem and the risk that they pose to the networks so the Product Supply Chain Risk Management Table would be most applicable (however in some cases an understanding could affect multiple tables). From the feedback, the existing process was established to be as follows:

- Mining engineers select new mining equipment.
- Vendor mining equipment occasionally goes through minimum security standard checks by the head office cyber teams.
- No formal risk management process exists for mining equipment.
- Mining engineers are not qualified to evaluate procured vendor devices for security vulnerabilities.

From this understanding the following can be documented for the SMM Product Supply Chain Risk Management comprehensiveness levels:

Level 1 describes the existing process:

> Mining engineers are responsible for security checks on procured equipment with occasional review by head office cybersecurity team for the compulsory minimum security standard checks.

Level 2 would be an improvement on the existing process with more coordination among teams.

> There is more frequent and formalized involvement from the cybersecurity team in the procurement and review of mining equipment. Mining engineers are still handling procurement, but the head office cybersecurity teams are now more aware of the possible vulnerabilities that could be found within the equipment.

Level 3 maturity builds from Level 2 in that now, new mine products are evaluated by trained cybersecurity professionals that are based both at the head office and at the mine sites, possibly in small isolation labs.

> Cybersecurity requirements on new equipment now form part of the procurement review process at head office and at mines prior to orders being placed as well as on delivery of the new product.

Level 4 is the highest level of maturity and includes continuous improvement, automation, and formalization.

> There is a formal security review of mine equipment considered for or under procurement. This happens on regular basis that is implemented across all mines operated by the mining company and is formalized with a centralized policy. The cybersecurity checks are now integrated as one of the compulsory requirements of the equipment procurement when conducting specification checks.

Once the maturity levels have been determined, the table can be filled. Other sources could and should also be used in addition to industry feedback to further enhance the security maturity considerations. The table below is an extract from the Product Supply Risk Management table from the Mining Extraction Profile only showing how the examples shown above would be

included. This is an example to show the level of detail of the text. Note that detailed controls and mechanism are not provided (but could be in a related SMM mapping document).

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)**
Industry-Specific Scope Considerations	Implement security requirements checks as per head office procedures.	Implement tight security controls for and inspection protocols for vendor supplied products prior to installation within the mine	Establish a database of approved vendors including product provided, security mechanisms included with product, international security verifications/certifications and past product performance	Supply chain database is frequently updated from suppliers should security vulnerabilities be listed by international security auditors- including breaches to vendor company and/or associated parent companies
	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**
	Mining engineers responsible for security checks on procured equipment with occasional review by head office cybersecurity team for the compulsory minimum security standard checks	Regular, formal review of supply chain equipment by head office cybersecurity team prior to installation/dispatch to the mines	Mine products are evaluated by trained cybersecurity professionals and reviewed at head office and at mines prior to procurement, and on delivery.	Trained formal security review of mine equipment under procurement and in line for procurement on regular basis across all mines with a centralized policy
	Indicators of accomplishment	**Indicators of accomplishment**	**Indicators of accomplishment**	**Indicators of accomplishment**
	New inventory introduced into the mining space have checks for minimum security mechanisms and lack of vulnerability	Formal inventory security checks are captured for new vendor equipment introduced into the mining space	Supply chain databases implemented with list of viable vendors with ordering priority based on previous performance during formal security checks by mine cybersecurity professionals	Up to date supply chain databases with autonomous end-to-end timeline updates provided as part of vendor risk reporting

2.6 Considerations Beyond Security

Although the IoT security maturity model is focused on security, other elements of trust, such as privacy and safety, are relevant drivers for security maturity target setting and thus should be documented when relevant. Even though the SMM has not yet been extended explicitly to consider other aspects of trust, the model is relevant to trust concerns and some exploration of this has been started[13]. In domains where security concerns are highly integrated with a safety process, the safety process can be documented within the SMM table, clarifying the relationship. The trustworthiness characteristics of safety, reliability, resilience, and privacy should be considered in terms of their relationship to security maturity. These characteristics and their relationship to security are discussed in the IIC Trustworthiness Framework Foundations guidance[14].

2.7 Think In Terms Of Target Setting

A good way to start defining comprehensiveness levels for the SMM tables is to consider creating a security roadmap for the business or application domain which identifies what needs to be done to progress into the next level of maturity. This should also consider how this process could extend beyond what is given in the general recommendations of the SMM.

Thinking about the process of setting SMM maturity targets is also useful when creating a profile, since anticipating how the profile will be used, both in setting SMM maturity targets as well as performing system SMM maturity assessments can help with resolving potential ambiguities in the table content.

It is important not to think in terms of security controls and mechanisms but rather in terms of business maturity needs, actions, and indicators of accomplishment.

3 Provide Domain or System-Specific Guidance in the Tables

The main effort in developing the SMM profile is to generate guidance written in small paragraphs and adding them in the appropriate comprehensiveness levels as

- What needs to be done to achieve that level and,
- Indicators of accomplishment to help assessors determine if the organization has met the requirements of the level.

Start by reviewing each table and the practice description, considering what more needs to be said for the domain about what that level means, what the considerations are, how to achieve it, and which indicators can be useful in an assessment to determine if it has been reached. Remember these are maturity levels, not security control levels. Try and avoid the prescription

[13] [IIC-ESMM2018]
[14] [IIC-TFF-2021]

of specific security mechanisms and algorithms (e.g. “achieve level 3 AES” or “ECDSA needs to be implemented”). Some relevant standards may be included as reference and as part of the mapping of the SMM levels to existing industry standards.

3.1 Reviewing and Enhancing ‘What Needs to Be Done’ Guidance

It is useful to start with the general considerations of a table as given in the SMM practitioners guide. To give an example, before creating profile guidance for the Physical Protection practice, one should review the “What needs to be done” text:

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?
Adopt physical security policies to protect devices from accidental or intentional physical damage or operational disruption.	Define trust zones in IT system architecture and establish physical security perimeters in IT and OT deployments to separate and protect the systems within each zone. Tamper-evident housings are deployed outside the secure perimeter.	Automate identity management and alerting systems to manage and report on physical access to locations and assets. Enforce more granular access control rules, such as time of day. Tamper-resistant housings for systems and things that are deployed outside of secure perimeter.	Clearly define security perimeters, with their siting and strength dependent upon the assets contained within the perimeter and the results of a risk assessment.

Table 3-1: General considerations.

As part of the review, the team can consider which additional guidance or detail would be useful. For example, the SMM Retail Profile team reviewed the table and noticed that there is mention of tamper-evident housing in level 2, and tamper resistant housing and automation in level 3. They noted, however, that in point-of-sale situations there needs to be additional guidance related to the use of RFID-like tags for tracking merchandise, and that there is sophistication related to passive and active tracking. They used these notes to write the following additional guidance:

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?
Protect equipment minimally using Key locks on doors. Shared PIN or combinations are used	Track device component changes through manual logging. Securely attach devices to fixtures (e.g., PIN pad to cash wrap counter). Devices have tamper-evident, and seals are visually inspected daily for tampering. Sensors are placed on gates and doors and anti-theft tags are placed on high value, or easily removable, assets. Anti-theft tags are added to store fixtures (shelf tags, PDAs, scanners, etc.)	Follow practices for PCI. Track sealed tamper evident seals in a database. Use video surveillance monitoring or access control (or both) to monitor physical access to restricted areas (PCI-DSS). Employees use a unique PIN/Badge based access.	Use integrated device alarm sensors for covers and doors. Segmented and restricted badge/card access for employees to facility (time/role based). Deploy video Analytics based alarming.

Table 3-2: Additional guidance or detail.

3.2 Providing Content for Maturity Levels in the Tables

The process below provides a general workflow on how to begin filling the SMM profile tables:

1. Start with a template having an empty table for each practice.
2. For each practice, consider the levels (remembering that each higher level includes the previous maturity level, so there is no need to repeat material).
3. Document what is appropriate for the domain but do not repeat what is said in the SMM Practitioners Guide. An existing security roadmap would be of great assistance for this process.

Leave a table cell blank if there is nothing to say and come back later to reconsider. If there is nothing at all in the table, leave it blank.

3.3 Extract Commonality

If you find that there are many repeats across the tables, then that guidance may apply to all the tables in the profile. In this case, this material may be documented once in a table that applies to all practices, provided in the template before the practice tables. An example of this is in the

digital twin profile[15] shown in Table 3-3. If that common table is empty at the end of creating the profile, remove the section with that table entirely to avoid confusion.

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.

[15] [IIC-SMM-DTP2022]

	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 3-3: Digital twin comprehensiveness level considerations for all SMM practices.

3.4 Explain the Key Domain Considerations for Each Table

Before each table add paragraphs of text as needed to explain the relevant domain specific concerns and resources related to the table content for the domain.

Provide references for standards, regulations, best practices, and other domain specific material that might be useful.

4 Best Process Practices for Creating an SMM Profile

This section includes some best practices and alternatives for creating a new SMM profile.

4.1 How to Start?

A good place to start is to review and mine any existing security documents, whitepapers, and reports for your industry or technology. These documents typically describe relevant industry scenarios, various requirements, security concerns and descriptions of the threat landscape, statistics, pain points, as well as relevant standards. You can you use the material you find to populate the related SMM practices.

It is beneficial to start with 1 or 2 tables to focus on and generate notes of what is unique that should be added, and if possible, what is added at which comprehensiveness levels (1 to 4). This provides the team with SMM familiarity and allows them to understand the process, ask question about it and refine the process before continuing. The SMM authors can review this initial work and provide feedback before you continue with the remaining practices.

4.2 How Often to Meet?

How fast a team works and how often they meet is up to the team. Generally, we have found it useful to hold meetings every two weeks with a smaller subgroup (minimum of 2-3 people) and report to the larger group once a month. Good progress can be made reviewing 2 tables per meeting.

4.3 Approach

4.3.1 Capturing the Notes

Once the team is comfortable after trying 1-2 tables, you can perform a pass across all tables for capturing the notes.

You can do a table at a time completely, but in practice it may be good to make a quick pass through all the practices, and then repeat the process for all the practices with the insights that has come from the first pass. This allows understanding of the dependencies that exist between tables, and possibly what should be added to more than one table. This also allows the team to catch any prescriptive descriptions that may have been accidentally included.

4.3.2 What Needs to Be Done

Once notes have been captured for all the tables, you need to write the paragraphs for what needs to be done.

4.3.3 Indicators of Achievement

Once all the paragraphs have been written for what needs to be done, revisit each table and add the corresponding indicators of achievement to identify how an assessor would confirm that someone has achieved what needs to be done. These indicators of achievement may end up containing identical phrasing as the paragraphs in what needs to be done, and that is acceptable.

4.3.4 Common Elements

If you observe that there are common elements that appear in every table, extract them into an upfront common table. Readers can use the common information as an "index" to identify what level is appropriate for them and check each practice to see if that level indeed fits them, or if they need to lower or raise the level as appropriate.

4.3.5 Capturing the Scenario

Capturing the industry scenario or system description can be performed in parallel to the practice scope extensions.

4.3.6 Collaborating with Other Organizations

To generate acceptance and adoption of the profile, it is recommended that the appropriate external SDOs, industry groups and consortia participate in the production of the profile, or at a minimum have the opportunity to review and comment on it. For example, the Digital Twin Profile was written jointly with the Digital Twin Consortium. The Retail Profile was written jointly with the OMG Retail Domain Task Force. The Mining Profile was reviewed by the IIC's Mining working group, the DTC's Mining working group, as well as by GMG.

5 Offer Implementation Guidance Elsewhere

It is useful to remember that the profile is about providing high level maturity level guidance, in terms of domain considerations for the practices, domain specific general considerations, actions, and indicators of accomplishment. The profile is about understanding what relates to setting a target and determining if it has been met.

A separate mapping document can be created for implementation guidance unique to standard(s) or other detailed implementation requirements. An example is the SMM 62443 Mappings[16].

If you wish to create such guidance, consider creating a mappings document as well.

[16] [IIC-SMM-62443M-2023]

6 REFERENCES

[IIC-TFF-2021] Buchheit, M., Hirsch, F., Martin, R. A., Bemmel, D. V., Espinosa, A. J., Zarkout, B., . . . Tseng, M. The Industrial Internet of Things Trustworthiness Framework Foundations. 2021. *https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf*

[IIC-SMM-62443M-2023] Eric Cosman (OIT Concepts), J. G. D., Frederick Hirsch (Upham Security), Pierre Kobes (Kobes Consulting), Ekaterina Rudina (Kaspersky), & Ron Zahavi (Microsoft). IoT Security Maturity Model: 62443 Mappings for Asset Owners, Product Suppliers and Service Providers (updated). 2023. *https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/08/SMM-62443-Asset-Owner-Product-Supplier-Service_20230809.pdf*

[IIC-ESMM2018] Frederick Hirsch (Fujitsu), R. Z. M., Sandy Carielli (Entrust Datacard), Ekaterina Rudina (Kaspersky Lab), Matthew Eble (Praetorian Group). Extending the IIC IoT Security Maturity Model to Trustworthiness. 2018. *https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI-Extending-the-IIC-Security-Maturity-Model-to-Trustworthiness.pdf*

[IIC-SMMP2020] Frederick Hirsch (Fujitsu), S. C. E. D.,Matt Eble (Praetorian), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft). IoT SMM Practitioner's Guide Version 1.2. 2020. *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

[IIC-SMM-RP2022] Frederick Hirsch (Upham Security), A. M. L., Bart McGlothin (Cisco), Leonid Rubhakin (Aptos), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft). IoT SMM: Retail Profile for Point-of-Sale Devices. 2020. *https://www.iiconsortium.org/pdf/SMM-Retail-Profile.pdf*

[IIC-SMM-MEP2023] Frederick Hirsch (Upham Security), L. L. M. M. P., Carel Kruger (Mandela Mining Precinct), Ron Zahavi (Auron Technologies). IoT Security Maturity Model Mining Extraction Profile. 11/12/23.

[IIC-SMM-DTP2022] Jon Geater (Jitsuin), F. H. U. S., Detlev Richter (TÜV SÜD), Michael Robkin (Six By Six), Ron Zahavi (Microsoft). IoT Security Maturity Model Digital Twin Profile. 2022. *https://www.digitaltwinconsortium.org/wp-content/uploads/sites/3/2022/06/SMM-Digital-Twin-Profile-2022-06-20.pdf*

[IIC-IISF2-2023] Keao Caindec (Farallon Technology Group), M. B. W.-S., Bassam Zarkout (IGnPower), Sven Schrecker (Amazon Web Services), Frederick Hirsch (Upham Security), Isaac Dungana (Red Alert Labs), Robert Martin (MITRE), Mitch Tseng (Tseng Info). Industry Internet of Things Security Framework (IISF), Version 2.0. 2023. *https://www.iiconsortium.org/wp-content/uploads/sites/2/2023/06/IISF-Version-2.pdf*

[IIC-SMMD2020] Sandy Carielli (Entrust Datacard), M. E. P., Frederick Hirsch (Fujitsu), Ekaterina Rudina (Kaspersky), Ron Zahavi (Microsoft). IoT Security Maturity Model: Description and Intended Use, Version 1.2. 2020. *https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1. 2.pdf*

[IIC-IIRA-2022] Shi-Wan Lin (Thingswise/Intel, A. C.-e., Eric Simmon (NIST, also co-editor), Daniel Young (Toshiba), Bradford Miller (GE), Jacques Durand (Fujitsu), Graham Bleakley (IBM), Amine Chigani (GE), Robert Martin (MITRE), Brett Murphy (RTI) and Mark Crawford (SAP). The Industrial Internet Reference Architecture, Version 1.10. 2022. *https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf*

ACKNOWLEDGEMENTS

This document is a work product of the Industry IoT Consortium Security and Trust Working Group, chaired by Keao Caindec (Farallon Tech) and Robert Martin (MITRE).

Authors: The following persons contributed substantial written content to this document: Frederick Hirsch (Upham Security), Ron Zahavi (Auron Technologies), Lehlogonolo Ledwaba (Mandela Mining Precinct).

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