

A Systematic Approach for the Definition of Countermeasures in Industrial IoT: An Automotive Case

Massimiliano Masi¹, Tanja Pavleska² and Simone Pezzoli¹

¹*Autostrade Per L'Italia S.p.A. 50, Via Alberto Bergamini - 00159 Roma, Italy*

²*Jozef Stefan Institute, Ljubljana, Slovenia*

Abstract

Inter-dependencies in critical industrial systems pose huge security challenges, which are tightly linked to the problems of interoperability and trustworthiness within and among those systems. In this paper, we try to establish the interconnection between these system properties in a way that allows the establishment of one property to positively affect and facilitate the establishment of the other. For that purpose, we design a methodology based on standardized and well-known models and frameworks, which are upgraded as needed and integrated into a single generic framework. Although this approach is meant to primarily help the security experts and the architects in their design practices, it also aims to facilitate the dialogue on important (cyber and physical) security issues among all relevant levels in an industrial IoT organization. The formal value and the practical applicability of the methodology are also demonstrated through a use case in the domain of road transportation and automotive industry.

Keywords

Critical Infrastructure, C-ITS, Cybersecurity Framework

1. Introduction

Industrial Automation and Control Systems (IACS) are usually physically located in remote, often unsupervised sites where they enable safety-critical processes. They are often managed remotely from a control room and are supervised by trained personnel via commands to sense and actuate the physical world either through the Internet (via cloud environments) or through a dedicated network. Some assets are also designed to preserve safety in case of networked systems. For example, in the road transportation sector, the tunnels or the Cooperative Intelligent Transport Systems (C-ITS) [1, 2] are such sites, whereas ventilators in the tunnels and the Infrastructure-to-Vehicle (I2V) messages have the role of an IACS. Malfunctioning of those IACS may result in traffic congestion and, ultimately, loss of lives.

Cyber-attacks in IACS have been on the rise [3]: critical infrastructures in general face continuous attacks, ranging from low-skilled and person-motivated to state-sponsored attacks. Loss of availability in one infrastructure may result in loss of availability in others as a result of

ITASEC'21: Italian Conference on Cybersecurity, April 7–9, 2021, Online


✉ mmasi@autostrade.it (M. Masi); atanja@e5.ijs.si (T. Pavleska); simone.pezzoli@autostrade.it (S. Pezzoli)

🌐 <https://www.autostrade.it/> (M. Masi); <https://www.e5.ijs.si/> (T. Pavleska)

🆔 0000-0003-4737-7107 (M. Masi)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

cascading effects propagating throughout the interconnected sites [4]. Establishing trust and interoperability in the shared cybersecurity practices, as well as an optimal security posture of the Essential Services [5] can dramatically improve the coordination of defenses and responses to attacks in the affected infrastructures.

IACS are composed of both cyber and physical assets, each having their own life-cycle. Detecting and protecting against cybersecurity events cannot be based solely on the expertise of the cybersecurity practitioner, nor evaluated ex-post through vulnerability assessment and penetration testing. The process of securing IACS shall be rigorous, measurable, and performed systematically¹, not only from a cyber, but also from a physical perspective. Although critical infrastructures are mandated to maintain a Cybersecurity department [7], vendors of IIoT systems are not, exposing the infrastructure to supply-chain based attacks [8]. Hence, the security architecture of system components cannot be addressed with typical cybersecurity countermeasures: patching systems may not always be possible, the protocols may be unknown and proprietary or their legacy systems may not be designed with security in mind.

Considering the growing complexity of the IIoT due to the interconnected systems of systems, deciding what to protect and how becomes a challenge and an important open question. Risks are usually elicited by publications [3, 9] or by performing a qualitative risk analysis on the IACS. But how to attain the same risk level across the interconnected critical infrastructures; and how to achieve the same technical level of trust when the selection of countermeasures are subject to the talent of the practitioner? There are some generic best practices guiding critical infrastructures towards a cybersecurity posture on their IACS [10, 11]. However, selecting the right countermeasures or defining the processes implementing a Cyber Security Management System (CSMS) is also problematic and requires qualitative risk-analysis. The NIST Cybersecurity Framework [12] helps the security architects by defining guidelines and a set of controls that can be *profiled* for a specific context. Profiling the framework requires high skills and competence of both the business and the cybersecurity context.

With this work, we aim to make the following contributions: *i)* we define a systematic approach to catalogue the relevant cyber and physical assets composing an IACS, including their interconnections, and over the entire life-cycle of each asset, *ii)* based on that, we design a model that elicits the high level security goals by interacting with all the stakeholders of the IACS, and *iii)* we define a profile based on the NIST Cybersecurity Framework which is repeatable and measurable, thus offering a way to practically implement the proposed elements and we show how to apply for defining the security posture of C-ITS. The higher goal is attaining the required level of trust within a system of interconnected critical infrastructures.

To achieve the goals outlined above, the paper is structured as follows: in Section 2, we overview relevant related studies and fit our work within the state of the art. Section 3 introduces the theoretical background needed to understand the methodology proposed in Section 4. This is further supported with an application to the C-ITS use case in Section 5. Finally, in Section 6 we conclude and provide some insights into other current and future updates of the presented work.

¹In fact, the EU Police Department, EUROPOL, requires that the constantly evolving threats are addressed in a *holistic and effective manner* [6].

2. Related work

When IT/OT systems grow in complexity, it is recommended to adopt *modularity* and *layering* as the principles of decomposition in order to attain security [13]. Such decomposition can be facilitated by the use of *enterprise architectures (EA)*, which define strategies and practices for logical grouping of assets with shared values. EAs achieve modularity by employing the concept of a *building block*, which represents a reusable module defining the life-cycle of a specific functionality. By combining building blocks in different manners, a variety of technologically and economically sustainable architectures can be created. In the context of interconnected critical infrastructures, deciding which (architectural) layers to use is crucial for the harmonization of security countermeasures, as architectural models can be devised only for a specific context. For instance, the SGAM[14] is defining a layering approach for the energy sector, while the EIRA [15] defines views for the European public administrations. Although our methodology is parametric with respect to the architectural model used, the choice of the particular model to be used still remains to be made. In this paper, we use RAMI 4.0 [16], as the de-facto EA for IIoT.

The use of Enterprise Architectures as facilitators for a systematic approach to devise security assessment in critical infrastructures is not new. For instance, Gottschalk et al. [17] describe how to use the SGAM for developing architectures in the Energy, Healthcare, and Smart City domains. The same has been done for the eAgriculture domain in [18]. In their book, the authors concentrate on applying the methodology to devise generic requirements and interoperability problems, leaving security to sector-specific analysis [19, 20]. However, extending IT assessment methodologies to IIoT does not automatically consider the specificity of the domain, thereby leaving out important security aspects [21]. We take this point as a starting premise in our work and propose a systematic approach that is specifically designed for the OT and IIoT domain. In that context, the US Cybersecurity and Infrastructure Security Agency profiled the Cybersecurity Framework (CSF) for the transportation sector [22], defining guidelines for the companies in the transportation sector to adopt the NIST CSF. However this guide was made for the previous version of the CSF, and it does not entail a systematic approach. Our work extends previous attempts to apply the same methodology to other sectors such as energy and healthcare [23, 24].

3. Preliminaries

To establish a sound theoretical base, we first introduce RAMI 4.0 in as the underlying architectural model. Then, we present the Reference Model for Information Assurance and Security (RMIAS), which will complement RAMI 4.0 to elicit the high level security goals for each stage of the assets' life cycles. Following a standardized process of designing architectural profiles with a sound security posture, we rely on the NIST recommendations and the NIST CSF profile. Finally, we describe IEC 62443 as the best practice used following the NIST CSF as informative reference in the context of OT/IIoT.

3.1. RAMI 4.0 for Defining the Architectural Model

The Reference Architectural Model for Industrie 4.0, RAMI 4.0 [16] is the de-facto standard for the design of IT architectures for Industrial interconnected systems [25]. It has been devised as a reference architecture model for the international projects involving Industrie 4.0 automation, whose supply chain of intermediate goods is composed of several companies with own security posture and legal context. Guaranteeing consistent trust levels and interoperability of processes, as well as secure information sharing in such heterogeneous contexts is a complex task. A single company or project alone cannot establish a governance scheme without having a systematic approach agreed upon by all stakeholders and implemented as a practice. RAMI 4.0 guarantees the interoperability of data flows, security processes, and data management in a holistic manner.

RAMI 4.0 is composed of 3 dimensions and 6 layers. The first dimension, the architectural viewpoints or *Layers*, groups the EA concepts into two models: *physical* (the asset and integration layers) and *digital* (all other layers). The *Asset* layer is where all the definitions of hardware components are contained. The *Integration* layer connects the physical with the logical world. Each item in the Asset layer has a counterpart in the Integration layer that serves as an interface to support the transition towards a fully digitized system. The *Communication* layer contains all the communications among industrial components (e.g., OPC-UA, MQTT). The communication protocols in this layer can be secured, as they either have their own security profile or they are part of the requirements for compliance with international standards. The *Information* layer defines the syntax and the semantics of the information shared by the industrial component. The *Functional* layer, on the other hand, defines the functionalities and processes supporting the business use cases and are typically subject to security reviews. Finally, the *Business* layer contains the business processes needed to build the use case in which each asset should be put in production.

The second dimension (Life Cycle and Value Stream) is used to categorize assets by their purpose - as either (proto) *type* or *instance/production*. The last dimension represents a typical automation pyramid [26]. There, the typical Industry 4.0 characteristics are defined as part of the *Connected World*, integrating the description of all cross-cutting concerns about the connection of the automation assets to the Internet. As a result, enabling remote access to the legacy operational technology exposes the systems (that were initially not designed with security in mind) to a series of new threats that can occur in each RAMI layer [27].

3.2. RMIAS: Risk-Based Countermeasures for Assets' Life-cycles

Each item in the RAMI 4.0 cube has its own life cycle: PLCs are designed, installed, and decommissioned; SCADAs are installed, patched, managed, and decommissioned, etc. To grasp the peculiarities of the assets' life cycles, we rely on the Reference Model for Information Assurance & Security (RMIAS) [28, 29] and integrate it within RAMI's layers.

The RMIAS cycle has four stages: an Information Taxonomy of the item's components and data; high level representation of the desired Security Goals (elicited through a risk assessment together with field's experts); selected relevant security Countermeasures to fulfill the security goals; and a Security information Development Life Cycle. It essentially defines a method to

elicit security countermeasures for each stage of a life cycle in view of its four dimensions.

3.3. NIST Cybersecurity Framework: Automating the Subcategory Choice

The NIST Cybersecurity framework (CSF) [12] provides guidelines for the critical infrastructures in assessing their security posture and for defining a roadmap for potential improvements. It introduces 5 high level functions, 23 categories, and 108 subcategories, each of which points to a set of informative references from best practices. In the context of industrial IoT systems, the NIST approach is integrated into the IEC 62443 standard, which is described in Section 3.4.

The NIST framework covers the necessary activities to *identify* the assets, flows, and requirements, to *protect* the items and the infrastructure, to *detect* anomalies, to *recover* and to *respond* to an incident. A framework *profile* (NIST CSF profile) is a subset of the 108 categories relevant in a specific context (e.g., road transport, tunnels, or intelligent transport systems, as discussed in Section 5). In fact, defining a profile for a specific context enables its stakeholders to share the same security posture, facilitating the trust establishment among them. The NIST CSF also defines a way to perform risk-based enhancements from the current security posture to a desired one, by selecting and enhancing those subcategories and the related countermeasures according to the profiling methodology. However, defining a profile is not an easy task [23]. Profiles creation is guided by the business objectives, the threat context (environment), and the security policies peculiar to the context.

In order to lower the extent of relying on cybersecurity experts for the selection of a proper subcategory, in our methodology we propose to elicit the profiling requirements in a way that creates a cybersecurity posture harmonised across the actors realising a given concept (for e.g., a road operator and a car manufacturer in C-ITS. This results in a process that is repeatable and measurable, as demonstrated in Section 4.

3.4. IEC 62443: Enhancing the profiling of NIST Subcategories

The IEC 62443 standard series addresses IT cyber and physical security requirements for IACS that had once represented a closed system, but are now exposed to both public and private networks. IEC 62443 encompasses the security requirements for both the systems and the components and is a set of informative references selected from the NIST framework. It allows to perform gap analysis between the current and the target security posture (as defined by NIST). To do that, IEC 62443 defines the concept of *Security Level Target* - the IACS' desired posture based on the risk analysis and a specific attacker profile. For each requirement, at least three additional *Requirement Enhancements*, (*REs*) are defined that show how the security posture is revised.

One of the pillars of IEC 62443 is the subdivision in *zone* and *conduits*. A zone is a grouping of logical or physical assets that share the same security requirements, while a conduit is a grouping of communication assets that protect the security of the channels contained in the conduit.

Our methodology helps the architect in defining the ways to enhance the profiling process for each subcategory. Thus, the application of the IEC 62443 starts by carrying out discussions with the business experts, with the aim to obtain the necessary items (devices, protocols,

semantic information, and business requirements). These are then categorized in the RAMI 4.0 cube according to the specific use cases. The process results with a first initial review of the requirements and its design.

4. The Methodology

The goal of the methodology is to obtain a profile of the framework devised for a specific context with a rigorous, measurable, and repeatable process to attain trust among different interconnected infrastructures. Although the methodology is parametric with respect to the architectural model chosen, RAMI 4.0 is used to define the architectural layers and viewpoints as the de-facto standard for the IIoT sector. The formal representation of this approach is shown in Algorithm 1. With the notation $d_{l,j,k}$ we identify the item d grouped in the layer l , with life cycle j (type/instance) and automation level k . For each of them, an RMIAS taxonomy entry (a tuple) is created, indicating the stage of the categorized item in its life cycle (e.g., a PLC that stays in layer *Asset*, life cycle *Type/Development*, automation level *Field Device* has different security requirements during the design, operation, and decommission stages).

Algorithm 1: The methodology

Result: A profile of the NIST CSF

```

1 Input: Business Objectives, Relevant Literature, Threat Environment, Regulations;
   // Perform interviews with business experts, and obtain items and use cases
2  $D \leftarrow$  item list,  $U \leftarrow$  use cases ;
   // Create RAMI matrices
3 foreach  $d \in D$  do
   | // Assign each architectural item to its RAMI 4.0 layer
4   assign  $d$  to its layer  $l$ , life cycle  $j$ , and automation level  $k$  ;
   | // For each RAMI identified location
5   foreach  $d_{l,j,k}$  do
6     Create a RMIAS tuple  $t := \langle \text{form, loc, state, sensitivity} \rangle$ ;
7     foreach  $t$  and item's life cycle stage do
8       | // Elicit security requirements
9       | create a high level goal,  $G \leftarrow g$ ;
10    end
11  end
   // Define the requirements
12 foreach  $g \in G$  do
13   create a requirement  $r \in R$  using language defined in rfc 2119;
14   assign  $r$  to the NIST subcategory;
15 end
16 Create the digital twin, simulate, and re-evaluate the posture;
```

Then, for each tuple t , the high level security goals are elicited (such as Availability of the data) This stage is also performed with interviews, focusing on *what* to protect instead of *how*

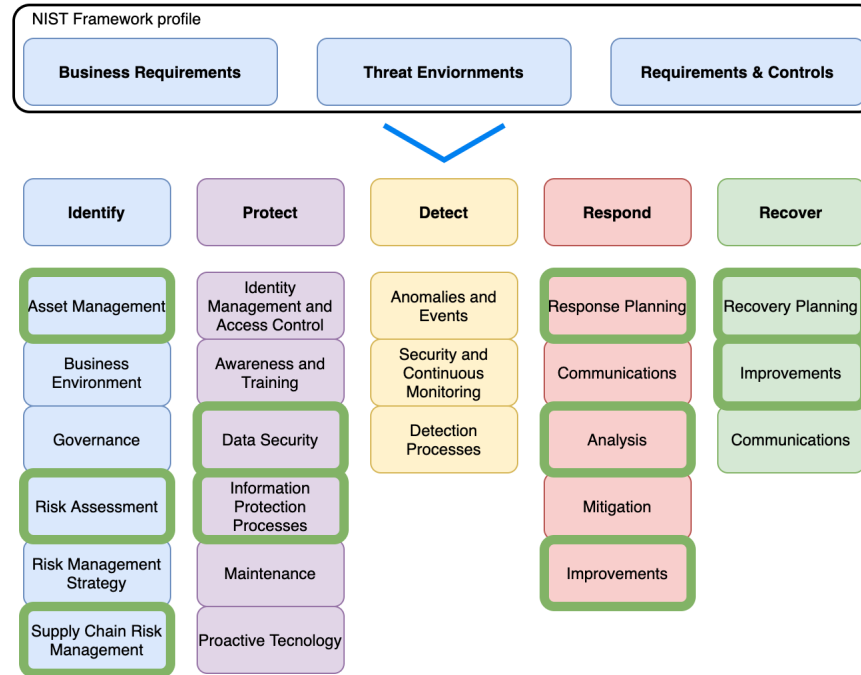


Figure 1: The auto-generated NIST CSF categories from the methodology.

to protect it. Then, the security architect performs a trade off analysis to define the requirement fulfilling the particular goal using the common rfc 2119 language. The resulting requirements are placed in the right subcategory of the CSF, resulting in the desired profile. Finally, a *digital twin* of the architecture is composed using a threat modeling tool (see Section 4.2). Security simulations are made and, whenever a new possible attack is found or a new device enters into the system, the architecture is updated and the posture is re-evaluated.

4.1. Relation to the NIST CSF

Although the connection between the methodology and the NIST guidelines and recommendations seems implicit, each of the stages of applying the reference models and standards can be traced back to a NIST requirement. For example: the iteration through RAMI layers fulfills the subcategory ID.AM-3 from the NIST CSF. Similarly, the risk analysis performed during the RMIAS cycle fulfills the ID.RA-4,5 and ID.RM-1. Furthermore, using a life cycle for each asset fulfills the requirements PR.DS-3, IP-2, IP-6, and PT-5. RAMI 4.0's hierarchy level dimension, on the other hand, elicits the risks related to supply chain, thus fulfilling ID.CS-1,2,3. Finally, the simulation on the digital twin fulfills the PR-IP.10. This concept of automatically selecting the NIST categories based on the architectural account of the assets' security through their life-cycles with our methodology is presented in Figure 1. The NIST CSF categories with bold contour contain subcategories whose requirements define actions and activities which are parts of the methodology.

4.2. The *digital twin*: Practical remarks

IEC 62443-2-1 requires the definition of zones and conduit to form the *reference architecture* (see Section 3.4). As part of our methodology, we model the reference architecture in securiCAD [30]. This model greatly supports the use of the reference architecture and enables the concept of *refactoring*: by defining high value assets that we want to protect (e.g., actuators, or private data), we reason over abstract architectural assets to check for potential attack paths, thus performing the cost-effective analysis required by RMIAS to evaluate the countermeasures. Typically, the MITRE ATT&CK for ICS matrix [31], which contains a list of attackers' techniques to reach high value assets, is used as a reference model for testing and proving that the architecture is resilient with respect to known attacks. The SecuriCAD model can be extended and further tailored to the context of the profile, as it is supported by a formal toolbox for that purpose [32]. This not only enables adaptability of the methodology, but it also allows for testability and repeatability of its results.

5. Use case: C-ITS and the Automotive Industry

Cooperative Intelligent Transport Systems (C-ITS) are an example of a critical infrastructure with strong inter-dependencies, where a security breach can trigger cascading effects. For instance, if an attacker forges messages impersonating a road operator, its message may cause vehicle crash in the motorway, while a failure in synchronizing the semaphores in a municipality to facilitate the journey of the emergency vehicle may lead to casualties. C-ITS are networks of ITS stations cooperating to deliver a set of use cases like: notification of road works ahead, danger in the motorway, and emergency vehicle approaching. They also represent the backbone of the next-generation automotive industry. Cooperation in these systems is established between municipalities, road and public transportation operators, vehicle manufacturers and users in order to attain the security and safety qualities in multi-modal transportation [33].

As essential services, C-ITS require high security posture and trustworthy operational environment, as they enable vehicles and the road infrastructure to "talk" to each other (Vehicle-to-Anywhere, V2X communications). This is done via messages (e.g., traffic notifications) generated by sensors installed on the road. The messages are then collected by a Central ITS Station [34] and wrapped in a standard-format message [35] to be forwarded to the devices installed on the road (at every 2 to 5 kilometres). Those devices, in turn, broadcast the messages to vehicles that act accordingly, by e.g., displaying a message on the driver's dashboard, actuating brakes or platooning trucks. Although this message exchange is highly regulated, some aspects of the value chain are left unspecified. ETSI TS 102 94 [35] defines the security for the messages broadcasted from the road devices to the vehicles, while other specifications describe best practices to secure the back-end environment. However, the attack surface is still uncovered in many aspects and left to be dealt with by the individual operators.

The EU Commission fosters trust by defining requirements that each C-ITS operator has to obey [36, 37]. However, the requirements do not address the entire life cycle of a message, from creation to usage, but only the communication interfaces between the operators. The remaining intermediaries and the definition of their security postures are left to the operator and may require bilateral trust agreement within a set of interconnected infrastructures, such

as operators and car manufacturers.

By employing our methodology, this problem can be overcome by providing a generic interoperable approach among the stakeholders of C-ITS. Starting from a road operator standpoint, initially all the data flows are systematically mapped in RAMI 4.0: road devices are *Assets*, while the ETSI standards [35] are *Communication* and *Information* layer's items. Then, for each asset, its life-cycle is evaluated with the RMIAS: for each item in RAMI, a risk assessment is performed with the traffic control experts to elicit the high level security goals, creating a taxonomy of all the architectural assets (road sensors, central ITS stations, communication protocols to road devices, etc). For each tuple in the taxonomy a cost-effectiveness analysis is performed of the off-the-shelf security countermeasures guided by the informative reference found and the legal context. As a results, a security architecture is proposed by the Security Architect, where each requirement, control, or process is categorized in the NIST CSF subcategories, as stated in Section 4. Finally, an initial security posture is obtained that is ready to be communicated to all other stakeholders. Car manufacturers build their posture by applying the methodology in the same way (defining the data flows of their on board equipment, performing risk analyses, and creating their own CSF profile). The profiles, once shared, facilitate the gap analysis, fostering the trust in the system and between the stakeholders. Interoperability is achieved as stakeholders are obliged to use best practices as informative sources (e.g., 62443, ETSI, or ISO), yet remaining at a sufficient high level to maintain confidentiality of the aspects that critical infrastructures cannot disclose [7].

6. Conclusions and Future works

In this paper we introduced a methodology that facilitates the creation of security postures using a systematic approach guided by the RAMI 4.0 architectural model that analyses each asset's life cycle eliciting security countermeasures. The output of the methodology is a profile of the NIST Cybersecurity framework that is then proposed as a method to attain interoperability and measurability of security postures when they have to be shared among interconnected infrastructures.

Although we relied on RAMI 4.0 for layering and module definition, the methodology itself is independent from the reference model used, as long as it has a clearly defined architecture. In future works we will investigate further the possibility of generalisation to other architectures, such as ISO IoT RA developed by ISO JTC 1/SC 41 or the Industrial Internet Architecture. That would allow implementation of the methodology in contexts other than the Industrial IoT.

References

- [1] European Parliament and of the Council, DIRECTIVE 2004/54/EC on minimum safety requirements for tunnels in the trans-european road network, 2004.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0054>, Last Accessed Feb 15, 2021.

- [2] The C-ITS Platform, C-ITS platform phase II, final report, Technical Report, The European Commission, 2017. <https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf>, Last Accessed Feb 15, 2021.
- [3] ENISA, From January 2019 to April 2020, The year in review, ENISA Threat Landscape, Technical Report, ENISA, 2020.
- [4] K. Moulinos, A. Drougkas, K. Dellios, P. Kasse, Good practices on interdependencies between OES and DSPs, Technical Report, ENISA, 2018.
- [5] European Parliament and of the Council, DIRECTIVE 2016/1148 concerning measures for a high common level of security of network and information systems across the union, 2016.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>, Last Accessed Feb 15, 2021.
- [6] Europol, Attacks on critical infrastructure, 2021. URL: <https://www.europol.europa.eu/iocta/2015/attacks-on-ci.html>.
- [7] The European Parliament and the Council of the European Union, Directive (eu) 2016/1148, 2016.
- [8] J. F. Miller, Supply Chain Attack Framework and Attack Patterns, Technical Report, MITRE Technical Report, 2013.
- [9] G. Ayoade, S. Chandra, L. Khan, K. Hamlen, B. Thuraisingham, Automated threat report classification over multi-source data, in: 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), 2018, pp. 236–245. doi:10.1109/CIC.2018.00040.
- [10] IEC 62443 2009-2018, IEC 62443 Security for Industrial Automation and Control Systems. Standard., Technical Report, International Electrotechnical Commission, 2009.
- [11] B. Leander, A. Čaušević, H. Hansson, Applicability of the iec 62443 standard in industry 4.0 / iiot, in: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19, Association for Computing Machinery, New York, NY, USA, 2019. URL: <https://doi.org/10.1145/3339252.3341481>. doi:10.1145/3339252.3341481.
- [12] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Technical Report, NIST, 2018.
- [13] R. Ross, M. McEvilly, J. C. Oren, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, *Special Publication (NIST SP) - 800-160*, Technical Report, NIST, 2018.
- [14] C. Neureiter, G. Eibl, D. Engel, S. Schlegel, M. Uslar, A concept for engineering smart grid security requirements based on sgam models, *Comput. Sci.* 31 (2016) 65–71. URL: <https://doi.org/10.1007/s00450-014-0288-2>. doi:10.1007/s00450-014-0288-2.
- [15] EIRA, Views, viewpoints and architecture building blocks, 2021. URL: <https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-3-views-viewpoints-and-architecture-building-blocks>.
- [16] R. Heidel, M. Hoffmeister, M. Hankel, U. Döbrich, Industrie 4.0, The Reference Architectural Model RAMI 4.0 and the Industrie 4.0 component, Beuth Verlag GmbH, 2019.
- [17] M. Gottschalk, C. Delfs, , M. Uslar, The Use Case and Smart Grid Architecture Model Approach: The IEC 62559-2 Use Case Template and the SGAM applied in various domains, *SpringerBriefs in Energy*, springer ed., Springer, 2019. URL: <http://www.springer.com/de/>

- book/9783319492285. doi:10.1007/978-3-319-49229-2.
- [18] B. Weinert, M. Uslar, Challenges for system of systems in the agriculture application domain, in: 2020 IEEE 15th International Conference on System of Systems Engineering (SoSE), 2020, pp. 000355–000360. doi:10.1109/SoSE50414.2020.9130552.
 - [19] M. Uslar, C. Rosinger, S. Schlegel, Security by design for the smart grid: Combining the sgam and nistir 7628, 2014. doi:10.1109/COMPSACW.2014.23.
 - [20] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, Technical Report, 2012. URL: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_security.pdf.
 - [21] J. Nurse, S. Creese, D. Roure, Security risk assessment in internet of things systems, IT Professional 19 (2017). doi:10.1109/MITP.2017.3680959.
 - [22] U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance, Technical Report, CISA, 2015. URL: https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf.
 - [23] T. Pavleska, H. Aranha, M. Masi, G. P. Sellitto, Drafting a cybersecurity framework profile for smart grids in EU: A goal-based methodology, in: S. Bernardi, V. Vittorini, F. Flammini, R. Nardone, S. Marrone, R. Adler, D. Schneider, P. Schleiß, N. Nostro, R. L. Olsen, A. D. Salle, P. Masci (Eds.), Dependable Computing - EDCC 2020 Workshops - AI4RAILS, DREAMS, DSOGRI, SERENE 2020, Munich, Germany, September 7, 2020, Proceedings, volume 1279 of *Communications in Computer and Information Science*, Springer, 2020, pp. 143–155. URL: https://doi.org/10.1007/978-3-030-58462-7_12. doi:10.1007/978-3-030-58462-7_12.
 - [24] H. Aranha, M. Masi, T. Pavleska, G. P. Sellitto, Securing mobile e-health environments by design: A holistic architectural approach, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2019, Barcelona, Spain, October 21–23, 2019, IEEE, 2019, pp. 1–6. URL: <https://doi.org/10.1109/WiMOB.2019.8923479>. doi:10.1109/WiMOB.2019.8923479.
 - [25] Reference Architecture Model Industrie 4.0 (RAMI 4.0), english translation of DIN SPEC 91345:2016-04, Technical Report, DIN, 2016.
 - [26] R. Cupek, M. Drewniak, A. Ziebinski, M. Fojcik, “digital twins” for highly customized electronic devices – case study on a rework operation, IEEE Access PP (2019) 1–1. doi:10.1109/ACCESS.2019.2950955.
 - [27] E. D. Knapp, J. T. Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd ed., Syngress Publishing, 2014.
 - [28] Y. Cherdantseva, J. Hilton, A reference model of information assurance security, in: 2013 International Conference on Availability, Reliability and Security, 2013, pp. 546–555. doi:10.1109/ARES.2013.72.
 - [29] A. Mosenia, N. K. Jha, A comprehensive study of security of internet-of-things, IEEE Transactions on Emerging Topics in Computing 5 (2017) 586–602. doi:10.1109/TETC.2016.2606384.
 - [30] Foreseeti, Foreseeti securicad solutions, 2021. URL: <https://foreseeti.com/securicad/>.
 - [31] MITRE, Att&ck for industrial control systems, 2021. URL: https://collaborate.mitre.org/attackics/index.php/Main_Page.

- [32] MAL, Meta attack language, 2021. URL: <https://mal-lang.org/>.
- [33] E. Commission, Collaborative its, 2021. URL: https://ec.europa.eu/transport/themes/its/c-its_en.
- [34] G. Wilhelm, H. Fouchal, K. Thomas, M. Ayaida, A c-its central station as a communication manager, in: M. Hodoň, G. Eichler, C. Erfurth, G. Fahrnberger (Eds.), *Innovations for Community Services*, Springer International Publishing, Cham, 2018, pp. 33–43.
- [35] ETSI, ETSI TS 102 941, Trust and Privacy management, Technical Report, 2019.
- [36] Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems, Technical Report, C-ITS Platform, 2017.
- [37] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems, Technical Report, C-ITS Platform, 2018.