Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems

Zhendong Ma, Aleksandar Hudic, Abdelkader Shaaban, Sandor Plosz
Digital Safety & Security Department
Austrian Institute of Technology, Austria
Email: {zhendong.ma aleksandar.hudic abdelkader.shaabaan.fl sandor.plosz.fl}@ait.ac.at

Abstract

Cyber-physical Production Systems (CPPS) are one of the technical driving forces behind the transformation of industrial production towards "digital factory of the future" in the context of Industry 4.0. Security is a major concern for such systems as they become more intelligent, interconnected, and coupled with physical devices. For various security activities from security analysis to designing security controls and architecture, a systematic and structured view and presentation of security-related information is required. Based on the draft standard of Reference Architecture Model for Industry 4.0 (RAMI 4.0), we propose a practical approach to establish a security viewpoint in the CPPS reference architecture model. We investigate the feasibility of using an architecture modeling tool to implement the concept and leverage existing work on models of layered architecture. We demonstrate the applicability for security analysis in two example case studies.

Keywords

Security, Cyber-physical Production Systems, Industry 4.0, reference architecture, RAMI 4.0

1. Introduction

Industrial production has transformed itself towards a smart manufacturing model in recent years. Referred to as *Industry 4.0* or *Industrial Internet*, the vision for the so-called 4^{th} *Industrial Revolution* is a highly automated, intelligent, interconnected, and interoperable production ecosystem across all segments in the value chain and product development lifecycle. A key enabler is the advancement of the Cyber-physical Systems (CPS) and their applications in the context of industrial production, referred to as Cyber-physical Production Systems (CPPS). The CPPS integrates and builds a variety of existing technologies and components such as robotics, industrial automation and control, Internet of things (IoT), big data, and cloud computing. Integration of these technologies is utilized on the following three fronts: horizontally, vertically and end-to-end. In a nutshell, CPSS interconnects industrial systems and CPS with manufacturing optimization and automation capabilities [1]. With CPPS, Industry 4.0 targets autonomous operation, mass product customization, collaborative manufacturing and end-to-end digital integration [2].

As a conglomeration of various technologies, Industry 4.0 is a complex and challenging topic. Therefore, a reference architecture is needed to conceptualize various sub-topics that I4.0 addressess into cohereent hierarchical layers of abstractions. It helps to build consistency and consensus among different stakeholders when integrating different technologies, methods, and processes of CPSS. There are several initiatives to date. In Germany, the working group for Industry 4.0 is developing a Reference Architecture Model for Industry 4.0 (RAMI 4.0), a three dimensional layered model [3]. The Industrial Internet Consortium (IIC) is developing the Industrial Internet Reference Architecture (IIRA) builting on Industrial Internet Systems (IIS) specified in four levels of "viewpoint" [4]. While RAMI 4.0 targets mainly industry automation, IIRA aims to bring IoT into a wider target area, including energy, healthcare, and transportation. Many similarities exist between these two architecture concepts [5].

Security is a major concern in CPSS when especially when it comes to modernizing industrial systems driven by interconnected ICT components. Unfrortunately, legacy industry systems did are not designed by having security-by-design in mind. Securing various parts of CPSS is a very challenging task [6]. Incorporating security aspects in a reference architecture model has the benefit of decomposing and structuring the problem into specific aspects and layers of abstraction for different stakeholders. Hence, in this paper we investigate the possibility to establish a security viewpoint in RAMI 4.0 to facilitate various security activities related to CPPS. By *security viewpoint*, we refer to the technique of focusing on security concerns within a reference architecture model using certain concepts and structuring rules. We argue that establishing a security viewpoint in a standard CPPS architecture model will greatly facilitate structured security analysis and design of legacy and greenfield systems, in which complex system descriptions can be represented in different levels of abstraction suitable for targeted audience. Moreover, as CPPS incorporates various aspects such as business model and production process, information system, and Industrial Automation and Control Systems (IACS), a security viewpoint based on standard reference architecture model can leverage many existing work on security from related fields.

Security is a major concern in CPSS when modernizing industrial systems driven by interconnected ICT components. Legacy industry systems did not start with security-by-design in mind. Securing various parts of CPSS is a very challenging task [6]. Incorporating security aspects in a reference architecture model has the benefit of decomposing and structuring the problem into specific aspects and layers of abstraction for different stakeholders. In this paper, we investigate the

possibility to establish a security viewpoint in RAMI 4.0 to facilitate various security activities related to CPPS. By *security viewpoint*, we refer to the technique of focusing on security concerns within a reference architecture model using certain concepts and structuring rules. We argue that establishing a security viewpoint in a standard CPPS architecture model will greatly facilitate structured security analysis and design of legacy and greenfield systems, in which complex system descriptions can be represented in different levels of abstraction suitable for targeted audience. Moreover, as CPPS incorporates various aspects such as business model and production process, information system, and Industrial Automation and Control Systems (IACS), a security viewpoint based on standard reference architecture model can leverage much existing work on security from related fields.

Our main contributions in this paper include: 1) to investigate the possibility of implementing the 6 layer RAMI 4.0 specification in UML-based models; 2) to integrate and link security concerns and requirements in RAMI 4.0 models for security analysis at the system architecture model level. Furthermore, we make initial effort in developing tool support for architecture modeling and demonstrate the feasibility of our approach in two case studies. We distinguish our work from existing work on model-driven security such as UMLSec [7] and SysML-Sec [8], in which we aim at leveraging the benefit of system model abstraction for practical security analysis and design of CPPS for industry usage rather than developing new method or formalism for extending modeling language to cover security aspects.

2. CPPS security and architecture model

In this section, we review current security concerns to CPPS and proposals for representing CPPS reference architecture.

2.1. CPPS security

CPPS consists of a variety of ICT technologies from enterprise data exchange and processing to physical monitoring and control, including enterprise IT, cloud computing, Industrial Automation and Control Systems (IACS), and IoT devices. Furthermore, information systems that involve enterprise resource planning (ERP), manufacturing execution (MES), and customer and supply chain management are included. Besides technologically advanced enterprise systems, CPPS also involves old and sometimes outdated legacy systems. Consequently, these systems inherit many old and new security weaknesses and problems and demonstrate an extended attack surface [6]. With the advance of interconnected production systems, an attacker is likely to be more motivated and determined due to increased economic and societal impact. Meanwhile, an attacker would have more targets to choose from because of the increased reachability and similarity in realization technologies.

Core enterprise systems such as Enterprise Resource Planning (ERP), Transaction Systems (TS), Manufacturing Execution Systems (MES), Supply Chain Management (SCM) or Customer Relationship Management (CRM) often contain enterprise patents, private information, trading secrets, design solutions. The evolution of divers technologies like visualization, containerization, cluster computing, etc., enabled enterprises to build their own powerful infrastructure or outsourcing their services to third part providers. Cloud computing as a prominent paradigm that reshaped the ICT landscape with regards to delivering service became a game changer. Cloud computing offers hybrid solutions that can combine private enterprise infrastructure with public third party to provide certain benefits for enterprises. Nonetheless, if we take into consideration MES or CPPS in general, enterprises like car manufacturers are highly reluctant to place them under external control. However, in the Industry 4.0 context, how to secure one's own systems and set up trust boundaries and data segmentation with others in the horizontal integration require extensive planning on the system architecture level.

On the other end of the cyber-physical spectrum, IACS monitors and controls production processes and physical actions and environments. They are different in many ways from enterprise IT systems [9]. Accordingly, IACS has specific security challenges. Traditionally, IACS were isolated systems running proprietary control protocols using specialized hardware and software. With the adoption of standard IT solutions within the IACS environment and the connectivity between the control systems and the cooperate network, IACS became less isolated and prone to most IT-related threats. Most conventional IT security solutions and practices cannot be directly applied to IACS environment due to different performance and reliability requirements in the Operational Technology (OT) environment. IACS are often installed in the field or industrial environment where the equipment must withstand harsh environmental conditions. They control processes which cannot easily be stopped without risking damage to the plant.

A large amount of the endpoints and hosts in CPPS are embedded systems or IoT devices. Coommonly, these are computer systems designed for dedicated functions, from sensors, micro controllers, and electronic control units (ECUs) to switches and routers. Embedded devices usually have CPU, memory, and power constraints, making them more vulnerable to attacks such as control hijacking, firmware reverse engineering, malware, crafted packets injection, eavesdropping, and brute-force attacks [10].

2.2. Reference architecture model

In our attempt to establish a security viewpoint, we investigate features from several existing reference architecture models. The main foundation of our approach is based upon RAMI 4.0, which we envision to be a standard way to represent Industry 4.0 systems in Europe. RAMI 4.0 is a reference architecture model for interconnecting industrial automation systems into the Internet of things. It has three axes: the architecture axis "layers" representing the information relevant to assets, the life cycle & value stream axis representing the

lifetime of an asset and the value-added process, and the hierarchy levels axis that align functional models to specific levels.

Although, the model described in the DIN SPEC 91345 standard is at the moment in draft state, the basic concept has been outlined. The elementary building blocks of the RAMI 4.0 are called assets, which comprise hardware, software, documents, measurements as well as human beings and knowledge, everything which represent value to the organization. In order to achieve interoperability between the cyber and physical world, the concept to represent assets in the virtual world is based on IEC 62832, the "Digital Factory" standard. A new component for that purpose called the administration shell has been introduced in RAMI 4.0. The administration shell intends to mask the peculiarities of the assets by providing a unified interface for describing asset capabilities, functionality and the ways for accessing the functions by means of services. This is in line with IT trends such as IoT and SoA (Service Oriented Architectures). The list of properties which form the vocabulary of description are adopted from existing standards such as IEC 61987 (List of Properties) and IEC 61360 (Common Data Dictionary). The administration shell stores the properties of its assets in the so-called manifest. The interface of the administration shell to access this information is based on semantic web, which is a standard of W3C for representing information, structure and relations in a well-defined way. The semantic web is a structure of the data format, taxonomies, ontologies, and protocols to interpret these. An important element is the Web Ontology Language (OWL) which provides ontology for describing properties, values and requirements. The administration shell of RAMI 4.0 structures the properties into nine different views. Each property can have aspects in one or more views. Security is one of the views and contains the properties relevant for security. There is, however, no further elaboration on these properties in the standard as is.

The Industrial Internet Reference Architecture (IIRA) [11] is a standardized open architecture based on industrial production systems. The main scope of IIRA is to maximize its value of broad industry applicability to drive interoperability, map eligible technologies, and technological guidelines and standard development. The IIRA abstracts the common characteristics, features and patterns from various case studies in the domain of communication, energy, healthcare, manufacturing, security, transporting and logistics, that have been defined by the Industrial Internet Consortium (IIC). The prior concerns identified by the IIS are classified and grouped together as four viewpoints (Business, Usage, Functional, Implementation). The IIC establishes security view across all viewpoints but unfortunately on a very high level. Pai [5] in his technical report demonstrates the mapping between the IIRA 3-tier functional viewpoint with the IT layers associated with the RAMI 4.0 architecture for the interconnected industrial organization and systematic model for asset efficiency testbeds. The author highlights how a combination of IIC and RAMI 4.0 guidelines may find relevance in end-to-end and complementary IIoT solutions going forward.

3. Security viewpoint

A security viewpoint in a standardized CPPS reference architecture model has the benefit of breaking complex systems into structured and consistent model representations, and to align various architectural artifacts in order to facilitate security-related activities from analysis to validation, even to support security management in operation. To be able to do so, we need to take in to consideration two fundamental questions:

- How to represent a system description with architectural artifacts in RAMI 4.0?
- How to extend the modeled architectural artifacts to include security?

3.1. Methodology

There will be diverse ways to describe various aspect of a CPPS including its business process, technology, system architecture and implementation. These descriptions might be in the forms of text documents and system diagrams. The descriptions might also be indeed models such as UML or Business Process Model and Notation (BPMN). Therefore, the first question deals with the mapping and transformation of existing descriptions into a layered model according to the definitions and rules set by RAMI 4.0. It is also likely that an existing system description does not include all information for a "complete" RAMI 4.0 model. In this case, additional artifacts can be added to enrich the model. Another important issue is to align and relate the architectural artifacts on the same layer (intra-layer relation) and across different layers (inter-layer relation). Since the RAMI 4.0 standard is still under development, for the sake of security viewpoint, we propose to map each of the elements from a system description to the model element of the six layers of RAMI 4.0, as visualized in Fig 1. The arrows shown in this figure represent the mapping process between security requirements in Security axis and different components in the levels of RAMI4.0. One component may connect with one or more security aspects based on the security gaps which should be covered. For example, the database component at the asset layer has some security facets which should be protected, such as Account Management, Data Protection, Back and Restore and so forth. We expect that with the maturity of RAMI 4.0 standard, explicit rules will be available to make this step more rigorous.

We use "security viewpoint" to collectively refer to security-related views and the references of the security-related information of the architectural artifacts (cf. Fig. 2).

Depending on the stakeholders, these security-related information can be security requirements, security risks, security controls and governance etc. To establish the security viewpoint, conceptually we include all security topics in one place and relate each of the topics to the architectural artifacts in the RAMI 4.0 model. In other words, the security viewpoint

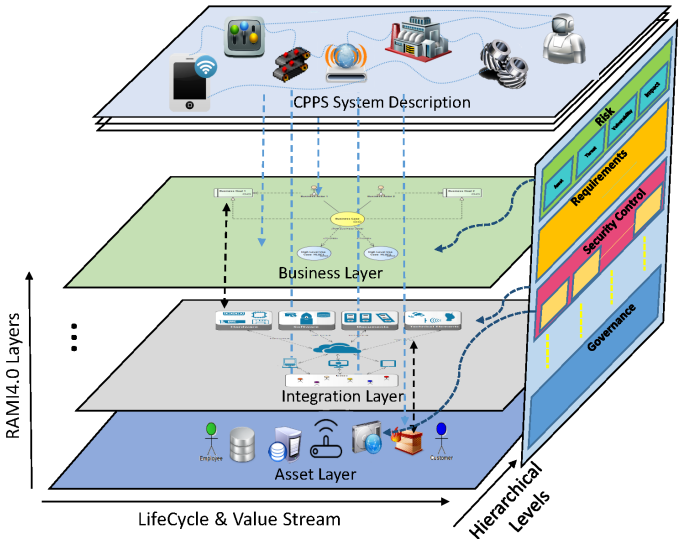

Fig. 1. Security viewpoint visualized as a vertical plane to RAMI 4.0 model

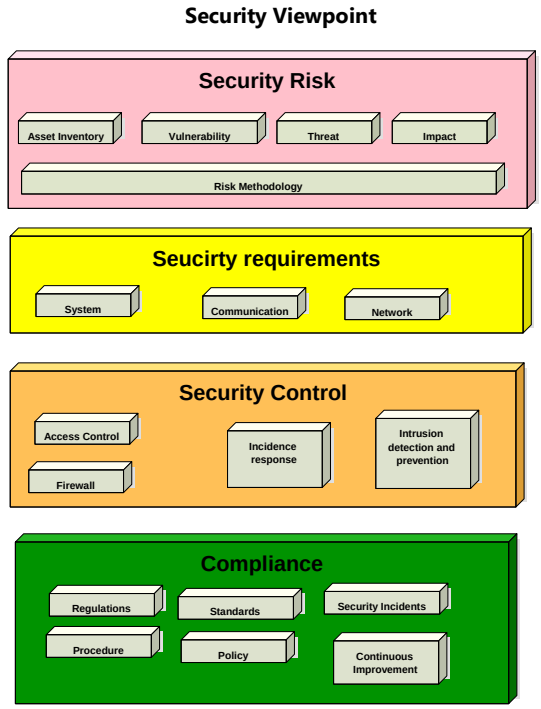

Fig. 2. Security viewpoint

in CPPS is modelled as a "3+1" approach, i.e. a three-dimensional RAMI 4.0 architecture model plus an additional axis for representing security. This is visualized as a vertical plane perpendicular to the six RAMI 4.0 layers in Fig. 1. The figure shows how elements of a CPPS system are mapped to the RAMI 4.0 layers. The architectural artifacts can be related with a same layer and across different layers using system modelling method supported by modelling tools. The security viewpoint is thus a collection of security topics that relate to the architectural artifacts. Representing security as a vertical plane to horizontal layers is a proven approach. It should be noticed that our purpose is to enrich the architectural artifacts in the RAMI 4.0 model with security-related information. Furthermore, with the viewpoint, these information can be aligned to architecture artifacts within and across the layers.

3.2. Implementation

Tool support is essential for practicability and relevance. We identify three basic requirements on the implementation:

- The implementation should be based on popular architecture modelling tools supporting common modelling languages such as UML with easy-to-use features.
- The implementation should be able to model a system in a layered structure and support the specification and establishment of inter- and cross- layer relationships.
- The implementation should provide the capability to structure and cluster relevant information into different model views with added intelligence to process and reason about the modelled information.

In this work, Enterprise Architect software used to achieve the designing and modelling process. Enterprise Architect is a visual modelling software and designing tool based on the OMG UML provided by Sparx Systems. EA provides a basis for modelling all forms of organizational architecture, for designing and implementing new systems or developing existing ones. Enterprise Architect ables to cover all aspects of the development cycle, providing full traceability from the initial design phase through to deployment, maintenance, testing, project management and change control, as well as, facilities for model-driven development of application code using an internal integrated-development platform [12]. Therefore, EA considers the best option to adapt the architecture models developed for smart grid architecture as one way to implement our CPPS security viewpoint approach.

Inspired by the Smart Grid Architecture Model (SGAM) toolbox [13], [14]. The SGAM focuses on a structured description of a distributed Smart Grid System in order to identify standardization gaps. The SGAM Toolbox was developed in order to ease the modeling of Smart Grid Systems in reference to the SGAM. The three-dimensional cube concept helps to analyze Smart Grid systems and interactions of assets. SGAM toolbox can be used under the umbrella of Enterprise Architect. So, in order to ease the work with the Toolbox some Model Templates have been created. Also, the SGAM provides some information concerning the representation of defined elements and some definitions for a model Import or Export [13]. SGAM toolbox is an extension of the Enterprise Architect [15] modelling tool for the Smart Grid Reference Architecture (SGRA) [16]. SGRA is an architecture model to ensure the consistency of electrical power grid between centralized and decentralized European energy systems with regards to distribution, transmission, bulk generation, operations and end customers. SGAM includes a methodology for designing smart

grid case studies as an architectural viewpoint. The framework consists of five abstraction layers that are representing business objectives and processes, functions, information exchange and models, communication protocols and components. Each of the layers selectively puts the focus on a particular operational part of the smart grid production, distribution or consumption aspect, and most importantly it shows how individual zones of information management mutually interact.

It is noteworthy that SGAM toolbox uses a metamodel to define model elements in each of the five layers and their relations. For example, in the metamodel, two model elements, Business Cases and Business Goals are defined at the business layer with relation realized. High-level Case Studies (HLCs) define an overview of an entire system, by identifying the main components that would be developed for the product and their interfaces. In this context, HLCs defined at the Function Layer, which is linked to Business Cases with invokes relation. Since there is not yet an official standard on the metamodel for RAMI4.0, at this stage, we adapted the SGAM metamodel and made certain justifications in our proof-of-concept implementations.

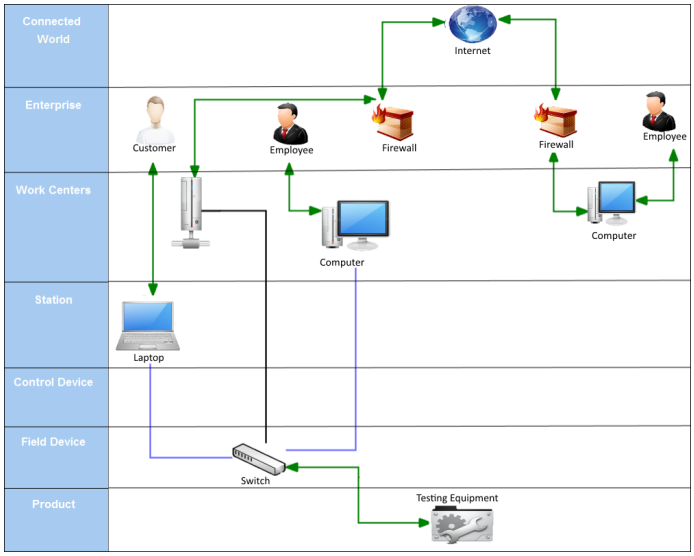

Fig. 3. Networked testing equipment in legacy system modeled on RAMI 4.0 asset layer

4. Case Studies

In this section, we use two simple examples to demonstrate the application and feasibility of our approach to illustrate the security viewpoint of these case studies which simulate a realistic CPPS scenarios that face security challenges in the context of Industry 4.0. The first case study shows the security requirements of IoT system components of the perspective of RAMI4.0 hierarchy level axis, while, the second example imitates a scenario of semiconductor production process to define the security aspects regarding architecture axis of RAMI4.0.

4.1. Interconnected testing equipment

The first case study is a legacy IoT automation system adapted to a cyber-physical system (CPS) interoperability framework that has been a product of the ARROWHEAD project[1]. We have performed a security assessment on an automotive use-case as it has been revised after each of the three succeeding generations of the ARROWHEAD framework. The challenge in adopting a legacy system to meet the needs of IoT and collaborative automation is to handle the increased attack surface without completely re-designing the existing system. However, there were no reference guides to follow for system adoption. Therefore, security-by-design principles have not been applied. This results in a sequential process of security risk modelling, analysis and threat mitigation solutions. An architectural concept such as RAMI4.0 can allow security to be handled separately from other functional aspects.

Accordingly, in the first case study, we model this legacy IoT automation system in the RAMI4.0 architecture and elaborate on how to map security issues to the layers of our proposed security axis. On top of that is the business goal of connecting the testing equipment to the outside world to offer services to both on-site and remote customers. Fig. 3 illustrates the graphical model on the asset layer in the perspective of RAMI4.0 hierarchy axis (hierarchy levels).

Illustrated in the figure, each asset is classified and assigned according to its hierarchy level in the RAMI4.0 model. The topology shows a real-life interaction between connected assets. The employees and customers are classified to the enterprise level who can communicate with the assets via computer devices. The Internet is classified as an entity at the connected world level which describes the relationship between assets or combination of assets. A switch is considered as a field device. Based on the model on the asset layer, a part of the security viewpoint, security requirements can be added to the model by using standard such as IEC 62443-2. In our implementation in Enterprise Architect, the security requirements from the standards are predefined as a collection of model elements as a template and added to the system model. For each of the assets, we can conveniently drag and drop a set of relevant security requirements to associate with the asset model element. Fig. 4 shows an example of the system security requirements applicable to the web service unit as specified in IEC-62443.

4.2. Semi-conduct manufacturing system

The second case study is a simplified semiconductor manufacturing system, largely based on [17]. Currently, the industries producing semiconductor and electronic parts face two major challenges: implementing IT-based structural reform and improving profitability. The establishment of IT-based “e-business” and “e-manufacturing” is a way to improve

1. www.arrowhead.eu

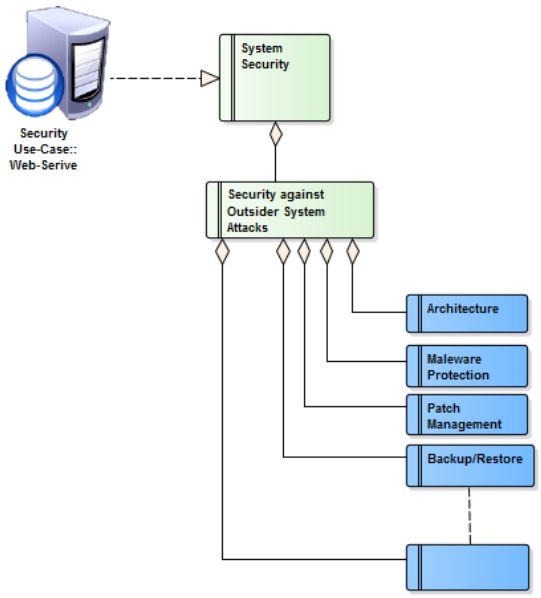

Fig. 4. System security requirements of web service unit

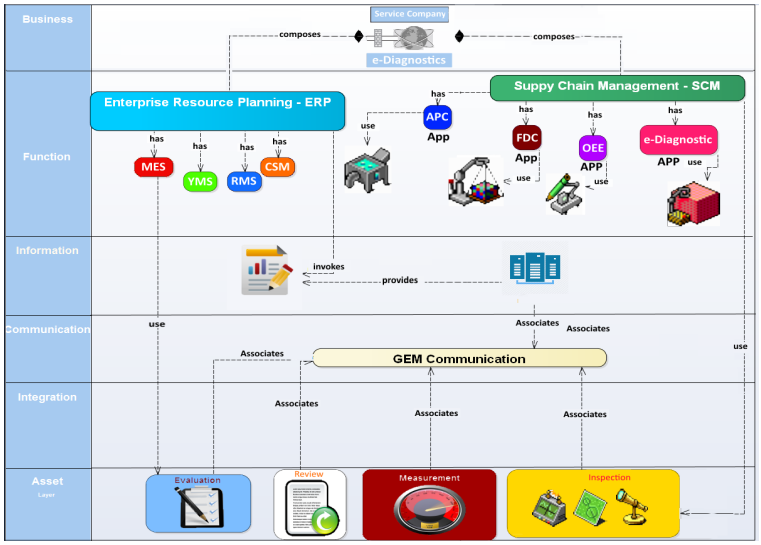

Fig. 5. Semiconductor production system modeled in RAMI 4.0 layers

development and equipment investment that put a negative impact on profitability. With such a complex system, RAMI 4.0 model has the benefit of reducing system complexity and align IT infrastructure and development with business goals, including security as well.

We show the interconnections between different architectural artifacts regarding the six RAMI 4.0 layers. Fig. 5 shows a semiconductor production system modelled on the architecture axis (layers) of RAMI 4.0. It is made up of six different layers indicating the information depending on the view of the asset. Note that it includes industry-specific terminologies and technologies, which can be annotated in an architecture modelling tool such as Enterprise Architect for even non-domain experts.

In this case study, we focus on the security of e-Diagnostic service. An e-Diagnostics service enables the manufacturing equipment to be diagnosed and maintained remotely via the Internet for activities such as distant start-up, diagnosis, and reparation. On the business side, it reduces maintenance cost and supports preventive maintenance. A security viewpoint on the e-Diagnostics services is a collection of security-related information on the additional security axis. Fig. 6 shows some examples of the security viewpoint including security risk, security requirement, and applicable security controls. The security viewpoint can include structured representation of security-related information that spans multiple areas to provide end-to-end security for remote support of equipment [18]. In e-Diagnostics, equipment can be accessed remotely by the vendor via the Internet. Some of the critical risks include factors such as leakage of confidential manufacturing data, hackers motivation, direct operational effects etc. Accordingly, security controls such as data encryption, access control, user authentication, and user identification are specified in

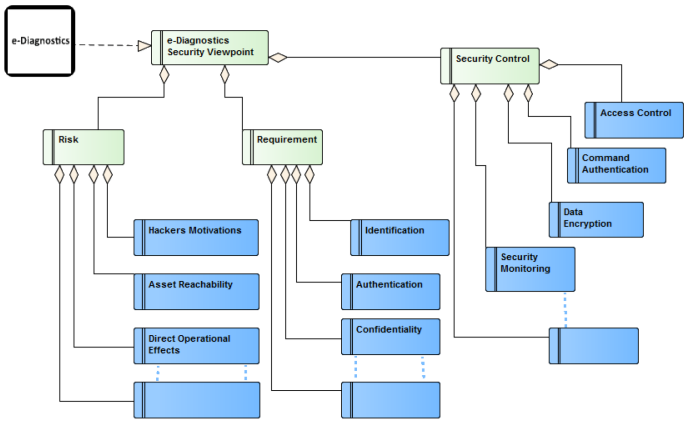

Fig. 6. Security viewpoint of e-Diagnostics service

the security viewpoint to mitigate the identified risks. These information can be encapsulated in one project file as the artifact and documentation during the system engineering process, allowing collaborations among security and domain experts as well as staff for business.

5. Conclusion

Cyber-Physical Production Systems (CPPS) integrate various technologies and systems for smart production in the context of Industry 4.0. Security is a major concern for such systems. In this paper, we review relevant security challenges and reference architectural models and propose method and tool support for establishing a security viewpoint in the Reference Architecture Model for Industry 4.0 (RAMI 4.0). Since

current RAMI 4.0 standard has not explicitly defined a viable approach to capture and represent security-related information in the layered model, we propose a "3+1" approach, in which security is an additional axis covering aspects along the layers as well as hierarchical levels. The security viewpoint includes security-related information and concerns such as security risks, requirements, and controls which can be conveniently linked to architectural artifacts using a modeling tool. As a proof-of-concept, we showed two case studies where we modeled the use-cases according to the RAMI4.0 architecture model and linked modeled elements in different layers to the topics on the security axis in a collective viewpoint.

Our future work will focus on two aspects. On the one hand, we will refine the underlying methods for system engineering and modeling and the inclusion of security aspects in CPPS. On the other hand, we will further develop tool support in Enterprise Architect and verify our approach in realistic use cases for securing CPPS.

Acknowledgment

A part of the work has been performed in the project Power Semiconductor and Electronics Manufacturing 4.0 (SemI40), under grant agreement No 692466. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal and - Electronic Component Systems for European Leadership Joint Undertaking (ECSEL JU). It is also partially supported by EU ARTEMIS JU funding within ARROWHEAD project, ref. ARTEMIS/001/2012, JU grant no. 332987.

References

[1] H. ElMaraghy and L. Monostori, "Variety management in manufacturing cyber-physical production systems: Roots, expectations and r&d challenges," *Procedia CIRP*, vol. 17, pp. 9 – 13, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212827114003497

[2] M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, "How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective," *International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering*, vol. 8, no. 1, pp. 37 – 44, 2014. [Online]. Available: http://waset.org/Publications?p=85

[3] "Das Referenzarchitekturmodell RAMI 4.0 und die Industrie 4.0-Komponente," http://www.zvei.org/Themen/Industrie40/Seiten/Das-Referenzarchitekturmodell-RAMI-40-und-die-Industrie-40-Komponente.aspx.

[4] "Industrial Internet Reference Architectural," https://www.iiconsortium.org/IIRA.htm.

[5] D. M. Pai, "Interoperability between IIC Architecture & Industry 4.0 Reference Architecture for Industrial Assets," Infosys, Tech. Rep., 2016. [Online]. Available: https://www.infosys.com/engineering-services/white-papers/Documents/industrial-internet-consortium-architecture.pdf

[6] M. Waidner and M. Kasper, "Security in industrie 4.0 - challenges and solutions for the fourth industrial revolution," in *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2016, pp. 1303–1308.

[7] J. Jürjens, *Secure Systems Development with UML*. Springer, 2005, vol. 54.

[8] L. Apvrille and Y. Roudier, "Designing safe and secure embedded and cyber-physical systems with sysml-sec," in *International Conference on Model-Driven Engineering and Software Development*. Springer, 2015, pp. 293–308.

[9] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ics) security," *NIST special publication*, vol. 800, no. 82, pp. 16–16, 2011.

[10] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," in *Privacy, Security and Trust (PST), 2015 13th Annual Conference on*. IEEE, 2015, pp. 145–152.

[11] S.-W. Lin, Industrial Internet Consortium, Tech. Rep., 2015. [Online]. Available: http://www.iiconsortium.org/IIRA-1-7-ajs.pdf

[12] E. Architect, "Sparx systems," 2010.

[13] C. Neureiter, "Introduction to the sgam toolbox," Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control, Salzburg University of Applied Sciences, Tech. Rep., 2013.

[14] C. Neureiter, G. Eibl, D. Engel, S. Schlegel, and M. Uslar, "A concept for engineering smart grid security requirements based on SGAM models," *Computer Science - R&D*, vol. 31, no. 1-2, pp. 65–71, 2016. [Online]. Available: http://dx.doi.org/10.1007/s00450-014-0288-2

[15] "SPARX Systems," http://www.sparxsystems.com/.

[16] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart grid reference architecture," CEN-CENELEC-ETSI Smart Grid Coordination Group, Tech. Rep., 2012. [Online]. Available: http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[17] Y. Usami, I. Kawata, H. Yamamoto, and H. Mori, "e-Manufacturing System for Next-generation Semiconductor Production," *Hitachi Review*, vol. 51, no. 4, p. 85, 2002.

[18] H. Wohlwend *et al.*, "E-diagnostics guidebook: Revision 2.1," *International SEMATECH Manufacturing Initiative(ISMI)*, 2005.