Towards Automated Security Evaluation within the Industrial Reference Architecture

1st Marco Ehrlich
Industrial Security
rt-solutions.de GmbH
Cologne, Germany
ehrlich@rt-solutions.de

2nd Martin Gergeleit
Telecommunication and Computer Architectures
Hochschule RheinMain
Wiesbaden, Germany
martin.gergeleit@hs-rm.de

3rd Henning Trsek
inIT - Institute Industrial IT
OWL University of Applied Sciences and Arts
Lemgo, Germany
trsek@th-owl.de

4th Georg Lukas
Industrial Security
rt-solutions.de GmbH
Cologne, Germany
lukas@rt-solutions.de

***Abstract*—The current developments towards the visions of Industrie 4.0 will create open and dynamic architectures being supervised by Industrial Automation and Control Systems. Due to this new connectivity and flexibility, future industrial production systems need to be inspected during all phases of the whole lifecycle from a security point of view as well. Frequent reconfiguration and adaptation based on smart services impose advanced requirements on the audits and certification with regard to security. To facilitate that, this work presents an approach for the modeling of security requirements and capabilities within the Industrial Reference Architecture and evaluates it based on the concrete system architectures of a number of industrial use cases. The result is the Sec4ICS tooling-based concept for the automated assessment of security-related functionalities within industrial systems.**

***Index Terms*—Security, Automation, OT, Sec4ICS, iRefA**

I. Introduction

Nowadays industrial automation systems are a major target for digitalization projects, because it allows optimizations of production systems and enables completely new, innovative approaches, such as highly flexible manufacturing systems. Technologies from the IT domain like cloud and edge computing or highly connected systems are increasingly important in the Operational Technology (OT) world. Ubiquitous connectivity is one enabler, which is required by the majority of industrial applications [1].

Due to this, The number of known and reported security incidents in industrial automation increases [2]. For instance, the ransomware attack on the Norwegian aluminium manufacturer Norsk Hydro in 2019 affected huge parts of their IT infrastructure in both the offices and the production. The complete recovery of their systems took several months and related costs of approx. 70 million US dollars were reported [3]. According to the SANS State of OT/ICS Cybersecurity Survey, the number of incidents grew substantially when comparing 2019 with 2017 [4], i.e. industrial automation environments are becoming a more and more interesting target for different groups of attackers. Besides this, internal threats, which occur in most cases accidentally, are another major concern [4].

The previous aspects evidently show that the security of such systems must be carefully considered in a holistic way, during the design phase as well as during the operation of the system. First of all, it is required to take security into account from the very beginning of the design, which is the architecture development. In the architecture development phase all parts of the system can be changed to achieve the required security. If security is only considered after the architecture design process or implementation of the use case, it is always difficult, often expensive, sometimes even impossible to achieve the required security levels. Second, the operation of a flexible manufacturing system requires frequent changes of the involved modules. The existing security approaches are very static and a lot of manual effort is needed to reassess changed systems. Hence, they are not able to address the required high flexibility in a sufficient way [5] and new approaches are required along the whole life-cycle of assets.

The Industrial Reference Architecture (iRefA) is a promising framework for the planning of new industrial systems [6]. Within this developments a methodology for the security analysis and subsequent automated deployment of iRefA Solution Architectures is shown in this work. A supporting tool named "Sec4ICS" has been implemented based on the IEC 62443 security abstractions and the "Topology and Orchestration Specification for Cloud Applications" (TOSCA) standard [7]. It is used for the security evaluation of the presented tooling approach and the corresponding use case scenarios.

The remainder of the paper is organized as follows: First the fundamental background is presented in order to understand the basic concepts of the related work and the security issues within future industrial architectures. Section III then shows the proposed approach with the Sec4ICS tool, the assessed use cases, and the corresponding evaluation. The last Section concludes the work and describes possible future work.

II. Fundamental Background

A. OT Security

Looking at currently growing landscape of threats and attackers, the topic of security becomes more and more important to nearly every industrial domain [2]. Therefore, governments, institutions, and organizations worldwide propose security-related standards, best practices, and regulations [5]. Although there is never a 100% guarantee to build a secure system, these proposals try to provide frameworks for stakeholders in order to perform evaluations, audits, and hardening of their systems to be secure against the majority of attacks or to become less attractive for adversaries. In general, these standards help organizations to describe the current and target states regarding their security. This is mostly done by identifying and prioritizing opportunities for improvements with e.g. countermeasures, evaluation of corresponding processes, and reporting frameworks for findings and risks towards all relevant stakeholders.

The common rule of thumb for OT as well as for IT environments is to perform security-related activities in a continuous manner as stated inside the ISO/IEC 27001 standard [8]. This is described e.g. within the Plan, Do, Check, and Act (PDCA) cycle and the Information Security Management Systems (ISMSs). These actions are used to raise awareness for security, to assign responsibilities and clarify processes, to incorporate the business management, and to maintain technical procedures for e.g. risk assessment, incident handling, auditing, and training [9]. A very similar approach is recommended inside the "IT Grundschutz" compendium specified by the German Federal Office for Information Security, which offers ten Process Building Blocks (PBBs) including e.g. an ISMS for all sectors from office to industry [10].

For the OT domain the IEC 62443 standard is the most important framework for security-related topics. The standard itself will be further explained in Section II-B to provide a basic understanding of the required knowledge for our proposed tooling approach with the Sec4ICS. In addition, it offers the Defense-in-Depth strategy including a collection of activities to establish a secure development, production, and operation of e.g. industrial components [11]. IEC 62443 adopts various approaches from the IT domain for the OT environments. This includes Cybersecurity Management Systems (CSMSs) and the definition of a Security Program (SP) containing 8 Security Program Elements (PEs) for the evaluation of security [12].

One of the foundation pillars for all security-related activities is Risk Management (RM), which is explained in Figure 1. The general framework for RM is described in the ISO 31000 standard, which specifies all required methods for a holistic RM application in organizations and businesses [13]. The main focus of these activities is put on the Risk Assessment (RA) process including the three steps risk identification, risk analysis, and risk evaluation. These steps represent the required manual work of the whole approach and the huge dependency on the experiences and skills of the specific security auditor. This is further amplified due to the given drawbacks with regard to a huge variety of standards and their implementation, such as the IEC 31010, several NIST Special Publications (SPs), German best practices, or the ISO/IEC 27005, which propose and add various RA techniques and approaches for a correct and secure RM [14]–[20].

The OT domain offers an own process to support industrial stakeholders with an approach to establish secure production plants and factories including risk assessment of assets and their corresponding countermeasures. The standard of choice there is the German VDI/VDE 2182, which is also referred to inside the IEC 62443-2-1 [21]. It proposes an eight step cyclic process to tackle the whole RM process: (1) Identify assets, (2) Analyse threats, (3) Determine relevant security objectives, (4) Analyse and assess risks, (5) Identify measures and assess effectiveness, (6) Select countermeasures, (7) Implement countermeasures, and (8) Perform process audits.

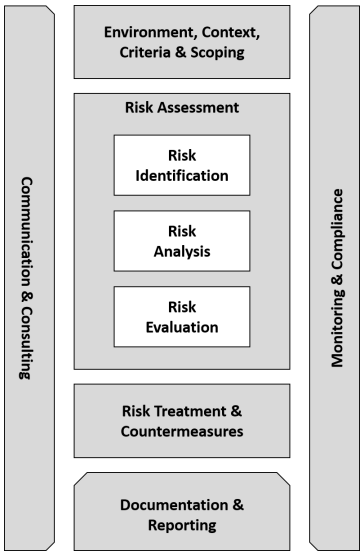

Fig. 1. General Risk Management (RM) framework [13]

The given landscape of standards from the IT and OT domains bring up several challenges for the future of industrial systems, especially with regard to the necessary certification of these systems [22], [23]. Each specified system configuration and corresponding changes have to be manually assessed by domain experts to find out whether they fulfill the demanded security requirements or not [24]. This imposes high efforts that lead to a trade-off between the dynamics of the adaptation of production processes and their security. Today's best practices are manual, static, and knowledge-intensive in a consistent and iterative cyclic manner which contradicts the overall requirement of availability and the possibility to update industrial systems due to e.g. newly discovered vulnerabilities. The main challenges are the lack of dynamic and adaptable RA methods, the coverage of all RA stages and asset lifecycle steps, the support of RA techniques with elaborate software tools for higher automation, the asset identification and management of available information, and the insufficient integration of security into engineering data for risk identifica-

tion [25]. To solve this in the future, developments within the I4.0 will be required to achieve the needed security levels in an automated way and to reduce the nowadays static procedures and manual efforts as much as possible.

Distinctive parts of this challenge are already addressed by various software-based tools developed by companies, research institutes, or governmental organizations [5], [25]. The most famous one for the OT domain is the Cyber Security Evaluation Tool (CSET)[1] which provides a well-designed entry point to the topic of security for businesses of every size. It contains generated checklists which have to be answered by the user in order to give an estimation about the security level of the evaluated company. Despite covering the main standards and guidelines, the CSET lacks an automated integration into industrial or business processes. Light and Right Security ICS (LARS ICS)[2] works in a similar way but lacks current updates and is still in a reworking phase. Another example is the ThreatModeler[3] from Microsoft which can be used for STRIDE-based RM preferably inside IT environments. Nevertheless, it still requires a huge manual effort to fill in all the information and lacks correspondence to new standards, such as the IEC 62443. In addition, there is a huge amount of threat intelligence and security management tools available on the market ranging from commercial, proprietary solutions to open-source research approaches [25]. The Collective Intelligence Framework (CIF)[4] or OpenVAS[2] could be mentioned here as examples. They provide mechanisms to collect information e.g. vulnerabilities about the evaluated system and to create analysis reports which need to be assessed manually. Another approach reflecting a new research direction is described in [26]. The authors developed a knowledge base as an ontology and specify the usage of information from engineering tools over the whole lifecycle of industrial systems. The collected data are integrated into a tool which can display security-related flaws inside the system automatically.

The Sec4ICS tool presented in this paper tries to resolve some of the mentioned drawbacks of the related work. It should provide automated security level analysis of a given industrial system with as least manual effort as possible by integrating various data sources given by the underlying system. In addition, the tool supports the most important industrial security standard IEC 62443 by adapting its concepts. The further description of the Sec4ICS tool and its evaluation is given the next sections.

B. Secure I4.0 Architecture

The Industrial Reference Architecture (iRefA) is developed inside the German research project Industrial Communication for Factories (IC4F) which aims to offer secure, robust, and real-time capable communication solutions within a technology kit [6]. It serves various business stakeholders, such as system architects or innovation managers, to define and assess technology-based architectures for their upcoming I4.0 use cases in almost any type or size of industrial environments. Figure 2 shows the basic iRefA framework with the corresponding inputs and outputs. The general idea is to collect the stakeholder's concerns and to formulate them into specific requirements in order to feed this information into the iRefA framework. The Architecture Building Blocks (ABBs) represent key technologies and their architecture principles. They can be used to follow a standardised process to create the desired industrial system architecture with a user guidance containing easy and user-friendly iterative steps.

The iRefA and its processes are designed to select a set of ABBs for an application scenario and expands it towards Solution Building Blocks (SBBs), which are used to create a "Solution Architecture". Such a Solution Architecture consists of hardware and software components and their corresponding interconnections. Thus, the iRefA provides the means to get from the initial business idea to the formalized architecture and finally an implementable solution [6]. Following the described approaches the iRefA ensures compliance by bridging the gap between business-oriented reference architectures, such as the Reference Architecture Model Industrie 4.0 (RAMI4.0) or the Industrial Internet Reference Architecture (IIRA), and concrete real-world industrial system architectures [6].

In this paper we will focus on the implementation and the evaluation of the Sec4ICS tool which was developed within the security-related parts of the iRefA framework and the corresponding Architecture Design Tooling (ADT). The Sec4ICS tool is based on public standards and open-source software in order to guarantee a possible utilization independent from the iRefA with a feasibility to be integrated into other reference architectures if required.

The IEC 62443 standard (cf. Section II-A) provides the fundamental principles for the integration of security into the iRefA. Therefore, the required information are briefly discussed in the following paragraphs. The IEC 62443 has become the most important security standard for the usage inside Industrial Automation and Control Systems (IACSs) covering the fundamental issues of industrial communication networks and their intrinsically linked topic of security. Therefore, the IEC 62443 is the standard of choice and this work adapts it to address security classification and modeling for an automated architecture evaluation. In part 3-3 of the IEC 62443 standard information security is classified in a four stage scaling system (plus a no-security-level). The stages are referred to as Security Levels (SL) [27].

- SL 0: No protection at all.
- SL 1: Delivers protection against casual or coincidental violation.
- SL 2: Provides protection against intentional violation using simple means.
- SL 3: Gives protection against intentional violation using sophisticated means.
- SL 4: Is described by protection against intentional violation using sophisticated means with extended resources.

[1] www.ics-cert.us-cert.gov/assessments
[2] www.bsi.bund.de/de/themen/industrie_kritis/ics/tools/tools_node
[3] www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
[4] https://github.com/csirtgadgets/cif-v5

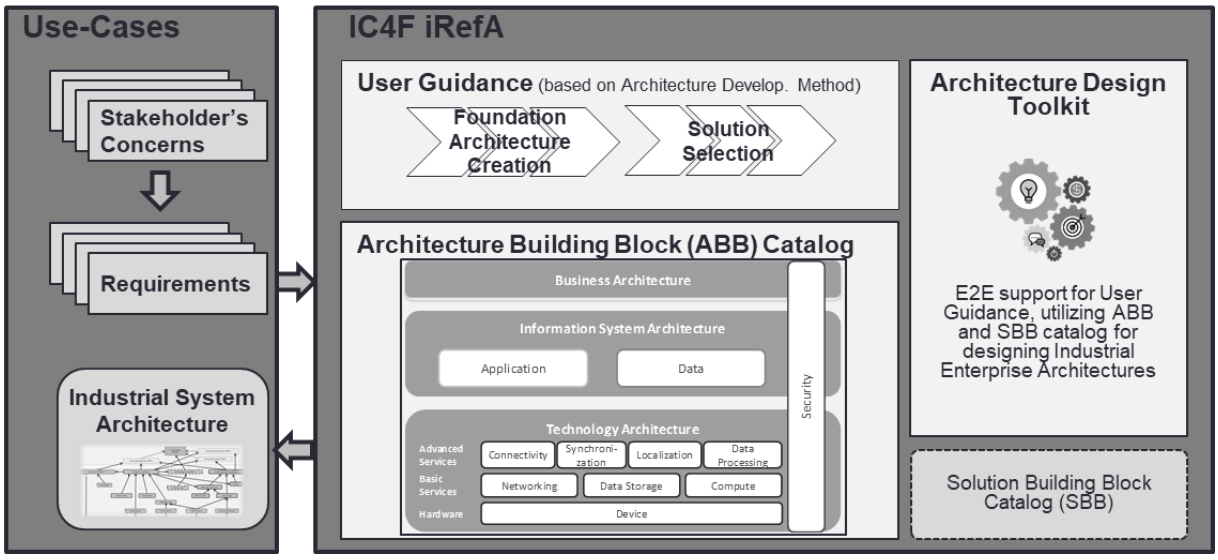

Fig. 2. Industrial Reference Architecture (iRefA) framework [6]

The SLs are designed in the way of using the attacker's motivation and resources, which is seen as a future-proof definition. The standard further describes 7 Foundational Requirements (FRs) based on multiple System Requirements (SRs) with varying quantity on each FR, which provide an abstracted view on the overall security goals. The FRs cover all usual dimensions of cyber security.

- FR 1: Identification and Authentication Control (IAC) - Identify and authenticate all users (humans, software processes, and devices) before allowing them to access the control system.
- FR 2: Use Control (UC) - Enforce the assigned privileges of an authenticated user (human, software process, or device) to perform the actions on the IACSs and monitor the use of these privileges.
- FR 3: System Integrity (SI) - Ensure the integrity of the IACSs to prevent unauthorized data or information manipulation.
- FR 4: Data Confidentiality (DC) - Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.
- FR 5: Restricted Data Flow (RDF) - Segment the control system via zones and conduits to limit the unnecessary flow of data.
- FR 6: Timely Response to Events (TRE) - Respond to security violations by notifying the proper authority, reporting needed evidence of the violation, and taking timely corrective action when incidents are discovered.
- FR 7: Resource Availability (RA) - Ensure the availability of the control system against the degradation or denial of essential services.

The desired SLs regarding the different FRs can be varying and they are dependent on the specific use case, which is described using the IEC 62443 standard. Generally, there is a differentiation between three characteristics of SLs.

- Target Security Level (SL-T): Desired level of security for a particular system during conception phase.
- Achieved Security Level (SL-A): Actual level of security for a particular system after finished setup.
- Capability Security Level (SL-C): Security level that the chosen components in a setup can provide.

The iRefA has a comprehensive approach to security. At the beginning of the architectural phase, the security requirements are analyzed and then defined for the seven FRs of the IEC 62443 standard. In the later phases, the requirements are used for the selection of technologies needed to achieve the identified security level. If the SL-As of the selected ABBs do not fulfill the SL-T of the use case, then further ABBs are added to improve the security level. With this approach security is already considered during the planning of the system, leading to a better and resource-saving integration of security in the overall system. Finally, even dynamically changing implementations of a typical I4.0 setup can be re-certified for security compliance before each deployment in an integrated process. Previously we have introduced a model-based approach [24] for the security analysis and subsequent automated deployment of these Solution Architectures based on the IEC 62443 abstractions and the TOSCA standard [7]. This approach, the new supporting tool named "Sec4ICS", and its application in the context of the iRefA will be further explained and assessed in the next section.

III. iRefA Security Evaluation

As explained above applying the iRefA to an industrial use case results in a Solution Architecture for its implementation. A Solution Architecture consists of a number of SBBs (hard- and software components, including physical devices) and their relations (like "connected with" or "hosted on"). For a (partially) automated deployment of such an architecture in an industrial edge cloud a formal description is required.

A common framework for these kind of deployment tasks is TOSCA. It has been proposed in 2014 by the "Organization for the Advancement of Structured Information Standards" (OASIS) for cloud deployment and orchestration inside typical IT domains. It includes a YAML-based declaration language that can be used for specifying topologies representing a set of components and their relations like Solution Architectures of the iRefA. Such a methodology becomes essential in dynamic I4.0 environments, where architectures are partly virtualized and can be adapted quickly.

TOSCA itself does not address security issues at all. However, its object-oriented approach allows for extending TOSCA types and specifications with SL-Cs without breaking the existing specification or already implemented TOSCA tools (like shown below in 1.) So, we decided to develop Sec4ICS by enhancing the existing open source TOSCA compiler "puccini" towards a security checker. The original puccini tool parses TOSCA topology descriptions in YAML and produces deployment scripts in various formats. The enhanced Sec4ICS now also evaluates whether a given application topology with its security capabilities can fulfill the stated security requirements. It needs the security-enhanced TOSCA model, which is typically provided by system architects, of the complete Solution Architecture as input. The output of Sec4ICS is a list of potential security flaws and, if possible, a deployment script (currently e.g. an Ansible Playbook for edge cloud deployment). The Sec4ICS tool and the extended TOSCA type declaration has been described in [28]. The tool is full functional and all analysis tasks described in this paper were done using this implementation of Sec4ICS on Linux.

The security capabilities of SBBs are modeled as SL-Cs according to the abstractions of the IEC 62443 standard as described above. Security requirements of the overall architecture are modeled as SL-Ts. However, a more complex factory scenario often consists of a number of different domains like physically secured areas, network segments, control hierarchies, and applications with interfaces beyond restricted domains. A one-size-fits-all approach with one single SL-T vector for the complete architecture is usually impossible. Instead, different domains within such a Solution Architecture will have different risks and different resulting security requirements. Thus the modeling has to reflect these differences and it introduces "Security Domains" for this purpose. A Security Domain specifies an area of equal security requirements. Each security domain defines one SL-T vector representing its security requirements as a result of a RA process. In a simple case the complete application topology belongs to one Security Domain, in a more complex setup an application might span over a number of Security Domains.

A. Modeled Uses Cases

For evaluation of our approach we modeled a set of real world use cases and applied the checking methodology to it. As use cases we have analysed the prototype applications of the IC4F project (www.ic4f.de) as a representative scenario for a typical future industrial production environment. For this process we modeled the use cases according to the iRefA guidelines, built the TOSCA model of the Solution Architecture, added security requirements and capabilities to it, and performed the analysis using the Sec4ICS tool. This shows how an automated support for the important risk identification and risk analysis phases in future dynamic ICS can be established. In the following we will first introduce the topology of the use cases at a more abstract level in order to explain the use case scenario. Then, the formal modeling of this topology and especially its security parameters will be described. Finally, the results achieved with our proposed methodology and the Sec4ICS tool will be presented.

We modeled three of the IC4F use cases that are all implemented in one common infrastructure, sharing numerous SBBs. Each use case is modeled as a separate Security Domain, resulting in three domains, each with distinct security requirements:

- TRUCK_TO_X: A use case of a Truck-to-X communication system.
- FORKLIFT_LOCALIZATION: A use case of a localization of a moving forklift.
- MES: A use case with a Manufacturing Execution System (MES) deployed on an industrial edge cloud.

The security requirements are expresses via the SL-T values of the identified Security Domain, i.e. the desired level of security for each of the seven dimensions. Figure 3 gives an overview of the values derived from the application architecture: for the use cases TRUCK_TO_X and FORKLIFT_LOCALIZATION as shop floor application a basic level of security (i.e. mostly SL1) is required. As these applications are physically protected by the factory buildings and have no direct connection to an external network, this seems adequate for an initial setup. In this case FR3 "System Integrity" has been even set to SL0. No explicit malware protection is required, as it is assumed that physical and logical access protection is sufficient. For the use case MES a higher degree of security is necessary, as it is connected to external systems and finally to the Internet. Thus, a SL2, protecting against the usual threats in the Internet is mandatory. For this setup here we require only basic Denial of Service (DoS) protection (FR7 equals SL1), as it is not a critical production system.

Security Domains (SL-T)	FR1	FR2	FR3	FR4	FR5	FR6	FR7
TRUCK_TO_X	1	1	0	1	1	1	1
FORKLIFT_LOCALIZATION	1	1	0	1	1	1	1
MES	2	2	2	2	2	2	1

Fig. 3. Required SL-Ts of the Security Domains

The three Security Domains are shown in Figure 4. It shows the components belonging to one or more of the three Security Domains. As one would expect, e.g. the central network gateways of the shared infrastructure are lying in the intersection of all domains, as they are relevant for every use case. Others, like the forklift, only belong to one application use case and as such to one Security Domain.

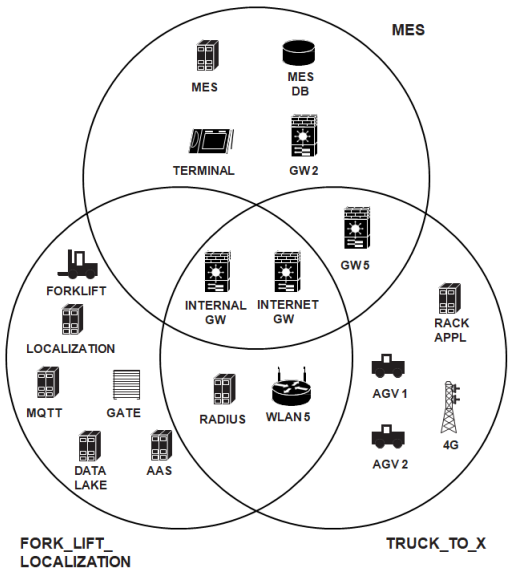

Fig. 4. Security Domains of the Use Cases

Figure 5 shows the structure of (partially virtualized) networks with all connected devices. VLAN2 contains components that are exclusively belonging to use case MES, VLAN4 those of use case FORKLIFT_LOCALIZATION, VLAN5 connects components of use case TRUCK_TO_X. VLAN3 contains an MQTT broker and a global data lake, which are shared components for multiple uses cases in a separate network segment. Additional components in external networks are connected via gateways and firewalls. For instance, a dedicated positioning server used in the FORKLIFT_LOCALIZATION use case is reachable via an internal gateway and the Public Key Infrastructure (PKI) on a public server which is accessible via a firewall in the Internet. The various WiFi clients share a common WLAN infrastructure and the second Automated Guided Vehicle (AGV) and the gate of use case FORKLIFT_LOCALIZATION are connected via a private 4G cell.

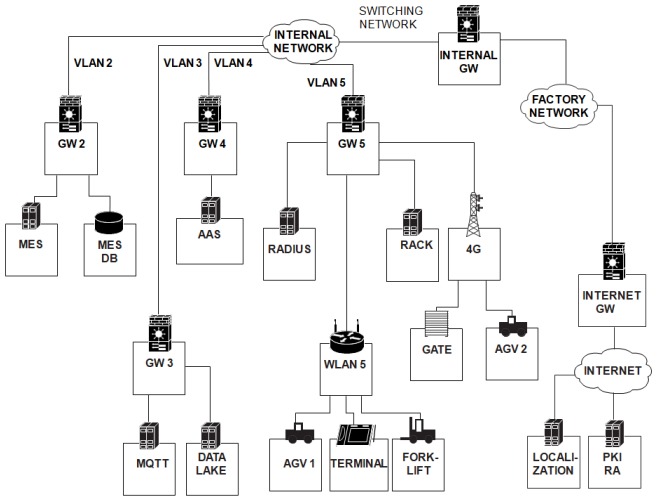

Fig. 5. Network Structure of the Uses Cases

The applications and their logical links are depicted in Figure 6. The terminal application as front end of the MES communicates to the MES server via HTTPS. The application server has a connection to its database. The forklift and the gate are communicating with the controlling Asset Administration Shell (AAS) via the central MQTT broker over a TLS-secured MQTT pub/sub communication. In the same way the data lake service publishes the spatial data received from the location service (received via plain MQTT). The WLAN access points receive their authentication data via the RADIUS protocol (RFC 2865) from the central server. The two AGVs are connected via a request/response protocol with their controlling applications (called "RACK"). The application modeling does not contain all logical components and links, especially not those that are not in the scope of the normal system runtime (e.g. the pre-runtime distribution of PKI certificates) and those that are not under control of the project team (e.g. external PKI software).

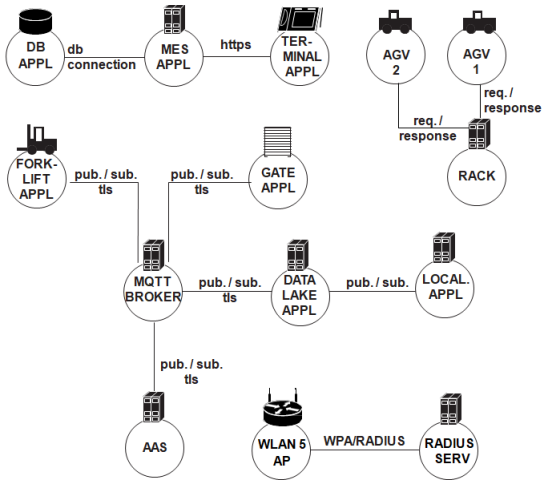

Fig. 6. Applications and Protocols of the Use Cases

B. Modeling Process and Security Analysis

Modeling starts by expressing the topology of the application given above in a TOSCA topology description as given in [24], separated in four files describing the physical and logical network topology as well as the SBBs and the Security Domains. It includes the declaration of all components of the architecture, incl. compute resources like physical and virtual machines as well as containers, also network functions and software components. The complete topology also contains all relevant relationships between these components. Relationships in TOSCA can be modeled using matching requirements and capabilities. The relation between machines and their hosted applications is modeled using the "host" requirement and the logical communication relationships using the "endpoint" requirement. The physical network connections are modeled via "network" attributes and the membership of a building block to a Security Domain is modeled via "member" requirements in the domains. The topology description finally

contains all the information to generate complete deployment scripts (for all components that support automated deployment). Our Sec4ICS tool can create Ansible Playbooks as deployment scripts in addition to the security evaluation.

Listing 1. TOSCA Description of the MQTT Broker with sec_vector

```
mqtt_appl:
  type: SecureApplication
  properties:
    sec_vector:
        [2, 2, 1, 2, 1, 3, 0]
  attributes:
    networks:
      vlan3:
        network_name: vlan3
  capabilities:
    generic_endpoint:
      properties:
        protocol: mqtt
        port: 1883
        secure: true
        network_name: vlan3
        initiator: peer
  requirements:
    - host: mqtt_vm
```

All SBBs are also attributed with their security properties given as vectors with the seven FRs of the IEC 62443 security standard. These security properties have to be assigned by experts during the definition of the SBB catalogue, the collection of all SBBs that can be used to implement a Solution Architecture. They depend on the features and the configuration of the component. Listing 1 gives an example of such a TOSCA description for an SBB, in this case the MQTT broker application, enhanced by the new sec_vector holding the SL-C values of this component. Figure 7 gives an overview of the security property SL-C assignments for all building blocks of the complete Solution Architecture.

Details of the requirements leading to this classification can be found in the tables of the IEC 62443 standard. An SL-C value of SL2 in the column FR1 "Identification and Authentication control" requires that all humans and machines are individually identified and authenticated. A user/password scheme for humans and an individual certificate per machine is able to fulfill such a requirement for many building blocks. On the other hand, it can be seen, that most components have a SL0 in the FR7 "Resource Availability" column of their SL-C. This results from the fact that SL1 already requires a battery back-up or a redundant power supply and also means to mitigate DoS attacks. In the use case setups this is mostly not given. The "d/c" (don't care) values in column FR5 "Restricted Data Flow" state that these values are not relevant for the overall security analysis, as there is no data flow through the affected components.

Applying the Sec4ICS tool to this model detects any mismatches between the required SL-Ts (from Figure 3) and the provided SL-Cs. These mismatches are not necessarily already security flaws, but a hint, that this issue requires further consideration by the system designer or integrator. This consideration might include some additional measures to increase the security of certain building blocks before final deployment, but it can also lead to an informed and documented decision, that either this issue is either already mitigated by other means or that somebody is willing to accept this risk.

Building Block	Name	FR 1	FR 2	FR 3	FR 4	FR 5	FR 6	FR 7
Network Components (SL-C)								
WLAN 5	wlan_access_point	2	2	1	2	3	3	0
4G	4g_access_point	2	2	1	2	3	3	1
GW X	gw_2 - gw_5, gw_factory, gw_internet	2	2	1	2	3	3	0
Physical/Virtual Machines (SL-C)								
MES	mes_vm	2	2	1	2	2	3	0
MES_DB	mes_db_vm	2	2	1	2	2	3	0
MQTT	mqtt_vm	2	2	1	2	2	3	0
DATA LAKE	data_lake_vm	2	2	1	2	2	3	0
ASSET ADM. SH.	asset_admin_shell_vm	2	2	1	2	2	3	0
RADIUS	radius_vm	2	2	1	2	2	3	0
RACK	rack_vm	2	2	1	2	2	3	0
TERMINAL	forklift_terminal_vm	2	2	1	2	2	3	0
FORKLIFT	forklift	1	1	0	2	d/c	3	0
AGV1	agv1	1	1	0	2	d/c	3	0
AGV2	agv2	1	1	0	2	d/c	3	0
GATE	gate_vm	1	1	0	2	d/c	3	0
LOCALIZATION	localization_vm	2	1	1	2	2	3	0
PKI	pk_ra	3	3	2	3	3	3	2
Applications (SL_C)								
MES APP	mes_appl	2	2	1	2	1	3	0
MES_DB	mes_db_appl	2	2	1	2	2	3	0
MQTT	mqtt_appl	2	2	1	1	1	3	0
DATA LAKE	data_lake_appl	2	2	1	1	1	3	0
AAS	asset_admin_shell_ap	2	2	1	1	2	3	0
RACK	rack_appl	2	2	1	1	2	3	0
TERMINAL	forklift_terminal_appl	1	1	1	1	d/c	3	0
AGV1	agv1_appl	1	1	1	1	d/c	3	0
AGV2	agv2_appl	1	1	1	1	d/c	3	0
GATE	gate_appl	1	1	1	1	d/c	3	0
LOCALIZATION	localization_appl	1	1	1	1	2	3	0

Fig. 7. Assignment of SL-Cs

The results of the analysis are given in a log file. The start of this log for the example use cases is shown in Figure 8. The analysis shows, that there are still some security deficits found in the overall application topology. These are mainly "System Integrity" concerns in use case MES. SL2 here would require some additional means concerning integrity of stored program and (configuration) data, secure boot, and physical tamper resistance. Also, several issues with the security of the mobile terminal are mentioned here. Some more complains notices about missing SL1 in FR7 "Resource Availability" are skipped in the listing. These are all clear hints on security concerns that should be considered before final deployment by the system designer or integrator. This consideration might

include some additional means to increase the security of certain building blocks before final deployment, but it can also lead to an informed decision, that somebody is willing to accept this risk.

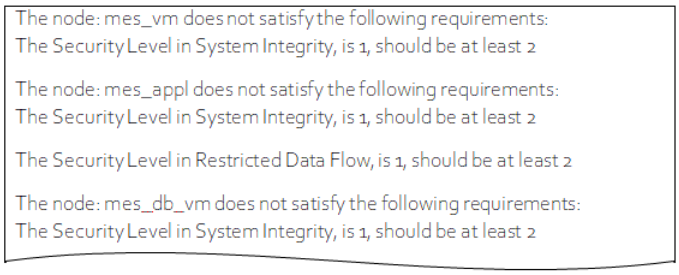

Fig. 8. Log of the Sec4ICS tool for the example uses cases

IV. Conclusion

In this work we have presented an approach for the modeling of security requirements and capabilities, which has been evaluated based on the concrete system architectures of a number of industrial use cases. It has been shown how the overall architecture and its security properties can be modeled using the abstractions of the IEC 62443 security standard and the TOSCA modeling language for cloud deployment. The automatic methodology and the supporting Sec4ICS tool provide a concise assessment of the system's security status and a clear guidance for possible improvements. As both the topology model as well as the security requirements can be easily updated and the final evaluation is automatic and supported by the Sec4ICS tool, the process of risk management can be applied repeatedly and reducing major manual efforts. This allows for an interactive design of secure industrial system architectures, for quick configuration changes during operation, and for assistance when new security requirements and capabilities have to be integrated. This overall improves the security management of the described I4.0 scenarios and enables us to benefit from the full potential of flexible systems.

Future work within this topic still includes various activities. First of all the evaluation of the Sec4ICS tool needs to be expanded towards additional industrial environments and use cases including real production systems. In addition, the amount of SBBs from additional vendors and manufacturers should be increased to get a broader impact on the industrial domain. Finally, the Sec4ICS tool needs an implementation with regard to dependencies and relationships between SBBs and the effects on the environment and other SBBs in order to further enhance the analysis results.

Acknowledgment

This work was funded within the research projects "Industrial Communication for Factories" (IC4F) by the German Federal Ministry for Economic Affairs & Energy and "Future Industrial Network Architecture" (FIND) by the German Federal Ministry of Education & Research.

References

[1] M. Wollschlaeger, T. Sauter, and J. Jasperneite, *The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0*, Industrial Electronics Magazine, 2017.

[2] A. Pattanayak and M. Kirkland, *Current Cyber Security Challenges in ICS*, ICII, Seattle, USA, 2018.

[3] Federal Office for Information Security, *The State of IT Security in Germany 2019*.

[4] SANS, *SANS 2019 State of OT/ICS Cybersecurity Survey*.

[5] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, *Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing*, IECON, Lisbon, Portugal, 2019.

[6] Industrial Communication for Factories (IC4F), *The Industrial Reference Architecture (iRefA) - Description and User Guidance for System Architects*, Project Consortium White Paper, Version 1.0, 2019.

[7] Organization for the Advancement of Structured Information Standards, "OASIS TOSCA Simple Profile in YAML Version 1.1," 2018.

[8] International Organization for Standardization & International Electrotechnical Commission, *DIN EN ISO/IEC 27001: Information technology - ISMS Requirements*, 2017.

[9] International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 27000: Information technology - ISMS Overview and Vocabulary*, 2014.

[10] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kompendium*, Reguvis Fachmedien GmbH, 2020.

[11] International Society of Automation, *IEC 62443-4-2: Technical security requirements for IACS components*, 2015.

[12] P. Kobes, *Guideline Industrial Security - IEC 62443 is easy*, VDE Verlag, Offenbach, Berlin, 2017.

[13] *DIN ISO 31000: Risk management guidelines*, DIN-Normenausschuss Organisationsprozesse (NAOrg), 2018.

[14] International Organization for Standardization & International Electrotechnical Commission, *IEC 31010: Risk management: Risk assessment techniques*, 2019.

[15] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, 2018.

[16] National Institute of Standards and Technology, *Information Security - Guide for Conducting Risk Assessments*, NIST SP 800-30, 2012.

[17] National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, Special Publication (SP) 800-82 Revision 2, 2015.

[18] Bundesamt für Sicherheit in der Informationstechnik, *BSI-Standard 200-1: Information Security Management System (ISMS)*, 2017.

[19] Bundesamt für Sicherheit in der Informationstechnik, *BSI-Standard 200-3: Risk Analysis base on IT-Grundschutz*, Version 1.0, 2017.

[20] International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 27005: Information technology — Security techniques — Information security risk management*, 2018.

[21] Verein Deutscher Ingenieure, *VDI/VDE 2182: IT-security for industrial automation - general model*, Verband der Elektrotechnik Elektronik Informationstechnik, 2011.

[22] European Cyber Security Organisation, *European Cyber Security Certification: A Meta-Scheme Approach*, WG1 – Standardisation, certification, labelling and supply chain management, v1, 2017.

[23] M. Carl and K. Gondlach, *Sicherheit 2027: Konformitätsbewertung in einer digitalisierten und adaptiven Welt*, 2b AHEAD, 2017.

[24] M. Ehrlich, M. Gergeleit, K. Simkin, and H. Trsek, *Automated Processing of Security Requirements and Controls for a common Industrie 4.0 Use Case*, NetSys, Garching, Germany, 2019.

[25] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, *Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges*, Journal of Internet Services and Information Security (JISIS), Volume: 9, Issue: 3, 2019.

[26] C. Tebbe, K.-H. Niemann, and A. Fay, *Ontology and life cycle of knowledge for ICS security assessments*, International Symposium for ICS/SCADA Cyber Security Research, Belfast, United Kingdom, 2016.

[27] International Society of Automation, *IEC 62443-3-3: System security requirements and security levels*, 2013.

[28] M. Gergeleit, H. Trsek, T. Eisert, and M. Ehrlich, *Modeling Security Requirements and Controls for an Automated Deployment of Industrial IT Systems*, 9. Jahreskolloquium Kommunikation in der Automation (KommA), Lemgo, Germany, 2018.