Aligning with cybersecurity framework by modelling OT security

Mithil Parekh [1], Karl Waedt[2] and Asmaa Tellabi[3]

Abstract: Before the last decade, production units and its related systems were considered nearly as island systems and were managed as an air-gaped in their daily operations. Information and network security was not an issue because their plant's safety and continues operations have the highest priority. In the recent years, many initiatives like smart factories, adopting Industry 4.0, complex mesh of connected devices and data privacy have shifted paradigm of value chain and trust model in the production environment. By this means, state-of-the-art manufacturing environment demands for the comprehensive framework and holistic approach to address cybersecurity that affects reliability of plant operations. Therefore, few standards are gradually evolving and are extended in to this field. The ISA/IEC 62443 is one of the standard series addresses the Security of Industrial Automation and Control Systems (IACS) throughout their lifecycle. On the other hand, NIST Special Publication 800–82 is a Guide to Industrial Control Systems Security and follows NIST CSF to address OT security. As with Operational Technology (OT) requirements in general, also considering to security-related requirements as per ISA/IEC 62443, ask for more effort to deal with it later. Accordingly, bearing in mind, the need for security from the beginning of the system engineering processes reduces the overall effort and complexity during the lifecycle of OT systems. The corresponding paradigm is called Security by Design. This paper proposes on how high level foundational security requirements from ISA/IEC 62443 can be modelled using AutomationML (AML) tool and consequently explains on how easy is to integrate seamlessly that model during the design phase of engineering process.

Keywords: OT security, AutomationML, ISA/IEC 62443, NIST, Security modelling

1 Introduction

Several trends have made cybersecurity as an essential property of IACS, along with safety, integrity, and reliability. First, over the last two decades, IACS technologies have migrated from vendor-proprietary to commercial off-the-shelf technologies. Second, the value of data residing in the IACS for the business has significantly increased the interconnectivity of IACS both internal and external to the organization. The combination of these trends has made IACS more vulnerable to cyberattack [Qu20]. To

[1] Otto von Guericke University Magdeburg, Fakultät für Informatik, Universitätsplatz 2, Magdeburg, 39106, mithil.parekh@ovgu.de, https://orcid.org/0000-0000-0000-0000

[2] Framatome GmbH, Henri-Dunant-Strasse 50, Erlangen, 91058, karl.waedt@areva.com

[3] University of Siegen, Chair of Data Communication Systems, Hoelderlinstr. 3, Siegen, 57076, asmaa.tellabi@student.uni-siegen.de

deal with it, it requires executing cybersecurity program to guide plant owner safeguarding their OT assets against cyberattacks. Finally, the means, resources and skills are required that run such security programs efficiently that results in time consuming and very expensive.

The current trend to secure manufacturing environment has gone through its early stage of evolution, reaching an initial level of maturity. Security experts are trying to characterize security in manufacturing environment is good and bring a balanced approach between tackling technical and nontechnical aspects. Technical aspects further characterize into IT and OT while nontechnical aspects characterize in to process and regulatory requirements. The most crucial part here, particularly as cultural issues and potential clashes, between OT and IT/security departments, can jeopardize efforts to tackle security problems [MG19].

However, this is a situation not comfortable especially for small and medium size companies. They should be able to provide and focus its special skills in in operational and safety related cases rather to shift their effort significantly in to OT security issues. Thus, already integrated technical capabilities are required during design phase supporting them to engineer, integrate and use security controls based on technology independent engineering support. The basic requirement is a security model for systems in all its facets, i.e. covering all fundamental security requirements from ISA/IEC 62443. Thereby, the necessary properties and conditions on all levels have to be expressible.

Different approaches are possible based on such a basic model. At first, modeling tool that can be applicable for existing OT systems. Such a tool can provide at least the device configurations and documentations for system installation and maintenance but this paper does not discuss more on this approach. Second, the design process can be supported by the provision of security model enabling security for the system from the beginning.

2 Current trends in OT security

With IT security being tasked with coordinating OT security, in most cases, OT is typically involved in the reviewing of the security processes and the controls to be deployed. This is key in enabling organizations to take into consideration safety and reliability concerns, which remain paramount [MG19].

Several products and services are emerging targeting security in the field of operational environment that can be divided into the general categories along with the core functions. Some of these category and functions may be delivered on-site as appliances (real and virtual), cloud services, or hybrids of on-site and the cloud [MG19]. Here, few categories are explained.

Continuous network monitoring requires gaining the visibility of assets and the means to profile, tracking and managing OT assets. Other than security, this capability also helps

engineering team have in-depth insight and properties of OT assets e.g. continuous tracking of configuration of OT assets helps engineering team in the change control management for their Good Manufacturing Practices (GMP) environment. Further, this category includes any capability that detects anomalies, threats and/or incidents, and provides functions to respond to them.

Network segmentation includes any capability that manages data flow between IT networks and OT environments or OT network segmentation. Unidirectional gateways (data diodes) technology used to compel traffic to travel only in one direction, thereby protecting highly critical environments. Related functionality keeps the data flow secure, particularly for smaller companies that use unified threat management (UTM) solutions. This may also include intrusion prevention system (IPS) functionality [MG19].

Remote access includes specialized solutions that allow for secure, third-party partners and employees' remote access.

Endpoint security for OT assets could be as anti-malware, personal firewall, port and device control, encryption, memory protection, configuration and security-related patch management, continuous assessment, portable media management, application control and allow-listing, integration with other security management systems, and forensic investigation of OT security compromises and impacts [MG19].

Other professional services represent capabilities to deliver risk assessments, strategic planning, policy development, architecture and design skills, as well as software and system integration across multiple technologies and processes. It also represents those managed or functional services that can be delivered via platform, infrastructure and/or software as a service (SaaS) from the cloud [MG19].

All described categories comparatively cover technical capabilities required for ISA/IEC 63443 and NIST Cybersecurity Framework (CSF). Several vendors provides their services in the different categories of OT security and they claim to be the best in the market. However, general implementation guidance and example proof-of-concept solutions is available that demonstrates how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) [CF19].

3 Modelling of system

In order to reduce the complexity of highly sophisticated security requirement and modern production systems, the architecture of OT systems and its process is broken down into various phases. This leads to different and specialized engineering tools for each phase. Naturally, a broad list of heterogeneous tools is witnessed with varied data formats and lack of support for data exchange among them [DR08]. Hence, AML was

developed as a vendor-independent, neutral data format based on XML to support such an lossless exchange of engineering information [PA17]. This paper does not include introduction of the basic architecture of AML as it is already explained in IEC 62714-1[EN14]. Further, AML objects (the core elements of AML) represent instances and can further consist of administration items, attributes, interfaces, relations and references [WH16].

3.1 Modelling of IACS system

To provide a better understandability of the approach, a simple example is used from [AU14]. This modeling methodology will be extended to model security relevant modelling in the next section. In this example, system consists of three logically connected control devices hosting the control application, a switch and three Ethernet wires establishing the physical network. The physical and logical topologies of the network example are depicted in Fig. 1 and its relevant modelling in AML is depicted in Fig. 2.

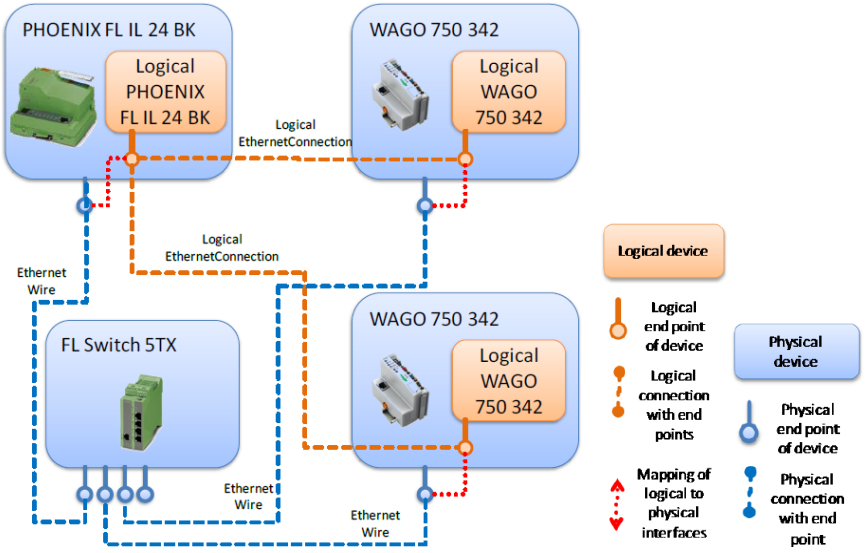

Fig. 1: Physical and logical topology of network example [AU14]

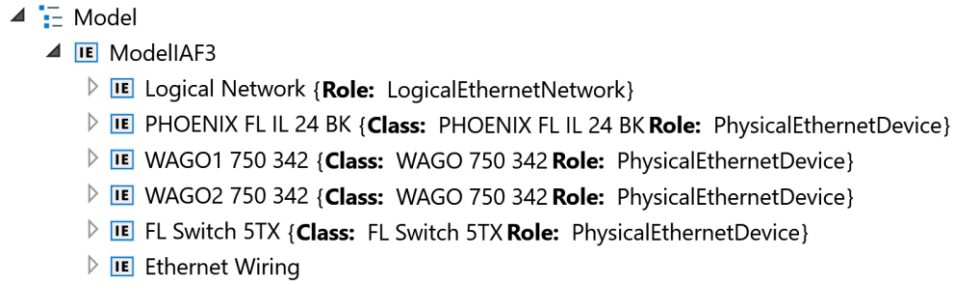

Fig. 2: Instance hierarchy of exemplary IACS

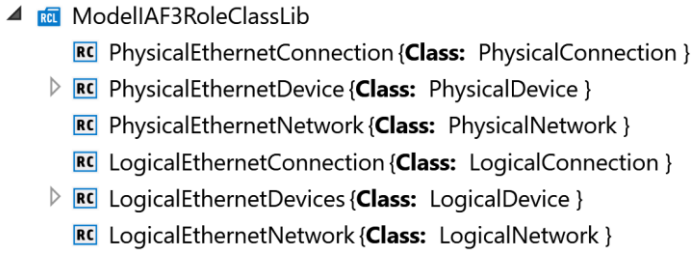

Fig. 3: RoleClass Library of exemplary IACS

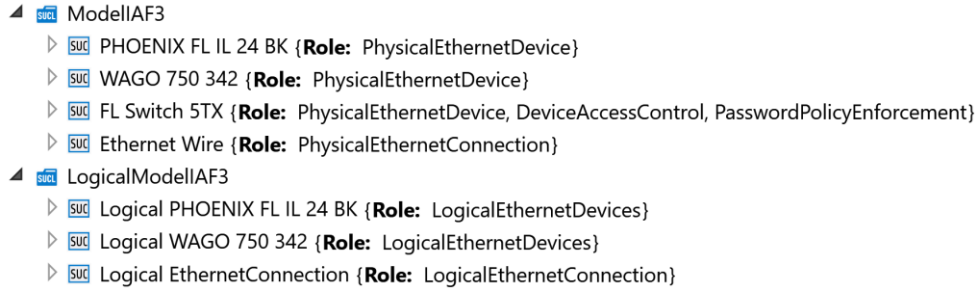

Fig. 4: SystemUnitClass Library of exemplary IACS

The above described modelling can be extended to any existing industrial plant to differentiate its logical and physical part as well as to describe requirements of relevant automation engineering. Already proposed automation model in [MP20] will be extended here for modelling its security relevant property in the following sections (see Fig. 6).

3.2 Modelling of high level security requirements

Before starting security relevant modelling, it is better to focus such a capabilities that comply with security requirements form standards. For an example, Foundational Requirements (FRs) form the basis for the technical requirements throughout the ISA/IEC 62443 series. All aspects associated with meeting a desired IACS security level (people, processes, and technology) are derived through meeting the requirements associated with the seven following Foundational Requirements:

- FR 1 – Identification and Authentication Control (IAC)
- FR 2 – Use Control (UC)
- FR 3 – System Integrity (SI)
- FR 4 – Data Confidentiality (DC)
- FR 5 – Restricted Data Flow (RDF)
- FR 6 – Timely Response to Events (TRE)
- FR 7 – Resource Availability (RA)

FRs include a series of Security Requirements (SRs) describing a number of layered security mechanisms as a baseline. To achieve a maturity for specific security control, a system may be required to demonstrate expected outcomes for specific SRs in their respective FRs. To narrow it down further, the following section targets mainly technical capabilities to fit in to the example, e.g. access control (The combination of FR 1 and FR 2 is sometimes called Access Control). Of course, proposed approach can also model non-technical capabilities but it is out of the scope of this paper.

Access control is the most commonly seen security requirement in any environment and is explained its applicability in manufacturing environment in the next section. Asset owners must develop and maintain a list of all users (humans, software processes and devices) and determine for each control system's component the required level of access control protection. The goal of access control is to protect the control system by verifying the identity of any user requesting access to the control system before activating the communication.

Mutual dependency of access control with other FRs (e.g. System Integrity and Data Confidentiality) are not specifically discussed here. Subsequently, this paper target explicitly security requirements from ISA/IEC 63443 and proposes relevant security modelling with most common SRs.

3.3 Access Control for IACS

To restrict physical and logical access to IACS systems and networks, users must be uniquely identified, authenticated, and authorized before gaining access. User authorization should follow the principle of least privilege that grants users with sufficient privileges to enable them to fulfil defined roles.

Authorization is the initial step in protecting an IACS system and its critical assets from unwanted breaches. It is the process of determining who and what should be allowed into or out of a system. Once this information is determined, defence-in-depth access control measures can be implemented to verify that only authorized people and devices can actually access an IACS system. The first measure is usually authentication of the person or device that is attempting access to an IACS system [IC13].

Authentication describes the process of positively identifying potential network users, hosts, applications, services and resources using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions. Based on the response received, the system may or may not allow the potential user access to its resources [IC13].

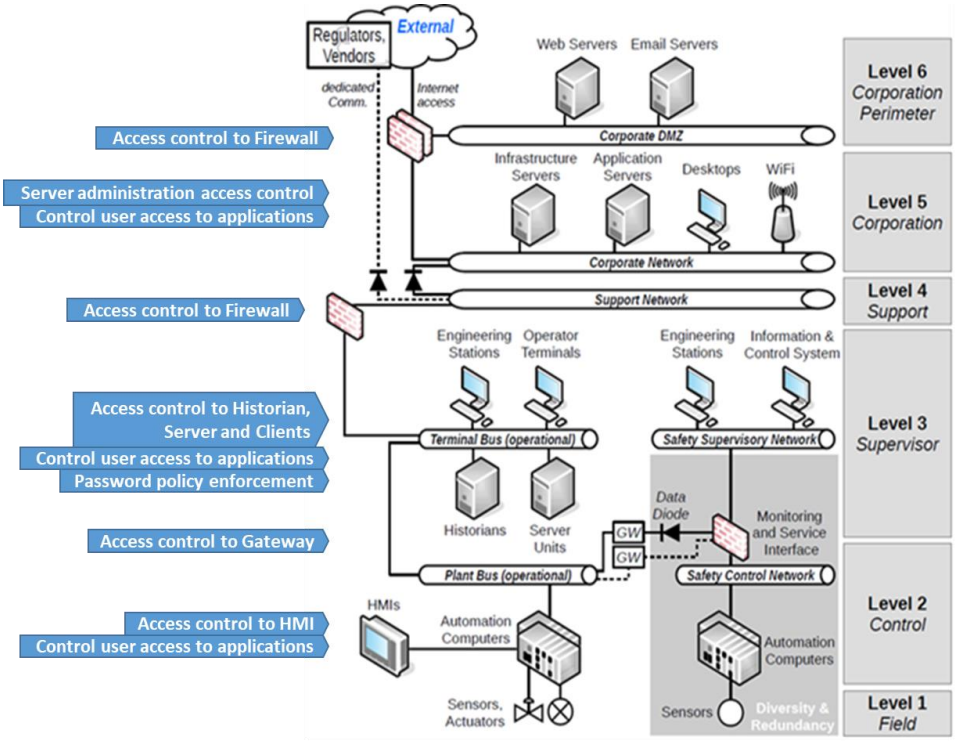

Fig. 5: Access Control for IACS

Fig. 5 illustrates the security patterns for the access control information security domain. The tags on the left side represent the access control security patterns that can be

consistently applied across the IACS network [OL15].

Using existing automation system communication model from AutomationML whitepaper [AU14], we can further extend that modelling to include access control requirements form ISA/IEC 62443 standard as per Fig.6.

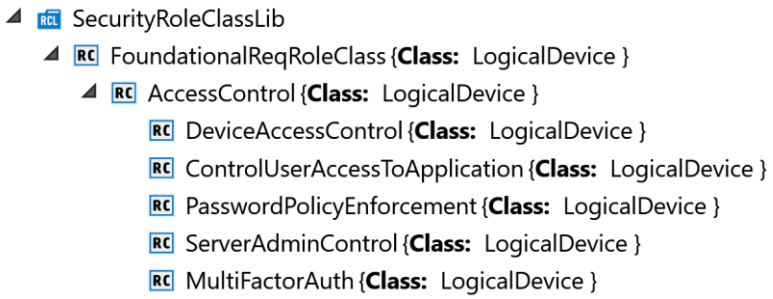

Fig. 6: SecurityRoleClass library (with AccessControl RoleClass) for IACS

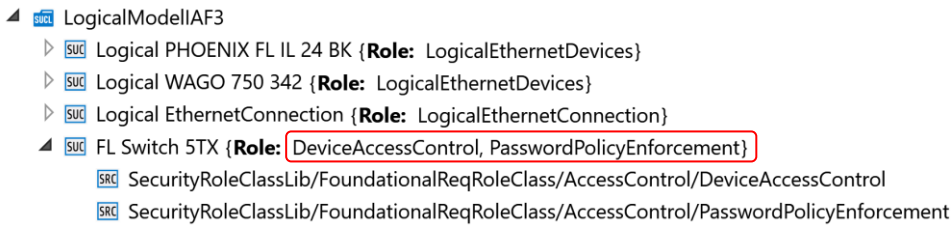

Fig. 7: SystemUnitClass library with assigned security RoleClass for the switch

The resulting AutomationML file is a condensed version, also covering data of interest. A receiving target tool can automatically import those AutomationML files and can import the modification immediately.

4 Conclusion

This paper explains the need of security modelling and on how it can help in the earlier phase of engineering lifecycle with the example of modelling access control. Such a model can avoid later all the possible effort that requires skills and resources to secure the existing IACS. The process of security abstraction and its modelling is based on ISA/IEC 62443 standard series that can be applied on real IACS and production lines,

and closely linked to existing issues and problems. Further, it can also help engineers to comply with regulatory requirements and to educate on security issues in their daily operations. The main element of this solution is a continuous, heterogeneous integration of IACS components, process engineering and the relevant stakeholders by considering all aspects of an OT security requirement. This enables suppliers, asset owner and integrators of such automation components to receive support from this model e.g. when creating a new system, selecting appropriate security controls, defining incident response plan and for troubleshooting. Modelling based on AML is an acceptable data format among automation vendors and is currently used for the seamlessly data exchange during design process. Therefore, its main advantage can also be leveraged as justification during further development of OT security standards and to increase its effectiveness.

Bibliography

[PA17] F. Patzer, A. Sarkar, P. Birnstill, M. Schleipen and J. Beyerer, "Towards the modelling of complex communication networks in AutomationML," 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, 2017, pp. 1-8, doi: 10.1109/ETFA.2017.8247571.

[Qu20] Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems 2020.

[IC13] IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

[MG19] Gartner: Market Guide for Operational Technology Security. Published 5 November 2019 - ID G00370177

[CF19] NISTIR 8183A Vol. 1: Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance 2019.

[DR08] R. Drath, A. L¨uder, J. Peschke, and L. Hundt, “Automationml-the glue for seamless automation engineering,” in Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on. IEEE, 2008.

[EN14] IEC 62714-1:2014 Engineering data exchange format for use in industrial automation systems engineering - Automation markup language - Part 1: Architecture and general requirements.

[WH16] AutomationML Consortium, “Whitepaper AutomationML Part 1 – Architecture and general requirements,” AutomationML - The Glue for Seamless Automation Engineering, 2016.

[AU14] AutomationML Consortium, “AutomationML Whitepaper Communication,” AutomationML - The Glue for Seamless Automation Engineering, 2014.

[MP20] Parekh, M., Gao, Y., Jockenhoevel-Barttfeld, M., and Waedt, K., "Confluent Modeling of Heterogeneous Safety and Operational Instrumentation and Control Systems."

ASME. ASME J of Nuclear Rad Sci. July 2020; 6(3): 031802. https://doi.org/10.1115/1.4046262

[OL15] Obregon. L, “Secure Architecture for Industrial Control Systems”, SANS.edu Graduate Student Research, 2015. https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327