Supporting Security in Industrial Automation and Control Systems using Domain-Specific Modelling

Robert Altschaffel[1], Ivo Hempel[1], Oliver Keil[1], Josef Schindler[2], Martin Szemkus[3], Jana Dittmann[1], Matthias Lange[3], Karl Waedt[2] and Yongjian Ding[3]

Abstract: This paper explores how domain specific modelling can be used to support the identification of potential vulnerabilities and risks in Industrial Automation and Control Systems (IACS) to enhance security by enabling a mitigation of these vulnerabilities. This approach can be used to support already deployed IACS or to include Security-by-Design and Security Defence-in-Depth principles in the planning of future facilities. This paper explores the requirements for such a modelling approach including domain and security specific aspects. Three interlinked aspects of IACS which require different modelling approaches are identified leading to three distinct types of models: Infrastructure, cyber-process, and physical process. These three types are relevant for different attack vectors and to judge the potential impact of any attack. This paper shows examples for these three models and how these models can be used to identify vulnerabilities with the aim to close them.

Keywords: Industrial Automation and Control Systems, Security, Modelling, Standards

1 Introduction

Security is of increasing importance in the domain of Industrial Automation and Control Systems (IACS) as shown by the increasing number of recent attacks [Al20, AS19]. IACS are cyber-physical systems - computer systems which can directly affect the physical world by attached actuators. Hence, a threat to the security of an IACS often carries negative implications for the safety of the physical process or environments associated with the IACS. Hence, an increase of security in IACS is needed.

This paper aims to improve the security of already deployed or currently planned IACS by using domain specific modelling. This domain specific modelling allows to describe the IACS in question in a way that supports the identification of potential vulnerabilities

[1] Otto-von-Guericke-University, Department of Computer Science, Universitätsplatz 2, Magdeburg, 39106, robert.altschaffel@iti.cs.uni-magdeburg.de, ivo.hempel@ovgu.de, oliver.keil@ovgu.de, jana.dittmann@iti.cs.uni-magdeburg.de

[2] Framatome GmbH, ICETA-G Department, Paul-Gossen-Straße 100, 91052, Erlangen, Germany, josef.schindler@covalion.net, karl.waedt@framatome.de

[3] Hochschule Magdeburg-Stendal, Magdeburg, 39114, martin.szemkus@h2.de, mathias.lange@h2.de, yongjian.ding@h2.de

and risks.

To achieve this, the domain specific modelling must consider all the factors which might affect the overall security of the IACS in question. Section 2 provides necessary background information as well as the requirement definition in Section 2.3. Based on these requirements, an approach for security-aware domain specific modelling is presented in Section 3. Section 4 closes with an outlook on further research.

2 Requirement Definition and Related Background

This chapter describes relevant terms and technologies in the scope of modelling IACS. Based on this knowledge, we define requirements that must be met by our modelling approaches proposed later in this paper.

2.1 Components of IACS

According to [Al20] an IACS is defined as "A communication network of Actors, Sensors and Processing units geared towards controlling a physical process". Therefore, these components are essential for IACS and relevant for modelling in this scope:

- **Sensor**: “Collects information about the environment [...]” [Al20]
- **Actuator**: “Manipulates the environment […]” [Al20]
- **Processing Unit** (short **PU**; here **Programmable Logic Controller**): “Evaluates the data gathered by sensors and/or gives control signals to actors.“ [Al20]
- **Communication Wiring**: “The physical and logical carrier that facilitates communication between sensors, actors, and processing units.” [Al20]

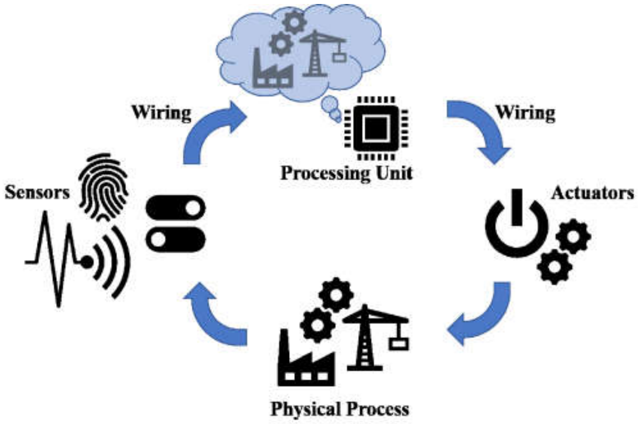

Fig. 1: Control loop with sensors, processing units and actuators in a physical process

Sensors measure a physical process while processing units compute how the physical process should be affected by the actuator implementing a control loop (see Fig. 1). This necessitates communication between sensors, processing units and actuators. This communication is handled by direct cable connections or more complex digital communication buses. Multiple control loops may be used to control complex physical processes. In addition to these control loops, other systems are usually included to provide an overview on the state of the entire physical process to an operator. Such a system is referred to as Supervisory Control And Data Acquisition (SCADA).

According to [Al20], the structure of these components follows a control hierarchy dictating the flow of communication within the network. A common and generalized way to describe such a control hierarchy is the Purdue Enterprise Reference Architecture (PERA; see [Wil92]). PERA consists of multiple levels of hierarchy. A brief overview on these levels can be found in [Ro11]:

- **Level 0**: Process sensors and actuators involved in the basic manufacturing process
- **Level 1**: Basic controllers (typically a PU) that direct and manipulate the manufacturing process
- **Level 2**: Area supervisory control applications and functions associated with the cell/area zone runtime supervision and operation
- **Level 3**: Site level plant-wide ICS functions

The higher levels provide business functions performed in an attached IT system. Although this summary references a manufacturing process, it is applicable to any other physical process as well. Within this structure, Level 0 components communicate with Level 1 components which in turn communicate with Level 2 components and so on. Hence, they form a control hierarchy which also acts as a communication hierarchy since it dictates the flow of communication.

The hierarchy (and therefore the communication) might also be specified by further domain-specific restrictions. In this paper, IACS in the domain of Nuclear Power Plants (NPP) are taken as an example having high complexity and requirements for security. The IAEA provides an exemplary implementation for a Defence-in-Depth-Architecture (also Graded Approach, see [IA11]) based on different Security Levels (SL) and Security Zones which restrict the communication flow. The SLs are based on the impact a potential failure or compromise could have on the physical process. A summary of these SLs is provided in [Hi20]:

- **SL1**: systems vital to the facility (e.g. physical emergency protection)
- **SL2**: operational control systems which require high security
- **SL3**: supervision systems not required for operations
- **SL4**: technical data management systems (e.g. used for maintenance)
- **SL5**: business systems

While lower security levels should be able to send information to higher security levels, the information flow in the other direction should be highly restricted. Therefore, the levels are connected via access systems like firewalls or data diodes (see [Hi20]).

2.2 Attacks on IACS

Three different principal targets of typical attacks on IACS were identified in [St14]:

- communication stack of the deployed devices
- lack of authentication requirements within the hardware
- security problems in the respective software implementations

Various attacks on IACS were reviewed in [Al20] to identify forensic traces caused by these attacks. These traces can be present in Non-Volatile Memory (Mass storage), Volatile Memory (Main memory) or Communication (Network communication). All reviewed attacks identified potential traces in the communication. This is because communication between various devices is a necessary component of all remotely executed attacks on IACS. Potential exceptions are supply chain attacks in which case a component is manipulated by an attacker before it is installed within an IACS. If the component in question can directly affect the physical process, communication with different Security Levels or Zones is not necessary.

2.3 Requirement Definition

This section discusses how the components and their communication within an IACS translate to the requirements for a modelling approach in order to increase security.

The general aim of the modelling is to describe both the current and the target state of the system. This enables system planning to be carried out more efficiently. It facilitates the creation of test cases and discovery of potential attack vectors. Also, it simplifies the risk assessment of changes and weak spots of the system.

Based on the previous considerations, we define the following requirements for modelling:

- **Technical requirements** (general modelling techniques and tools):
  - Any present physical components, logical entities and possible communication channels must be depicted.
  - The visualization must enable fast and easy comprehension of the infrastructure with its static components and dynamic behaviour.
  - Model elements must be both standardizable and customizable.
  - The resulting model files must be of reasonable size in data.
- **Subject-specific requirements** (dependent on the domain and system):
  - The PERA [Wil92] levels must be depicted.
  - The security zones and levels from the "Graded Approach" [IA11] must be depicted.

3 Modelling Aspects and Approaches

Covering security and its implications in an industrial facility requires various aspects to be explored and modelled. This chapter discusses these aspects and explores means to model them.

3.1 Modelling Aspects

To provide a complete view of the industrial facility, we define the following three aspects which must be covered by the models:

- **Static infrastructure**: These models visualize the physical components contained in the infrastructure together with their connections between each other. They include the control technology for the physical process (sensors, actuators and control devices) and network devices (e.g. switches and firewalls).

- **Physical process**: These models visualize the sequence of the physical process implemented by the control technology. They show the individual steps that happen within the process which also includes switching between physical states. This modelling aspect describes the dynamic behaviour of the system.
- **Control loop and its technology**: These models visualize the components which supervise and control the physical process. This includes sensors, actuators and their controllers as well as the communication between these devices. Hence, these models describe the IACS. This modelling aspect emphasizes the signals and information that is being exchanged between the devices as well as their consequences. It enables a more detailed reflection of attack vectors for the industrial facility. Thus, it also describes the dynamic behaviour.

Together, these three aspects allow modelling of the infrastructure and behaviour for the entire industrial facility. The distinction between physical process and control circuit is made due to the following reasons:

The physical process focuses on the sequences of physical states that are based on logical conditions and resulting actions.

The modelling of control circuits and technology then describes the implementation of these logical conditions and resulting actions with actual devices and their actual communication between each other.

This distinction allows a more fine-granular view on the infrastructure with its components and processes depending on the needs of the administrator or researcher.

However, all these models are closely interlinked with each other. The model of the control circuit includes communication with other systems. Hence, remote attacks would have to move through the modelled IACS to have an impact. In this case, the model of the physical process is necessary to understand the potential consequences of a vulnerability within the control loop. This connection allows for the identification of a safety impact due to a security problem. The modelling of the infrastructure covers supply chain attacks. Again, the connection to the control loop model is necessary to understand how such an attack could propagate within the network. The connection to the model of the physical process is again necessary to consider potential impacts on the physical process.

3.2 Modelling Approaches

This section describes two possible approaches: Manual and automated modelling.

Manual Modelling

For the process of manual modelling, we chose the tool “draw.io” (available at [Dr21]). This tool is a JavaScript based open-source software for creating diagrams. It is easy to use, the created files are usually smaller than one megabyte and the creation of custom symbols is possible. The models are highly reusable and adaptable. Also, linking multiple models is possible. This makes the tool a practical solution for the modelling process.

The exemplary models in this paper are based on the Integrated Nuclear Evaluation System 7 (INES-7) of the Research Group of Multimedia and Security at OvGU. It is a demonstrator for the physical and control processes of power plants. In this case, the reactor is represented by a radio-controlled water heater.

One aspect of modelling is the static infrastructure. The modelling of a plant takes place in separated plant areas. That means different factory buildings are depicted in different sections of the model. Actuators and sensors control the physical process. Hence, they belong to PERA level 0 in the model. All physical and logical controllers (e.g. PLCs) are denoted as entities. Each entity gets assigned to a zone, a PERA level and a security level. Each entity has symbols assigned to it as well as communication channels drawn for it. Also, they are classified as bidirectional, unidirectional receiving or unidirectional sending. The modelling of the static infrastructure is separated into two zones: Water heater and phone (see Fig. 2). The heating control circuit consists of a sensor for the water temperature, a sensor for the water level and an actuator for the heating element. The sensors use an ellipse as the symbol, the actuator uses an adapted valve symbol.

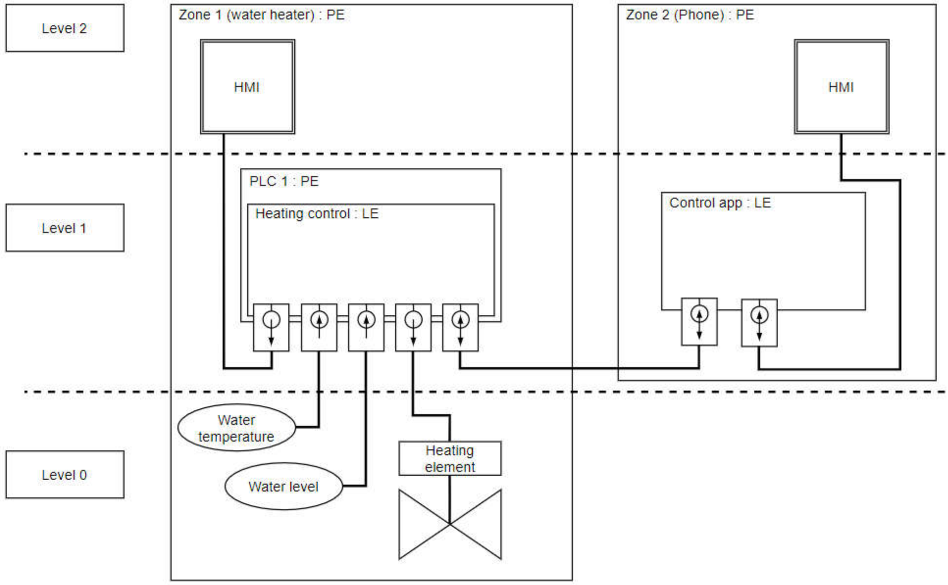

Fig. 2: Modelling of the static infrastructure of a Wi-Fi water heater

For the modelling of the physical process, a flow chart or a more complex Unified Modelling Language (UML) diagram for the process steps is sufficient. A simple flow chart (see Fig. 3) is sufficient to show the process of heating up water.

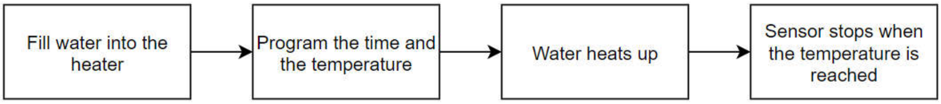
Fill water into the heater
Program the time and the temperature
Water heats up
Sensor stops when the temperature is reached

Fig. 3: Modelling of the physical process of heating water with a flow chart

In the modelling of the control loop and its technology, we differentiate between static and dynamic behaviour. In the static case, we depict each PLC individually. The model includes these elements:

- **Sensors**: Gathers information about the environment.
- **Calculation**: Transforms the sensor input into usable data representation.
- **Distribution**: The result of the calculation is distributed on the wiring.
- **Aggregation**: The data is aggregated and processed using a defined logic.
- **Logic**: Definition for the behaviour of the actuators.
- **Actuators**: Affects the environment based on the logic.

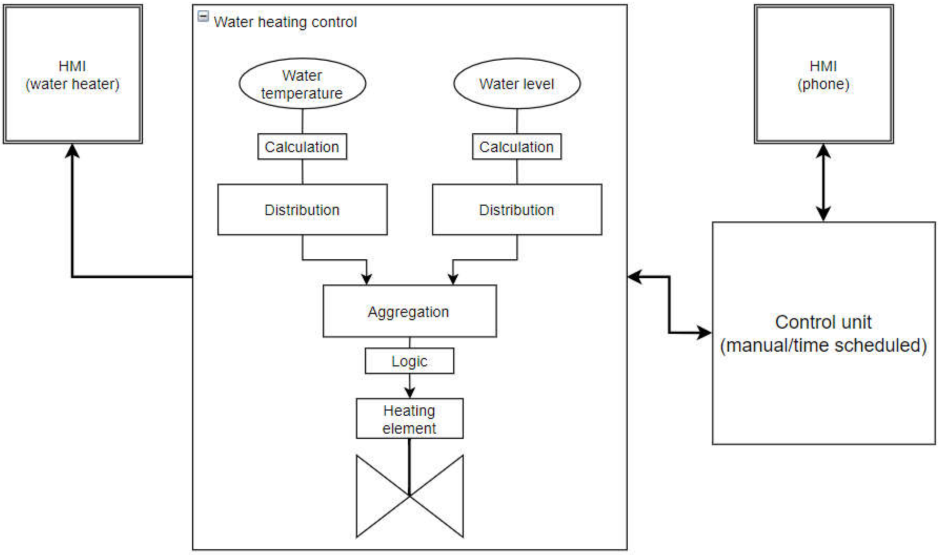

Fig. 4: Generic modelling of the control loop and its technology of a Wi-Fi water heater

The sensors and actuators are connected to the PLC with an indicator for the unidirectional communication. The physical entity of the PLC consists of the logical entity of the heating control. The PLC communicates with the second zone in a bidirectional way. A logical entity in form of an app controls the process parameters and displays sensor values. A bidirectional channel exists for the Human Machine Interface (HMI) on the phone. Each entity is aligned according to its PERA level. The security levels could be colour-coded with different background of the entities.

Fig. 4 shows the static behaviour of the control loop and its technology. Sensors and actuators are put into a control loop with these steps: Calculation, distribution, aggregation and logic. A control unit is used as the logical entity for defining the process parameters if necessary. Additionally, the HMIs are depicted. With this simple, but meaningful example the weak spots for potential threats of a system can be assessed fast and they can be easily visualized.

Automated Modelling

Besides manual modelling, we also want to point out the possible use of automation in modelling. Creating models automatically could come with several advantages over manual modelling:

- **Less time cost for human resources**: Manual modelling of infrastructures requires an employee to invest time to create the model. Automatic modelling would only require the employee to start the process. Then, the automated modelling tool creates models based on its configuration. A final manual check might be required but would consume far less time than going through the entire process of manual modelling.
- **Gather additional information**: An automated modelling process may be able to gather new information that would have been undetected when using manual modelling with reasonable time investment. For instance, an administrator knows that he uses a specific network protocol for any communication within all applications on a device. To verify that this is the only protocol on the wire to and from this device, he looks at the network traffic for a certain amount of time with analysis tools like Wireshark [Wi21]. However, the operating system may communicate with other devices via more protocols which the administrator does not yet know about. In this case, an automated modelling tool could gather more information as it is a continuous process of gathering and modelling information.
- **Overcoming human failure factors**: Modelling a communication setup could include scanning and assessing all ports in use on a specific device. When having long lists of information (here ports), manual assessment may lead to lapse (defined in [An18]) due to human error. This can result in security issues along the modelling, development & engineering pipeline. Automation provides higher reliability and overcomes these potential failures.

4 Outlook

This paper discussed how domain specific modelling can support security in IACS by enabling the identification of vulnerabilities. To achieve this, the modelling has to fulfil domain specific requirements including the ability to model domain specific security measures. Various possible attack vectors and the complexity of IACS and the physical processes they control lead to the establishment of three types of models which are interlinked. Some basic methods to conduct such a modelling are proposed - including the establishment of specific sets of modelling symbols to describe domain specific elements.

The Research Group of Multimedia and Security at the Otto-von-Guericke-University (OvGU) of Magdeburg is currently working on two publications based on this paper. First, an automated approach on modelling will be created and evaluated. In section 3.2, the Research Group Multimedia and Security at OvGU Magdeburg has already introduced the possibility for automation. Second, the Research Group of Multimedia and Security at OvGU introduced the interlinked approach with its aspects in section 3.1 in this paper and plans to create an interlinked concept for models which combines the three aspects with regards to popular forensic models like data streams, data types and incident ontologies (see [BS11]).

Acknowledgments

The work on this paper was partly funded by the German Federal Ministry for Economic Affairs and Energy within the project SMARTEST2 (Grant No.: 1501600B).

Bibliography

[AG21] AGCS: Managing the impact of increasing interconnectivity: Trends in cyber risk. Report, Allianz Global Corporate & Specialty, 03 2021.

[Al20] Altschaffel, R.: Computer forensics in cyber-physical systems: applying existing forensic knowledge and procedures from classical IT to automation and automotive, https://opendata.uni-halle.de/handle/1981185920/35574, accessed: 17/06/2021, 2020.

[An18] Anu, V.; Hu, W.; Carver, J.; Walia, G.; Bradshaw, G.: Development of a human error taxonomy for software requirements: A systematic literature review. Information and Software Technology, 103:112–124, 2018.

[AS19] A., Saravanan; S., Bama S.: A Review on Cyber Security and the Fifth Generation Cyberattacks. Oriental Journal of Computer Science and Technology, 12:50–56, 2019

[BS11] BSI: Leitfaden „IT-Forensik". Technical guideline, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn (DE), 03 2011.

[Dr21] draw.io. Online: https://github.com/jgraph/drawio (Last access: 2021/06/18)

[Hi20] Hildebrandt, M.; Altschaffel, R.; Lamshoft, K.; Lange, M.; Szemkus, M.; Neubert, T.; Vielhauer, C.; Ding, Y.; Dittmann, J.: Threat Analysis of Steganographic and Covert Communication in Nuclear I&C Systems. In: In Third International Conference on Nuclear Security: Sustaining and Strengthening Efforts (ICONS 2020). 2020.

[IA11] IAEA: Computer Security at Nuclear Facilities. Technical guidance: Reference manual, International Atomic Energy Agency (IAEA), Vienna (AT), 12 2011

[Ro11] Rockwell Automation: Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. Design and implementation guide, Rockwell Automation, 09 2011.

[St14] Stirland, J.; Jones, K.; Janicke, H.; Wu, T.: Developing Cyber Forensics for SCADA Industrial Control Systems. In: The International Conference on Information Security and Cyber Forensics (InfoSec). pp. 98–111, 2014.

[Wi21] Wireshark. https://www.wireshark.org/about.html, Online; Accessed: 2021-06-18.

[Wi92] Williams, T. J.: The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. 1992