Onni Eho

EVALUATION TOOL FOR ASSESSING AN ORGANIZATION'S OT SECURITY POLICY

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2024

ABSTRACT

Eho, Onni
Evaluation Tool for Assessing an Organization's OT Security Policy
Jyväskylä: University of Jyväskylä, 2024, 84 pp.
Cyber Security, Master's Thesis
Supervisor(s): Frantti, Tapio

This research focuses on the cybersecurity of Operational Technology (OT). OT encompasses various programmable systems that operate in the intersection of the physical and virtual world. Consequences of cyberattacks on systems controlling physical processes can be severe. The evolution of OT systems has made them more vulnerable against cyberthreats. Simultaneously, the rising concern over the security of OT has increased the research on the domain.

The research methodology of this thesis is design science research. The outcome of the iterative process is an artifact that can be used for assessing an organization's OT security policy. In the context of this thesis, OT security policy is understood as a collection of countermeasures an organization has implemented or plans to implement for safeguarding its OT environment.

The Evaluation Tool is based on the information included in MITRE ATT&CK for ICS® framework. It aids organizations in assessing their current approach to OT security against the mitigations included in the framework. Based on the results of the assessment, organizations can seek to improve their defensive capabilities against cyberattacks targeted at OT environments.

The novelty of the artifact is supported by the literature review. It is successfully applied for assessing an OT security policy of a case-company to demonstrate its applicability. The proposed artifact is concluded to meet its design criteria for the most part. However, the research presents multiple areas where further effort could be directed to make the artifact more mature.

Keywords: Operational Technology, OT Security, MITRE ATT&CK for ICS, Evaluation Tool, Design Science Research

TIIVISTELMÄ

Eho, Onni
Arviointityökalu organisaation OT-tietoturvapolitiikan arvioimiseen
Jyväskylä: Jyväskylän yliopisto, 2024, 84 s.
Kyberturvallisuus, pro gradu-tutkielma
Ohjaaja(t): Frantti, Tapio

Tämä tutkimus keskittyy tuotantoteknologian (OT) kyberturvallisuuteen. Tuotantoteknologia koostuu moninaisista ohjelmoitavista järjestelmistä ja laitteista, jotka toimivat fyysisen ja virtuaalisen maailman rajapinnassa. Fyysisiä prosesseja ohjaaviin järjestelmiin kohdistuvan kyberhyökkäyksen seuraukset voivat olla vakavia. OT-järjestelmien kehitys on tehnyt niistä haavoittuvampia kyberuhkia vastaan. Kasvava huoli OT-turvallisuudesta on lisännyt alan tutkimusta.

Tässä tutkimuksessa käytetty tutkimusmetodologia on suunnittelutiede. Sen mukaisen iteratiivisen prosessin lopputulos on artefakti, jonka avulla organisaatiot voivat arvioida OT-turvallisuuspolitiikkaansa. Tämän tutkielman kontekstissa OT-turvallisuuspolitiikka ymmärretään kokoelmana niistä hallintakeinoista, jotka organisaatio on ottanut tai suunnittelee ottavansa käyttöön OT-ympäristöidensä suojaamiseksi.

Arviointityökalu perustuu MITRE ATT&CK for ICS®-viitekehykseen sisältyvään tietoon. Se auttaa organisaatioita arvioimaan nykyistä lähestymistapaansa OT-turvallisuuteen viitekehykseen kuuluvia hallintakeinoja vasten. Arvioinnin tulosten perusteella organisaatiot voivat pyrkiä parantamaan suojautumiskykyään OT-ympäristöihin kohdistuvien kyberhyökkäysten varalta.

Työn kirjallisuuskatsaus tukee artefaktin uutuusarvoa. Sen soveltuvuutta demonstroidaan käytännössä tutkimukseen osallistuneen yhteistyöyrityksen OT-tietoturvapolitiikan arviointiin. Esitellyn artefaktin katsotaan täyttävän sen suunnittelukriteerit suurimmalta osin. Tutkimus kuitenkin esittelee useita alueita, joilla tapahtuva jatkokehitys tekisi ratkaisusta kypsemmän.

Asiasanat: Tuotantoteknologia, OT-turvallisuus, MITRE ATT&CK for ICS, Arviointityökalu, Suunnittelutiede

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Operational Technology (OT) encompasses a broad range programmable systems that operate in the intersection of the physical and virtual world (Toker, Ovaz Akpinar & Özçelik, 2021, p. 1; Stouffer et al., 2023, p. 8). OT systems comprise a unique set of software and hardware used to monitor, control, and regulate industrial processes (Miller et al., 2021, p. 1; Koay et al., 2023, pp. 4 -5; Hollerer, Kastner & Sauter, 2021, p. 1) and have been described as the backbone of our society (Rencelj Ling & Ekstedt, 2023a, p. 1). Such systems control various parts of critical infrastructure, including, but not limited to, energy, water, maritime, manufacturing, healthcare, food and agriculture, and transportation (Rencelj Ling & Ekstedt, 2023a, p. 1; Kapalidis et al., 2022, p. 13; Conklin, 2016, p. 1; Flaus, 2019, p. 6; Stouffer et al., 2023, p. 9).

The topic of this thesis relates to cybersecurity of Operational Technology. The cyber risks related to OT have increased substantially in recent years (Toker et al., 2021, p. 1). The often-provided reasoning for the development is the evolution of OT environments, the so-called IT/OT convergence (Toker et al., 2021, p. 1; Jadidi & Lu, 2021, p. 1 & 2; Rencelj Ling & Ekstedt, 2023a, p. 1; Koay et al., 2023, p. 8; Wagner et al., 2020, p. 1; Conklin, 2016, p. 1; Zanasi et al., 2022, p. 1; Padée et al., 2019, p. 1). In the past, OT systems have been specialized systems operated in isolation and have had little resemblance to IT. The convergence of the two has introduced various business benefits. Simultaneously the cybersecurity related risks have grown through expansion of systems attack surface and introduction of new attack vectors (Stouffer et al., 2023, p. 1).

Cybersecurity risks exist through ever-present vulnerabilities in systems and architectural components. These risks can be described as threats against the confidentiality, integrity, and availability of systems and data. Such risks may adversely affect an organization's operations in various ways, for example through unauthorized access, disclosure, modification of information, denial-of-service or even destruction. Attempts to exploit such vulnerabilities can be targeted or non-direct with both direct and indirect effects. (Progoulakis, Rohmeyer & Nikitakos, 2021, p. 4; Malik et al., 2023, p. 1.)

Organizations OT infrastructures are threatened by a large variety of cyberattacks with a plethora of motivations and means. The complexity of the attacks, as well as the targeted systems, challenge organizations defending their infrastructure. In cybersecurity, controls can be described as technical or organizational measures and techniques to mitigate or delay attacks (Luh et al., 2022, pp. 1 - 3). Such countermeasures greatly affect the possibility of an adversary reaching its goal against the organization's network (Georgiadou, Mouzakitis & Askounis, 2021, p. 4).

Understanding the underlying cybersecurity concepts is key for implementing effective defensive measures. However, gaining this fundamental understanding and associating specific attacks with effective controls is challenging (Luh et al., 2022, p. 1). There are various well-developed frameworks and references to support designing relevant controls and effective cybersecurity risk treatment. While design of the control architecture should address individual needs of an organization, existing approaches can be of great value (Progoulakis et al., 2021, p. 16).

An example of the above-mentioned well-developed frameworks is MITRE ATT&CK® which consists of three matrices – Enterprise, Mobile and ICS (MITRE 2023a; MITRE 2023b; MITRE 2023c). It is a curated and publicly available knowledge base of external adversary tactics and techniques that describes how an adversary behaves in a network during various phases of an attack lifecycle (Strom et al., 2020, p. 1). Out of the three matrices, MITRE ATT&CK for ICS focuses on OT (MITRE 2023c).

This thesis was put in motion by the author's interest to explore how MITRE ATT&CK for ICS can be used to assess the coverage of an organization's OT security policy. Security policies can be created on multiple levels to define objectives and constraints of a security program. The levels vary from a corporate policy to specific operational controls (Stouffer et al. 2023, p. 167). In the context of this thesis, OT security policy is understood as a collection of the policies defining the countermeasures an organization has implemented or plans to implement for safeguarding its OT environment.

As further elaborated in section 3.3, MITRE ATT&CK for ICS is widely applied by business and scientific community and was therefore considered suitable in principle. What the author believed made the matrix potentially suitable in practice are the mitigations included in the framework. MITRE ATT&CK for ICS is a collection of tactics describing adversary's goal, and techniques explaining how this could be achieved. For each technique there are one or more mitigations which are concepts that can be used to prevent the technique (MITRE 2023c). Therefore, the association of the mitigations and the potential activities of an adversary are embedded in the framework.

The purpose of this thesis is twofold. With the above-mentioned interest in mind, the author approached a case-company to propose a collaboration. Upon presenting the initial idea, the case-company agreed that the topic is of relevance and addresses an identified need.

The case-company has wished to stay anonymous due to the sensitive nature of the topic and the need to safeguard its operations and protect its intellectual property. Therefore, the case-company is only briefly described in this chapter. Furthermore, all case-company related material and results were left out of this thesis.

The case-company is a large undertaking according to the Finnish Accounting Act (Accounting Act 1336/1997). The organization's operations are dependent on its OT systems. The case-company has created an OT security policy to encompass the protection of its OT environment including various technical and organizational controls. Whereas the current policy was considered comprehensive, the case-company was interested in assessing its coverage to enable continuous improvement.

To evaluate the applicability of MITRE ATT&CK for ICS and to respond to the need of the case-company, the author proposed creating an evaluation tool based on the knowledge derived from the matrix. Through creating the tool and demonstrating it in practice, the aim of this thesis is to provide suggestions on how the current state of the case-company's OT security policy could be improved. Furthermore, the thesis seeks answers for the following research questions:

(1) How can MITRE ATT&CK for ICS be employed for assessing an organization's OT security policy?
(2) What are the benefits of such a solution?
(3) What are its limitations?

This thesis presents an evaluation tool based on MITRE ATT&CK for ICS. The tool was created and applied in practice to assess the OT security policy of the case-company to find practical answers to the research questions. To support the artifact-centric approach, the research was conducted as Design Science Research and followed Design Science Research Methodology introduced by Peffers et al (2007).

The content of this thesis is as follows. The next chapter introduces the research methodology. The third chapter provides a more comprehensive introduction to the OT, OT security, MITRE ATT&CK and relevant prior research. The artifact and its design process are introduced in the fourth chapter followed by chapters describing the demonstration and evaluation of the artifact. The seventh chapter summarizes the answers to the above-proposed research questions in the form of discussion before the eighth chapter concludes this thesis.

2 RESEARCH METHODOLOGY

Research is commonly understood as the creation of new knowledge. Research methods are the set of appropriate activities that the research community has accepted for producing knowledge (Vaishnavi & Kuechler, 2021, p. 2). The research methodology followed in this thesis is Design Science Research (DSR). The next section provides an introduction on DSR in general. Section 2.2 focuses on how the chosen methodology was applied in this thesis.

2.1 Design Science Research

Design science research is a method for creating Design Science (DS). Design science is a specific type of knowledge. According to Vaishnavi & Kuechler (2021) it is described "knowledge in the form of constructs, techniques and methods, models, and/or well-developed theory for performing this mapping—the know-how for creating artifacts that satisfy given sets of functional requirements". (Vaishnavi & Kuechler, 2021, p. 4.)

Design science research is a relatively new and still growing research paradigm although it has been practiced under various labels for some time (Baskerville et al., 2018, p. 363; Gregor & Hevner, 2013, p. 337). It is applied in disciplines and fields highly interconnected with the topic of this thesis such as engineering and computer sciences (Vaishnavi & Kuechler, 2021, p. 1). Furthermore, design science research is a widely adopted paradigm in Information Systems (IS) research (Gregor & Hevner 2013 p. 337; Peffers et al 2007, p. 2).

March & Smith (1995) describe the aim of design science as an attempt to create things serving human purposes whereas natural science tries to understand reality. The value or utility of DS is based on whether the product works or is an improvement. Instead of providing general theoretical knowledge, design science aims at applying knowledge to create artifacts. (March & Smith, 1995, p. 253.)

The basic activities associated with design science are building and evaluating. Building refers to creating an artifact and thus demonstrating it can be built. Evaluation aims at answering how well the artifact works and why it did or did not. (March & Smith, 1995, pp. 253 - 254 & 258.)

The artifacts created through design science research process can be for example algorithms, system design methodologies or languages (Vaishnavi & Kuechler, 2021, p. 1). In information systems design science research, the constructions include a wide range of socio-technical artifacts. These include, but are not limited to, decision support systems, modeling tools, governance strategies and methods for information system evaluation (Gregor & Hevner, 2013, p. 337).

In addition to creating an artifact, design theorizing, with the emphasis on design, is an expected norm in design science research (Baskerville et al., 2018, p. 363). Design theory is the theory formalizing knowledge in design science research which aims at explaining "how to do something" (Gregor & Hevner, 2013, p. 339). Both Baskerville et al. (2018) and Gregor & Hevner (2013) argue that there are two schools of design science research – one highlighting artifacts as the essential element of DSR output and the other emphasizing design theory as the key contribution (Baskerville et al., 2018, p. 359; Gregor & Hevner, 2013, p. 338). While the so-to-say schools might weigh the outputs differently, Baskerville et al. (2018) believe that the purpose is likely not to argue over the superiority of one or the other, but to demonstrate the nuances of the perspective of each paper (Baskerville et al., 2018, p. 359).

Baskerville et al (2018) continue the discussion about the topic later in their article, noting that "Gregor and Hevner (2013) attempt to dispel the perception that there are two "camps" in DSR—a design theory camp and an artifact camp (Baskerville et al., 2018, p. 363). In the corresponding article, Gregor & Hevner (2013) argue that design science research may provide various contributions. In their view, contribution to knowledge may be in the form of partial theory, incomplete theory or a new design artifact given that the artifact is "particularly interesting and perhaps surprising empirical generalization" (Gregor & Hevner, 2013, p. 339). While fully developed theory is not an expected outcome of a single DSR effort, some advance in design knowledge is expected (Baskerville et al., 2018, p. 363).

The "DSR Knowledge Contribution Framework" presented by Gregor & Hevner (2013) aims at explaining the types of knowledge contribution a design science research effort may have. The below figure illustrates the adaptation of Vaishnavi & Kuechler (2021, p. 18) of the framework (figure 1).

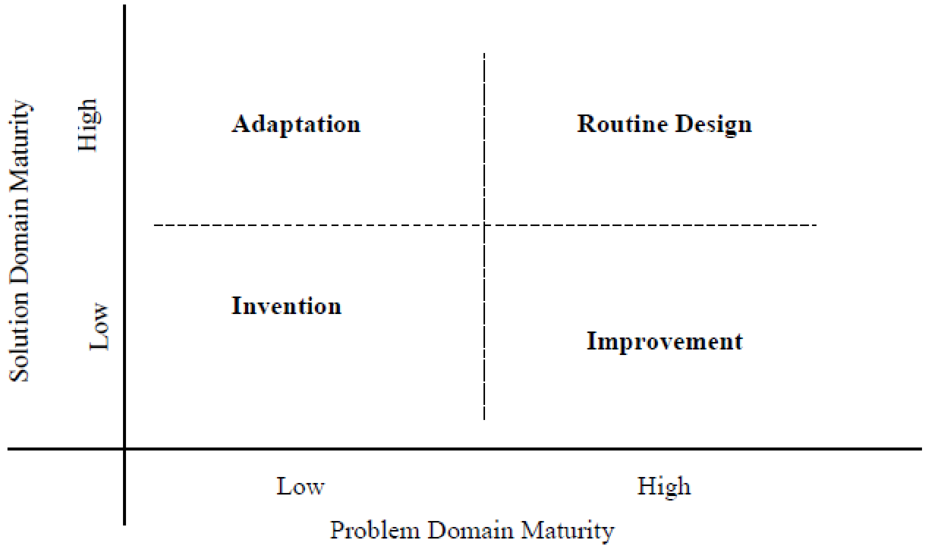


Figure 1: Design Science Knowledge Contribution Framework

Invention – a radical breakthrough – can be described as a new solution to a new problem. These types of knowledge contributions are considered rare yet possible outcomes in DSR. The other extreme – routine design – is also considered as a rare outcome but for a different reason. While invention is clearly something new, routine design applies existing knowledge in well understood problem area. Situations like these seldom require research methods. While routine design might lead to new discoveries, such findings typically shift the research to one of the other three quadrants. (Gregor & Hevner, 2013, pp. 346 - 347.)

Improvement in DSR is seen to create new solutions to known problems. This requires that either useful solutions do not exist or are clearly suboptimal. Exaptation – or adaptation – in DSR is in some sense the opposition of improvement. Adaptation applies known solutions to new problems. Similarly, as in improvement, in adaptation useful solutions do not exist or are clearly suboptimal. Such solutions might, however, exist in related problem areas and could be applied to a new problem context. (Gregor & Hevner, 2013, pp. 346 – 347.)

2.2 Application of the Methodology

Design science research is distinguishably artifact-centric research methodology and as such suitable for an artifact-centric research approach of this thesis. This thesis introduces an artifact to research how MITRE ATT&CK for ICS could be employed for assessing an OT security policy. The artifact is derived from existing knowledge in the form of MITRE ATT&CK for ICS and expanded it to an area where it is not routinely applied in a similar way. Therefore, the knowledge contribution of this thesis is arguably somewhere between adaptation and improvement in the framework proposed by Gregor & Hevner (Gregor & Hevner 2013, pp. 346 - 347).

Design science research includes various considerations as introduced in the prior section. Hevner et al. (2004, p. 83) have established seven guidelines for effective design science research (table 1).

Table 1: Design Science Research Guidelines

Guideline	Activity
(1) Design as an Artifact	"Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation."
(2) Problem Relevance	"The objective of design-science research is to develop technology-based solutions to important and relevant business problems."
(3) Design Evaluation	"The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods."
(4) Research Contribution	"Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies."
(5) Research Rigor	"Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact."
(6) Design as a Search Process	"The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment."
(7) Communication of Research	"Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences."

The research effort introduced in this thesis followed Design Science Research Methodology (DSRM) for Information Systems research introduced by Peffers et al (2007) to satisfy the aspects proposed above and throughout the previous section. The aim of the methodology is to serve as a commonly accepted approach to design science research. It is grounded on influential prior literature on what design science researchers have done or should do, including the above-introduced Design Science Research Guidelines by Hevner et al. (Peffers et al., 2007, p. 9; Hevner et al., 2004.)

The below table summarizes the activities associated with each of the six phases of DSRM (table 2).

Table 2: Deign Science Research Methodology

Phase	Activity
(1) Identify Problem & Motivate	Define the research problem and justify its value.
(2) Define Objectives of a Solution	Infer the objectives for the solution based on problem definition and knowledge of what is possible and feasible.
(3) Design & Development	Determine artifact's functionality and architecture. Create a suitable artifact.
(4) Demonstration	Demonstrate the use of the artifact with suitable method.
(5) Evaluation	Evaluate how well the artifact supports solving the problem.
(6) Communication	Communicate the research, including all the above-mentioned phases.

The above phases provided the general structure for the research process. Furthermore, as suggested by the process model (Peffers et al. 2007, p. 11), but not highlighted in the table, the research effort was iterative. The iterative approach is mostly visible in the chapter describing the designing and development of the artifact. However, this thesis is an outcome of multiple small and interconnected phases all formed through one or more iterations.

The structure of this thesis follows the "Publication Schema for a Design Science Research Study" by Gregor & Hevner (2013). The six phases of the DSRM are presented as follows. The problem identification and motivation were initially discussed in the introduction and will be further elaborated in literature review. The fourth chapter introduces the second and third phases and their outcomes. Demonstration and evaluation are covered in the fifth and sixth chapter and are further discussed in the seventh. The final phase, communication, is covered throughout this thesis concluding to chapter eight.

3 LITERATURE REVIEW

This chapter introduces the key concepts of this thesis and summarizes the examined prior research. The objective of the literature review is to provide sufficient theoretical understanding of OT security, summarize relevant prior research, and by doing so, provide validation on the novelty of the artifact proposed in this thesis.

Relevant literature was initially searched from JYKDOK[1], ScienceDirect[2] and IEEE Xplore[3]. The following key words were used:

- "OT Security"
- "OT" *AND* "Cybersecurity" *AND* "Control"
- "OT Security" *AND* "Control" *AND* "Assessment"
- "MITRE" *AND* "OT"
- "MITRE ATT&CK" *AND* "OT"
- "MITRE ATT&CK" *AND* "MITIGATIONS"
- "MITRE ATT&CK ICS"

In addition, relevant literature was found from the bibliographies of the assessed articles and based on the author's previous findings.

Peer-reviewed academic literature was used as a primary source of information. Other, non-academic publications such as standards, books, and white papers, that are based on their authors own authority have been used to supplement sections 3.1, 3.2, and 3.3. For the non-academic publications, the material found from the bibliographies of peer-reviewed academic publications was favored.

1 https://jyu.finna.fi/

2 https://www.sciencedirect.com/

3 https://ieeexplore.ieee.org/

3.1 Operational Technology

Operational Technology was defined in the first chapter as a broad range of systems that comprise a unique set of software and hardware used to monitor, control, and regulate industrial processes. This section provides a more detailed presentation of the underlying technology before the focus is shifted to the cybersecurity aspects of OT. The first subsection will provide a brief overview of OT in general while the following introduces some common OT components. The third and fourth subsections will present the components as parts of a wider setting.

3.1.1 Overview

All OT systems are unique in their own way (Miller et al., 2021, p. 1). They operate under a variety of different names depending on the type of system, environment conditions as well as the type and span of control. Examples of such include Industrial Control System (ICS), building automation, and physical environment monitoring and measurement systems (Conklin, 2016, p. 1; Stouffer et al., 2023, p. 8).

The uniquity of OT systems is based on the need to fit the systems to serve exact process driven requirements (Conklin, 2016, p. 1). However, they share standard components and logical frameworks (Miller et al., 2021, p. 1). As explained by Stouffer et al., (2023, p. 11) and illustrated below, a typical OT system includes multiple control loops, human-machine interfaces, and remote maintenance and diagnostics functions (figure 2).

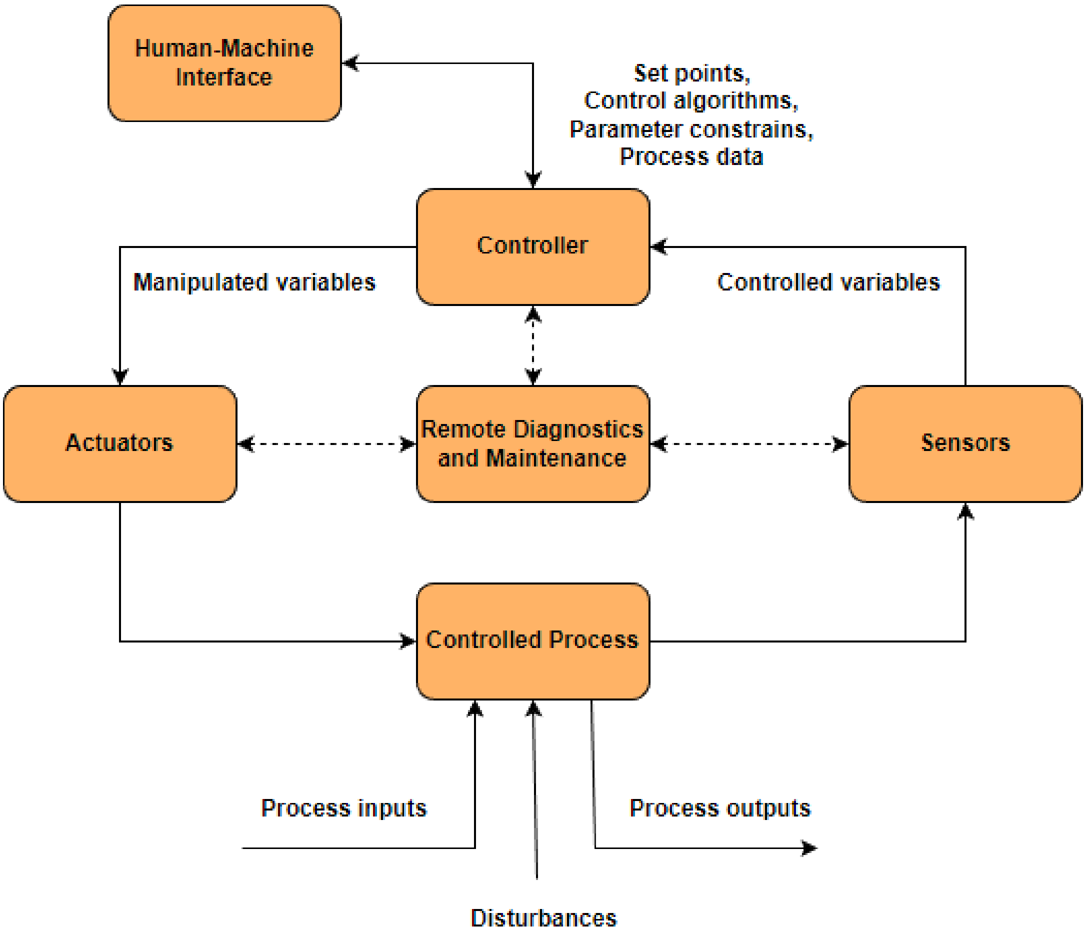


Figure 2: Basic operation of a typical OT system

A control loop manipulates the controlled process by utilizing sensors, controllers, and actuators. A sensor is a device that measures some physical property. It sends the measured information to a controller, which interprets the information, and based on a control algorithm and target set points, generates manipulated variables which are transmitted to an actuator. An actuator, for example a motor or valve, then manipulates the controlled process according to the instructions. (Stouffer et al., 2023, p. 11.)

Quite commonly, instead of direct connection between the sensors and actuators, the sensor values are sent to a monitoring station for a human to analyze. human-machine interfaces provide operators and engineer as capability to monitor and configure the system. To prevent, identify and recover from abnormal operations or failures, the system includes diagnostic and maintenance functions. (Stouffer et al., 2023, p. 11.)

3.1.2 Common OT Components

In general, in an industrial setting, OT environment comprise in part elements similar to traditional IT, such as workstations, servers, network equipment, printers, and storage. The other part includes devices specifically designed to manage interaction with a physical system through an appropriate human-machine interface (Flaus, 2019, p. 6). These common components – namely Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Safety Instrumented Systems (SIS), Human-Machine Interfaces (HMIs), sensors and actuators – apart from sensors and actuators already discussed above - are briefly introduced below. (Koay et al., 2023, pp. 4 -5; Flaus, 2019, p. 6).

Programmable Logic Controllers are an essential part of system automation. PLCs provide the capabilities to modify, trigger or modulate physical actions based on a measured input and a predetermined program. Therefore, a PLC provides control and regulation of a physical process. (Flaus, 2019, p. 8 & 10; Ackerman, 2017, p. 13.)

A PLC can be thought of as a microcomputer without a human-machine interface. It generally includes a power unit, a microprocessor, memory, a programming device, input and output modules as well as a communications interface. PLC programs are developed in a brand-specific programming environment and a programming device is used to load the program to a PLC. The memory contains the PLC operating system, the control program, and related data. The microprocessor runs the program, reads inputs, and writes outputs. Input signals, for example on-off-values or temperature, are received through an input module. After processing the signal, the output module transforms the outputs calculated by the program into a signal. The communication interface enables the PLC to communicate with other systems, such as other PLCs or Supervisory Control and Data Acquisition (SCADA). (Flaus, 2019, pp. 10 & 17.)

Safety Instrumented Systems are typically built from specific, reinforced PLCs with redundant hardware. Such systems are designed to take measures to mitigate the consequences of an industrial hazard by taking over control of the process if the basic process control fails to maintain the system at a safe state. When specific conditions are violated, SIS should ensure that the process evolves automatically to a safe state. When the specified conditions allow it, SIS lets the process evolve safely. (Flaus, 2019, pp. 13 – 14.)

Remote Terminal Units are used to connect a physical system to a master system, such as a PLC or SCADA. RTUs are microprocessor-controlled devices that transmit telemetry data and receive control messages via a modem, cellular connection, radio or by other communication technologies. (Flaus, 2019, p. 12.)

Human-machine interfaces allow users to monitor the system by visualizing how the system works and allows users to control the system by taking required actions. These devices directly interact with other OT equipment such as PLCs and servers. There are several types of HMIs. HMI can be a PC running purpose-built software on top of a traditional operating system. Such are typically used in SCADA supervision stations. Tablet-like devices equipped with a touch screen running on top of an embedded operating system such as Windows Embedded are another example. These devices are typically located close to physical systems. (Flaus, 2019, pp. 14 – 15; Ackerman, 2017, p. 13.)

3.1.3 Topologies

This subsection briefly introduces three common OT topologies to further ground previously introduced components as parts of a wider setting. Namely, PLC-based topology, SCADA and Distributed Control Systems (DCS). For further reference, for example NIST SP 800-82R3 (2023) provides relatively comprehensive introduction on all three, as well as on Building Automation Systems (BAS), Physical Access Control Systems (PACS), and Industrial Internet of Things (IIoT) (Stouffer et al., 2023, pp. 12 – 28).

Smaller OT system configurations can use **a PLC-based topology** where PLCs are the primary controller instead of a central control server. As an example of such a setting NIST SP 800-82R3 describes an instance where a PLC controls the manufacturing process and is accessible by a programming interface on an engineering workstation. The Local Area Network could also include an HMI, a data historian used to store data from the control systems, communication equipment, sensors, such as a proximity sensor and photo eye, as well as actuators such as servo drives and variable frequency drives. (Stouffer et al., 2023, p. 21; Flaus, 2019, p. 17.)

PLCs are also used as the control components in both Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) systems. However, in these settings their role is different (Stouffer et al., 2023, p. 21). Advanced, distributed industrial control systems can be divided into two types: SCADA and DCS. Because both share many common features the boundary between them is not sharp (Padée et al., 2019, pp. 1 - 2; Flaus, 2019, pp. 4 - 5).

In a **SCADA** system, a PLC may provide functionality similar to an RTU (Stouffer et al., 2023, p. 21). SCADA systems enable centralized control of an installation (Flaus, 2019, p. 5). Such systems are used to control distributed assets in cases where centralized data acquisition is as important as control (Stouffer et al., 2023, p. 12).

SCADA systems collect information from the field-devices which is transferred to a control center where it can be displayed to the operator graphically or textually. This enables centralized monitoring in nearly real time. Furthermore, depending on the setup of the system, control operations of any individual system, operation, or task can be automated or done based on operators' commands. (Stouffer et al., 2023, p. 12.)

Such systems are used for example in water distribution, oil and gas pipelines, and public transportation systems. The common components include control servers, HMIs, data historian, communication equipment, PLCs and/or RTUs, actuators and sensors (Flaus, 2019, p. 5; Stouffer et al., 2023, p. 12). Whereas the RTU or PLC controls the local process, a control server in the control center processes their inputs and outputs. Based on the programmed instructions, the software tells the system what to monitor and when, as well as the acceptable parameter-ranges, and how to act when the process variables breach the acceptable ranges. The control center is also responsible for centralized alarm, trend analyses, and reporting (Stouffer et al., 2023, p. 12).

DCS systems use PLCs as local controllers (Stouffer et al., 2023, p. 21). A DCS is a set of network-connected control systems which include a central unit for supervision. Historically DCSs have been very different from more heterogeneous SCADAs. However, this difference has faded in time (Flaus, 2019, p. 6; Ackerman, 2017, p. 15). In the past, the difference between the two has been that SCADA has been used to control distributed systems in larger geographical areas, while DCS has more often been used in a single plant or facility (Ackerman, 2017, p. 15).

DCSs are used for example in chemical manufacturing and automotive production. A DCS control architecture consists of a supervisory level and multiple integrated sub-systems. The supervisory level centrally controls a group of localized controllers which share the overall production process. The subsystems control the details of the local process in a way where the key process or product conditions are automatically kept around a desired set point. (Stouffer et al., 2023, p. 19.)

In general, the components in DCS are like the ones in SCADA. A control server communicates with field controllers to request data and provide set points. The field controllers receive feedback from process sensors. Based on this information and the control server commands, the controllers control process actuators. In addition to the supervisory and local control, a DCS may include an intermediate level responsible for controlling a cell within a plant. A cell could include multiple local controllers. For example, a machine controller for processing a part, and a robot controller which would handle raw stock and final products. (Stouffer et al., 2023, p. 19.)

3.1.4 Purdue Model

Finally, we will look at an overview of an OT network as a part of a larger enterprise setting. Typically, such a setting consists of several types of networks – the enterprise network (IT network), the production network, the control network, and the field network. There are several models for representing such a structure. One commonly seen is the Purdue model (Ocaka et al., 2022; Sangkhro & Agrawal, 2023; Koay et al., 2023; Flaus 2019; Ackerman 2017) that has been adapted from the Purdue Enterprise Reference Architecture by ISA-99 (Ackerman, 2017, p. 16). The below-figure is adapted from the illustrations of Flaus (2019, p. 26) and Ackerman (2017, p. 17) (figure 3).

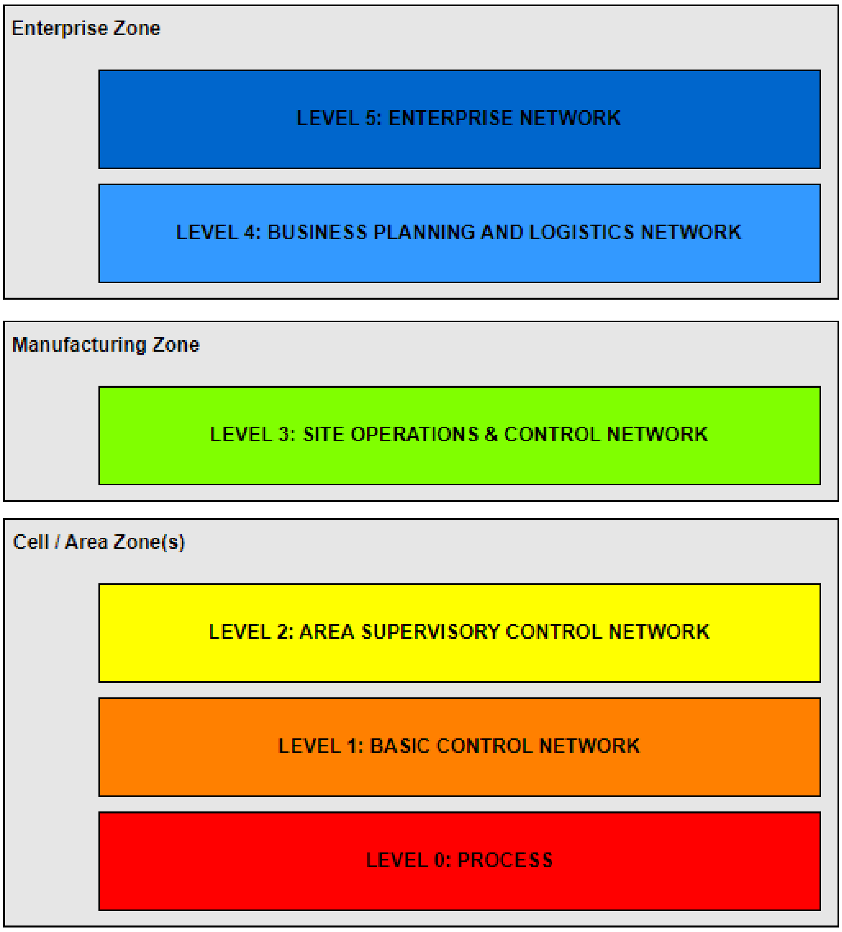


Figure 3: Purdue model

The above figure visualizes the interconnections and interdependencies of the overall installation (Ackerman, 2017, p. 16). While it is a simplification of the reality (Flaus, 2019, p. 26), it is useful to present the core-idea of the whole IT/OT network structure by dividing it into smaller pieces.

Enterprise Network (level 5) is a part of the IT network. It may span over multiple sites. While technically it is not a part of the OT network, it handles data gathered from the OT networks to support business decisions. (Ackerman, 2017, p. 18.)

Business Planning and Logistics Network (Level 4) is also considered as part of the IT network. It facilitates IT systems that support the site's operations by providing functions involved in the management of the manufacturing and processing. An example of a system located in this level is Enterprise Resource Planning (ERP). Ackerman (2017) associates Manufacturing Execution System (MES) on this level, whereas Flaus (2019) places MES on the third level. (Ackerman, 2017, p. 18; Flaus, 2019, p. 27.)

Site Operations and Control Network (level 3) is the highest level of the OT network. The systems it facilitates provide site-wide control and monitoring. These systems also aggregate the data from the lower levels of the network and may send the data to the systems on level 4. As mentioned, Flaus (2019) places

MES on this level. Other examples of such systems are SCADA, Data Historians, and other types of servers. (Ackerman, 2017, p. 21; Flaus, 2019, p. 27.)

The systems facilitated on the **Area Supervisory Control Network (level 2)** provide functions to monitor and control the physical process for a smaller part of the overall system. Examples of such equipment include line control PLCs which are in nature supervisory rather than controlling and standalone or system client HMIs (Ackerman, 2017, p. 21; Flaus, 2019, p. 27). Ackerman (2017) explains that the functions and the systems of the third and second level are similar to one another. The difference is the area that the systems cover. One could visualize level three as a centralized control room and level two as one of the monitored areas (Ackerman, 2017, p. 21).

Basic Control Network (level 1) facilitates the controlling equipment that can detect, observe, and control a physical process. Examples of systems at this level are SIS, PLC and RTU. These are used to control **the Process (level 0)** which includes the physical systems used for production that are controlled by the higher-level devices. The devices on the lowest level include motors, pumps, valves, and sensors. (Ackerman, 2017, p. 21; Flaus, 2019, p. 27).

3.2 Operational Technology Security

This section provides an overview of the domain of this research effort. The section will firstly introduce the topic in general before presenting some commonly seen challenges in the domain through comparing OT security to its IT counterpart. The third subsection centers around the measures of defending OT environments while the last subsection briefly discusses the threats towards OT.

3.2.1 Introduction to OT Security

The cybersecurity issues arising from the evolution of OT have been recognized for several years (Wagner et al., 2020, p. 1). The OT of today has evolved from the insertion of IT capabilities into existing physical systems. The increase of cost and performance efficiency has encouraged this evolution and has resulted in today's smart technologies (Stouffer et al., 2023, p. 8). While the adaptation of new technologies has brought upon new opportunities, it has raised new security concerns (Stouffer et al., 2023, p. 8; Hayden, Assante & Conway, 2014).

Conklin (2016) claims that the true challenge of IT/OT convergence is aligning security with the business objectives of each system. Connecting IT and OT systems is an increasing interest as businesses desire information from control systems (Conklin, 2016, p. 1). Asset owners benefit from new and more efficient methods of communication, on more robust data collection and aggregations methods, faster time-to-market, and interoperability (DHS, 2016, p. 1). Emerging technologies have also improved plant operations and maintenance (de Peralta, 2020, p. 1).

Simultaneously, modernizing OT environments to meet the demands of automation and advanced data analytics has brought upon various cybersecurity threats and vulnerabilities, previously contained in physical isolation (de Peralta, 2020, p. 2). In the past securing OT systems has heavily relied on security through obscurity. In practice the systems were operated through proprietary protocols, using specialized hardware and software in a physically isolated network and only few understood their complex architectures or the operational mechanisms (Zanasi et al., 2022, p. 1; Koay et al., 2023, p. 8; DHS, 2016, p. 1; Stouffer et al., 2023, p. 28).

This approach has been considered sufficient in environments with no external connections. Thus, cybersecurity has not been a primary design criterion in OT. However, technological advancements have made the systems much less isolated and much more vulnerable (Toker et al., 2021, p. 1; Jadidi & Lu, 2021, pp. 1 & 2; DHS, 2016, pp. 1 & 4; Koay et al., 2023, p. 8). Given the recent development, physical separation has become an unviable business option for managing, utilizing, and securing OT environments. The change in the modern OT architectures, driven by business requirements, has not only made the security model of the past obsolete but has exposed the weaknesses of these systems (Zanasi et al., 2022, p. 1; DHS, 2016, p. 1). OT systems no longer operate in isolation. Many of these systems rely on constant external connections for control, updating and vendor management (Padée et al., 2019, p. 1; Mohammed et al., 2023, p. 4). Furthermore, solutions such as IIoT rely on connections between cloud platforms and OT environments (Koay et al., 2023, p. 8).

Still, throughout the IT/OT convergence, the need for reliable delivery of critical infrastructure services has outweighed cybersecurity concerns (de Peralta, 2020, p. 2). Instead of being designed to be secure against cyberthreats, devices and applications in OT environments are designed for long lifetimes and high availability. It is not uncommon that such systems run with elevated privileges in an "always on" mode on shared devices (Koay et al., 2023, p. 8). But the effects are not only negative from a wider security perspective.

As an example, Gourisetti et al. (2022) discuss Distributed Ledger Technology (DLT) in power systems which include interactions with OT systems. Such technology is seen to increase the resilience and agility of electricity infrastructure to better respond to all hazards (Gourisetti et al., 2022, pp. 1 -2). Similarly, modern ships use computerized systems for multiple purposes, including navigation, communication, and cargo handling. These systems have improved operational efficiency and safety of such vessels (Oruc, Amro & Gkioulos, 2022, p. 1; Rajaram, Goh & Zhou, 2022, p. 3).

Despite the benefits, sectors such as manufacturing (Rahman, Wuest & Shafae, 2023, p. 12) and maritime industry (Rajaram et al., 2022, p. 1) have seen an increase in cybersecurity-related risks. OT is not only more vulnerable than in the past but also an attractive target for cyberattacks as modern societies rely on OT systems (Rencelj Ling & Ekstedt, 2023a, p. 1; Rahman et al., 2023, p. 12; Ocaka et al., 2022, p. 7). Therefore, cybersecurity has arguably become a necessity in OT (Toker et al., 2021, p. 1).

3.2.2 OT Security Challenges

Although the IT/OT convergence has brought IT and OT closer together, the underlying distinction remains the same. OT systems control physical devices whereas IT systems process and store information. In cybersecurity, many of the differences between the two relate to this foundational difference. (Stouffer et al., 2023, p. 1; Flaus, 2019, p. 4.)

Firstly, in cybersecurity, CIA-triad is a commonly used acronym that represents Confidentiality, Integrity, and Availability. Confidentiality aims at protecting information from unauthorized access and disclosure. Integrity is concerned with guarding information from improper modification or destruction. Availability aims at ensuring that information can be accessed reliably and timely. (Cawthra et al., 2020, p. 1.)

Padée et. al. (2019) and Boeding et al. (2022) argue that the priorities in IT security reflect the order of the letters, making Confidentiality as the number one priority, followed by Integrity and Availability. The priorities in OT environments would generally be AIC instead of CIA (Boeding et al., 2022, p. 2; Padée et al., 2019, p. 2). It is also noteworthy that while availability and integrity are considered to outrank confidentiality, safety is an overarching priority in OT (Stouffer et al., 2023, p. 2).

In IT networks, data is the primary commodity. In this sense, ensuring the confidentiality of the data – which in most cases is irrecoverable – is highly important. For OT networks, the availability is equally as important as the primary focus is in keeping the physical process running at optimal conditions and ensuring the safety of the people and property. (Boeding et al., 2022, p. 2; Padée et al., 2019, p. 2.)

The loss of the integrity of the data in IT networks can also have severe effects. However, whereas the confidentiality of the data is typically irrecoverable, integrity can in many cases be recovered through reinstalling the system or by recovering it from backups. In OT networks, unauthorized alteration of the system state may lead to severe consequences. Yet, if the system remains operational, countermeasures minimizing the negative impact may be immediately applied. (Boeding et al., 2022, p. 2; Padée et al., 2019, p. 2.)

Affecting the availability of an IT network, for example through a denial-of-service attack, often requires considerable effort, and only affects the system for as long as the attack takes place. In OT networks, the loss of data is typically seen by far the least important factor. While the data can be used to gather knowledge about the system for further attacks, it typically consists mainly of logs and monitoring data. (Boeding et al., 2022, p. 2; Padée et al., 2019, p. 2.)

Whereas the above-mentioned examples are generalizations, they reflect the fundamental difference of the environments and the purposes they serve. Likewise, the history and evolution of IT and OT are different. This is clearly visible in the current state of OT security. As explained in the beginning of this section, OT systems have evolved in an isolated environment. Due to the isolation, cybersecurity has not been a primary design criterion. IT systems on the other hand have evolved alongside various threats in much less isolation. (Boeding et al., 2022, p. 6).

Whereas securing IT is conceptually well understood in academic literature and to a degree in practice, in OT the understanding is narrower in focus. The domain of OT security is dominated by thinking centered around the process under control. While IT environments have learned to embrace the external risk, OT environments are still in the process of understanding the risk introduced by network connectivity and outside issues that do not directly affect the process under control. (Conklin, 2016, p. 1.)

The fundamental challenge in OT security is that many devices in OT networks have either been designed and built completely without common security functions such as authentication and cryptography, or with minimal functions that have no real use in the modern world (Conklin, 2016, p. 2). As an example, commonly used OT protocols ModbusTCP, DNP3 and OPC DA lack authentication and encryption (Mohammed et al., 2023, p. 1). For example, ModbusTCP originates from a simple point-to-point serial connection and thus lacks security mechanisms. However, as it is now used in Ethernet networks, these shortcomings create a whole new problem (Padée et al., 2019, p. 2).

Vulnerabilities found in OT environments are typically not easy to fix as most of the components and protocols would require either a design update or an extra layer of security added to them (Koay et al., 2023, p. 9). Using network security solutions such as firewalls to provide a certain level of access control to the OT network lessens the risk but does not solve the underlying issue. OT components have not been designed to operate in untrusted spaces (Conklin, 2016, pp. 1 - 2).

The lifespan of OT systems is relatively long, typically around 10 – 15 years, but may even exceed 20 years. In IT, the typical lifespan is between 2 – 5 years (DHS, 2016, p. 4; Flaus, 2019, p. 69; Stouffer et al., 2023, p. 30). Hence, OT environments typically involve legacy systems running outdated software with no vendor support (Rahman et al., 2023, pp. 1 -2; DHS, 2016, p. 4). In cybersecurity, it is common knowledge that this not only promotes general lifecycle related challenges but will introduce vulnerabilities that cannot be patched.

In contrast to the Agile development methods “continuous delivery” model, the mentality in OT settings is typically “if it isn’t broken, don’t fix it” (Køien, 2021, p. 4; Conklin, 2016, p. 2). Even though the systems would still be supported, patch and change management in OT is not trivial. The availability requirements of the OT environment may only allow small windows for introducing changes to the system (Stouffer et al., 2023, p. 29; DHS, 2016, p. 4; Flaus 2019, p. 69; Padée et al., 2019, p. 5; Conklin, 2016, pp. 1 - 2). Some OT networks run 24/7/365 and even longer without interruptions (Conklin, 2016, p. 2). Hence, outages must be planned, and exhaustive testing might be required before any changes are made (Stouffer et al., 2023, p. 29; DHS, 2016, p. 4). The challenge of valuing availability over everything else may cause cybersecurity controls to be overlooked due to the potential impact in availability (Padée et al., 2019, p. 6). If restarting an OT supported process takes three days, it understandably creates an asymmetric risk environment with a severe risk avoidance culture where "unnecessary" configuration changes are avoided (Conklin, 2016, p. 2).

Vendors' role in OT setting also differs from IT. IT systems can typically be supported by multiple vendors. In OT, service support may only be available through a single vendor. Vendor licensing and service agreements might also forbid the usage of third-party security solutions (Stouffer et al., 2023, p. 29).

As all the above-introduced differences indicate, security solutions designed for IT-systems might not be suitable for OT systems (Stouffer et al., 2023, p. 29; DHS, 2016, p. 4; Padée et al., 2019, p. 4). Furthermore, OT systems are designed to support intended industrial processes. This may limit the availability of memory and computing resources for supporting security capabilities designed to a different kind of system (Stouffer et al., 2023, p. 29). This is problematic, as Jadidi & Lu (2021) claim that most security solutions have been designed for IT networks (Jadidi & Lu, 2021, pp. 2 - 3). Progoulakis et al. (2021) claim that the same applies to many security standards, policies, and directives (Progoulakis et al., 2021, p. 19).

OT security specific standards and guidelines exist, but are not completely mature (Padée et al., 2019, p. 4; Staves et al., 2023; Sangkhro & Agrawal, 2023, p. 4). Sangkhro and Agrawal (2023) propose that management complexity and costs associated with their implementation makes OT asset owners hesitant to use them (Sangkhro & Agrawal, 2023, p. 4). Staves et al. (2023) suggest that the vast number of standards and guidelines make it difficult for OT asset owners to know what route to take (Staves et al., 2023, p. 2).

Staves et al. (2023) have proposed a model for assessing OT security standards and guidelines. The researchers have evaluated NIST CSF, IEC 62443, NIST SP 800-82, ISO/IEC 27019, NCSC CAF, ONR SyAPs, and ERC CIP against the criteria. They conclude their findings by stating that the controls presented in the standards and guidelines are generally mature. However, they lack OT specific implementation guidance but instead often refer to IT-focused standards and include several inconsistencies in terms of content. Their conclusion is that OT standards must mature further to address the security and risk mitigations needed for protecting interconnected IT and OT environments. (Staves et al., 2023.)

Wagner et al. (2020) studied the applicability of OT security standards – namely, IEC 62443, NIST SP 800-82, and VDI/VDE 2182 - from the perspective of small and medium-sized (SME) as well as large manufacturing organizations. IEC 62443 was seen especially complex, while NIST SP 800-82 and VDI/VDE 2182 less so. Out of the three, only NIST SP 800-82 is free of charge. According to their results, the standards are well applicable for large enterprises, whereas SME organizations find themselves struggling due to limited capabilities. To address the issue, SME organizations seek external support from security experts, who for their part struggle with lack of OT specific experience. (Wagner et al., 2020.)

3.2.3 Protecting OT

In cybersecurity, countermeasures can be described as technical solutions, process or actions that are used to prevent or mitigate the consequences of an attack (Rahman et al., 2023, p. 6). Covering all possible – sometimes conflicting – practices for protecting OT environments is not the purpose of this thesis. Neither does this section provide in-depth knowledge about any specific control. We merely summarize one commonly suggested OT security approach and some associated, frequently proposed, countermeasures as an overview of the topic.

A commonly suggested approach towards securing OT environments is defense-in-depth (Jiang et al., 2018, p. 1; Padée et al., 2019, p. 4; Zanasi et al., 2022, p. 2; Ara, 2022, p. 9; Stouffer et al., 2023, p. 67; Mosteiro-Sanchez et al., 2020, p. 10; DHS, 2016) – a concept that has previously been adapted in IT security (DHS, 2016). Stouffer et al. (2023) suggest that defense-in-depth is considered as a best practice which has been integrated into multiple standards and regulatory frameworks (Stouffer et al., 2023, p. 67). Padée et al. (2019) confirm that the approach is one of the most important general design rules in “Computer Security at Nuclear Facilities” while Zanasi et al. (2022) identify it as the current approach in industrial cybersecurity promoted by security standards such as ISA/IEC 62443 (Padée et al., 2019, p. 4; Zanasi et al., 2022, p. 2).

Applying a defense-in-depth approach to securing OT environments is one way of safeguarding the environment by making it unattractive to adversaries (DHS, 2016). The strategy assumes that there is no single origin of threats. Therefore, it promotes the use of different overlapping countermeasures and pursues a state where single points of failure are prevented (Jiang et al., 2018, p. 1; Stouffer et al., 2023, p. 67).

The multilayered countermeasures applied in defense-in-depth seek to improve the protection of operations, personnel, and technology. The core idea of the strategy is to improve the probability of detecting adversary actions and thus the likelihood that these can be countered. By doing so, organizations can increase the “cost” of an intrusion by making lateral movement in a network harder and force the malicious actor to increase the investment for accomplishing their goal (DHS, 2016, p. 5).

Based on their research of prior literature Mosteiro-Sanchez et al. (2020) suggest that the traditional layers of defense-in-depth are “Physical”, “Perimeter”, “Network”, “Host” and “Application and Data” (Mosteiro-Sanchez et al., 2020, p. 10). NIST’s “Guide to Operational Technology (OT) Security” on the other hand proposes relatively similar five-layer approach, where the layers are “Security Management”, “Physical Security”, “Network Security”, “Hardware Security” and “Software Security” (Stouffer et al., 2023, p. 69). The difference between these is that NIST’s approach includes “Security Management”, a layer that is lacking in the prior mentioned. Furthermore, the model introduced by Mosteiro-Sanchez et al. address topics related to network security in two layers - “Perimeter” and “Network” – where the prior is concerned with isolating OT network, and the latter with dividing the OT network in various segments. In the NIST's model both aspects are addressed in "Network"-layer (Stouffer et al., 2023, pp. 69 – 79; Mosteiro-Sanchez et al., 2020, pp. 5 - 6).

To provide an overview of the layers, the following paragraphs propose some key considerations related to each layer. The layers follow the proposal of Stouffer et al. (2023) due to its slightly wider approach. In addition to the layers, some commonly seen countermeasures suggested in prior literature are introduced for each layer.

Layer 1 - Security Management: Effective integration of cybersecurity into the operation of OT requires a comprehensive OT security program. Security management or security governance is considered as the organizational or programmatic decisions that guide and impact the decisions made for the latter layers. Therefore, an overarching OT cybersecurity program should be created before attempting to implement the others. (Stouffer et al., 2023, pp. 33 & 69.)

The program should define the scope and objectives for OT security, establish a cross functional team that understands OT and cybersecurity, identify the capabilities to manage cyber risk including people, process, and technology, and define policies and procedures. Furthermore, it should consider day-to-day operations of event monitoring and auditing for compliance and improvement. The plan should be regularly updated to reflect changes in technologies, operations, standards, regulations, and the security needs of specific facilities. (Stouffer et al., 2023, p. 33.)

While the controls introduced in the upcoming paragraphs should initially be planned at this stage, we provide some examples of controls that could be associated to this layer due to their overarching nature. Examples include but are not limited to creating policies for forbidding the use of weak passwords (Rajaram et al., 2022, p. 8; Mosteiro-Sanchez et al., 2020, p. 3 – 4), creating back-up procedures, business continuity and disaster recovery plans (Ara, 2022, p. 9), and performing risk assessments (Ocaka et al., 2022, pp. 6 -7; Ara, 2022, p. 9). Additionally, organizations should train their personnel (Padée et al., 2019, p. 5; Ocaka et al., 2022, pp. 6 -7; Rajaram et al., 2022, p. 5; Ara, 2022, p. 9). The purpose of providing security related training is to ensure that the personnel are aware of the organization's security policies and understand them. In addition to the OT related staff such as engineers, security training should be provided to all staff, even to the ones who have nothing to do with plant operations. The reasoning for this is that attacks targeted at office personnel may further propagate through office network to OT network as will be further elaborated on the next subsection (Padée et al., 2019, p. 5).

Regardless of its specific content, the OT security program should always be part of the wider OT safety and reliability programs. It needs to address the OT specific requirements, but organizations should make sure that it is consistent and integrated with potentially existing IT security programs and other practices (Stouffer et al., 2023, pp. 2 & 33). The need to address OT specific requirements is further elaborated by Conklin (2016) as he claims that the business objectives of IT and OT systems are very different. Hence, in some cases applying IT solutions to OT systems can create a mismatch. The challenge is that people with IT security background might not understand the OT operating environment and hence, might make a hasty judgement that OT personnel do not value security. On the other way around, OT personnel might feel that the risk and potential consequences the imperatives might have are not respected (Conklin, 2016, pp. 1 & 4).

To prove a point, Conklin (2016) explains that addressing a software vulnerability by patching the system would be the go-to solution in an IT environment. Therefore, personnel with IT security background and years of experience in patching and other IT security best-practices might take these as self-evident solutions – as OT equipment may be seen as "just another computer system". In OT, bearing in mind the potential effect the patch might have should it lead to operational issues, it would be beneficial to consider how the patch might affect the system and whether there are any other external controls that could be applied to the system without interfering with its current risk profile, but that would provide appropriate level of protection. (Conklin, 2016, pp. 4 - 5.)

For addressing the issue Padée et al. (2019) suggest that OT personnel should have influence on security policies. While this might help addressing OT specific needs, it could help promote compliance. Too restrictive policies might easily be overlooked if they are seen to hinder the operations (Padée et al., 2019, p. 5). Furthermore, Conklin (2016) proposes that in OT, resilience should be added to supplementing the CIA-triad. Beginning the considerations from resilience could promote two changes. The personnel with IT security background would need to confront the fundamental differences between IT and OT systems by addressing the potential negative effects the security control might have on system performance. Additionally, OT personnel would need to widen their understanding of the risk profiles by including outside issues that are frequently ignored – as for example newly discovered vulnerabilities might as well be the source of the next failure in the connected environment. These changes in combination might lead to a state where the security controls would be better aligned with the business objectives of an OT system which is a key success factor for a security program (Conklin, 2016, pp. 1 & 4 – 5).

Layer 2 - Physical Security: Countermeasures in the physical layer aim at safeguarding the assets and surrounding environment from accidental or deliberate damage (Stouffer et al., 2023, p. 69). Such controls may include restricting access to certain physical locations, for example to equipment rooms or cabinets (Stouffer et al., 2023, p. 70; Rajaram et al., 2022, p. 5), forbidding USB devices in certain areas or physically blocking USB-ports (Padée et al., 2019, p. 6; Rajaram et al., 2022, p. 5), and classical perimeter protection such as fences, walls, gates, guards and camera surveillance (Stouffer et al., 2023, p. 70).

The controls related to physical security are applicable throughout the organization's infrastructure, and hence may include a variety of controls for different needs. Therefore, organizations should reflect on the requirements set by their operating environment. Among other, requirements related to relevant regulations, legislation, environment, and safety should be considered (Stouffer et al., 2023, p. 70; Mosteiro-Sanchez et al., 2020, p. 5).

Layer 3 - Network Security: The area of network security includes various aspects. According to Stouffer et al. (2023) the foundational ones are network segmentation, centralized logging, network monitoring and malicious code protection (Stouffer et al., 2023, p. 71).

Maintaining separation between the IT and OT networks is a best practice (Koay et al., 2023, p. 8). OT networks should be separated from IT networks and especially from the Internet (Anton et al., 2021, p. 14; Ocaka et al., 2022, pp. 6 -7; Padée et al., 2019, p. 2; Ara, 2022, p. 9; Mosteiro-Sanchez et al., 2020, pp. 3 – 4; Stouffer et al., 2023, pp. 71 – 73). A common way to achieve this is with firewall(s) (Anton et al., 2021, p. 14; Jiang et al., 2018, p. 1; Stouffer et al., 2023, p. 73).

A topic commonly discussed as a part of IT/OT network separation is demilitarized zone (DMZ) (Anton et al., 2021, p. 14; Jiang et al., 2018, p. 1; Stouffer et al., 2023, p. 72; DHS 2016, p. 19). DMZ is a concept of an enforcement boundary between network segments (Stouffer et al., 2023, p. 72). In OT security context, the DMZ, or industrial DMZ (IDMZ), is a perimeter network between IT and OT networks. Its purpose is to act as an intermediary between any communications between the two (Zanasi et al., 2022, p. 2). If the OT resources that need to be accessed from IT network are placed on the DMZ, no direct communications paths are required between the IT and OT networks (DHS, 2016, p. 19).

Demilitarized zone adds an extra layer of security on organizations internal network (DHS, 2016, p. 19). Jiang et al. (2018) have also researched the effect of network performance with industrial demilitarized zones and without it. While they point out that IDMZ increases costs and management complexity, their simulation indicates that IDMZ can enhance the networks' performance (Jiang et al., 2018). An illustration of a recommended security architecture by DHS (2016, p. 17) including DMZs can be seen below (figure 4).

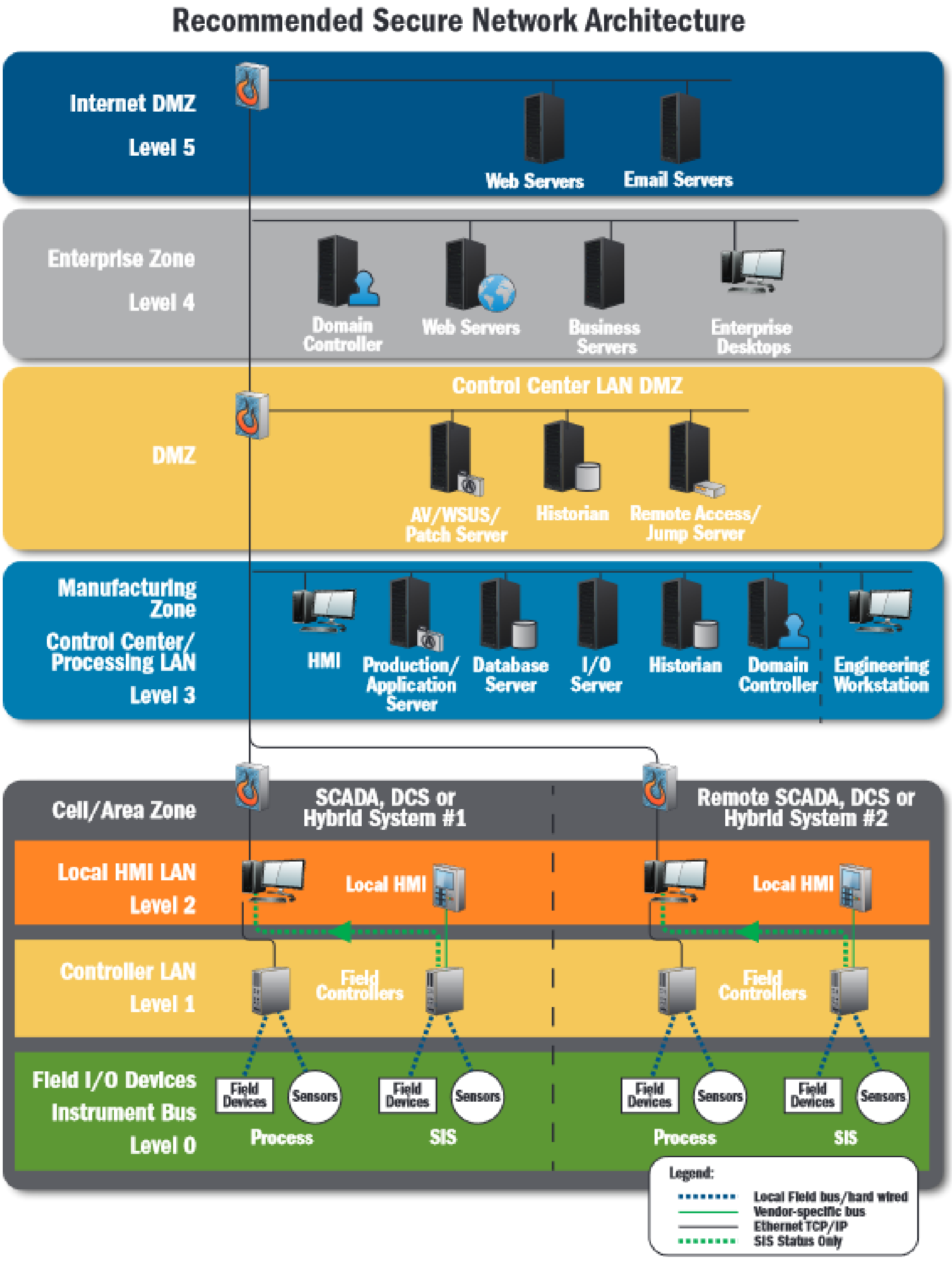


Figure 4: Recommended secure network architecture

As illustrated above, in addition to isolating the OT network, organizations should proceed to further segment the OT network. Models such as Purdue Model, ISA-95 or Three-Tier IIoT System Architecture can be used to divide the network into proper zones. The communications between these zones should be controlled with appropriate firewall configurations permitting only authorized communications. Furthermore, as a rule of thumb, for example in the case of Purdue Model-based implementation, direct communications hopping over a level – for example connection from level 4 device to level 2 device - should be prevented. (Stouffer et al., 2023, pp. 71 – 72.)

In cases where remote access is required, organizations should implement controls to prevent unauthorized access to the networks, systems, and data. Technologies such as VPN support secure remote access (Stouffer et al., 2023, p. 122; Rajaram et al., 2022, p. 5). Moreover, organizations should define processes for requesting and enabling remote connections. When remote access is provided for justified needs, it should be limited to only what is required (Stouffer et al., 2023, pp. 122 - 123).

It is worth noting that while from cybersecurity point of view the abovementioned approaches are considered as best practices, there might be other needs to consider. For example, from the maintenance perspective, the engineering personnel might argue that limitation of remote access capabilities might lower the safety of the process due to potential increase in response time caused by limited or non-existing remote access capabilities (Padée et al., 2019, p. 2). Hence, as suggested in NIST SP 800-82, during the planning process organizations should consider how the network architecture affects operations, safety, and response capabilities (Stouffer et al., 2023, p. 72).

In addition to the network separation, segmentation, and secure remote access, enabling logging function of network devices should be done to support network monitoring, alerting and incident response (Stouffer et al., 2023, p. 73; Ara, 2022, p. 9; Rajaram et al., 2022, p. 5). Similarly, using Intrusion Detection/Prevention System (IDS/IPS) (Ocaka et al., 2022, pp. 6 -7; Rajaram et al., 2022, p. 5; Ara, 2022, p. 9; Stouffer et al., 2023, p. 74), Security Information and Event Management (SIEM) and Behavioral Anomaly Detection (BAD) (Stouffer et al., 2023, p. 74) tools and capabilities can identify and alert about inappropriate behavior in the network.

Layer 4 - Hardware Security: Hardware security is focused on providing foundational support for security and trust for the devices in scope. The functions and security requirements associated with the layer are for example access control, integrity protection and secure configuration and management. Upon achieving the device trust, the state must also be maintained and tracked. (Stouffer et al., 2023, p. 76). Measures such firmware patching (DHS, 2016, p. 26) and where possible, using vendor-provided technologies such as Trusted Platform Module (TMP) (Stouffer et al., 2023, p. 76) are examples of countermeasures associated to hardware security.

One key consideration related to hardware security is asset management. It is worth noting that although the topic is discussed here - as the term asset management very much relates to physical devices - those are only types of assets to consider. The other types are at least data, personnel, systems, and facilities (Stouffer et al., 2023, p. 91) as well as processes (DHS, 2016, p. 9). Nonetheless, asset identification is foundational in understanding and managing OT risks as effective security depends on the capability to identify the assets that need to be protected. This is especially true in OT security where unique system-specific nuances and realistic conditions need to be considered (DHS, 2016,

p. 9; Stouffer et al., 2023, p. 91). In addition to identifying the assets, organizations should also be able to determine the most important ones to protect – or the so to say - "crown jewels" (Ara, 2022, p. 9).

Layer 5 - Software Security: The measures on the fifth layer focus on capabilities that ensure the proper usage and maintenance of the applications and services used to support OT (Stouffer et al., 2023, p. 76). Such countermeasures include software patching (Stouffer et al., 2023, p. 77; Anton et al., 2021, p. 14; Ocaka et al., 2022, pp. 6 -7; Rajaram et al., 2022, p. 8; Mosteiro-Sanchez et al., 2020, pp. 3 - 4), application allowlisting (Stouffer et al., 2023, p. 77; Ocaka et al., 2022, pp. 6 -7), configuration management and application hardening – such as deactivating unused services to decrease potential attack surface (Anton et al., 2021, p. 14; Ocaka et al., 2022, pp. 6 -7; Stouffer et al., 2023, p. 77), antimalware software (Ocaka et al., 2022, pp. 6 -7; Rajaram et al., 2022, p. 5) as well as user access management related controls such multifactor authentication or password security mechanisms (Mosteiro-Sanchez et al., 2020, pp. 3 – 4; Rajaram et al., 2022, p. 5; Anton et al., 2021, p. 14).

Whereas OT security faces lots of challenges, some of which have been addressed throughout this chapter, it is worth noting that in OT security, application allowlisting provides a refreshing opportunity for organizations. The idea of application allowlisting is to restrict the number of applications that the host is allowed to run. When configured correctly, non-authorized applications will not be executed. As OT environments are typically relatively static, application allowlisting is potentially a very usable countermeasure. (Stouffer et al., 2023, p. 77.)

Finally, while the above-described are arguably good practices, it is worth noting that they are only examples. Approaches for securing OT environments are by no means limited. Furthermore, even the proposed measures are not immune to criticism.

An interesting example found in the literature relates to zero-trust. Zero-trust can be described as a cybersecurity paradigm that is gaining attention in IT security (Zanasi et al., 2022, p. 2; Stouffer et al., 2023, p. 75). In NIST SP 800-207 (Zero Trust Architecture), zero trust is defined as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised." (Rose et al., 2020, p. 4).

Zanasi et al. (2022) claim that industrial DMZs – or even generally, the layered network architectures such as Purdue model-based ones - are becoming obsolete. The reasoning behind their argument is that they do not guarantee protection nor the flexibility for a modern industrial plant adopting technologies such as cloud, edge computing and increasingly connected services. These solutions collect, process, and send vast amounts of data even at level 1 directly to the cloud bypassing the hierarchical data flows of the Purdue model. To address these challenges, the researchers propose a zero-trust-based approach. (Zanasi et al., 2022.)

On the other hand, Stouffer et al., (2023) state in NIST SP 800-82 that the application of zero-trust architecture (ZTA) in OT environment is not straightforward. Single solutions for ZTA can be hard to find which creates a need for using multiple technologies with varying levels of maturity. The migration of an existing environment may also require more investments in the form of time, resources, and technical ability. Furthermore, the devices in the lower levels of Purdue-model might not support the required technologies or protocols, and shared credentials may impact the ability to fully implement the architecture. Instead, applying ZTA on higher levels might be feasible, but the potential impact on operations and safety should be kept in mind. (Stouffer et al., 2023, pp. 75 – 76.)

However, Zanasi et al. (2022) summarize their research effort by stating that the results from a working prototype that implementing such solution is doable in industrial setting "to increase the security and flexibility of the system while providing complete visibility over the entire network." (Zanasi et al., 2022). Furthermore, the research effort of Køien (2021) was also reviewed as a part of the literature review. His study provided 12 zero trust principles for legacy components especially with ICS in mind (Køien, 2021). Hence, the topic might very well raise its head in the future.

At the end of this section is worth reminding that complete protection against cyberattacks is impossible to achieve (Padée et al., 2019, p. 4) and no single solution can on its own address the cyberthreats against OT environments (Sangkhro & Agrawal, 2023, p. 4; DHS 2016, p. 2). There are no one-size-fits-all approaches either. Therefore, each organization must make these decisions based on their own operating environment and by considering various factors such as managed assets, culture, finances, risk appetite, work force, and their current cybersecurity posture (Boeding et al., 2022, p. 2). Applying the same level of security for all components in OT network is not considered practical either nor necessary. Different areas require different acceptable levels of security (Jiang et al., 2018, p. 1).

3.2.4 Understanding the Threat

Cyberattacks affecting OT might be targeted or indirect. Indirect attacks affect OT environments as a byproduct, whereas target attacks specifically target the OT systems (Koay et al., 2023, pp. 7 -8; Hemsley & Fisher, 2018, p. 5). The cyberthreat towards an OT system manifests through a malicious actor with an intent, capability, and /or opportunity to affect the system through the organizations personnel, operations and / or technology (DHS, 2016, p. 2).

Possible attack paths include, for example exploiting OT devices connected to the Internet or using hijacked or stolen remote access credentials. Without direct access to OT devices, an adversary may exploit other accessible network connected devices and move laterally towards the OT environment or use infected mobile media such as USB-memories (DHS, 2016, p. 3). When describing typical industrial attack Anton et al. (2021) adapt Langner's (2013) explanation claiming that they consist of three stages:

(1) "Breaking in and propagating".
(2) "Moving laterally to and manipulating".
(3) "Damaging physical devices".

In a typical scenario, the first stage involves an adversary exploiting either internet-facing resources, or resources reachable from the intranet on the IT-layer. From there, the adversary needs to be able to move to the ICS-layer, where the industrial process is controlled or monitored. At this stage, the adversary can maliciously influence the OT devices, or perform espionage and theft of intellectual property. The physical impact will materialize on the third stage, where the actions in the digital domain will transform into actions in the physical domain. (Langner, 2013, p. 4; Anton et al., 2021, p. 3.)

Among other, more general negative effects, potential impacts of an attack to OT system could be environmental damage, loss of human lives, and breakup of costly, hard-to-replace equipment (Stouffer et al., 2023, p. 2). Furthermore, as Boeding et al. (2022) explain, failure of certain OT systems may have cascading effects throughout society as is the case with power grids (Boeding et al., 2022, p. 7).

Malicious activities leading to such outcomes vary. Examples include interference of safety system operations, denial-of-service of OT network, unauthorized changes to instructions, commands, or alarm thresholds, modified software or configurations, and inaccurate information sent to system operators. (Stouffer et al., 2023, p. 2.)

The actors that are seen to pose a rising risk for OT environments according to Ocaka et al. (2022) are nation-states, organized criminal groups, and hacktivists (Ocaka et al., 2022, p. 7). Stouffer et al. (2023) supplement the list by including terrorist organizations and generally malicious intruders (Stouffer et al., 2023, p. 2). In addition to external threats, both Stouffer et al. (2023) and Miller et al. (2021) mention internal individuals as potential threat actors. While the insider threat may be deliberate, for example in a case of disgruntled employee, human error, and failure to follow given policies and procedures can also materialize the damage caused by internal stakeholders. (Miller et al., 2021; Stouffer et al., 2023, p. 2.)

Whereas the cyberthreat has become more relevant in OT environments, the threat is by no means new. Both Miller et al. (2021) and Hemsley & Fisher (2018) have analyzed OT related cybersecurity incidents based on publicly available sources. Miller et al. introduce over 40 incidents between the years 1988 and 2020, whereas Hemsley & Fisher summarize 22 incidents that have occurred between 2000 and 2017 (Miller et al., 2021; Hemsley & Fisher, 2018). The following four paragraphs provide summaries of the key findings of both research efforts.

From the lessons-learned-perspective, Hemsley & Fisher (2018) propose a few key findings. Firstly, a well-financed and technically capable threat actor is likely able to attack any system it desires. Still, while protecting all systems is impossible, developing the capability to detect and recover from cyberattacks is important as simple techniques can also get the job done. In addition, organizations should pay attention to the first steps of the attack chain where threat actors are performing reconnaissance to gather as much information as is needed to fulfill their goal. (Hemsley & Fisher, 2018, p. 27.)

Hemsley and Fisher (2018) also claim that nation state adversaries are actively developing capabilities to attack critical infrastructure. They summarize the research effort by stating that the technical capabilities of the adversaries have evolved significantly, and the threat actors are willing to cause physical damage (Hemsley & Fisher, 2018, p. 27). Miller et al. (2021) came to a similar conclusion, noting that in their timeline, the year 2009 marks a clear transition (Miller et al., 2021, p. 10).

Prior to 2009, 13 out of 20 incidents were conducted by external or internal individuals, whereas between the years 2009 and 2020, 15 of the 23 attacks were either confirmed or allegedly conducted by nation states or organized groups. This shift is also visible in the motivation behind the attacks. Whereas many individuals have carried out attacks for personal reasons, such as financial gain or as a method of retribution, the motivations of organized groups were mostly political. (Miller et al., 2021, p. 10.)

Furthermore, Miller et al. (2021) present two clear trends derived from the observed attacks between the years 1988 and 2020. Firstly, attacks conducted by a single individual with limited skills and resources are increasingly difficult. The increased complexity of the systems, security awareness and commonly implemented security strategies have resulted in less incidents through simple attack vectors. On the other hand, increased interconnectivity and complexity of modern OT systems have increased the attack surface that can be exploited by groups equipped with better resources. Hence, organized threat capabilities, often provided by extensive resources through nation-state funding, have increased. (Miller et al., 2021.)

3.3 MITRE ATT&CK

Employing adversary models can help security professionals to better understand adversary objectives, tactics, and behavior. This understanding aids organizations in taking appropriate steps to remediate vulnerabilities in their systems (Naik et al., 2022, p. 1). MITRE ATT&CK has been described as a today's de facto framework to structure threat actors' tactics and techniques (Villalón-Huerta, Ripoll-Ripoll & Marco-Gisbert, 2021, p. 3) and has been used for various purposes in areas related to cyber-defense (Georgiadou et al., 2021, p. 2).

Strom et al. (2020) position MITRE ATT&CK as a mid-level adversary model. By contrast, low-level models such as exploit and vulnerability databases describe specific instances of exploitable software but lack the context of how these are used and by whom. Furthermore, such data sources do not consider how legitimate software can be used for malicious purposes. On the other end of the spectrum, high-level models, such as Lockheed Martin Cyber Kill Chain® (Lockheed Martin, 2023), describe high-level processes and the goals of an adversary, but miss the specifics. These include for example actions that an adversary makes, how the actions relate to one another, and how the actions correlate with defenses (Strom et al., 2020, pp. 22 - 23).

A mid-level model helps in putting the concepts of lower-level models in context by explaining - to a degree - how these can be used to achieve a goal. Similarly, the concepts of a high-level model are broken down into more descriptive categories. This makes it possible to define and describe individual actions towards a system. Therefore, mid-level adversary models, such as MITRE ATT&CK enable more effective defensive mapping by tying some of the above-mentioned components together. (Strom et al., 2020, pp. 22 -23.)

MITRE ATT&CK is a curated and publicly available knowledge base of external adversary tactics and techniques. It describes how an adversary behaves in a network during various phases of an attack lifecycle. The framework is grounded in observed adversary behaviors. Instead of theoretical techniques, ATT&CK builds upon knowledge derived from threat intelligence reports, blogs, webinars, social media, malware samples, open-source code repositories and conference presentations. (Maynard & McLaughlin, 2020, p. 2; Strom et al., 2020, pp. 1 & 21.)

Tactics in MITRE ATT&CK are contextual categories representing adversary's tactical objectives. They cover standard concepts in adversaries' operations. Techniques explain how these objectives are reached or what an adversary gains by performing the action. Sub-techniques breakdown the techniques into more specific descriptions. Furthermore, ATT&CK includes documented adversary usage of techniques, their procedures, and other metadata. From this thesis perspective, one of the key aspects of MITRE ATT&CK is the mitigations it includes. Mitigations are security concepts and classes of technologies that can be employed to prevent a successful execution of a technique or subtechnique. (Strom et al., 2020, pp. 1 & 8-9.)

The first ATT&CK model was created in 2013 and was made publicly available in 2015. The original model focused on Microsoft Windows. In time it has expanded to include Linux, macOS and eventually covering entire technology-domains. (Strom et al., 2020, p. 1.)

MITRE ATT&CK is currently organized in three technology domains - Enterprise, Mobile and ICS. All matrices incorporate the above–described high-level concept (Strom et al., 2020, p. 8; MITRE 2023a, MITRE 2023b, MITRE 2023c). ATT&CK for ICS, which is employed in this thesis, was created based on the need to better understand adversary behavior in ICS domain. (Alexander, Belisle & Steele, 2020a, p. 1)

Alexander et al. (2020a) explain that the targets and actions of an adversary differ significantly between IT and OT environments. The initial attack steps against ICS could have been described through ATT&CK for Enterprise – as introduced in previous section. However, the later stages of an attack on lower levels of an OT network were not in scope. MITRE ATT&CK for ICS primarily focuses on the levels 0 – 2 of the Purdue architecture – the level that an adversary typically needs to control to cause an impact in OT environment. The ICS-matrix includes some overlap with the Enterprise one. This is because some critical OT applications, such as HMIs, are hosted on IT platforms. Nonetheless, enterprise IT is not the focus of the MITRE ATT&CK for ICS. (Alexander et al., 2020a, pp. 1 -2.)

MITRE ATT&CK is widely adopted in both industry and research (Køien, 2021, p. 3; Georgiadou et al., 2021, p. 2; Koay et al., 2023, p. 23). Strom et al. (2020, p. 3) present the following uses cases to which MITRE ATT&CK for Enterprise can be applied to:

(1) adversary emulation
(2) red teaming
(3) behavioral analytics development
(4) defensive gap assessment
(5) SOC maturity assessment
(6) cyberthreat intelligence enrichment.

Furthermore, Alexander et al. (2020a, pp. 4 -5) explain that the ICS expansions extends the use cases to:

(7) failure scenario development
(8) educational resource.

Out of these use cases, this thesis primarily focuses on defensive gap assessment.

In the industry, well-known cybersecurity companies such as CrowdStrike, Darktrace, Dragos and Microsoft have integrated MITRE ATT&CK mapping as a part of their detection tools (CrowdStrike, 2018; Darktrace, 2023; Dragos 2023; Microsoft, 2023a). Similarly, in academia, finding research employing ATT&CK is common.

Prior literature in the domain of OT security employing MITRE ATT&CK was searched as a part of this literature review. Typical use case for ATT&CK has been threat hunting, threat evaluation, threat intelligence and threat modelling (Sen et al., 2022; Arafune et al., 2022; Rencelj Ling & Ekstedt, 2023a; Zhang et al., 2022; Jadidi & Lu, 2021; Firoozjaei et al., 2022). However, the framework has also served in creating educational game (Luh et al., 2022) and guidance (de Peralta et al., 2021). Another common use case for MITRE ATT&CK has been supplementing risk assessments (Gourisetti et al., 2022; Lee et al., 2023; Oruc et al., 2022) and the measuring capabilities of proposed artifacts (Havlena et al., 2023; Mashima, 2022). Rather obvious use-case is also attack analysis (Mohammed et al., 2023; Miller et al., 2021; Jo et al., 2022; Simola, Pöyhönen & Lehto, 2023; Rencelj Ling & Ekstedt, 2023b). Some researchers have mapped attack data collected from honeypots against ATT&CK (Nursidiq & Lim, 2022; Izzuddin & Lim, 2022) while other have used the knowledge for creating attack methods for testing purposes (Toker et al., 2021; Ayub, Yoo & Ahmed, 2021). Finally, some have even focused their effort on complementing the MITRE ATT&CK framework (Maynard & McLaughlin, 2020; Villalón-Huerta et al., 2021).

3.4 Prior Research

Whereas cybersecurity processes have become a necessity in OT environments (Toker et al., 2021, p. 1), the increased number of cyberattacks targeted at critical infrastructure and OT environments have increased the OT security focused research (Mohammed et al., 2023, p. 1). The purpose of this section is to summarize relevant prior research examined as a part of this thesis. While the previous section already introduced the research employing MITRE ATT&CK, this section aims to extend the coverage by summarizing other research efforts regarding OT security, OT security controls and assessments.

In summary, the findings indicate that the area of research is relatively novel. While few of the reviewed articles dated to the midst and late 2010s, the majority were published during 2020s. The themes of the reviewed articles included some variation.

Multiple research efforts focused cybersecurity threats, controls and / or guidance. Some of such research focused on a specific sector. Boeding et al. (2022) paid specific attention to North American energy sector (Boeding et al., 2022), Rajaram et al. (2022) propose guidelines to enhance cyber hygiene of vessels (Rajaram et al., 2022). While Padée et al. (2019) summarize past research on OT security and outlines good practices for securing OT networks, their paper also introduces how nuclear industry related standards may aid in securing other industries employing OT systems (Padée et al., 2019).

Sangkhro & Agrawal (2023) took a more general approach by presenting an overview of ICS architectures and their components, evolution of attacks targeted to such systems as well as various cybersecurity solutions and their effectiveness. Finally, they point out future challenges and research areas from ICS security perspective (Sangkhro & Agrawal, 2023). Ara (2022) focus on the state of IT and OT security in SCADA systems and provides security recommendations (Ara, 2022), whereas Rahman et al. (2023) review current taxonomical classifications in manufacturing cybersecurity. Based on the review, they propose a novel meta-taxonomy for smart manufacturing cybersecurity. Furthermore, they introduce use-cases for attack taxonomies related to assessing cybersecurity threats and associated risks as well as mitigation strategies (Rahman et al., 2023).

Some of the prior research included the creation of an artifact. Hollerer et al. (2021) propose a threat modelling technique for OT environments that combines Common Vulnerability Scoring System (CVSS), Security Level (SL) from IEC 62443 and Safety Integrity Level (SIL) from IEC 61508 (Hollerer et al., 2021).

Mosteiro-Sanchez et al. (2020) analyze what they claim to be the most relevant security strategies in Industry 4.0, paying particular attention to defense-in-depth. Furthermore, they present an end-to-end encryption algorithm for industrial environment (Mosteiro-Sanchez et al., 2020). Lastly, Zanasi et al. (2022) propose a zero-trust architecture tailored for industrial setting and validate its security capabilities by simulating a realistic attack scenario (Zanasi et al., 2022).

A few technical assessments were also conducted. Jiang et al. (2018) study industrial demilitarized zones and assess network performance with and without it (Jiang et al., 2018). Anton et al. (2021) employ Shodan and vulnerability databases to search PLCs exposed to Internet and to map known vulnerabilities to them (Anton et al., 2021).

In addition to control-specific assessments, researchers have focused on assessing existing OT security standards and guidelines. Knowles et al. (2015) present an extensive survey of cybersecurity management in ICS-environments based on standards, guidelines and best practices (Knowles et al., 2015). Ocaka et al. (2022) examines IEC 62443, NIST SP 800-82 Guide to ICS Security, NERC CIP Standards, CISA Recommended Practices and MITRE ATT&CK for ICS, existing threats and vulnerabilities, and proposes security measures for protecting OT environments (Ocaka et al., 2022). Wagner et al. (2020) studied the applicability of OT security standards – namely, IEC 62443 NIST SP 800-82 VDI/VDE 2182 - from the perspective of small & medium-sized (SME) and large manufacturing organizations (Wagner et al., 2020). Staves et al. (2023) propose a model for assessing OT standards and guidelines and evaluate NIST CSF, IEC 62443, NIST SP 800-82, ISO/IEC 27019, NCSC CAF, ONR SyAPs, and ERC CIP against the criteria (Staves et al., 2023).

Finally, to conclude the literature review, two articles are highlighted. While the domain of the prior-mentioned research introduced both in this chapter and the previous one is the same as this thesis', similar research has not been conducted from the best of the author's knowledge. However, the research effort of Bartusiak et al. (2023) and Georgiadou et al. (2021) come close.

Bartusiak et al. (2023) propose a partially automated cybersecurity assessment approach for critical infrastructure. The purpose of the assessment is to identify the implementation level of cybersecurity controls derived from a selected security standard. The assessment is conducted as an extended gap analysis. At the highest level, the phases include identifying an organization's current state, defining the target state, and highlighting the existing gaps by comparing the two. The extended part refers to using multiple standards and guidelines instead of one as the baseline for the assessment. (Bartusiak et al., 2023.)

In their approach, the requirements derived from the standards and guidelines are grouped in multiple domains – such as device security, network security, and physical security. The process of matching security controls with corresponding device features can be automated by using keyword search and classification. The approach is suggested to be suitable for initial in-depth security reviews. (Bartusiak et al., 2023, p. 10.)

Therefore, the research effort of Bartusiak et al. is closely related to the topic of this thesis. At high-level, it incorporates a gap analysis to identify potential shortcomings in the organization's defense and includes an OT-perspective. However, both the approach and the scope of the assessment differs from the one proposed in this thesis. The assessment approach of Bartusiak et al. focuses on the implementation of controls whereas this thesis looks at the gaps at a programmatic level. This difference is well-visible in the results obtained in the practical test conducted by Bartusiak et al., which include findings such inconsistent documentation as well as insufficient firewall and device configuration (Bartusiak et al., 2023, pp. 9 - 10).

While Bartusiak et al. use existing standards and guidelines as the baseline for the assessment of, MITRE ATT&CK for ICS is not employed. This is not the case with Georgiadou et al. (2021). Their approach combines Cyber-Security Culture Framework and MITRE ATT&CK for Enterprise and ICS mitigations in a way which enables Cyber-Security Culture Framework to be used to assess the implementation status of the mitigations (Georgiadou et al., 2021).

Cyber-Security Culture Framework introduced by Georgiadou et al. (2020) is an evaluation and assessment methodology that can be used to assess both the individuals' as well as organizations' security culture readiness. The framework has been created with critical infrastructure in mind, with specific focus on energy sector (Georgiadou et al., 2020; Georgiadou et al., 2021, p. 4).

Hence, the artifact introduced provides very similar results as the one introduced in this thesis. Among other shortcomings, it reveals security gaps from MITRE ATT&CK mitigations perspective (Georgiadou et al., 2021, p. 11). However, the proposed assessment approach is different. The assessment methodology of Georgiadou et al. (2021) is based on a prior created assessment framework. Furthermore, the scope of the assessment takes a wider look at the whole organization by focusing on both MITRE ATT&CK for Enterprise and ICS in addition to the factors derived from the Cyber-Security Culture Framework. Therefore, the key differences between the research effort of Georgiadou et al. and the in this thesis is the assessment methodology and scope.

It can be well argued that the overarching approach proposed by Georgiadou et al. is the "way to go". As explained by Jadidi & Lu (2021) and Alexander et al. (2020b) the Enterprise and ICS matrices supplement each other ICS enabling organizations to assess adversary behavior in the organization's entire network (Jadidi & Lu, 2021, p. 5; Alexander et al., 2020b). Theoretical boundaries of IT and OT do not stop threat actors from moving across the two (Alexander et al., 2020b). The lighter approach proposed in this thesis is justified due to its scope as we further elaborate in section 4.1.

3.5 Summary of the Literature Review

The literature review summarized in this section had two purposes. Firstly, the first two sections introduced the two key concepts discussed throughout this thesis – OT and OT security. The two latter introduced relevant prior research around the area of this research effort.

The topic is in general rather novel based on the dates of the publications reviewed. While the domain of OT security is by no means new, most of the prior literature reviewed has been published after the year 2020. The amount of recently published literature can be interpreted to speak for the growing relevancy of the topic.

Sections 3.1 and 3.2 introduced OT and OT security in general. The sections also advocate for the importance of this research effort. Securing OT environments is highly relevant as modern societies are increasingly relying on such solutions. Cyberattacks on systems which not only support physical processes but among other operations - critical infrastructure - can at worse lead to catastrophic consequences. At the same time, both the history and recent evolution of OT has made the systems more vulnerable against cybersecurity related threats. Therefore, the creation of solutions supporting protection of such systems is arguably valuable. Furthermore, the sections provided valuable considerations to guide the objectives of the solution addressed in the next chapter.

Section 3.3 focused on MITRE ATT&CK for ICS. The matrix has been used to support lots of different types of OT security related research. The finding indicates that the matrix is commonly seen as mature. Along with the design philosophy, proposed use cases and practical implementations of the matrix, it argues for the applicability of MITRE ATT&CK for ICS in this thesis.

Section 3.4 introduced relevant prior research. Identical research efforts were not found. However, we paid special attention to two closely related ones. The introduction of both highlighted the differences between the two and this thesis to justify the novelty of the artifact proposed in next chapter. However, it is worth noting that existing prior research close to the topic of this thesis can also be viewed as encouraging. In part, it speaks for the relevancy of the effort.

4 DESIGN AND DEVELOPMENT

This chapter focuses on the second and third phase of the Design Science Research Model proposed by Peffers et al. (2007). During the second phase - "Define Objectives of a Solution" - the researcher is assumed to define the quantitative or qualitative objectives for the proposed solution (Peffers et al., 2007, p. 12). Section 4.1 will introduce the objectives of the solution proposed in this thesis. Once the objectives for the solution are defined, the Design Science Research Model moves to "Design and Development". The phase includes activities such as designing the artifacts functionality and architecture as well as creating it (Peffers et al., 2007, p. 12). This process is introduced in section 4.2. Lastly, section 4.3 will introduce the final artifact.

4.1 Objectives of the Solution

The artifact proposed in this thesis is referred to as "Evaluation Tool". It is used for assessing the coverage of an organization's OT security policy. As explained in introduction, organizations may have various security policies at several levels ranging from corporate policies to specific operational constraints (Stouffer et al. 2023, p. 167). In the context of this thesis, OT security policy is understood as a collection of the policies defining the countermeasures an organization has implemented or plans to implement for safeguarding its OT environment. In the literature review, creation of such policy was associated with the first layer of the defense-in-depth approach.

The knowledge base of the Evaluation Tool is derived from the mitigations identified in MITRE ATT&CK for ICS. MITRE ATT&CK for ICS v13 was the current version at the time of creating the artifact and was thus employed (MITRE 2023d). The mitigations in MITRE ATT&CK are understood as security concepts and classes of technologies that can be employed to prevent a successful execution of a technique or sub-technique of an adversary.

As mentioned in the literature review, an adversary model such as MITRE ATT&CK aids organizations to better understand adversary objectives, tactics, and behaviors. Therefore, using the mitigations derived from MITRE ATT&CK for ICS as the knowledge base was believed to provide added value through equipping organizations to better understand how the defensive measures relate to actual adversary behavior.

The objectives of the solution were defined based on the knowledge acquired through the literature review, in cooperation with the case-company. The objectives were:

(1) The tool can be used for assessing coverage of an OT security policy.
(2) The tool is designed specifically for OT environments.
(3) The tool should be relatively lightweight, and its usage should be intuitive.
(4) The tool should be modifiable.
(5) The results of the assessment conducted with the tool should be easily interpreted.
(6) The results of the assessment conducted with the tool should be visualizable.
(7) The results of the assessment conducted with the tool should provide enough information so that justified plans for further improvement can be made.
(8) The tool should support monitoring of development.

These objectives reflect the general needs that can be assumed such a tool has. The first and second objectives are in line with the scope of the assessment. Furthermore, as mentioned in the literature review, OT environments differ from their IT counterparts. Solutions created from IT security perspective might be unsuitable or imperfect for OT. Thus, the Evaluation Tool is created specifically with OT in mind. Using MITRE ATT&CK for ICS is well justified from this perspective as well.

The third and fourth objective seeks to make the Tool applicable for organizations of all shapes and sizes. The fourth objective also addresses a key consideration of Strom et al. (2020) regarding MITRE ATT&CK. It should not be viewed as a checklist of all the things an organization should address. Covering every aspect is not possible, or even relevant (Strom et al., 2020, pp. 4 – 5). Therefore, an organization performing the assessment should be able to modify the knowledge base according to organization-specific needs.

The fifth, sixth, seventh, and eighth objective aim to create a tool that does not only point out potential shortcomings. It should help organizations to understand them in context and aid in planning how the current situation could be improved. The solution should be viewed as a tool or model used to support organizations in enhancing their defenses, not to demonstrate compliance.

In addition, while the limitations of the Evaluation Tool are further discussed in chapter 6, we point out a few limitations based on the decisions made during the design phase. Firstly, the scope of this thesis is OT security. Therefore, the artifact is based on the knowledge derived only from MITRE ATT&CK for ICS, not from the other matrices.

Likewise, MITRE ATT&CK for ICS matrix is the only source of information embedded in the Tool. There are plenty of other potential references that could be used for creating an evaluation criterion, or that could supplement the proposed one. Many of those are mentioned in section 3.2. For example, NIST SP 800-82 includes a vast amount of information regarding mitigations and has been a valuable source throughout this thesis. However, the adversary-perspective of MITRE ATT&CK for ICS made it the most interesting from the author's point of view and thus, was proposed as the knowledge base. Furthermore, as stated in introduction, this thesis aims to assess how well the MITRE ATT&CK for ICS matrix serves the above-elaborated purpose. For this purpose, it has been decided that the Evaluation Tool is created purely based on the information derived from ATT&CK for ICS.

4.2 Development Process

The outcomes of the initial phases of the overall design process have been introduced in the prior chapters. The process began from problem identification and solution proposal introduced in introduction. The problem was identified in cooperation with the case-company. Once a potential solution was identified it was proposed to the case-company and to the supervisor of this thesis. After the proposed solution was approved, a more specific design process was initiated. The first step was a thorough familiarization with the chosen research methodology, MITRE ATT&CK for ICS and relevant prior literature.

The prior section summarizes the outcomes of the phase that followed. Once the objectives of the solution were approved, a first draft version of the Evaluation Tool was created and introduced to the case-company. The Evaluation Tool was built in Microsoft Excel (Microsoft 2023b).

Initially, the Evaluation Tool consisted only of "Evaluation Criteria". Its purpose is to serve as the worksheet for each assessment conducted with the Tool. It includes a group of rows for each of the 52 mitigations included in MITRE ATT&CK for ICS and columns including relevant information about the mitigation, its status, and free space for notes.

The Evaluation Criteria was approved as such. Yet, it did not address the need for visualizing the results. The case-company proposed that the results of an assessment should be visualized in a way that the essence of MITRE ATT&CK for ICS remains. In practice, this meant that mitigations could be easily associated with the techniques they address, and the techniques can be associated with related tactics. Therefore, the Tool needed to be extended.

Microsoft Power BI was proposed for visualizing the assessment results (Microsoft 2023c). However, this approach required a separate database. As illustrated below, in MITRE ATT&CK for ICS, each mitigation can be associated with multiple techniques which can be further associated with multiple tactics (figure 5).

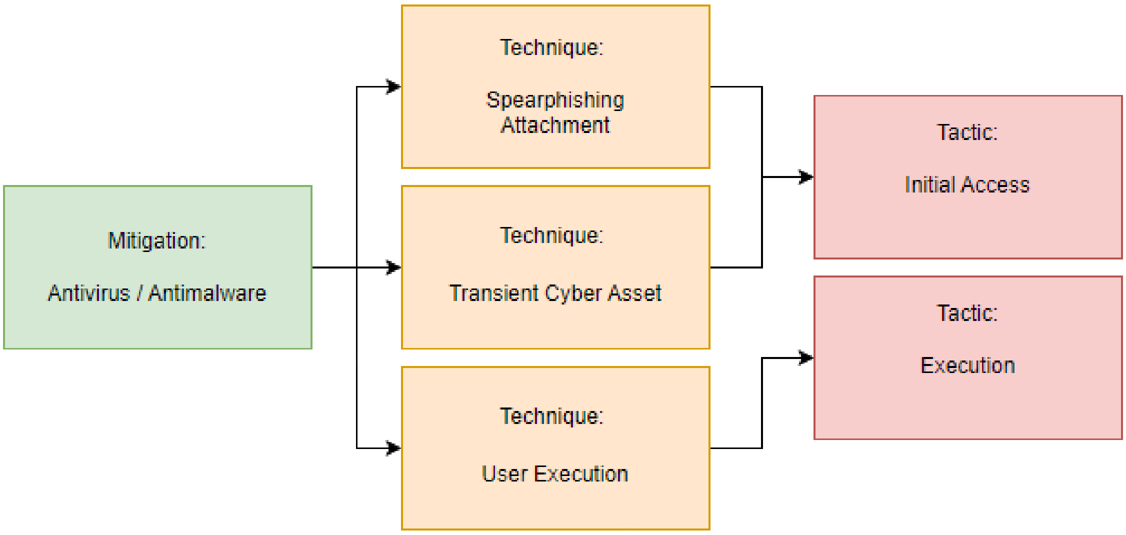


Figure 5: Relationship between mitigations, techniques, and tactics

The above-figure illustrates the relationship between “Antivirus / Antimalware”-mitigation and the associated techniques and tactics. The database needed to have a row for each relationship to enable the visualization. The above example could be stored in the database as seen below (table 3).

Table 3: Relationships of "Antivirus / Antimalware"

Tactic	**Technique**	**Mitigation**
Initial Access	Spearphishing Attachment	Antivirus/Antimalware
Initial Access	Transient Cyber Asset	Antivirus/Antimalware
Execution	User Execution	Antivirus/Antimalware

After the iteration, a new demo version of the Evaluation Tool including the Evaluation Criteria and the “Database” like the one in table 3 was made. Moreover, the version was extended to include examples of potential ways to visualize the assessment data.

The latest version was reviewed with the case-company. The early versions of the visualization were deemed promising, and therefore the Evaluation Tool was determined to suit the needs of the case-company. However, it was decided that the visualizations would be further enhanced once the actual assessment was done.

The below-figure illustrates an abstraction of the final version of the Evaluation Tool. It consists of two Excel sheets. All information included in both sheets is derived from MITRE ATT&CK for ICS version 13. The results of an assessment can be visualized with Power BI (figure 6).

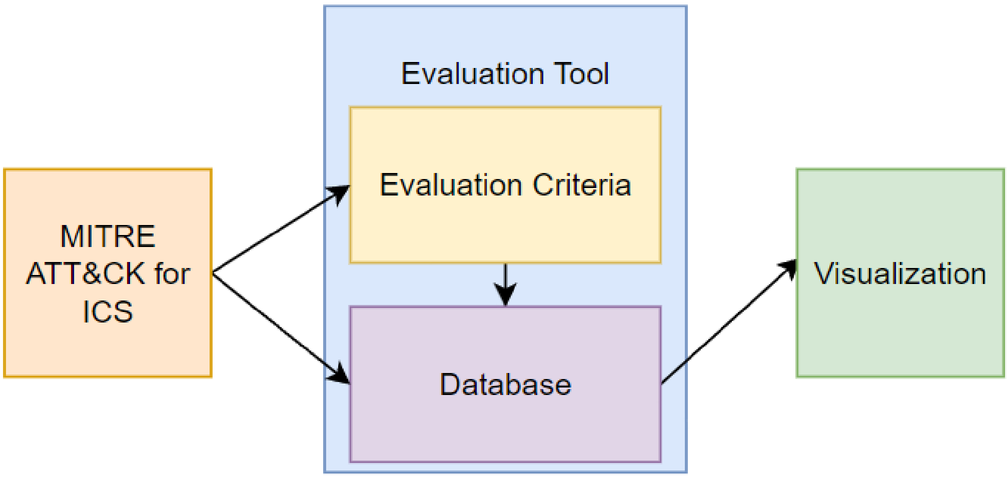


Figure 6: Abstraction of the Evaluation Tool

Upon approval, the demo version of the Evaluation Tool consisting of four mitigations was extended to include all 52 mitigations. For this purpose, the "ATT&CK in Excel"-version of MITRE ATT&CK for ICS was deemed useful (MITRE 2023e). Despite using a ready-made Excel data set, the creation of the tool required surprisingly much manual labor. As will be seen in the next section, the ready-made Excel-format of ATT&CK differs significantly from the format of the Evaluation Tool.

4.3 Evaluation Tool

Due to its simplicity, the Evaluation Criteria part of the Evaluation Tool[4] has remained relatively similar throughout the design process. It is an Excel-sheet including one group of rows for each mitigation as can be seen from the below figure (figure 7).

4 The final version of the Evaluation Tool has been published at https://github.com/onn13/evaluation_tool/

ID	Name	Description	Associated Techniques	Associated Tactics	Status	Notes
M0801	Access Management	Access Management technologies can be used to enforce authorization polices and decisions, especially when existing field devices do not provided sufficient capabilities to support user identification and authentication. (Citation: McCarthy, J et al. July 2018) These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials. (Citation: Centre for the Protection of National Infrastructure November 2010)	Activate Firmware Update Mode Change Operating Mode Default Credentials Detect Operating Mode Device Restart/Shutdown Execution through API Hardcoded Credentials Modify Alarm Settings Module Firmware Point & Tag Identification Program Download Program Upload Remote Services System Firmware Valid Accounts	Collection Evasion Execution Impair Process Control Inhibit Response Function Initial Access Lateral Movement Persistence		
M0936	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.	External Remote Services Valid Accounts	Initial Access Lateral Movement Persistence		
M0915	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use security identifier (SID) Filtering, etc.	Valid Accounts	Lateral Movement Persistence		

Figure 7: Evaluation Criteria

The above figure includes the first three mitigations in alphabetical order. As mentioned in the previous section the Evaluation Criteria is used for the assessment. Thus, the sheet includes fields that were deemed necessary to support such an effort. To keep the tool lightweight and easy to use, it does not include detailed information about the techniques and tactics. Rather, further information is made easily accessible through hyperlinks that lead to MITRE's descriptions.

In addition to the mitigation-related information, the Evaluation Criteria includes two fields for the assessment. "Notes" is a free space reserved for mitigation related comments. "Status" is used to indicate how the mitigation has been addressed in an organization's OT security policy. The alternative options indicated by colors in the above figure are "Addressed" (green), "Partially Addressed" (yellow), and "Not Addressed" (red). Whereas "Addressed" and "Not Addressed" are obvious choices, "Partially Addressed" was included to represent situations where the mitigation is not completely addressed, but some parts of it have clearly been included.

In addition to the Evaluation Criteria, the Tool includes a separate Database-sheet. It is used to store the assessment data in a format which can be used to visualize the results with Power BI. As can be seen below, the fields used in the Database are mostly like the ones in the Evaluation Criteria (figure 8).

Tactic	Technique	Mitigation	Status	Description
Initial Access	Remote Services	Access Management		Access Management technologies can help enforce authentication on critical remote service, examples include, but are not limited to, device management services (e.g., telnet, SSH), data access servers (e.g., HTTP, Historians), and HMI sessions (e.g., RDP, VNC).
Execution	Change Operating Mode	Access Management		Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs. Centralized authentication techniques can help manage the large number of field controller accounts needed across the ICS.
Execution	Execution through API	Access Management		Access Management technologies can be used to enforce authorization policies and decisions, especially when existing field devices do not provide capabilities to support user identification and authentication. [2] These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials.
Persistence	Hardcoded Credentials	Access Management		Ensure embedded controls and network devices are protected through access management, as these devices often have unknown hardcoded accounts which could be used to gain unauthorized access.
Persistence	Module Firmware	Access Management		All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.
Persistence	System Firmware	Access Management		All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.
Persistence	Valid Accounts	Access Management		Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs. Centralized authentication techniques can help manage the large number of field controller accounts needed across the ICS.

Figure 8: Database

The "Status"-fields are linked to a corresponding field in the Evaluation Criteria-sheet. Therefore, the value of the status field in the "Database" will be updated based on the value of the "Status"-field in the "Evaluation Criteria"-sheet. Hence, while the "Database" contains 396 rows representing all mitigations and their associations with the corresponding techniques and tactics, this sheet does not need to be manually modified.

Furthermore, it should be noted that the information in "Description"-field in the Database-sheet may differ from the corresponding field in the Evaluation Criteria-sheet. This is because the overall description of a mitigation can be slightly different than the description provided for the mitigation in the context of a technique. Examples of the "Antivirus /Antimalware"-mitigation descriptions can be seen from the below table (table 4).

Table 4: Antivirus/Antimalware-mitigation descriptions

Context	Description
General description	"Use signatures or heuristics to detect malicious software. Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations. To minimize the impact to system availability, all products should first be validated within a representative test environment before deployment to production systems." (MITRE 2023f).
Spearphishing Attachment-Technique	"Deploy anti-virus on all systems that support external email." (MITRE 2023f).
Transient Cyber Asset-Technique	"Install anti-virus software on all workstation and transient assets that may have external access, such as to web, email, or remote file shares." (MITRE 2023f).
User Execution-Technique	"Ensure anti-virus solution can detect malicious files that allow user execution (e.g., Microsoft Office Macros, program installers)." (MITRE 2023f).

As the above shows, the description can change to provide technique-specific guidance related to mitigation. However, this does not apply to all cases, as can be seen from the above figure (figure 8).

All in all, it can be concluded that the Evaluation Tool as an artifact is simple, although the visualization-related needs increased its complexity. While the preferences of the author and the case-company guided the outcome of the creation process, it is worth noting that Evaluation Tool can just as well be modified to serve different needs. For example, the Evaluation Criteria layout could be different. The amount of information embedded in the sheet could be either increased or decreased, depending on the needs and preferences. The same applies to the Database. However, the format of the Database does influence the visualization-capabilities, which are further introduced in the next chapter.

5 DEMONSTRATION

The fourth phase of the Design Science Research Model proposed by Peffers et al. (2007) is "Demonstration". During the phase, the researcher should demonstrate how the artifact is used to solve one or more instances of the problem. In practice, this can be conducted for example as a simulation, case study or other appropriate activity. (Peffers et al. 2007, p. 12.)

In this thesis, the demonstration was made by using the Evaluation Tool for the purpose it was designed for. As the research effort was made in cooperation with a case-company, the Tool was used to assess the OT security policy of the case-company. Due to the sensitivity of the topic, the case-company requested all company-related material be left out of the thesis. However, an additional assessment was made to better document the process introduced in this thesis.

An additional assessment was conducted, in accordance with the spirit of the times, with the aid of ChatGPT. ChatGPT (GPT 3.5) was prompted to create an OT security program (OpenAI, 2023). The program was assessed as an additional demonstration to provide visualizations to be used in this thesis, and to provide further experience about using the Evaluation Tool. The prompt used was:

> Create a OT security program for an organization. The program should include a list of mitigations that an organization should implement to protect its OT environment. For each mitigation, include a name of the mitigation and a short description about its content. Create the program based on defense in depth approach.

In response, ChatGPT provided an OT security program consisting of 22 controls under 11 themes. The proposed OT security program is seen below (table 5).

Table 5: OT security program proposed by ChatGPT

Operational Technology (OT) Security Program
I. Access Control and Authentication
1. Role-Based Access Control (RBAC): Implement RBAC to restrict access to OT systems and components based on job roles, ensuring that only authorized personnel can perform specific tasks. **2. Multi-Factor Authentication (MFA):** Require the use of MFA for all access to OT systems, adding an extra layer of security beyond passwords.
II. Network Segmentation
3. Network Isolation: Segment the OT network from the corporate network using firewalls and VLANs, limiting the potential for lateral movement by attackers. **4. DMZ for Remote Access:** Create a Demilitarized Zone (DMZ) for remote access to the OT network, enabling secure access for authorized personnel.
III. Intrusion Detection and Prevention
5. Intrusion Detection System (IDS): Deploy IDS to monitor network traffic for suspicious activity, sending alerts when anomalies are detected. **6. Intrusion Prevention System (IPS):** Enhance security with IPS, which not only detects but can also actively block malicious traffic.
IV. Asset Inventory and Management
7. Asset Discovery: Continuously discover and inventory all OT assets to maintain an up-to-date record of hardware and software. **8. Asset Classification:** Categorize assets based on criticality, helping prioritize security efforts.
V. Patch and Vulnerability Management
9. Patch Management: Establish a process for timely patching and updating of OT devices and software. **10. Vulnerability Scanning:** Regularly scan the OT network for vulnerabilities, addressing them promptly to minimize risks.
VI. Security Monitoring and Incident Response
11. Security Information and Event Management (SIEM): Implement a SIEM system to collect, correlate, and analyze logs from OT devices for early threat detection. **12. Incident Response Plan:** Develop a comprehensive incident response plan to handle security incidents, minimizing downtime and damage.
VII. Physical Security
13. Access Control to Facilities: Restrict physical access to OT facilities and equipment, using access control systems and surveillance cameras. **14. Environmental Controls:** Implement safeguards like temperature and humidity monitoring to protect OT equipment from environmental hazards.
VIII. Security Training and Awareness
15. Employee Training: Provide security training to OT personnel, ensuring they understand their roles and responsibilities in maintaining a secure environment. **16. Phishing Awareness:** Train employees to recognize and report phishing attempts, which are a common entry point for cyberattacks.
IX. Encryption
17. Data Encryption: Encrypt sensitive data in transit and at rest within the OT environment to protect it from eavesdropping. **18. Secure Communication Protocols:** Use secure communication protocols like TLS/SSL to ensure data integrity and authenticity.
X. Vendor and Supply Chain Security
19. Supplier Assessment: Assess the security practices of third-party vendors and suppliers to prevent vulnerabilities from entering the environment through the supply chain. **20. Security Requirements in Contracts:** Include security requirements in vendor contracts to ensure their commitment to OT security.
XI. Compliance and Regulation
21. Regulatory Compliance: Stay up to date with relevant OT security regulations and ensure full compliance with legal and industry standards. **22. Auditing and Documentation:** Maintain thorough documentation of security measures and audit compliance regularly.

The table above includes all mitigation-related content provided by ChatGPT. The rest of this chapter will explain the process of the assessment conducted with the Evaluation Tool. Next section will introduce the evaluation process. Section 5.2 will provide examples of assessment result visualizations.

5.1 Assessment Process

The usage of Evaluation Tool is not tied to any strict process. The process introduced in this section is like the one that was followed in the case-company related assessment. The figure below illustrates the phases through the functionalities of the tool (figure 9).

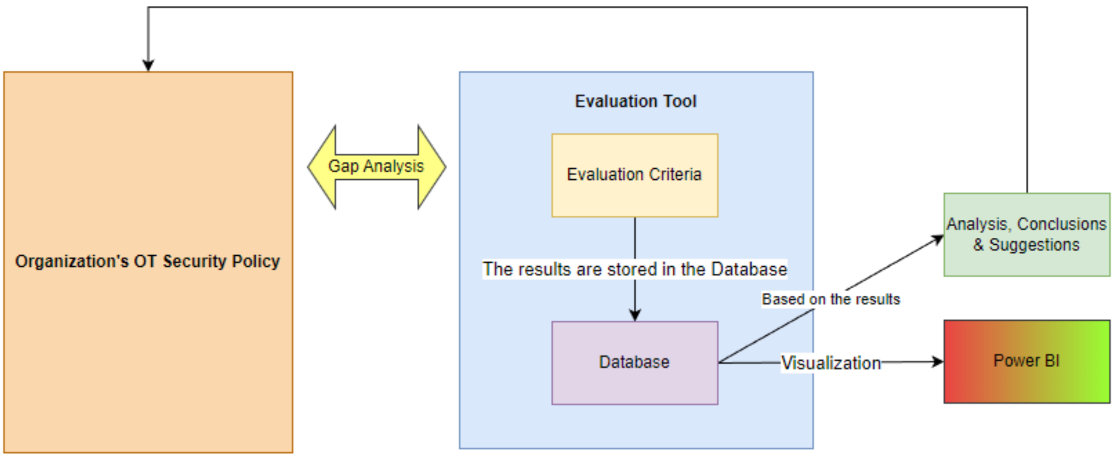


Figure 9: Evaluation process

The assessment is performed as a gap analysis, which is defined by Bartusiak et al. (2023) as a method for assessing an internal current state against corresponding external requirements to identify gaps between the two (Bartusiak, et al. 2023, p. 3). In practice, an organization's OT security policy is compared to the mitigations derived from MITRE ATT&CK for ICS that are included in the Evaluation Criteria.

An organization may choose to exclude certain mitigations from the Criteria based on organization-specific needs by, for example, marking the status of these as "Not applicable". In the proposed approach, the status of applicable mitigations is marked either as "Addressed", "Not addressed", or "Partially Addressed". However, the assessor may choose to use a different criterion if deemed necessary.

The assessment is done via the Evaluation Criteria and the results are automatically stored in the Database. If required, the results stored in the Database can be visualized. The Evaluation Tool does not include ready-made visualizations. Whereas Excel provides visualization capabilities which can be used for this purpose, tools such as Power BI can extend the capabilities. Depending on the needs of the organization, the Database can be reorganized to support different kinds of visualizations.

The most important part of the process is interpreting the results. The findings of the assessment should be analyzed and concluded. Furthermore, where feasible, suggestions on enhancing the OT security policy of an organization should be made based on the results. Upon reviewing the results, conclusions, and recommendations the organization can use the information to extend the existing policy.

The Evaluation Tool itself is easy to use. From the Tools perspective, a person or an organization using the tool should focus on understanding its content. As explained earlier, the Evaluation Criteria includes descriptions of each mitigation and the relationships of mitigations, techniques, and tactics. The technique-specific descriptions are easily available through the Database. Furthermore, the Evaluation Criteria includes hyperlinks to MITRE ATT&CK for ICS v13 for further details about each tactic and technique.

Understanding the other entity of the gap analysis is equally important. Therefore, all relevant documentation about the organization's OT security policy should be reviewed. Involving the organization's subject matter experts can help by providing information that is not documented, and aid in interpreting the documentation.

5.2 Visualizations

The visualizations introduced in this section were created with Power BI based on the demonstration assessment made against the OT security policy created by ChatGPT. Similar ones were created to visualize the results of the assessment made for the case-company. They represent examples of what can be done but are not the only feasible ones. Each assessor is encouraged to present the results based on the organization-specific needs or preferences.

In total, three Pages were created to visualize the results. The first represents the overview of the results (figure 10), the second represents the results from the tactics-perspective (figure 13), and the third from techniques-perspective (figure 14).

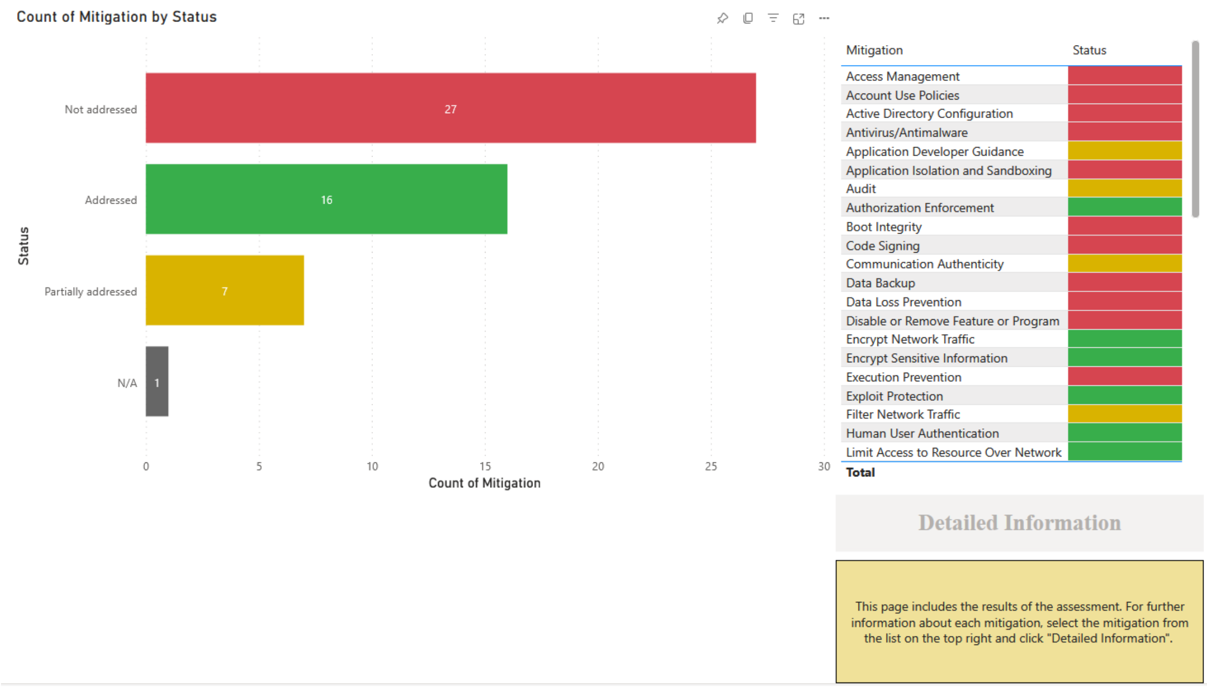


Figure 10: Overview of the results

In the example assessment, in total 51 Mitigations were assessed. The results in figure 10 show the status of each. The one Mitigation marked as N/A is “Mitigation Limited or Not Effective”, which in MITRE ATT&CK for ICS is used to highlight that a certain attack technique abuses system features and cannot therefore be effectively mitigated with preventative controls (MITRE 2023g).

For further information about each mitigation, one can select the mitigation of interest from the table on the right. This highlights its status and activates the “Detailed Information”-button on the bottom right (figure 11).

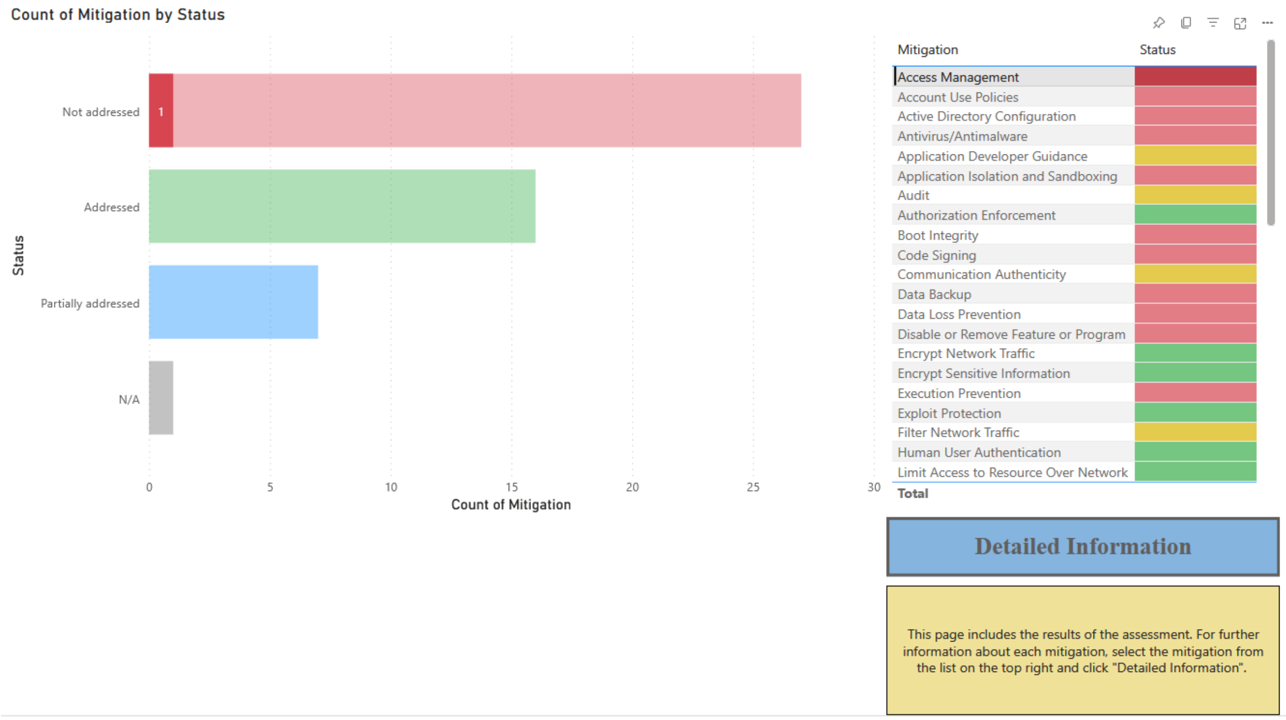


Figure 11: Overview filtered by a mitigation

Upon pressing the "Detail Information"-button, the Page-will open a drill-down view of the selected mitigation. In this case, "Access Management"-mitigation was selected for further review (figure 12).

Mitigation	Technique	Tactic	Description	Status
Access Management	Activate Firmware Update Mode	Inhibit Response Function	All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.	
Access Management	Change Operating Mode	Evasion	Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs. Centralized authentication techniques can help manage the large number of field controller accounts needed across the ICS.	
Access Management	Change Operating Mode	Execution	Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs. Centralized authentication techniques can help manage the large number of field controller accounts needed across the ICS.	
Access Management	Default Credentials	Lateral Movement	Ensure embedded controls and network devices are protected through access management, as these devices often have unknown default accounts which could be used to gain unauthorized access.	
Access Management	Detect Operating Mode	Collection	Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs. Centralized authentication techniques can help manage the large number of field controller accounts needed across the ICS.	
Access Management	Device Restart/Shutdown	Inhibit Response Function	All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.	
Access Management	Execution through API	Execution	Access Management technologies can be used to enforce authorization policies and decisions, especially when existing field devices do not provide capabilities to support user identification and authentication. [2] These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials.	
Access Management	Hardcoded Credentials	Lateral Movement	Ensure embedded controls and network devices are protected through access management, as these devices often have unknown hardcoded accounts which could be used to gain unauthorized access.	
Access Management	Hardcoded Credentials	Persistence	Ensure embedded controls and network devices are protected through access management, as these devices often have unknown hardcoded accounts which could be used to gain unauthorized access.	
Access Management	Modify Alarm Settings	Inhibit Response Function	All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all management interface access attempts, especially when the device does not inherently provide strong authentication and authorization functions.	
Access Management	Module Firmware	Impair Process Control	All devices or systems changes, including all administrative functions, should require authentication. Consider using access management technologies to enforce authorization on all	

Figure 12: Detailed information about a mitigation

The drill-down table shows in total 21 rows 11 of which are visible in the above-picture, all representing separate entries in the Database. As mentioned earlier, the Database includes an individual row for each association between the mitigation and technique(s) as well as the association between technique(s) and tactic(s). In this visualization, all possible associations were left visible, as each mitigation might have a different description in the context of each technique it addresses.

Figure 13 represents the results through tactics. The functions included on Page are mostly like the ones introduced above in figure 10 (figure 13).

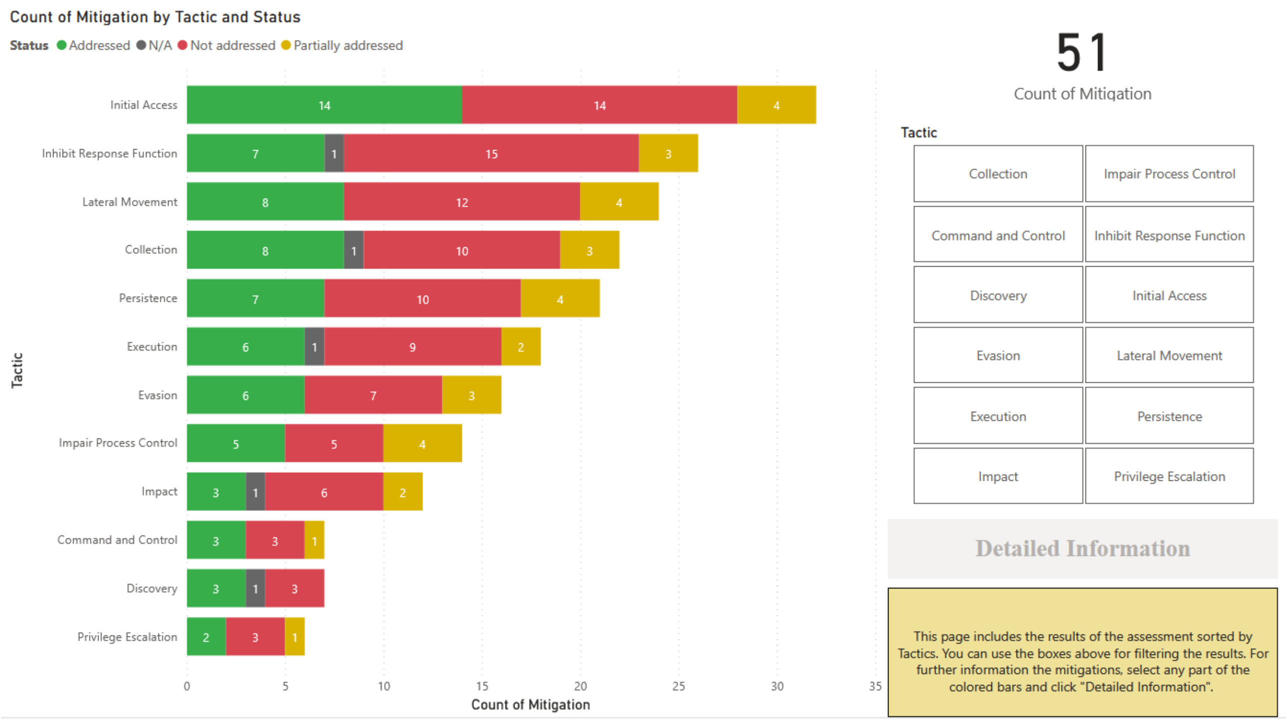


Figure 13: Results by tactics

In addition, the Page includes a list of Tactics represented as boxes that can be used to filter the results by any tactic. The same functionality has been included in the Results by Techniques-Page as dropdown menu, visible in the figure below (figure 14).

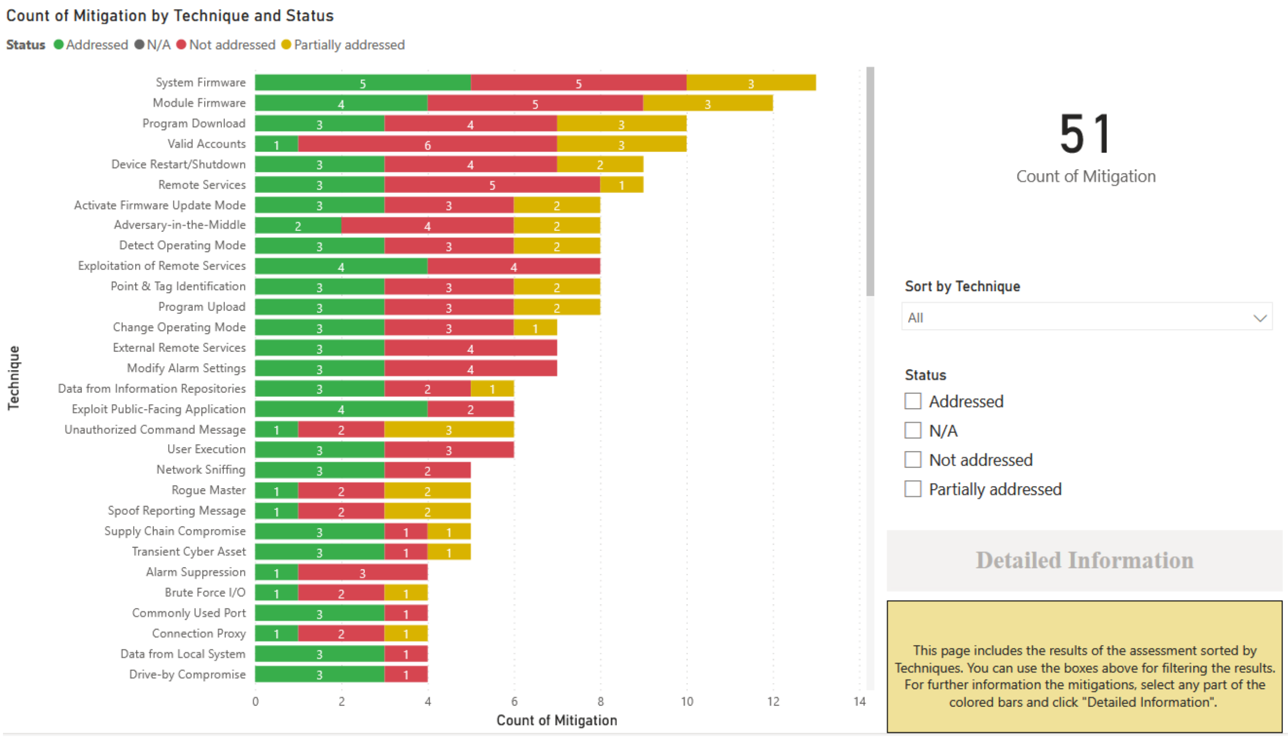


Figure 14: Results by techniques

The above-page also includes a Filter-by-Status functionality, visible above “Detailed Information”-button. Furthermore, all pages include a short introduction on the functionalities of the Page. This is seen in the bottom right corner of figures 10, 13, 14.

6 EVALUATION

The fifth phase of the Design Science Research Model proposed by Peffers et al. (2007) is "Evaluation". The phase focuses on observing and measuring the performance of the artifact. The objective of the phase is to evaluate actual results obtained in the demonstration by comparing them to the objectives of the solution. Depending on the results of the evaluation, the researcher can either iterate back to "Design and Development" or choose to leave further improvement to following projects. (Peffers et al. 2007, p. 13.)

The form of the evaluation can vary depending on the nature of the problem (Peffers et al. 2007, p. 13). In this thesis, the evaluation was conducted by comparing the results obtained through the demonstration against the objectives of the solution introduced in section 4.1. The evaluation criteria used for this purpose were initially created in parallel with defining the objectives of the solution.

The evaluation criteria reflect the objectives of the solution. In practice, each criterion aims to assess whether an objective is addressed or not. The Evaluation Tool was evaluated against the following criteria:

(1) The Evaluation Tool can be used for assessing coverage of an OT security policy.
(2) The Evaluation Tool has been designed specifically for OT environments.
(3) The Evaluation Tool is relatively lightweight.
(4) The Evaluation Tool is easy to use.
(5) The Evaluation Tool is modifiable.
(6) The results of the assessment conducted with the Evaluation Tool are easily interpreted.
(7) The results of the assessment conducted with the Evaluation Tool can be visualized.

(8) The results of the assessment conducted with the Evaluation provide enough information so that justified plans for further improvement can be made.
(9) The Evaluation Tool supports monitoring of development.

The evaluation process was divided into two phases. Firstly, two subject-matter experts of the case-company were asked to participate in an interview centered around artifact evaluation. The interview process and its results are further introduced in the next section. Secondly, the author of this thesis has kept extensive notes of thoughts, experiences and findings related to the Evaluation Tool throughout the research process. The summary of these observations in accordance with the evaluation criteria is introduced in section 6.2. The subsections are separated to help the reader to better distinguish the reflections of both parties.

6.1 Evaluation Interviews

The evaluations made by the case-company were conducted as a qualitative semi-structured interview. Quantitative interview according to Myers & Newman (2007) is "the most common and one of the most important data gathering tools in qualitative research". Unstructured and semi-structured interviews on the other hand are the types most employed in qualitative information systems research (Myers & Newman, 2007, p. 3 - 4).

Semi-structured interview centers around an incomplete script. The researcher is assumed to prepare some questions beforehand, but the interview is not strictly tied to the questions (Myers & Newman, 2007, p. 4). Therefore, semi-structured interviews built around the evaluation criteria introduced above were seen as a feasible method for gathering observations made by the case-company.

Two subject-matter experts with years of experience in cyber security related topics in the case-company were asked to participate in the process. Both interviewees were actively involved in the research effort from its early stages as the case-company's contact persons. Therefore, the interviewees were familiar with the Evaluation Tool, its development process, and the assessment conducted for the case-company.

The interviews were held on 17.11.2023 and 27.11.2023. The contact persons were interviewed separately during around one-hour sessions organized in Microsoft Teams. The evaluation criteria and pre-planned questions guiding the interview were delivered beforehand. The Evaluation Tool and the results of the assessment conducted with it were introduced to the interviewees before the meetings. Both participants also had a chance to familiarize themselves with all the material independently.

During the interview, the participants were asked to evaluate each criterion either as "Yes", "No", or "Partly". After the initial response, the participants were asked to elaborate on the given answer. Both interviews were recorded, and the interviewer – the author of this thesis – made notes throughout the session.

The information gathered during the interviews was analyzed by re-listening to the recordings, making further notes, and validating the existing ones. Finally, the key considerations were summarized. The table below includes the evaluations of the interviewees (table 6).

Table 6: Results of the evaluation

Criteria	Interviewee 1	Interviewee 2
(1) The Evaluation Tool can be used for assessing coverage of an OT security policy.	Yes	Yes
(2) The Evaluation Tool has been designed specifically for OT environments.	Yes	Yes
(3) The Evaluation Tool is relatively lightweight.	Yes	Yes
(4) The Evaluation Tool is easy to use.	Yes	Yes
(5) The Evaluation Tool is modifiable.	Yes	Yes
(6) The results of the assessment conducted with the Evaluation Tool are easily interpreted.	Yes	Partly
(7) The results of the assessment conducted with the Evaluation Tool can be visualized.	Yes	Yes
(8) The results of the assessment conducted with the Evaluation provide enough information so that justified plans for further improvement can be made.	Yes	Yes
(9) The Evaluation Tool supports monitoring of development.	Partly	Partly

The conclusions of the evaluation can be summarized by stating that the Evaluation Tool has fulfilled its design objectives well. None of the criteria was completely overlooked although two criterions were only partly addressed. The rest of this section will further elaborate on the thoughts of the interviewees by summarizing the key considerations of both.

> According to my understanding, MITRE ATT&CK for ICS is generally accepted source of information to which a current state of an organization can be compared against. From that perspective, the chosen approach is justified. (Interviewee 1)

The interviewees agreed that the Evaluation Tool is suitable for assessing an OT security policy within the boundaries of MITRE ATT&CK for ICS. The matrix itself was seen as a suitable knowledge base for the purpose. Interviewee 2 highlighted that the relationships of mitigations, techniques and tactics built in MITRE ATT&CK for ICS provide useful context and enabled valuable visualizations of the assessment results.

> The Evaluation Tool is designed specifically for OT environments, and the source material is chosen accordingly. (Interviewee 1)

The chosen knowledge base scoped the assessment specifically to OT environments. Whereas MITRE ATT&CK for ICS mostly focuses on the level 0 – 2 of the Purdue architecture, the scope was not considered to be too narrow. Rather, it is something that an organization performing the assessment should be aware of. However, Interviewee 1 noted that most of the controls were quite technical. The Evaluation Tool would be more comprehensive if the amount of governance and process related mitigations could be increased.

The scope was not considered to be too wide. Interviewee 2 underlined that the scope is mitigations in MITRE ATT&CK for ICS. If one wishes to assess the current state of an OT security policy against these mitigations, nothing should be excluded by default. An organization performing the assessment can adjust the scope if necessary.

> Yes, the Evaluation Tool is relatively lightweight. However, it includes lots of details that one should get familiar with – but that's how it should be. (Interviewee 2)

The Evaluation Tool was seen as relatively lightweight. Interviewee 2 supplemented the above citation by noting that the assessment process in which the Evaluation Tool is used can affect how lightweight or heavy it is to use. One can perform lightweight assessment and focus only on the mitigations – or, where necessary, more focus can be put on every bit of detail that the Tool includes in the form of various relationships between the mitigations, techniques, and tactics.

Interviewee 1 noted that because one mitigation can address multiple techniques, in some cases one needs to focus on how the mitigation is implemented. For example, if we look at "Antivirus/Antimalware" mitigation – while overall the mitigation might be addressed, the way it has been implemented might affect the way it addresses the techniques. The chosen solution and the way it has been configured may affect its capability to address the Techniques it can be used to mitigate. However, in the current form of the Evaluation Tool, only one status can be given to each mitigation.

> The Evaluation Tool is Excel-based, and from that perspective, yes, it is easy to use. (Interviewee 1)

Both interviewees agreed that the Evaluation Tool is easy to use. Interviewee 1 believed that the challenge is not about how to use the Tool, but rather about how easily the mitigations can be mapped against the target of the evaluation. To support this process, a certain level of automation could be beneficial. For example, a list of keywords or other metadata could be created and used to search for matches from the target of the evaluation. Found matches could be highlighted to indicate that certain mitigations might be partially or fully addressed. Yet, the assessor would be required to evaluate the findings and make the final decision about the status of each mitigation.

> The Evaluation Tool needs to be modifiable because the source material is also updated from time to time. (Interviewee 2)

The interviewees agreed that the Evaluation Tool can be modified. However, making modifications can be laborious. Interviewee 2 also noted that one should be aware of how the modifications might affect the Tool. Furthermore, as mentioned earlier, Interviewee 1 mentioned that the Evaluation Tool could benefit from adding more mitigations from other sources.

> Interpreting the results through Excel (Evaluation Tool) is easy, but it requires effort to sort them and make them visually understandable. (Interviewee 2)

According to both interviewees, the assessment results were easily interpreted through the visualizations made for the case-company. Both interviewees agreed that the visualizations could also be modified based on organization-specific needs. Whether different kinds would be needed is a matter of opinion as stated by Interviewee 2. Top management would appreciate different types of visualizations than subject-matter specialists and each organization might have different needs and preferences.

The ones proposed to the case-company were valued. Interviewee 1 felt that the visualizations were useful and helped interpreting the results. The explanation included to each Page to describe what visualization aims to show was beneficial. The assessor had put in effort on behalf of the one interpreting the results, which was appreciated. Interviewee 2 agreed that the visualizations were useful. They aided in understanding what has been addressed as well as potential shortcomings therefore clearly show the current state. Furthermore, the ability to "drill-down" to the results was useful. These features helped to form opinions on what should be improved in the future.

However, both agreed that the Evaluation Tool on its own is not visually as good as it could be for interpreting the results. The results can be interpreted from the Tool as well, but it is more laborious. Therefore, the consensus was that the Evaluation Tool could be enhanced as a standalone source of the assessment results if deemed necessary.

Both interviewees had suggestions that would make the results easier to interpret from the Evaluation Tool. Interviewee 1 suggested that the Evaluation Criteria-sheet could include filters, which were included in the Database-sheet. Interviewee 2 on the other hand mentioned that the Evaluation Tool could include high-level visualizations. Furthermore, the Evaluation Tool could include a separate sheet that would automatically filter the Mitigations that are not addressed or are partially addressed to form a sort of "task list" on which further effort should be focused on.

> The results not only showed the status of each mitigation but also aided in planning future development. (Interviewee 1)

The interviewees agreed that the Evaluation Tool served its purpose as a point-in-time assessment tool. However, it did not fully address monitoring of development. Although both mentioned that similar assessments can be repeated, and the results can be compared against each other, as such the Evaluation Tool only represents current state in certain point of time.

The results obtained through the assessment were seen useful. Some gaps were identified, and justified plans could be made based on the results. Neither interviewee felt that the results lacked anything that would have further supported such an effort. However, Interviewee 1 noted that the results are not prioritized in any way. Therefore, each organization must figure out what is meaningful for the organization. This was not seen as an issue as in general the goal should not be to address every identified gap.

Both interviewees also addressed that the results obtained also depend on the assessor and the assessment process. The Evaluation Tool is just a supporting solution. Interviewee 2 also noted that if instead of a Policy-level, an organization would like to assess the implementation of certain controls, the assessment would be more challenging – especially for large organizations with multiple sites and varying practices. Therefore, the scoping of the assessment also influences the results.

> The Evaluation Tool is easy to use, but if instructions were included, it would be very easy to use. (Interviewee 2)

Finally, Interviewee 2 pointed out that the Evaluation Tool in its form at the time did not include instructions. This was not problematic in this case because the Evaluation Tool was introduced to the case-company, but such should be included for further users. The instructions should include basic details about the tool, its scope as well as the purpose for which it has been designed and some practical examples of its usage. Furthermore, the relationship between the Evaluation Tool and Power BI could be elaborated in the instructions.

6.2 Authors Thoughts

Instead of arguing for or against the reflections of the interviewees, the author of this thesis is content with stating that based on the discussions had with the case-company contact persons, the observations made were not based on misconceptions about the Evaluation Tool. Rather, both interviewees had invested time in familiarizing themselves with the target of the evaluation and had prepared well for the interviews. The rest of this section presents the author's observations made throughout the designing, creating, and demonstrating the Tool.

The high-level evaluation introduced in table 6 is well in line with the general observations made by the author. The Evaluation Tool has for the most part addressed its design criteria. However, in its current form, it is at an early stage, and includes plenty that could be improved.

MITRE ATT&CK for ICS was a suitable knowledge base for the Evaluation Tool. The framework provides plenty of validated information that both make the Tool robust, yet relatively lightweight. Furthermore, the context provided by MITRE ATT&CK is what the author believes makes it particularly fitting. The assessor does not need to spend much time thinking about what the objective of a mitigation is. Rather, the focus can be kept on what it means for the target of the assessment.

However, for evaluating an OT security policy, MITRE ATT&CK for ICS and therefore the Evaluation Tool, is not without its limitations. The purpose of the mitigations in MITRE ATT&CK is to address how the techniques can be countered. As such, mitigations provide lots of meaningful countermeasures. Yet, both demonstrations done as a part of this thesis revealed shortcomings from MITRE ATT&CK for ICS-perspective as well. One can observe these gaps by comparing the OT security policy created by ChatGPT and the MITRE ATT&CK for ICS Mitigations.

The mitigations that the OT security policy included, but Evaluation Tool did not address were:

- Asset Discovery
- Asset Classification
- Incident Response Plan
- Regulatory Compliance

In addition, while Auditing and Documentation can be said to be partially addressed in the Evaluation Tool, the perspective of MITRE ATT&CK for ICS is different than the one proposed by ChatGPT. Similar observations were made in the assessment conducted against the OT security policy of the case-company. These findings are not addressed in this thesis.

The shortcoming can also be seen by comparing the countermeasures introduced in subsection 3.2.3 against the mitigations of MITRE ATT&CK for ICS. Organizational controls, such as risk assessments, disaster recovery and business continuity planning, incident response, or cybersecurity governance, that do not directly counter any technique are not in scope of MITRE ATT&CK for ICS. Therefore, when using the Evaluation Tool, its user should be aware of its limitations.

The Evaluation Tool is designed specifically for OT environments. Fulfilling this objective was achieved by choosing MITRE ATT&CK for ICS for the knowledge base. The decision to use MITRE ATT&CK for ICS as the only source of information was justified due to the scope of the thesis. However, it does limit the current scope of the Evaluation Tool. As addressed in section 3.3 MITRE ATT&CK for ICS mainly focuses on levels 2 – 0 of the Purdue architecture. A typical attack targeting OT would involve steps taken on the higher levels of the enterprise architecture. Therefore, an overarching approach to address also the higher layers would be more realistic. However, similarly, the target of the assessment should not be limited to OT security but should address the IT security policy as well.

The author felt that the tool was easy to use. The Evaluation Criteria is simple and made the evaluation process easy. The “Status” and “Notes”-fields used for the assessment were both employed. The information provided by the “Description”-field was essential. The “Tactics” and “Techniques”-fields were less employed – however, this depends on the assessor.

The Database supported the evaluation process well. It was designed to store the results of the assessment for visualization. Conveniently, it automatically updated the all “Status”-fields on each row representing the mitigation and its individual associations to techniques and tactics to match the “Status”-field on the Evaluation Criteria. On this part, it fulfilled its purpose exactly as designed. The Database also proved to be useful for the assessment itself. As mentioned in section 4.3, the Database includes technique-specific descriptions for the mitigations that have such. However, whereas this information was available in the Database, a more intuitive location for this would be on the Evaluation Criteria-sheet.

The Evaluation Tool can be modified according to the needs or preferences of its user or the target of the assessment. As the introduced version of the Evaluation Tool is created in Excel, this is easily done. Expanding the scope of the Evaluation Tool to include the other two MITRE ATT&CK matrices would be straightforward. Expanding the scope to include other mitigations can be done. However, one should pay attention to how these would be mapped against the structure of MITRE ATT&CK.

In principle, the results obtained through the assessment are simple. They represent how an organization has addressed the mitigations derived from MITRE ATT&CK for ICS. Therefore, it can be argued that the results themselves are easily interpreted, especially if the assessor uses the “Notes”-field to provide reasoning for the status of each mitigation.

The format of the Database supported the creation of the visualizations introduced in section 5.2 well. However, as mentioned earlier, these were examples. While similar visualizations were approved by the case-company, another organization might require different ones. Creation of different kinds of visualizations might require modifying the Database. During the case-company assessment, it was agreed that the results would be visualized with Power BI. Therefore, the Evaluation Tool itself does not include separate visualizations. Whereas Power BI provides more granular ways of representing the data, Excel itself could be used to create simpler ones that would be automatically updated to represent the results of the assessment.

The Evaluation Tool does not tie its user to any strict process. Hence, it is the responsibility of the assessor to organize the assessment to suit the needs of the use-case. Based on the experience of the author, the gap analysis itself can be conducted quite quickly – in the case of the assessments made to demonstrate the Tool, these took around two hours. However, this very much depends on external factors – such as whether the assessment is conducted as an internal or external effort, who is participating in the assessment, amount and quality of the material assessed and so on.

In its essence, the evaluation is done by comparing two sources of qualitative information against one another. Inconveniently, the mitigations in Evaluation Tool might not exactly match the ones stated in the organization's OT security policy. According to authors' experience however, in most cases, determining the status of each mitigation in the Evaluation Tool was straightforward. However, especially when assessing a policy that the assessor is not too familiar with, involving subject-matter experts that are aware of how the mitigations are, or are planned to be, implemented is suggestable for achieving more accurate results.

In any case, creating meaningful suggestions based on the results is the most important part of the assessment process. Again, the time this consumes varies. However, it is important to note that the Evaluation Tool has not been designed to serve as an audit tool, and the purpose of the results is not to demonstrate compliance. While the tool is used for identifying potential gaps in the organization's OT security approach, the Tool itself does not address the importance or relevance of the findings. The Evaluation Tool only shows how the assessor has determined an organization has addressed the mitigations of MITRE ATT&CK for ICS. The findings as such provide a good starting point for further analysis and provide ideas for further development. However, at this stage, creating meaningful suggestions for an organization very much depends on the ability of the involved stakeholders to identify what is relevant and feasible, and what is not.

The case-company has stated that the suggestions created during the assessment conducted during the demonstration were justified and satisfied the expectations of the company. The information that could be created with the Evaluation Tool supported the creation of these suggestions. More importantly, the quality of the information and support received from the case-company made the suggestions justifiable. Therefore, the Evaluation Tool itself is just a tool to support the process. As such, it was useful. To provide value, the process through which it is used, the documentation it is used to assess, and the organization-specific context are equally as important.

Finally, to monitor how the organization has improved its OT security policy in comparison to the mitigations of MITRE ATT&CK for ICS, an organization can choose to re-assess its current state. Whether this is necessary is up to the organization to decide. As emphasized throughout this thesis, the mitigations of MITRE ATT&CK for ICS and the Evaluation Tool are not a strict list of measures that an organization must address. Rather, an organization should carefully evaluate which ones are relevant in their operating environment.

In conclusion, the Evaluation Tool can be said to have fulfilled its objectives. The Tool itself is by no means without its limitations. However, based on the research introduced in this thesis, it can be said to be at least a promising concept. The fact that the case-company related demonstration showed results which satisfied expectations strengthens this argument. Thus, further development, excluding the Instructions-sheet proposed by Interviewee 2 (Annex 1), was decided to be left for potential subsequent research effort.

7 DISCUSSION

The research effort introduced in this thesis aimed to answer the following questions:

(1) How can MITRE ATT&CK for ICS be employed for assessing an organization's OT security policy?
(2) What are the benefits of such a solution?
(3) What are its limitations?

Chapter 4 provided a detailed description of how MITRE ATT&CK for ICS could be employed for creating an evaluation tool for assessing an organization's OT security policy. The demonstration showed that the Evaluation Tool can be used for assessing an OT security policy. The evaluations confirmed that the Evaluation Tool fulfilled its design criteria reasonably well and was seen to provide value to the case-company. Therefore, while the results are still limited, they can be considered promising.

In the literature review, we presented two prior research efforts with similar objectives. Both Bartusiak et al. (2023) and Georgiadou et al. (2021) introduced assessment approaches for identifying defensive gaps. A more comprehensive description of each was presented in section 3.4. Whereas both approaches included several differences in comparison to the one proposed in this thesis, the key difference of the Evaluation Tool in comparison to the two can be said to be its more lightweight approach.

The in-depth observations in the form of benefits and limitations of the artifact were introduced in the previous chapter. However, the objectives of the solution aimed to reflect both the needs of the case-company as well as some key considerations introduced in the literature review. Therefore, we reflect on these considerations and argue that the Evaluation Tool addresses the following.

Firstly, as mentioned in the introduction, Luh et al. (2022) argue that understanding the association between specific attacks and effective controls is challenging (Luh et al., 2022, p. 1). Through its knowledge base, the Evaluation Tool includes built-in associations between the defensive mitigations and adversary techniques and tactics. Therefore, it can aid in tackling this challenge by providing practical explanation on what action(s) a mitigation concretely tries to counter.

In section 3.2 we referred to Conklin (2016) who claims that the domain of OT security is still in the process of understanding the risk introduced by network connectivity and outside issues. Furthermore, the potential misunderstandings between the personnel with IT security background and OT personnel might create a mismatch (Conklin, 2016, p. 1). Through the above-mentioned practical associations that are based on real-life scenarios, we argue that the Evaluation Tool might help to pave the way for more mutual understanding of the risks.

Without downplaying the Tools limitations, the fact is that it has been designed specifically for OT. As mentioned in the literature review, security solutions designed for IT systems might not be suitable for OT systems (Stouffer et al., 2023, p. 29; DHS, 2016, p. 4; Padée et al., 2019, p. 4). Arguably the Evaluation Tool does not carry such a burden.

As mentioned in section 3.2, Sangkhro and Agrawal (2023) propose that management complexity and costs associated with the implementation of OT security standards and guidelines makes OT asset owners hesitant to use them (Sangkhro & Agrawal, 2023, p. 4). Furthermore, Wagner et al. (2020) studied the applicability of OT security standards IEC 62443, NIST SP 800-82, and VDI/VDE 2182 from the perspective of SMEs and large manufacturing organizations. According to their results, the standards are well applicable for large enterprises, whereas SME organizations find themselves struggling due to limited capabilities (Wagner et al., 2020). The artifact proposed in this thesis does not solve either of the above-proposed. However, it is based on a publicly available knowledge base and is planned to be made publicly available in the future. It was designed to be relatively lightweight and easy to use. Therefore, the Evaluation Tool itself can be argued to suit organizations of all shapes and sizes. Furthermore, although not visible in this thesis, the descriptions of the mitigations MITRE ATT&CK for ICS include references pointing out various sources on which they are based. Therefore, it can be said that the matrix – and therefore the Evaluation Tool - also summarizes lots of existing good practices proposed by various parties.

Finally, while the Evaluation Tool fulfilled the expectations of the case-company and most of its design criterion, the objective of this thesis was not to create a complete tool for all use cases. Rather, it presented a concept, a foundation on which further research can be built upon. Whether this is worth the effort is for others to decide. While the previous chapter included multiple considerations about how the artifact could be further improved, the rest of this chapter summarizes some topics for further research.

Firstly, the current knowledge base of the Evaluation Tool is based on v13 of MITRE ATT&CK for ICS. The latest version – v14 at the time of writing – was published on 31.10.2023. Therefore, updating the Evaluation Tool is recommended especially as MITRE ATT&CK is only updated bi-annually (MITRE 2023h). In addition to smaller version updates on existing information, the latest version introduced new metadata that may be useful in the form of "assets", which represent typical OT devices and systems. Each of these objects is mapped to techniques to indicate that the asset may be targeted due to its capability and function (MITRE 2023i). Including assets might prove to be valuable metadata to supplement the Evaluation Tool.

Due to the scope of this thesis, the Data Sources included in the matrix were left out of the Evaluation Tool. Data Sources are "various subjects/topics of information that can be collected by sensors/logs.". Data sources also include data components which "identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique." (MITRE 2023j). Including such to complement the mitigations would extend the Evaluation Tool.

Larger extensions to the knowledge base can also be made. The most obvious direction would be to include the Enterprise matrix to enable more overarching assessments (MITRE 2023a). Another potential publicly available knowledge base for OT security controls would be NIST SP 800-82r3 (Stouffer et al. 2023). However, this would require one to figure out how the controls are mapped against the techniques and tactics if one wishes to keep the core of the Evaluation Tool intact. Taking a modular approach to the Evaluation Tool could be one solution.

The proposed Evaluation Tool with its current knowledge base can be improved as well. For example, Interviewee 1 proposed increasing the automation of the Tool. The lack of visualizations included in the Evaluation Tool could be improved as proposed by both Interviewees. To take the Tool even further, one might take the concept introduced in the form of Excel and create a more mature tool with more sophisticated tools.

Finally, the number of assessments made with the Evaluation Tool is still limited. One could apply it for assessing other organizations' OT security policies to provide more practical experience. Such projects might also raise more limitations to be addressed in the future.

8 CONCLUSIONS

In the past securing OT systems has heavily relied on security through obscurity. In practice, the systems were operated through proprietary protocols, using specialized hardware and software in a physically isolated network. The increased connectivity of OT has made the past model obsolete. The growth of attack surface and new attack vectors have increased the relevancy cybersecurity of OT.

The purpose of this thesis was twofold. Firstly, it explored how MITRE ATT&CK for ICS could be employed to assess an organization's OT security policy. Through creation, demonstration and evaluation of the Evaluation Tool, the thesis provided observations of the benefits and limitations of the artifact. Secondly, the cooperation between the author of this thesis and the case-company aimed to provide relevant insights on how the case-company could improve its OT security posture.

The artifact-centric approach of this thesis was guided by the Design Science Research Model of Peffers et al. (2007). The methodology supported the effort well. It provided a clear structure that was rigorously followed throughout the research.

The literature review introduced the key themes of this thesis. It emphasized the growing need for OT cybersecurity and explained some of the challenges and solutions in the domain. Furthermore, it showed that MITRE ATT&CK for ICS is widely adapted by academic community for multiple purposes including defensive gap assessment and advocated for the novelty of the Evaluation Tool.

The artifact proposed in this thesis reassured that MITRE ATT&CK for ICS can be used for assessing an organization's OT security policy. The mitigations included in MITRE ATT&CK for ICS provide plenty of meaningful measures to counter the observed techniques adversaries employ and include plenty of useful metadata that lower the barrier for applying it. However, its scope does not cover everything that mature OT security policy should include. Examples of such are risk assessments, disaster recovery and business continuity planning, incident response, and cybersecurity governance.

The Evaluation Tool proposed in this thesis fulfilled its objectives for the greater part. Through the demonstration, MITRE ATT&CK for ICS-based tool was shown to be capable of providing added value for the case-company. Nonetheless, it was not without its limitations. Hence, the initial version of the Evaluation Tool can be described as a concept to which further improvements can be built upon. To support such an effort, the thesis proposed a plethora of potential improvements and topics for further research around the artifact.

The practical application of the Evaluation Tool is still limited. So far, it has been applied for only one real-life assessment – the one made for the case-company. Further demonstrations may provide additional findings. However, in the scope of this thesis, the Evaluation Tool succeeded in the purpose it was built for – it has aided an organization in assessing their current defensive measures and has provided justifiable solutions for enhancing the current state. Therefore – in conclusion - this thesis has reached its objectives.

BIBLIOGRAPHY

Ackerman, P. (2017). Industrial Cybersecurity. Packt Publishing. https://sfx.finna.fi/nelli09?url_ver=Z39.88-2004&ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/sfxit.com:opac_856&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&sfx.ignore_date_threshold=1&rft.object_id=4110000000007547&svc_val_fmt=info:ofi/fmt:kev:mtx:sch_svc&

Alexander, O., Belisle, M., & Steele, J. (2020a). MITRE ATT&CK for industrial control systems: Design and philosophy. The MITRE Corporation: Bedford, MA, USA, 29.

Alexander, O., Kapellmann Zafra, D., Lunden, K., Brubaker, N., & Agboruche, G. (2020b). In Pursuit of a Gestalt Visualization: Merging MITRE ATT&CK® for Enterprise and ICS to Communicate Adversary Behaviors. MITRE & Mandiant. Accessed 11.10.2023 https://medium.com/mitre-attack/in-pursuit-of-a-gestalt-visualization-merging-mitre-att-ck-for-enterprise-and-ics-to-communicate-3523daa7b580

Anton, S. D. D., Fraunholz D., Krohmer D., Reti D., Schneider D., & Schotten, H. D. (2021). The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities Around the World. IEEE Internet of Things Journal, 8(24), 17525–17540. https://doi.org/10.1109/JIOT.2021.3081741

Ara, A. (2022). Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions. IOP Conference Series. Earth and Environmental Science, 1026(1), 12030. https://doi.org/10.1088/1755-1315/1026/1/012030

Arafune, M., Rajalakshmi, S., Jaldon, L., Jadidi, Z., Pal, S., Foo, E., & Venkatachalam, N. (2022). Design and Development of Automated Threat Hunting in Industrial Control Systems. 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops), 618–623. https://doi.org/10.1109/PerComWorkshops53856.2022.9767375

Ayub, A., Yoo, H., & Ahmed, I. (2021). Empirical Study of PLC Authentication Protocols in Industrial Control Systems. 2021 IEEE Security and Privacy Workshops (SPW), 383–397. https://doi.org/10.1109/SPW53761.2021.00058

Bartusiak, A., Kühne, M., Nitschke, O., Lässig, J., Nicolai, S., & Bretschneider, P. (2023). First step into automation of security assessment of critical infrastructures. Sustainable Energy, Grids and Networks, 36, 101139. https://doi.org/10.1016/j.segan.2023.101139

Baskerville, R., Baiyere, A., Gergor, S., Hevner, A., & Rossi, M. (2018). Design Science Research Contributions: Finding a Balance between Artifact and Theory. Journal of the Association for Information Systems, 19(5), 358–376. https://doi.org/10.17705/1jais.00495

Boeding, M., Boswell, K., Hempel, M., Sharif, H., Lopez, J., & Perumalla, K. (2022). Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. Energies (Basel), 15(22), 8692. https://doi.org/10.3390/en15228692

Cawthra, J. L., Ekstrom, M. R., Lusty, L. N., Sexton, J. T., Sweetnam, J. E., & Townsend, A. R. (2020). Data integrity: Identifying and protecting assets against ransomware and other destructive events.

Conklin, W. A. (2016). IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilience. 2016 49th Hawaii International Conference on System Sciences (HICSS), 2642–2647. https://doi.org/10.1109/HICSS.2016.331

CrowdStrike. (2018). CrowdStrike Demystifies Threats with MITRE ATT&CK. Accessed 7.9.2023 https://www.crowdstrike.com/blog/crowdstrike-demystifies-threats-with-mitre-attck/

Darktrace. (2023). Darktrace: Mapping to MITRE. Accessed 7.9.2023 https://assets-global.website-files.com/626ff4d25aca2edf4325ff97/641051a81dac1ecde1b79c8b_Mapping%20to%20MITRE.pdf

de Peralta, F. A., Watson, M. D., Bays, R. M., Boles, J. R., & Powers, F. E. (2021). Cybersecurity Resiliency of Marine Renewable Energy Systems Part 2: Cybersecurity Best Practices and Risk Management. Marine Technology Society Journal, 55(2), 104–116. https://doi.org/10.4031/MTSJ.55.2.4

de Peralta, F. A. (2020). Cybersecurity Resiliency of Marine Renewable Energy Systems-Part 1: Identifying Cybersecurity Vulnerabilities and Determining Risk. Marine Technology Society Journal, 54(6), 97–107. https://doi.org/10.4031/MTSJ.54.6.9

DHS. (2016). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. U.S. Department of Homeland Security.

Dragos. (2023). MITRE ATT&CK for ICS. Accessed 7.9.2023 https://www.dragos.com/mitre-attack-for-ics/

Finnish Ministry of Economic Affairs and Employment. (2017). Accounting Act 1336/1997. UNOFFICIAL TRANSLATION. Accessed 20.11.2023. https://www.finlex.fi/en/laki/kaannokset/1997/en19971336_20161376.pdf

Firoozjaei, M. D., Mahmoudyar, N., Baseri, Y., & Ghorbani, A. A. (2022). An evaluation framework for industrial control system cyber incidents. International Journal of Critical Infrastructure Protection, 36, 100487. https://doi.org/10.1016/j.ijcip.2021.100487

Flaus, J.-M. (2019). Cybersecurity of Industrial Systems. Wiley Data and Cybersecurity. https://sfx.finna.fi/nelli09?url_ver=Z39.88-2004&ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/sfxit.com:opac_856&url_ctx_fmt=info:ofi/fmt:kev:mtx:ctx&sfx.ignore_date_threshold=1&rft.object_id=4100000008701109&svc_val_fmt=info:ofi/fmt:kev:mtx:sch_svc&

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors (Basel, Switzerland), 21(9), 3267. https://doi.org/10.3390/s21093267

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer Information Systems, 62(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Gourisetti, S. N. G., Lee A., Reddi R., Isirova K., Touhiduzzaman M.,. Sebastian-Cardenas D. J, Lambert K., Cali Ü., Mylrea M., Rahimi F., Nitu P., Huff P., Pasetti M., & Saha, S. S. (2022). Assessing Cybersecurity Resilience of Distributed Ledger Technology in Energy Sector Using the MITRE ATT&CK® ICS Framework. 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain), 1–6. https://doi.org/10.1109/iGETblockchain56591.2022.10087078

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly, 37(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Havlena, V., Matoušek, P., Ryšavý, O., & Holík, L. (2023). Accurate Automata-Based Detection of Cyber Threats in Smart Grid Communication. IEEE Transactions on Smart Grid, 14(3), 2352–2366. https://doi.org/10.1109/TSG.2022.3216726

Hayden, E., Assante, M., & Conway, T. (2014). An abbreviated history of automation & industrial controls systems and cybersecurity. SANS Analyst White Papers.

Hemsley, K. E., & Fisher, E. (2018). History of industrial control system cyber incidents. Idaho National Lab.(INL), Idaho Falls, ID (United States).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28(1), 75–105. https://doi.org/10.2307/25148625

Hollerer, S., Kastner W., & Sauter, T. (2021). Towards a Threat Modeling Approach Addressing Security and Safety in OT Environments. 2021 17th IEEE International Conference on Factory Communication Systems (WFCS), 37–40. https://doi.org/10.1109/WFCS46889.2021.9483591

Izzuddin, A. B., & Lim, C. (2022). Mapping Threats in Smart Grid System Using the MITRE ATT&CK ICS Framework. 2022 IEEE International Conference on Aerospace Electronics and Remote Sensing Technology (ICARES), 1–7. https://doi.org/10.1109/ICARES56907.2022.9993475

Jadidi, Z., & Lu, Y. (2021). A Threat Hunting Framework for Industrial Control Systems. IEEE Access, 9, 164118–164130. https://doi.org/10.1109/ACCESS.2021.3133260

Jiang, N., Lin, H., Yin, Z., & Zheng, L. (2018). Performance Research on Industrial Demilitarized Zone in Defense-in-Depth Architecture. 2018 IEEE International Conference on Information and Automation (ICIA), 534–537. https://doi.org/10.1109/ICInfA.2018.8812486

Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. Sensors (Basel, Switzerland), 22(5), 1860. https://doi.org/10.3390/s22051860

Kapalidis, C., Karamperidis, S., Watson, T., & Koligiannis, G. (2022). A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. Journal of Marine Science and Engineering, 10(10), 1486. https://doi.org/10.3390/jmse10101486

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. Journal of Intelligent Information Systems, 60(2), 377–405. https://doi.org/10.1007/s10844-022-00753-1

Køien, G. M. (2021). Zero-Trust Principles for Legacy Components: 12 Rules for Legacy Devices: An Antidote to Chaos. Wireless Personal Communications, 121(2), 1169–1186. https://doi.org/10.1007/s11277-021-09055-1

Langner, R. (2013). To Kill a Centrifuge—A Technical Analysis of What Stuxnet's Creators Tried to achieve.

Lee, A., Gourisetti, S. N. G., Sebastian-Cardenas, D. J., Lambert, K., Navarro, V., Pasetti, M., Cali, Ü., Isirova, K., Reddi, R., Nitu, P., Touhiduzzaman, M., Mylrea, M., Huff, P., Rahimi, F., & Saha, S. S. (2023). Assessment of the Distributed Ledger Technology for Energy Sector Industrial and Operational Applications Using the MITRE ATT&CK® ICS Matrix. IEEE Access, 11, 69854–69883. https://doi.org/10.1109/ACCESS.2023.3288428

Lockheed Martin. (2023). Cyber Kill Chain. Accessed 12.9.2023 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Luh, R., S. Eresheim, Größbacher, S., Petelin, T., Mayr, F., Tavolato, P., & Schrittwieser, S. (2022). PenQuest Reloaded: A Digital Cyber Defense Game for Technical Education. 2022 IEEE Global Engineering Education Conference (EDUCON), 906–914. https://doi.org/10.1109/EDUCON52537.2022.9766700

Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. Computers (Basel), 12(4), 79. https://doi.org/10.3390/computers12040079

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. DECISION SUPPORT SYSTEMS, 15(4), 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

Mashima, D. (2022). MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems. Sustainability (Basel, Switzerland), 14(3), 1256. https://doi.org/10.3390/su14031256

Maynard, P., & McLaughlin, K. (2020). Big Fish, Little Fish, Critical Infrastructure: An Analysis of Phineas Fisher and the 'Hacktivist' Threat to Critical Infrastructure. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1–7. https://doi.org/10.1109/CyberSA49311.2020.9139715

Microsoft. (2023a). Understand security coverage by the MITRE ATT&CK® framework. Accessed 7.9.2023 https://learn.microsoft.com/en-us/azure/sentinel/mitre-coverage

Microsoft. (2023b). Microsoft Excel. Accessed 26.10.2023 https://www.microsoft.com/en-us/microsoft-365/excel

Microsoft. (2023c). Microsoft Power BI. Accessed 26.10.2023 https://powerbi.microsoft.com/en-us/

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. International Journal of Critical Infrastructure Protection, 35, 100464. https://doi.org/10.1016/j.ijcip.2021.100464

MITRE. (2023a). MITRE ATT&CK – Enterprise Matrix. Accessed 12.9.2023 https://attack.mitre.org/matrices/enterprise/

MITRE. (2023b). MITRE ATT&CK – Mobile Matrix. Accessed 12.9.2023 https://attack.mitre.org/matrices/mobile/

MITRE. (2023c). MITRE ATT&CK – ICS Matrix. Accessed 12.9.2023 https://attack.mitre.org/matrices/ics/

MITRE. (2023d). MITRE ATT&CK – ICS Matrix v13. Accessed 26.10.2023 https://attack.mitre.org/versions/v13/matrices/ics/

MITRE. (2023e). Working With ATT&CK. Accessed 26.10.2023 https://attack.mitre.org/versions/v13/resources/working-with-attack/

MITRE. (2023f). ICS Mitigations - Antivirus/Antimalware. Accessed 27.10.2023 https://attack.mitre.org/mitigations/M0949/

MITRE. (2023g). ICS Mitigations – Mitigation Limited or Not Effective. Accessed 13.11.2023 https://attack.mitre.org/versions/v13/mitigations/M0816/

MITRE. (2023h). ATT&CK FAQ. Accessed 29.11.2023 https://attack.mitre.org/resources/faq/#faq-1-0-header

MITRE. (2023i). ATT&CK Assets. Accessed 29.11.2023 https://attack.mitre.org/assets/

MITRE. (2023j). ATT&CK Data Sources. Accessed 29.11.2023 https://attack.mitre.org/datasources/

Mohammed, A. S., Anthi, E., Rana, O., Saxena, N., & Burnap, P. (2023). Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication. Computers & Security, 124, 103007. https://doi.org/10.1016/j.cose.2022.103007

Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0. Journal of Manufacturing Systems, 57, 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and Organization, 17(1), 2–26.

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. 2022 IEEE International Symposium on Systems Engineering (ISSE), 1–7. https://doi.org/10.1109/ISSE54508.2022.10005490

Nursidiq, A. H., & Lim, C. (2022). Threat Analysis on Industrial Control System Based on Attacker's Behaviors using Honeypots. 2022 IEEE International Conference on Aerospace Electronics and Remote Sensing Technology (ICARES), 1–6. https://doi.org/10.1109/ICARES56907.2022.9993566

Ocaka, A., Briain, D. Ó., Davy, S., & Barrett, K. (2022). Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial Control and Automation Systems: A Technical Review. 2022 Cyber Research Conference - Ireland (Cyber-RCI), 1–8. https://doi.org/10.1109/Cyber-RCI55324.2022.10032665

OpenAI. (2023). ChatGPT. Accessed 28.10.2023. https://chat.openai.com/

Oruc, A., Amro, A., & Gkioulos, V. (2022). Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework. Sensors (Basel, Switzerland), 22(22), 8745. https://doi.org/10.3390/s22228745

Padée, A., Wójcik, M., Ćwiek, A., Klimaszewski, K., Kopka, P., Kozioł, S., Kuźnicki, K., Możdżonek, R., Wiślicki, W., & Włodarski, T. (2019). On Preventing and Detecting Cyber Attacks in Industrial Control System Networks. Journal of Telecommunications and Information Technology, 2(2019), 21–28. https://doi.org/10.26636/jtit.2019.131219

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering, 9(12), 1384. https://doi.org/10.3390/jmse9121384

Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. Journal of Manufacturing Systems, 68, 196–208. https://doi.org/10.1016/j.jmsy.2023.03.009

Rajaram, P., Goh, M., & Zhou, J. (2022). Guidelines for cyber risk management in shipboard operational technology systems. Journal of Physics. Conference Series, 2311(1), 12002. https://doi.org/10.1088/1742-6596/2311/1/012002

Rencelj Ling, E., & Ekstedt, M. (2023a). Estimating Time-To-Compromise for Industrial Control System Attack Techniques Through Vulnerability Data. SN Computer Science, 4(3). https://doi.org/10.1007/s42979-023-01750-z

Rencelj Ling, E., & Ekstedt, M. (2023b). A threat modeling language for generating attack graphs of substation automation systems. International Journal of Critical Infrastructure Protection, 41, 100601. https://doi.org/10.1016/j.ijcip.2023.100601

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). NIST special publication 800–207 zero trust architecture. National Institute of Standards and Technology, US Department of Commerce: Washington, DC, USA. https://doi.org/10.6028/NIST.SP.800-207

Sangkhro, R., & Agrawal, A. K. (2023). Cybersecurity in Industrial Control Systems: A Review of the Current Trends and Challenges. 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), 355–359.

Sen, Ö., van der Velde, D., Wehrmeister, K. A., Hacker, I., Henze, M., & Andres, M. (2022). On using contextual correlation to detect multi-stage cyber attacks in smart grids. Sustainable Energy, Grids and Networks, 32, 100821. https://doi.org/10.1016/j.segan.2022.100821

Simola, J., Pöyhönen, J., & Lehto, M. (2023). Smart Terminal System of Systems' Cyber Threat Impact Evaluation. In A. Andreatos, & C. Douligeris (Eds.), Proceedings of the 22nd European Conference on Cyber Warfare and Security (pp. 439-449). Academic Conferences International. Proceedings of the European Conference on Cyber Warfare and Security, 22. https://doi.org/10.34190/eccws.22.1.1070

Staves, A., Maesschalck, S., Derbyshire, R., Green, B., & Hutchison, D. (2023). Learning to Walk: Towards Assessing the Maturity of OT Security Control Standards and Guidelines. 2023 IFIP Networking Conference (IFIP Networking), 1–6. https://doi.org/10.23919/IFIPNetworking57963.2023.10186424

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) Security (NIST Special Publication (SP) NIST SP 800-82r3; NIST Special Publication (SP) NIST SP 800-82r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). Mitre att&ck: Design and philosophy. In Technical report. The MITRE Corporation.

Toker, F. S., Ovaz Akpinar, K., & Özçelik, İ. (2021). MITRE ICS Attack Simulation and Detection on EtherCAT Based Drinking Water System. 2021 9th International Symposium on Digital Forensics and Security (ISDFS), 1–6. https://doi.org/10.1109/ISDFS52919.2021.9486331

Vaishnavi, V., & Kuechler, W. (2021). Design Science Research in Information Systems. http://www.desrist.org/design-research-in-information-systems/

Villalón-Huerta, A., Ripoll-Ripoll, I., & Marco-Gisbert, H. (2021). CNA Tactics and Techniques: A Structure Proposal. Journal of Sensor and Actuator Networks, 10(1), 14. https://doi.org/10.3390/jsan10010014

Wagner, P., Hansch, G., Konrad, C., John, K.H., Bauer, J., & Franke, J. (2020). Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises. 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 1, 1544–1551. https://doi.org/10.1109/ETFA46521.2020.9212126

Zanasi, C., Magnanini, F., Russo, S., & Colajanni, M. (2022). A Zero Trust approach for the cybersecurity of Industrial Control Systems. 2022 IEEE 21st International Symposium on Network Computing and Applications (NCA), 21, 1–7. https://doi.org/10.1109/NCA57778.2022.10013559

Zhang, S., Wang, S., Bai, G., Zhang, M., Chen, P., Zhao, C., Li, S., & Zhou, J. (2022). Design of Threat Response Modeling Language for Attacker Profile Based on Probability Distribution. Wireless Communications and Mobile Computing, 2022, 1–16. https://doi.org/10.1155/2022/2323228

ANNEX 1 EVALUATION TOOL: INSTRUCTIONS-SHEET

Evaluation Tool

Version:	v. 1.0
Date:	18/12/2023
Note:	This version of the Evaluation Tool is based on MITRE ATT&CK for ICS® v13. Please be aware that the latest version of the framework (v14) was published on 31.10.2023 (MITRE 2023a).
Created by:	Onni Eho

Introduction

The Evaluation Tool is originally designed for assessing the coverage of an organization's OT security policy* against the mitigations included in MITRE ATT&CK for ICS v13 (MITRE 2023b). Therefore, its knowledge base is purely based on MITRE ATT&CK for ICS v13 (MITRE 2023c). Based on the findings of such an assessment organization can seek to enhance their current defensive approach by including relevant countermeasures to supplement their existing policies.

*For context, OT security policy is in this case understood as a collection of the policies defining the countermeasures an organization has implemented or plans to implement for safeguarding its OT environment.

Scope

"The major architectural focus of ATT&CK for ICS are the systems and functions associated with functional levels 0 – 2 of the Purdue architecture. Enterprise IT is not the focus of the ATT&CK for ICS knowledge base. Due to the use of IT platforms to host critical ICS applications such as HMIs, there is some overlap between the Enterprise and ICS technology domains. Nonetheless, ATT&CK for ICS has a primary focus on the actions that adversaries take against the non-IT based systems and functions of ICS." (Alexander et al. (2020, p. 2).

Therefore, as the Evaluation Tool in its current form is purely based on the knowledge derived from MITRE ATT&CK for ICS, similar limitations apply to its scope.

Content

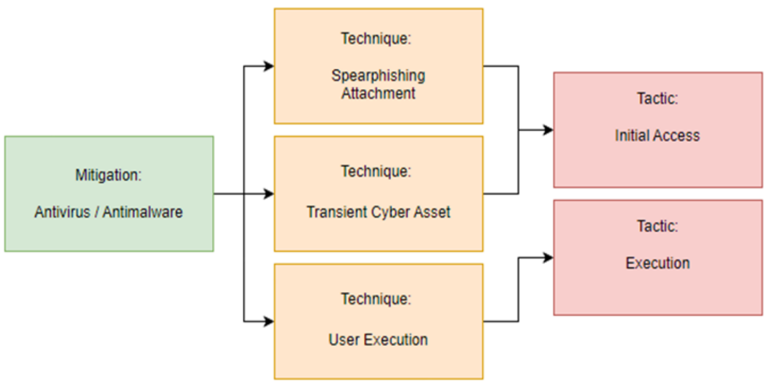
Evaluation Criteria

The "Evaluation Criteria"-sheet includes one group of rows for each mitigation included in MITRE ATT&CK for ICS v13. This sheet was created to serve most of the assessment-related needs. Thus, the sheet includes fields that were deemed necessary to support such an effort. To keep the tool lightweight and easy to use, it does not include detailed information about the techniques and tactics. Rather, further information is made easily accessible through hyperlinks that lead to MITRE's descriptions.

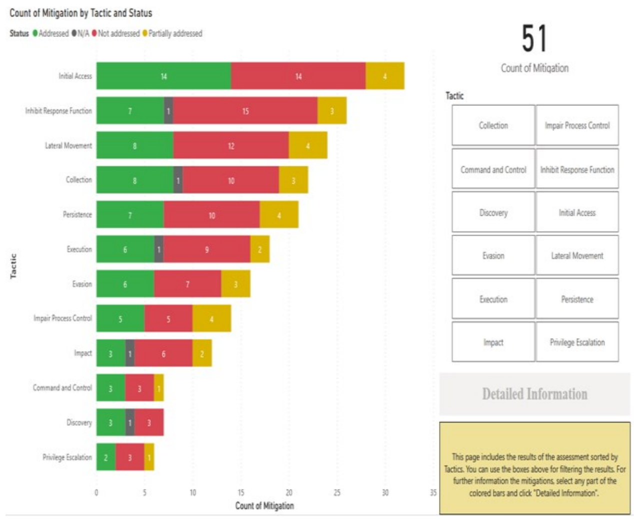
In addition to the mitigation-related information, the Evaluation Criteria includes two fields for the assessment. Firstly, "Notes" is a free space reserved for mitigation related comments. "Status" is used to indicate how the mitigation has been addressed in an organization's OT security policy. The assessor can choose the values used for the evaluation. As an example, one can use a three-level classification for each mitigation: "Addressed", "Not Addressed" and "Partly Addressed". Whereas "Addressed" and "Not Addressed" are obvious choices, "Partly Addressed" can be used for situations where the mitigation is not completely addressed, but some parts of it have clearly been included. Furthermore, if one wishes to exclude some of the mitigations from the assessment, for example "Not Applicable" can be used.

Database

Each mitigation in MITRE ATT&CK for ICS may be associated with multiple techniques which can be further associated with multiple tactics.



Database-sheet is used to store the assessment data in a format which can be used to visualize the results with Power BI in a way that the essence of MITRE ATT&CK for ICS remains. In practice, this means that mitigations can be associated with the techniques they address, and the techniques can be associated with the related tactics. Examples of such visualizations can be seen below. The examples are created from demo-data and do not represent the status of any real-life organization.

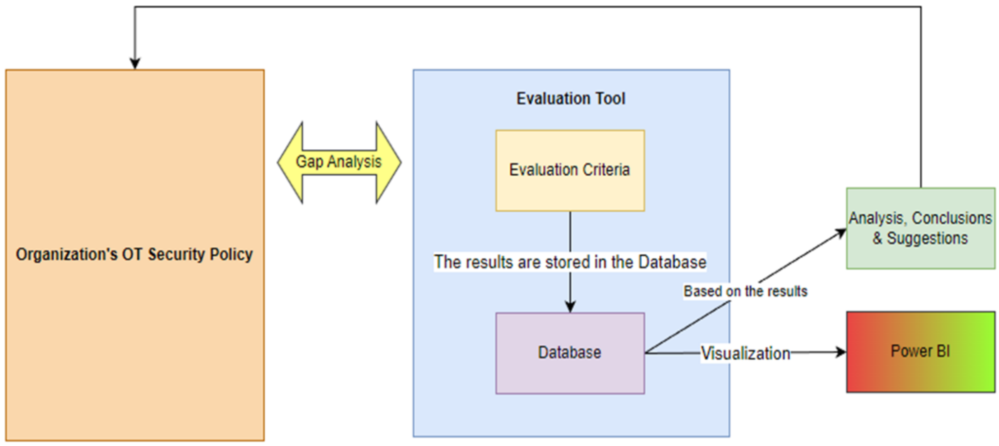


The "Status"-fields in the Database-sheet are linked to a corresponding field in the Evaluation Criteria-sheet. Therefore, the value of the status field in the Database will be updated based on the value of the "Status"-field in the Evaluation Criteria-sheet. Hence, while the Database contains 396 rows representing all mitigations and their associations with the corresponding techniques and tactics, this sheet does not need to be manually modified.

Furthermore, it should be noted that the information in "Description"-field in the Database-sheet may differ from the corresponding field in the Evaluation Criteria-sheet. This is because the overall description of a mitigation can be slightly different than the description provided for the mitigation in the context of a technique. For further reference, look at for example "Antivirus/Antimalware"-mitigation (MITRE 2023d).

Assessment Process

The usage of Evaluation Tool is not tied to any strict process. However, the below figure represents an example process through the functionalities of the Evaluation Tool.



The assessment is performed as a gap analysis. In practice, an organization's OT security policy is compared to the mitigations derived from MITRE ATT&CK for ICS that are included in the Evaluation Criteria. An organization may choose to exclude certain mitigations from the Criteria based on organization-specific needs by, for example, marking the status of these as "Not Applicable". In the proposed approach, the status of applicable mitigations is marked either as "Addressed", "Not Addressed", or "Partly Addressed". However, the assessor may choose to use a different criterion if deemed necessary.

The assessment is done via the Evaluation Criteria and the results are automatically stored in the Database. If required, the results stored in the Database can be visualized. The Evaluation Tool does not include ready-made visualizations. Whereas Excel provides visualization capabilities which can be used for this purpose, tools such as Power BI can extend the capabilities. Depending on the needs of the organization, the Database can be reorganized to support different kinds of visualizations.

The most important part of the process is interpreting the results. The findings of the assessment should be analyzed and concluded. Furthermore, where feasible, suggestions on enhancing the OT security policy of an organization should be made based on the results. Upon reviewing the results, conclusions, and recommendations the organization can use the information to extend the existing policy.

The Evaluation Tool itself is easy to use. From the Tools perspective, a person or an organization using the tool should focus on understanding its content. Understanding the other entity of the gap analysis is equally important. Therefore, all relevant documentation about the organization's OT security policy should be reviewed. Involving the organization's subject matter experts can help by providing information that is not documented, and aid in interpreting the documentation.

Finally, it is important to note that the Evaluation Tool has not been designed to serve as an audit tool, and the purpose of the results is not to demonstrate compliance. While the tool is used for identifying potential gaps in the organization's OT security approach, the Tool itself does not address the importance or relevance of the findings. The Evaluation Tool only shows how the assessor has determined an organization has addressed the mitigations of MITRE ATT&CK for ICS. The findings as such provide a good starting point for further analysis and provide ideas for further development. However, at this stage, creating meaningful suggestions for an organization very much depends on the ability of the involved stakeholders to identify what is relevant and feasible, and what is not.

References

Alexander, O., Belisle, M., & Steele, J. (2020a). MITRE ATT&CK for industrial control systems: Design and philosophy. The MITRE Corporation: Bedford, MA, USA, 29.

MITRE. (2023a). Versions of ATT&CK. https://attack.mitre.org/resources/versions/

MITRE. (2023b). ICS Mitigations. https://attack.mitre.org/versions/v13/mitigations/ics/

MITRE. (2023c). MITRE ATT&CK for ICS v13. https://attack.mitre.org/versions/v13/

MITRE. (2023d). Antivirus/Antimalware-mitigation. https://attack.mitre.org/versions/v13/mitigations/M0949/