Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Engineering Cybernetics

Sander Endresen

Cyber security handling in manufacturing plants

Master's thesis in Cybernetics and Robotics
Supervisor: Mary Ann Lundteigen
Co-supervisor: Daniel Lovborn
July 2022

NTNU
Norwegian University of
Science and Technology

Sander Endresen

Cyber security handling in manufacturing plants

Master's thesis in Cybernetics and Robotics
Supervisor: Mary Ann Lundteigen
Co-supervisor: Daniel Lovborn
July 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Engineering Cybernetics

NTNU
Norwegian University of
Science and Technology

Cyber security handling in manufacturing plants

Author:
Sander Endresen

Supervisor:
Mary Ann Lundteigen

Co-supervisor:
Daniel Lovborn

Master's thesis
Department of Engineering Cybernetics
Norwegian University of Science and Technology

July 29, 2022

Preface

When I was about to choose a new subject to fulfill in my degree, I got permission to take some courses within information security and ethical hacking, which increased my interest for the subject area. During a summer internship within cyber security in 2021, I was lucky to have the opportunity to participate online at the BlackHat security conference in Las Vegas. This experience was valuable for me and my interest for cyber security grew. During the last year of my studies I have also participated in a student organization within information security, where I have participated in information security competitions. With this interest for cyber security it was natural for me to learn more about cyber attack targeted against the control systems of industrial facilities. The target group for this thesis is people within the industry of cyber security and OT systems, especially those for manufacturing plants, or others who wants to learn more about the cyber security aspects of industrial control systems. It is also for people with basic technical computer knowledge, as some basic computer terminology is not described in detail.

Acknowledgements

I want to thank my supervisor, Mary Ann Lundteigen, for great guidance and interesting discussions. Mary Ann has always been positive and engaged and has been a pleasure to have as my supervisor. In addition I want to thank my co-supervisor, Daniel Lovborn, making this thesis a cooperation with Orkla. Daniel has also given valuable feedback and interesting discussions. During the penetration test I have also learned a lot from the security experts in Orkla, so I also want to thank them as well. The main contact I had at the collaborating manufacturing plant set up the test system for the penetration test and allowed the penetration test to happen at the manufacturing plant, which I really appreciate. I also want to thank Kenneth Titlestad and Einar Færaas for great tips and feedback regarding the penetration testing process and tools. The participants at the CDS-forum seminars have also given interesting presentations and been a part of exciting cyber security discussions. At the end I will thank my family for support, encouraging words and motivation.

Executive summary

The Purdue model is a layered network topology model used for segregating the IT networks and the OT networks in industrial facilities. The IT part of the Purdue model is the office layer and the OT part consists of the levels operation, control, process logic and process field. All traffic between the IT and OT must pass a security zone. IEC 62443 is a series of standards that is considered to be the industry standard for cyber security for OT systems. It consists of the four main parts General, Policies and Procedures, System and Component. The part General gives an overview of the series of the series of standards. Policies and procedures involves security policies and risk management for a secure system. The System part provides guidance for implementing and designing a secure OT system. Components considers the technical functionality levels for industrial network components.

The number of cyber attacks against OT is increasing, and the attackers are more sophisticated than before. The attacker objectives can be categorized as either loss, denial or manipulation. Loss of view and control are the objectives for the office level in the IT infrastructure. Denial of view, control and safety are objectives for the operation and control levels in the OT infrastructure. Manipulation of view, control, sensors and safety are the objectives for the process logic and process field layers in the OT infrastructure. Stuxnet, the attacks against the Ukrainian Energy and Triton are three major influential attacks against OT, that modifies control processes at industrial facilities.

These five recommendations are according to Dragos (2022a) those to provide the best effect to cyber threats against OT networks: A defensible architecture, OT network monitoring, remote access authentication, key vulnerability management and OT incident response plan. To identify conditions and limit damages, both technical, organizational and operational barrier elements need to be implemented. In the risk assessment for loss of food safety, remote access systems and the systems connected directly to the Internet will have the highest desired level of security. In the penetration test at a physical manufacturing plant, a remote access solution was exploited to gain access to an engineering workstation in the OT network.

The overall security of an organization can be seen as the combination of implementing systems and components, and the maturity of the organization. Multi-factor authentication, security training of personnel and network monitoring are some of the most important measures in order to improve the overall cyber security of an OT system.

Executive summary in Norwegian

Purdue-modellen er en nivådelt modell for nettverkstopologi som brukes for å skille IT-nettverk og OT-nettverk i industrielle anlegg. IT-delen av Purdue-modellen er kontorlaget og OT-delen består av nivåene drift, kontroll, prosesslogikk og feltustyr. All trafikk mellom IT og OT må passere en sikkerhetssone. IEC 62443 er en serie av standarder som anses å være industristandarden for cybersikkerhet for OT-systemer. Den består av de fire hoveddelene Generelt, Retningslinjer og prosedyrer, System og Komponent. Delen Generelt gir en oversikt over serien av standarder. Retningslinjer og prosedyrer involverer retningslinjer for sikkerhet og risikostyring for et sikkert system. System-delen gir veiledning for implementering og utforming av et sikkert OT-system. Komponent-delen vurderer de tekniske funksjonalitetsnivåene for industrielle nettverkskomponenter.

Antall cyberangrep mot OT øker, og angriperne er mer sofistikerte enn før. Angripernes mål kan kategoriseres som enten tap, tjenestenekt eller manipulasjon. Tap av oversikt og kontroll er angrepsmålene for kontornivå i IT-infrastrukturen. Tjenestenekt, kontroll og sikkerhet er mål for drifts- og kontrollnivåene i OT-infrastrukturen. Manipulering av oversikt, kontroll, sensorer og safety er målene for nivåene for prosesslogikken og feltutstyret i OT-infrastrukturen. Stuxnet, angrepene mot det ukrainske strømnettet og Triton er tre store innflytelsesrike angrep mot OT, som endrer kontrollprosesser ved industrielle anlegg.

Disse fem anbefalingene er i henhold til Dragos (2022a) de som gir den beste effekten mot cybertrusler for OT-nettverk: En forsvarssterk arkitektur, monitorering av OT-nettverk, autentisering for trådløse løsninger, håndtering av viktige sårbarheter og en handlingsplan for OT-hendelser. For å identifisere forhold og begrense skader må både tekniske, organisatoriske og operasjonelle barriereelementer implementeres. I risikovurderingen for tap av food safety vil systemer for fjerntilgang og systemene koblet direkte til internett ha høyest ønskede Security Level Target. I penetrasjonstesten ved en fysisk fabrikk ble en løsning for fjerntilgang utnyttet for å få tilgang til en engineering workstation i OT-nettverket.

Den overordnede sikkerheten til en organisasjon kan sees på som kombinasjonen av implementering av systemer og komponenter, og organisasjonens modenhet. Multifaktor-autentisering, sikkerhetstrening av personell og nettverksmonitorering er noen av de viktigste tiltakene for å forbedre den overordnede cybersikkerheten til et OT-system.

Table of Contents

List of Tables

List of Figures

Abbreviations

Abbreviation	Description
AES	Advances Encryption Standard
AMS	Anti-malware system
CDS-forum	Industry Forum for Cybersecurity in IACS
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DoS	Denial of service
EWS	Engineering workstation
HMI	Human machine interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
ICT	Information Communication Technology
IEC	International Electrotechnical Comission
IMS	Information Management System
I/O card	Input/Output card
IPsec	Internet Protocol security
IRP	Incident response plan
ISA	International Society of Automation
IT	Information technology
MFA	Multi-factor Authentication
MWS	Monitoring workstation
OT	Operational Technology
P2P	Peer-to-peer
PLC	Programmable Logic Controller
PMS	Patch Management System
RAS	Remote Access Server
RDP	Remote Desktop Protocol
RSA	Rivest-Shamir-Adleman
RTU	Remote Terminal Unit
SANS	System Administrator, Audit, Network, and Security
SCADA	Supervisory control and acquisition
SIS	Safety Instrumented System
SL	Security Level
SL-A	Security Level Achieved
SL-C	Security Level Capability

SL-T	Security Level Target
SSH	Secure Shell
SuC	System under consideration
SS	Shutdown System
SSS	Safe State System
TLS	Transport Layer Security
TR	Technical Report
TS	Takeover System
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network
WPA2	Wi-Fi Protected Access

1

Introduction

This chapter will first present the background for the choice of topic, then the problem description and the delimitations. The structure of the thesis with the content of the upcoming chapters will at the end be presented.

1.1 Background

The control and automation systems in industrial facilities are attractive targets for sophisticated cyber criminals. These systems are called Operational Technology systems (OT), which are the systems operating the industrial facility. By gaining access to these systems malicious attackers may put the control of production in an unintended state and manipulate the monitoring systems. Today IEC 62443 is considered the series of standards for cyber security in industrial control and automation systems. What differs OT systems and traditional IT systems in a cyber security view, is the connection to safety and live operation of an industrial plant. As industrial facilities both have networks for information and operation, these systems are more critical and complex than standard office networks. The Purdue model is a generic reference architecture for traditional OT systems and their corresponding IT networks, which is used by most industries today.

Most of the advanced industrial attacks are conducted by specialized groups with high motivation and resources. As these threat actors do not give up until they have reached their target, it is important to have layers of cyber security protection in these systems.

We have seen a noticeable increase in cyber attacks the last decade, targeted against critical infrastructure. These attacks occur in different continents and target various sectors, e.g. manipulation of the centrifuge's speed in a uranium enrichment plant in Iran, shutdown of the national power grid in Ukraine and attempt of poisoning the water supply in a municipal water system in the United States. As for the latter, manufacturing plants for food and drinks need to consider food safety, which makes them even more complex and interesting. This is to ensure that the products have not been tampered with, e.g. added allergens, unintended ingredients and change of temperature. One interesting correlation between control systems and cyber security, is how cyber attacks against control systems can lead to loss of safety, both within the facility and for third party customers.

This thesis is a cooperation with Orkla, where Orkla has proposed the case and contributed with guidance. A cooperation in this manner is motivating for me and I hope that this work can contribute to Orkla's future.

1.2 Problem description

By discussing the topics from the background with the supervisor and co-supervisor, we decided to consider cyber security in manufacturing plants as the central topic. Thereby the main objective of this master's thesis is the following overall question:

> How should cyber security be handled in manufacturing plants, and how can testing of these systems be implemented to make them less vulnerable to attacks?

To explore the overall question, the following related topics will be studied:

- Which best practices for cyber security in OT systems that are transferable from other critical infrastructure industries to manufacturing plants
- How historical cyber attacks targeted against OT systems are relevant for cyber security in manufacturing plants today
- How penetration testing can be a tool to discover vulnerabilities and improve the cyber security barriers

The work has been split into the following main tasks:

1. Propose a generic Purdue model of the OT system for a manufacturing plant
2. Identify central terms within OT and cyber security and explain the series of standards IEC 62443. Also identify methods for risk and vulnerability assessments
3. Describe how the attackers approach OT systems, and their evolution over time. Also explore major, known cyber attacks targeted against OT systems. Point out causes, implemented countermeasures and recommended guidelines for avoiding such attacks in the future
4. With the Purdue model as a starting point: Plan and execute a vulnerability assessment of the OT system in manufacturing plants, and identify relevant cyber security barriers based on IEC 62443

5. Plan and execute a penetration test for parts of the OT system in an actual manufacturing plant. Utilize the results to identify actual security challenges, and show how the implementation of cyber security measures can be a method to contribute to improved cyber security

6. From the work in the aforementioned tasks, compare own findings to discoveries from the literature and recommend concrete measures for improved cyber security in manufacturing plants

1.3 Delimitations

As the focus is cyber security, details about the safety aspects of cyber attacks are limited. IEC 62443 is by most industrial actors today considered the preferred standard for cyber security in industrial automation and control systems, and will therefore have a wider coverage than other standards. In this thesis there is an overlap between risk assessment and vulnerability assessment and the main focus is the vulnerability assessment part. Due to limited time and resources, the scope of the penetration test has been simplified from the initial plan, which is attached in Appendix A.

1.4 Structure of the thesis

Chapter 2 presents the methods used. In chapter 3 the theory of industrial automation and control systems (IACS) and operational technology systems (OT) ans information technology systems (IT) in general is covered, and a specific network topology model is proposed for manufacturing plants for food and drinks. Then IEC 62443, which is considered the industry standard for cyber security in these systems, is explained. Chapter 4 first gives a historical overview of cyber attacks targeted against OT systems and then covers the types of attackers and how they approach OT systems. At the end of the chapter some selected major attacks are presented, and their corresponding countermeasures and lessons learned. In chapter 5 the cyber security barriers are considered and a risk and vulnerability assessment of manufacturing plants is made. Chapter 6 is the vulnerability part of the assessment and includes the process and execution of a penetration test of a real manufacturing plant. Chapter 7 is a discussion of the previous chapters and finally chapter 8 draws the conclusion.

2

Method

This chapter presents the methods used for the rest of the thesis. First the literature is described briefly, followed by my engagement within industrial cyber security. Then the method for the risk and vulnerability assessment and penetration test is considered.

2.1 Literature studies

ScienceDirect, which is a website where academic papers are published, has been the main resources for the literature studies. It has a huge database of new publications. The key search words for this thesis has been ”OT security”, ”Industrial cyber attacks”, ”Cyber attacker strategies” and similar. IEC 62443, especially part 3-2 of the series of standards, has been read thorough and is central for multiple parts of the thesis. Known cyber attacks against OT systems is another big part of the literature studies, which also considers the future of cyber attacks against OT systems.

2.2 Industrial networking

I am engaged in the professional forums CDS-forum, ROSS seminars and other seminars I have been invited to through my supervisor’s academic network, to utilize uptake of industry experience and knowledge. CDS-forum is an industry forum for cyber security in OT systems. In all these forums professionals share their experiences and knowledge within OT cyber security, and how to prepare for the future threat landscape. Through a penetration test of a manufacturing plant, in chapter 6, I have also learned from Orkla’s cyber security professionals, by digitally intruding a real manufacturing plant. In addition I am also interested in the latest industrial cyber security news, so I like to participate in cyber security conferences live and also watch video recordings of previous ones.

2.3 Risk and vulnerability assessment

IEC 62443 has been the baseline for the risk and vulnerability assessment in chapter 5. It is a methodically framework where a risk assessment determines how the system is divided into zones and conduits, and which demands need to be set for each part of the system. The risk and vulnerability assessment is divided into a risk assessment, which suggests security demands for each part of the system, and a vulnerability assessment, covered in chapter 6, which is a penetration test of a physical manufacturing plant.

The focus for the risk assessment is loss of food safety, which is modification of food production processes. There exist various methods for risk assessment that follows IEC 62443, like NAMUR, ISA TR and DNV GL RP G108 (DNV-GL, 2017). As none of these are specified for food safety, the chosen method for the risk assessment is to directly follow the steps in IEC 62443-3-2. These steps are covered in chapter 3.

2.4 Penetration test of a physical manufacturing plant

A test system has been set up in a physical manufacturing plant, where I in cooperation with security experts from Orkla, have executed a penetration test of the test system. The goal with penetration test is to gain access to an engineering workstation, and it is a white-box penetration test, which means that all available documentation on the networks and systems are given before the penetration test starts. The penetration test was physically executed at the manufacturing plant and lasted for five days.

3

Manufacturing plants and IEC 62443

This chapter will first present the manufacturing plants with corresponding Purdue model and the differences between Operational technology (OT) and information technology (IT). Then the IEC 62443 series of standards is focusing on cyber security in OT systems, will be presented.

3.1 Manufacturing plants with corresponding Purdue model

This section presents an overview of the network architecture in OT systems, which will be described in the next subchapter. First we will consider a generic network architecture model for industrial control and automation systems and then a manufacturing plant specific model. The components mentioned for both network architecture models are described below the manufacturing plant specific model.

As intrusion detection and cryptography itself doesn't protect the OT systems from cyber security threats, like traditional IT systems, other measures should be made. The IEC 62443 series of standards is specifically considering cyber security in industrial control and automation systems. The main philosophy is to separate IT and OT into segregated zones to control the data flow between them. It is based on the Purdue/ISA-95 reference architecture model, which can be considered an industry standard today (Williams, 1989). This model is shown in Figure 3.1 and will later in this document be referred to as the "Purdue model". The data flow between the IT and OT network must go through a demilitarized zone, shortened DMZ. This zone makes sure that only the accepted traffic between IT and OT can pass. The levels within the Purdue model and terminologies are described below the figure.

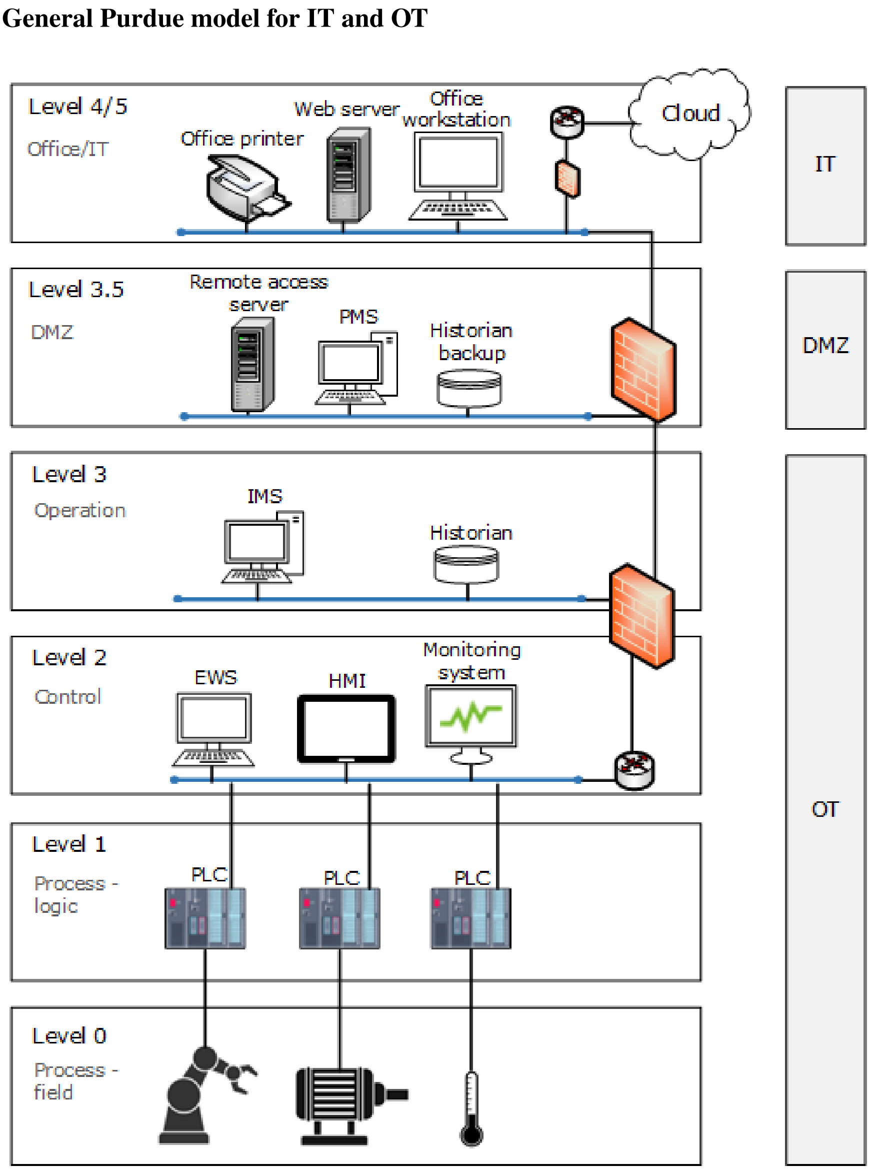


Figure 3.1: General Purdue model for IT and OT, adapted from Jaatun et al. (2021).

Based on the Purdue/ISA-95 architecture, Jaatun et al. (2021) defines each level in the Purdue model in Figure 3.1 as follows:

Level 4/5: Office network and enterprise zone, where connections to the Internet and external systems outside the company are separated by a firewall. This is typically vendor specific systems or applications that need access to devices in the OT network, and cloud services.

Level 3.5 (DMZ): Demilitarized zone between level 4/5 and level 3, which controls the data traffic between the two levels. All data from the OT network need to pass the DMZ to access the IT network, and vice versa. It consists of firewalls and devices, which make sure that level 4/5 can't directly access devices in level 3 and lower. The DMZ also handles ICT security, which includes servers and applications for monitoring incidents, malware and similar. ICT, Information Communication Technology means technology related to data communication.

Level 3: Applications like maintenance systems and other specialized operation systems, and corresponding servers for data backup. Traffic from level 3 to level 2 goes through a switch.

Level 2: Network for IMS, EWS, operator workstations and corresponding servers for data exchange. IMS is an information management system and EWS is an engineering workstation. An EWS can be located in level 1 or as an addition or alternative in level 2.

Level 1: Network for safety systems and process control, including controllers and corresponding servers for data exchange.

Level 0: The physical processes, including field devices for surveillance and control. Field devices are in some sources part of level 1, but as both DNV-GL RP G108 and ISA TR 84 00.09 define field devices in level 0, then level 0 is chosen here (DNV-GL, 2017).

Purdue model for a generic manufacturing plant

The Purdue model is a generic and industry independent model, used in both land-based and offshore industries. As different facilities will have some adjustments from the generic model, the main structure and segregation philosophy is kept the same for all industrial automation and control systems. As different industries and facilities have variations of the Purdue model, so does manufacturing plants. Figure 3.2 shows a generic Purdue model specific for manufacturing plants, which is adapted from a proposed structure from an OT system vendor. As a similar structure is used by the manufacturing plant for the penetration test in chapter 6, it has been chosen for security reasons, to not identify the vendor or manufacturing plant, as this is a ”live production plant” today.

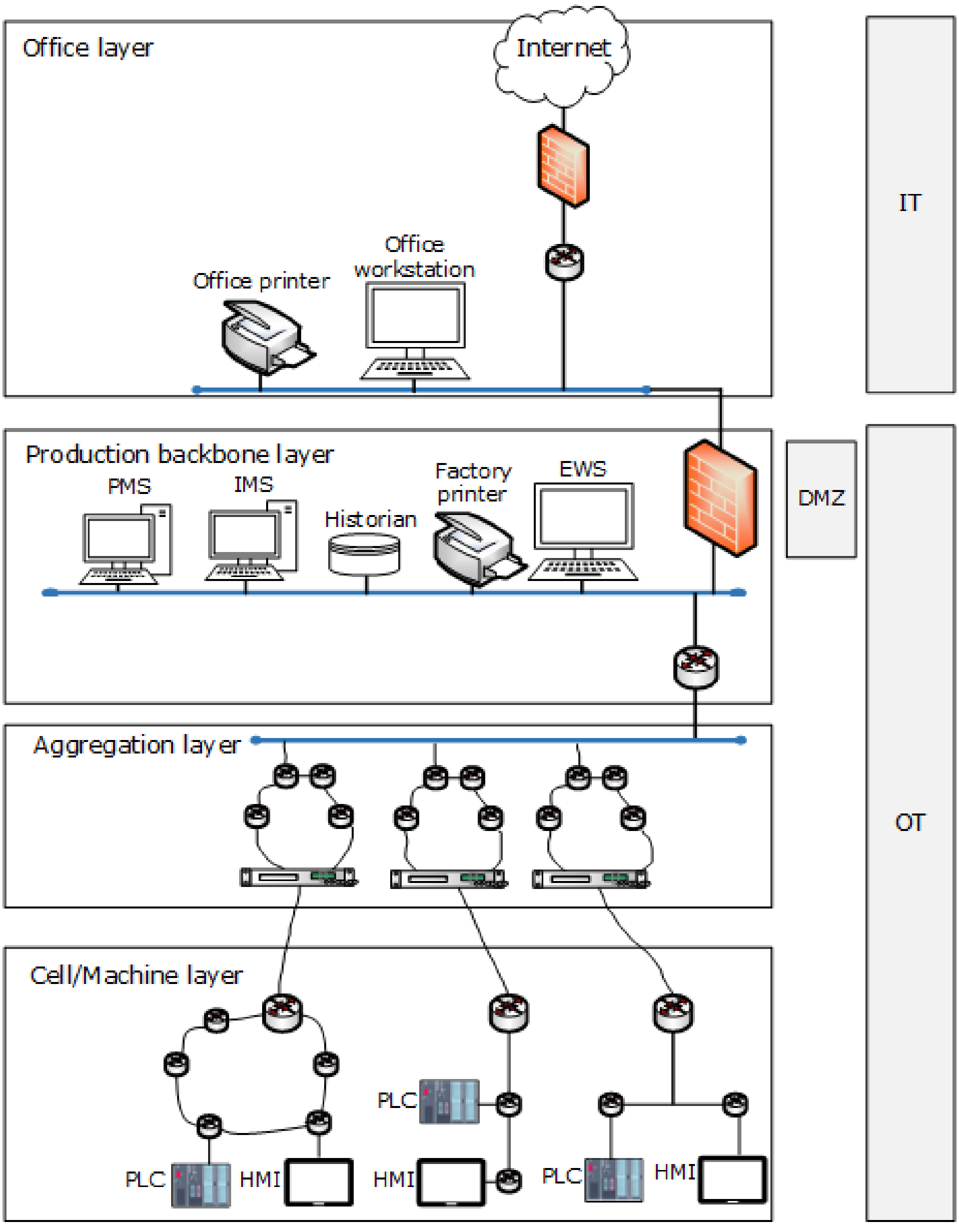


Figure 3.2: Purdue model for a generic manufacturing plant.

Each level in Figure 3.2 and its connection to the Purdue levels in Figure 3.1 is described below.

Office layer: This is the office network of the manufacturing plant, which typically consists of multiple office workstations, office printers and a network architecture to connect to the Internet through a firewall. It is the IT network, which corresponds to level 4/5 in the IT/OT Purdue model. Connections to and from the Production backbone layer must go through a DMZ firewall at the top of the Production backbone layer.

Production backbone layer: All the production systems except the process logic and process field devices are located here. These systems include systems for updating and patching software, monitoring data flow and production data and controlling the process logic devices. The traffic between the office layer and the production backbone layer must go through a firewall. Level 3.5, 3 and 2 from the IT/OT Purdue model forms the Production backbone layer.

Aggregation layer: The aggregation layer is a layer connecting devices and data flow between the systems within the Production backbone layer and the process logic and the field devices in the Cell/Machine layer. It consists of a ring network of switches, which means that every switch is connected to two other switches, which forms a ring, and the data flows from switch to switch. This corresponds to an intermediate level between level 2 and level 1 in the IT/OT Purdue model.

Cell/Machine layer: The process logic and field devices, which are illustrated as PLCs and HMIs in Figure 3.2, are located in the Cell/Machine layer. A PLC is a programmable logic controller that can control field devices. Each subsystem of PLCs, HMIs and other devices are connected to the Aggregation layer through various networks of switches. From the IT/OT Purdue model this layer represents layer 1 and 0.

The abbreviations and terminology in Figure 3.1 and Figure 3.2 is described below.

EWS (Engineering workstation): Computer on the production floor which is connected to process control devices, and can send executable program files to these systems. It is mostly used for diagnostics, maintenance and configurations.

Office Workstation: Computer in the office network which typically is connected to an office printer and used by a regular office employee. It has access to the public Internet through an enterprise firewall.

HMI (Human machine interface): A system visualizing data from control processes, which users can interact with. It can be a panel with buttons, an interactive screen or similar.

Firewall: A physical device or software that traffic needs to pass to travel through the network. It filters the network traffic based on the security policies set by the organization.

PMS (Patch management system): A system responsible for updating software on the machines in the industrial facility. It identifies unpatched systems and updates software to mitigate security holes.

IMS (Information management system): The system controlling and monitoring the flow of information within the industrial facility. This includes the features of accessibility, processing and distribution of information.

DMZ (Demilitarized zone): A zone separating the IT and OT networks, with high security demands. It typically consists of strong firewalls and is applied to add an extra layer of security protection between layers in the Purdue model.

Remote access server (RAS): Server for remote connection to the industrial facility. Can be used for remote control within the facility, by connecting to an EWS.

Historian: A backup server that stores and can restore system backups, which also can retrieve and collect information.

PLC (Programmable logic controller): Device connected to an EWS and field devices. It can run executable programs sent from an EWS and makes decisions for the connected field devices based on this program.

Switch: A switch is a connection point between devices or other switches in the network, which handles data packets. Illustrated in both figures above as a circular grey box with a red cross. A switch variant called a switch rack is shown at the bottom of the Aggregation layer in Figure 3.2.

3.2 Operational technology vs. information technology

Information technology (IT) is mostly information handling and consists of software and hardware processes and transmission of data. Operation technology (OT) is a familiar concept but differs from IT as it is the systems within industrial and critical infrastructure. As for IT, OT also handles data, but for OT there is a physical interface with different sensors and actuators, and field equipment that needs to be watched and handled. IT is primary used to have control over information, while OT primary is for controlling physical processes (Jaatun et al., 2021).

Modern power grid, transport systems, process facilities and fabrics are some of the industrial facilities that depend on OT-systems. Effective operation and safety are important aspects of OT systems, as physical processes and people are directly involved. Deviations from the expected values in the field devices can lead to huge destruction, in worse case loss of life, so it is important that the OT-systems controlling the processes ensures that the processes stay operative and are robust against errors and deviations.

OT systems are not commercially available for anyone, they get special adaption for its use and contents, and often consist of the organization's own developed hardware. Some OT systems may have the same functions as others and look to be similar, but it is often small and important difference between them physically and digitally. Physically it is in the aspect of which components that exist in the system and how they interact with each other. Digitally in the case of their technical specifications. One uniqueness of OT-systems compared to IT systems is that each different system has to be upgraded individually. It is assumed that the responsible personnel at the facility have high OT competence and understands how changes may affect the systems functions to avoid unwanted effects. The vendors of OT systems are usually the ones with the most knowledge on how it works and how it should be maintained. Often the OT-systems are maintained by the vendor themselves.

Within traditional IT security there are three main objectives, which in prioritized order are confidentiality (C), integrity (I) and availability (A), shortened CIA. Confidentiality is the principle of keeping data secret, typically prevent unauthorized access. Integrity means that data should be consistent and not changed during transit. Availability is the concept of information being accessible. Confidentiality is highly prioritized, because the needs to avoid unwelcome to get access to sensitive data is important. Accessibility is less critical, and IT users often have a certain tolerance for shorter periods of downtime.

For OT systems the CIA is also important, but because the main task is to control physical processes, the order of priority is different. Availability and integrity have higher priority than confidentiality, the order is the opposite compared to IT systems. In addition to the AIC, one can say that control of the processes has higher priority than the three others, so within OT the prioritized order is CAIC. This stands for control, availability, integrity and confidentiality. This is summarized in Table 3.1.

Table 3.1: IT and OT priorities.

Priority	IT	OT
1	Confidentiality	Control
2	Integrity	Availability
3	Availability	Integrity
4	-	Confidentiality

Traditionally the confidentiality and the integrity in IT-systems have been secured by access control where access is only granted for those who need to read and write a specific file. The most used access control model is discrete access control, shortened DAC. For this method one establishes a matrix that tells which users shall have which kind of access type (read, write, operate) to the specific file. Later the concept with role based access control, shortened RBAC was introduced, where specific roles are given rights (operator, leader and similar). This gives users specific rules for a shorter or longer period of time. When a person changes the department within the organization this person shall lose its role, and get a new role.

OT-systems usually control processes with highly damage potential. Therefore loss of control because of mistakes and shutdown needs to be avoided. In critical processes the tolerance for deviation may be so small that even short periods of downtime or mistakes may lead to critical and catastrophic situations. OT systems are therefore designed with the main focus on security and reliability, with diverse security barriers to avoid some mistakes caused by bigger incidents.

Traditionally, OT-systems have not been exposed for considerable cyber threats, so the security barriers have primarily been designed to make the systems more functional against accidental errors and situations. Cyber threats have mainly been handled to isolate the OT networks from its environment, so attackers and malware don't have access.

In the recent years it has been common to establish data traffic transmissions between OT systems and other networks, to get better overview over operations, simplify process optimization and make remote access support possible. Measures like this can increase efficiency and reduce the costs. It also causes more cyber risk because it leads to OT systems being exposed to threats from the Internet and other unsecured networks.

Compared to IT devices that can be security upgraded, OT systems are in general much less flexible, because they contain components that can't or should not be upgraded. OT systems have much longer expected lifetime than IT systems, and it is not unusual that OT systems last for more than 15 years in operation. Some OT components control important processes and should work without being disturbed by updates. Some OT system also operates software that doesn't have upgrades.

In the cases where OT components can have security upgrades, it will still be necessary to verify the upgrades before they are installed, to avoid the unknown side effects from the upgrades to cause problems in the OT system. Because of operational considerations, it is difficult to protect OT systems against cyber threats in the same way as for IT systems. OT systems are therefore in general much more vulnerable than the IT systems if attackers gain access to the system. The passwords strength and lifetime vary from system to system, but from the experiences and interviews from Jaatun et al. (2021) the password culture is generally weaker in OT than in IT.

3.3 IEC 62443

IEC 62443 is a series of standards focusing on cyber security in IACS systems, which is applied as the industry standard today. It is designed for reducing the risk of deploying and operating an IACS, and defines the roles of organisation, policies and processes which are applicable to each role. The roles of organisation are structured into the three types asset owner, system integrator and product manufacturer, which is described below (IEC, 2020).

Asset owner: Is an individual or organization who operates and owns a system which is responsible for one or more IACSs. Typically the asset owner is the end user.

System integrator: Creates a system by integrating components. The system integrator builds IACSs for the asset owners by integrating hardware and software from multiple product manufacturers.

Product manufacturer: Responsible for supplying and developing components for a system. The product manufacturer designs and creates the individual components that the system integrator uses to build the automation system.

The series of standards is divided into the four categories General (IEC 62443-1), Policies and Procedures (IEC 62443-2), System (IEC 62443-3) and Component (IEC 62443-4), as shown in Figure 3.3. The abbreviation TS specifies that the document is a Technical Specification and TR specifies that it is a Technical Report. The main focus in this thesis is part IEC 62443-3-2, but aspects from the other parts will also be considered. The main content of all IEC 62443 parts are shown in the figure. Each part and its connection to roles of organisation is described below the figure.

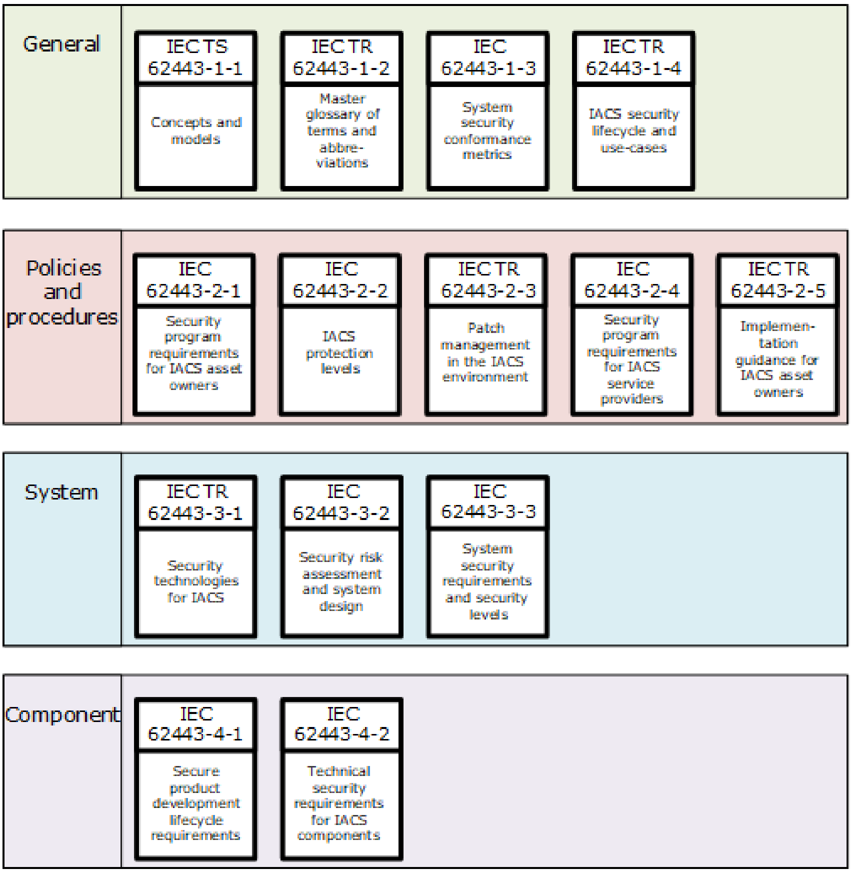

General
IEC TS 62443-1-1
Concepts and models
IEC TR 62443-1-2
Master glossary of terms and abbre-viations
IEC 62443-1-3
System security conformance metrics
IEC TR 62443-1-4
IACS security lifecycle and use-cases
Policies and procedures
IEC 62443-2-1
Security program requirements for IACS asset owners
IEC 62443-2-2
IACS protection levels
IEC TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Security program requirements for IACS service providers
IEC TR 62443-2-5
Implemen-tation guidance for IACS asset owners
System
IEC TR 62443-3-1
Security technologies for IACS
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Secure product development lifecycle requirements
IEC 62443-4-2
Technical security requirements for IACS components

Figure 3.3: Structure of the IEC 62443 series of standards, adapted from (IEC, 2020).

General (IEC 62443-1): It forms the foundation for the other categories, as it gives an overview of the IEC 62443 security process and introduce concepts which are found throughout the series of standards.

Policies and procedures (IEC 62443-2): Provides guidance on creating and maintaining a secure system, including security policies and risk management. This part is for asset owners who want to secure their network, as it will help to set up the cyber security policies. It will inform the asset owner what can be required from the system integrators and how these requirements can be measured. Policies are also defined, which allows the asset owner to confirm that the system integrator has applied secure products. In addition it conforms that these products has been adapted into a secure system based on the security policies, procedures and risk assessment.

System (IEC 62443-3): Provides guidance on designing and implementing a secure IACS, including cyber security technologies and mitigating methods. This is for system integrators and has two purposes: 1) assist the system integrator to evaluate the asset owner's requirements and translate them into a system design, and 2) provide a method to determine that the components bought from the product manufacturer have been securely developed and support the functionality that is required by the asset owner.

Component (IEC 62443-4): Describes the development lifecycle requirements and technical functionality levels for industrial network components. It is for product manufacturers and provides clearly defined objectives for the design and capability of the products. This ensures that the developed and manufactured products will meet the requirements of the system integrator.

During the CDS-forum seminar in May 2022, one of the authors of IEC 62443 presented what is new in IEC 62443. For the time being the committee is updating IEC 62443-1-1, IEC 62443-2-1, IEC 62443-2-2, IEC 62443-3-3 and IEC 62443-2-4. Also, a new part of the series of standards will be added, namely IEC 62443-1-5, which considers cyber security profiles and how a profile is described. It is also planned to include a security evaluation methodology for IEC 62443-2-4 in the next version.

The requirements based on the asset owner's Security Level Target, which is the desired security protection, flow down the chain from the asset owner via the system integrator to the product manufacturer. The solution based on the product and system security capability flows back up the chain to the asset owner. The connection between roles of organisation and part of IEC 62443, and the flow for requirements and solution, is shown in Figure 3.4.

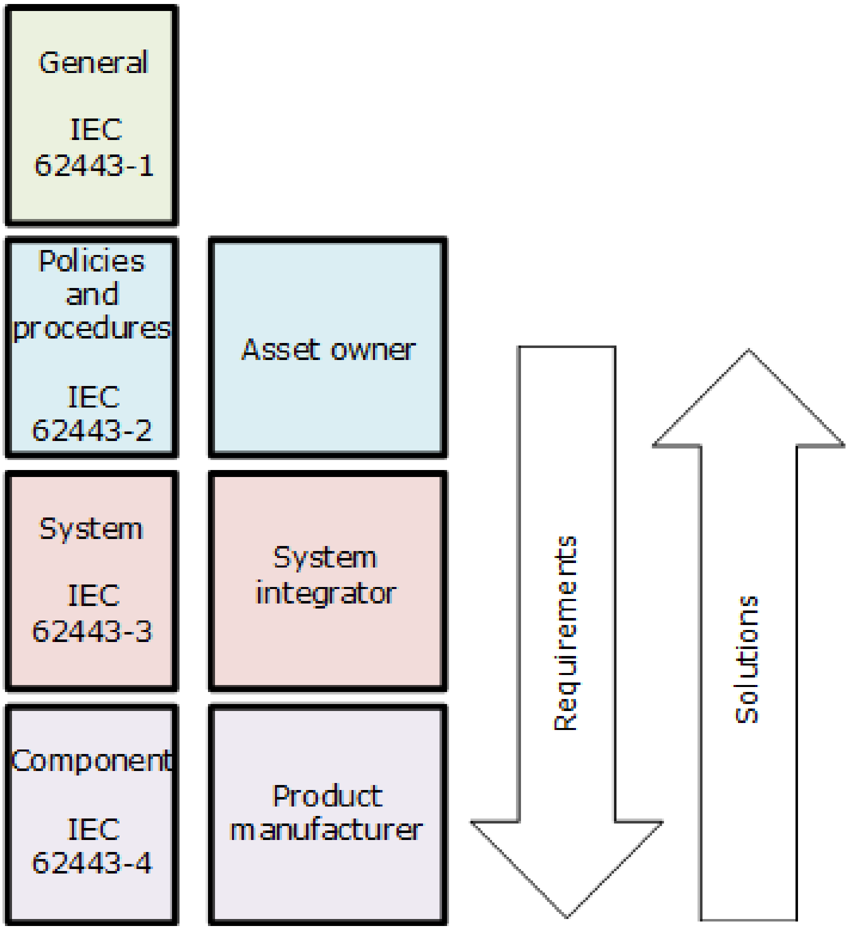


Figure 3.4: Correlation between IEC 62443 part, role of organisation, requirements and solutions.

In IEC 62443-3-2 the requirements for the risk assessment is set, which leads to the partitioning of zones and conduits. It also assesses the Security Level Target (SL-T) for the zones and conduits, based on the risk assessment.

Figure 3.5 shows the security lifecycle of OT systems, introduced in IEC 62443-3-2 (IEC, 2020). It also includes the relation between the different Security Level categories, and sequence of their implementation and verification. The steps marked with blue, alone or in combination with red, are briefly covered in this section and the steps in red are described in this section and will be applied in the risk and vulnerability assessment in chapter 5.

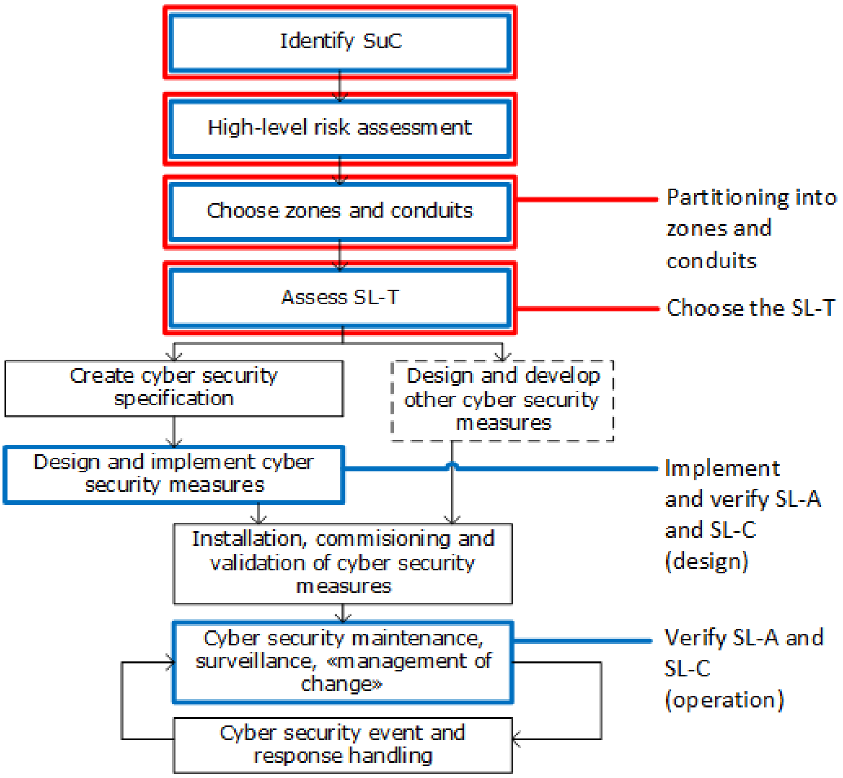

Identify SuC
High-level risk assessment
Choose zones and conduits
Assess SL-T
Partitioning into zones and conduits
Choose the SL-T
Create cyber security specification
Design and develop other cyber security measures
Design and implement cyber security measures
Implement and verify SL-A and SL-C (design)
Installation, commisioning and validation of cyber security measures
Cyber security maintenance, surveillance, «management of change»
Verify SL-A and SL-C (operation)
Cyber security event and response handling

Figure 3.5: Security lifecycle including the different Security Level categories.

Identify system under consideration, SuC

The system under consideration, shortened SuC, is the entire system to consider when performing a cyber security analysis. Before continuing to the next steps, the SuC needs to be defined, in addition to the security perimeter and every entry point to the SuC. The SuC shall contain all IACS systems necessary to form the automation solution, and can be illustrated by architecture diagrams, dataflows, network diagrams and system inventory.

High-level risk assessment

The main objective is to gain initial insight to the worst-case risks within the SuC, would it be compromised. The threats and vulnerabilities for the SuC shall be identified. This assessment identifies critical consequences that may arise from a cyber attack targeted against critical IACS operations. Assessing the initial risk is usually done with a risk matrix, where the initial risk is determined by the connection between the likelihood and severity. The risk and vulnerability analysis in chapter 5 applies one example of an initial risk matrix. The initial risk becomes the basis to determine the partitioning into zones and conduits in the next step (IEC, 2020).

Partitioning into zones and conduits

Based on the initial risk, IACS-related systems and components should be grouped into zones and conduits. The grouping could also be based on other criteria, like operational function, required access and criticality. The intention is to gather assets which share security requirements, to identify the common security countermeasures for risk mitigation. One should give special attention to systems directly related to safety and systems connected to Internet endpoints.

IEC 62443-3-2 suggests to follow these guidelines when partitioning the SuC into zones and conduits:

- Each IACS-related asset should be based on the initial risk. In addition, other important factors are operational function, criticality, required access and logical or physical location
- Business assets should be physically or logically separated from the IACS assets, as IACS assets may impact environment, safety and health
- Safety related assets should be physically or logically separated from non-safety assets. If separation is not possible, the whole zone should be categorized as a safety related zone
- Devices that are temporarily connected to the SuC, should be in a zone separated from devices permanently connected
- Wireless and wired devices should be separated in different zones
- Devices connecting remotely through external networks should be separated in a remote connection zone

DNV has published a report that presents guidelines and best practises of utilizing IEC 62443 (DNV-GL, 2017). In the report, DNV points out that the guidelines in IEC 62443-3-2 defines what to do, but not exactly how. The key suggestions from the report are grouped into the three categories *separation of zones*, *systems and networks* and *remote access* and are systematically presented in a project thesis from Endresen (Endresen, 2021), as seen below. This is a supplement to the recommendations from IEC 62443-3-2, as it is more detailed than the series of standards itself.

Separation of safety zones

Data from the safety zone to other zones should be read-only. In the case of a cyber attack, the safety functions should not be prevented. Safety system communication and process control communication should be physically or logically separated. Every safety system shall have a unique password, only available for authorized personnel. When safety systems and process control are connected physically in a network, they need to be logically separated.

Systems and networks

Functional or operational independent systems should be partitioned into different zones by firewalls. This is to reduce the likelihood that malware spreads to other systems and provides better access control for particular computers in selected zones. Also, this limits the exposure of the internal systems to external systems. All different systems within a zone should have the same criticality. If countermeasures can't be implemented for certain systems in the SuC, network segmentation can be a countermeasure in itself. These systems may have reached their end-of-support, so security patches and antimalware software can't be updated, so they should have limited access to other systems and be placed in a separate zone. If the number of zones within the SuC is too high, the security and availability may be affected, as administrative procedures are needed.

Firewalls should have a whitelisting approach, which means that only explicitly allowed traffic should pass. Within firewalls, the communication between zones should be controlled and logged, and the firewalls themselves should be monitored.

Wireless communication in office networks should be separated from wireless communication in industrial networks. Wired and wireless communication should be divided in one or more zones. Access to the wireless networks should only be granted for authorized devices, and strong encryption schemes should be applied, like TLS and WPA2. TLS, Transport Layer Security is a cryptography protocol for security and WPA2, Wi-Fi Protected Access, is a cryptographic method for wireless networks. Wireless connection to the office networks and industrial networks should not happen at the same time.

To reduce the attack surface, only a minimum of services and features should be available in software and hardware, and all unnecessary features should be disabled by default. As Microsoft Windows is the dominating operating system in IACS, one should auxiliary configure security parameters, both with a primary and secondary domain controller. Any unused protocols or ports, like HTTP, should be disabled, and access should only be available through secure methods like HTTPS and SSH, where the network ports only should be allowed for the required devices. HTTP, Hypertext Transfer Protocol, is an outdated transfer protocol without encryption. SSH, Secure Shell is a protocol where users can get access to a command line on another machine. HTTPS, Hypertext Transfer Protocol Secure, is a cryptographic and more secure variant than HTTP. Modification of firewalls and switches should be denied locally after it has been configured initially. Devices within the network should only be controlled by a remote administration with a centralized management account.

The principle of least privilege should be followed for user accounts. This means that users only should have access to their intended services and systems, but no more. Users with higher privileges should not be able to provide these privileges to other users, i.e. the principle of segregation. All passwords and user accounts should be stores in a secure manner. Computers that are not critical for operation should be automatically logged out after a given time of inactivity. A separate system to manage the software updates should be included as a Patch Management System. Communication to Microsoft update services through the Internet is not advised for the control systems.

Proper authorization needs to be implemented, i.e. the process of assigning rights or permissions to access a system resource. Only a minimum of authorization and roles should be given for each specific task, and every permission should be removed when the task is finished. Read-only and write permissions should be handled by separate systems. Production devices should not be able to access the data transmitted from the production to the enterprise network.

A system for malware protection, to protect against unwanted cyber attacks like viruses, should be installed on all computers. To monitor the protection status of every computer and manage malware incidents, a centralized server should be placed in a specific zone or in the DMZ zone, and include functionality for policies, updates and reporting.

To reduce losses, data corruption and downtime, a backup system with fast recovery is needed. Dissimilar backup types should be handled and stored by a dedicated backup server, and backups should be copied physically or sent to backup servers in other locations. Within the backup system, it should be impossible for malware to tamper with backup availability.

The conduits between high criticality zones should apply secure tunnels, which includes endpoints in each zone. A conduit is a connection between two zones, in which the connected zones can transfer data. In particular these conduits should be properly configured with mutual authentication, packet integrity and encryption. Cryptography is important for confidentiality, the principle of keeping sensitive data private. An encrypted file needs either a decryption key or a password to be decrypted. Today AES, Advanced

Encryption Standard, with key length of 128 bits or RSA, Rivest-Shamir-Adleman, with a key length of 2048 bits, are the recommended encryption schemes. Especially within IACS, it is important that the encryption devices are compatible with the applications, so the encryption itself doesn't affect the operations.

Remote access

For availability, the conduits for remote control rooms within zones of high criticality, is recommended to have two independent network routes between the remote control room and the local control room. Mutual authentication and verification and encryption of packets are recommended to be implemented for the conduits, to avoid unauthorized access, man-in-the-middle attacks and eavesdropping. Man-in-the-middle attacks means that attackers have gained access to the communication between two parties and can intercept the traffic. Eavesdropping is when attackers are able to see the data traffic between two parties and monitor their communication.

Remote file transfer should be handled by the Remote Access Server, shortened RAS, which also should be accessible from computers within IACS. Transferred files should frequently be scanned for malware. It is also important that remote service computers are patched and has the latest anti-malware software before connected to the IACS zones.

When connecting to the production network remotely, multi-factor authentication, shortened MFA, should be used. It is a multiple step process of identifying hosts, applications, network services and users. The most common types of MFA are unique tokens, SMS, passwords, PIN codes, access cards, fingerprints and facial recognition. To ease the process of identifying users, the remote access user accounts should be personal and exclusive. The login credentials for the office network and the RAS should differ. Cryptography should be used for the transferring of authentication data, and it is common to have an inactivity timeout for the authentication processes.

Full tunneling with cryptography is recommended to keep the communications secure during remote access. It means establishing a secure communication tunnel through the user's business network, from the remote account to the RAS. This is done using a VPN gateway. The most common technologies for VPN today are SSH, SecureShell, TLS, Transport Layer Security and IPsec, Internet Protocol security. VPN, virtual Private Network, is a service that gives access to a private network through a public network.

The RAS should either be put in a separate RAS zone or in the DMZ. A remotely connected resource not part of the process control should only have access to file transfer from the RAS. It should be possible for remotely connected users to upload files, but they need to be scanned for malware before they are available in the process control. When the task for a remote user is done, the secure tunnel should be terminated. For new remote connections, a new authorization and authentication process should be done.

Figure 3.6 shows a generic suggestion from DNV on how zones and conduits can be applied (DNV-GL, 2017). Each zones is marked with a dashed border. The goal is to show the partitioning of zones and conduits, so details of each device is omitted. The devices are similar to the ones in the Purdue model figures shown earlier in the chapter.

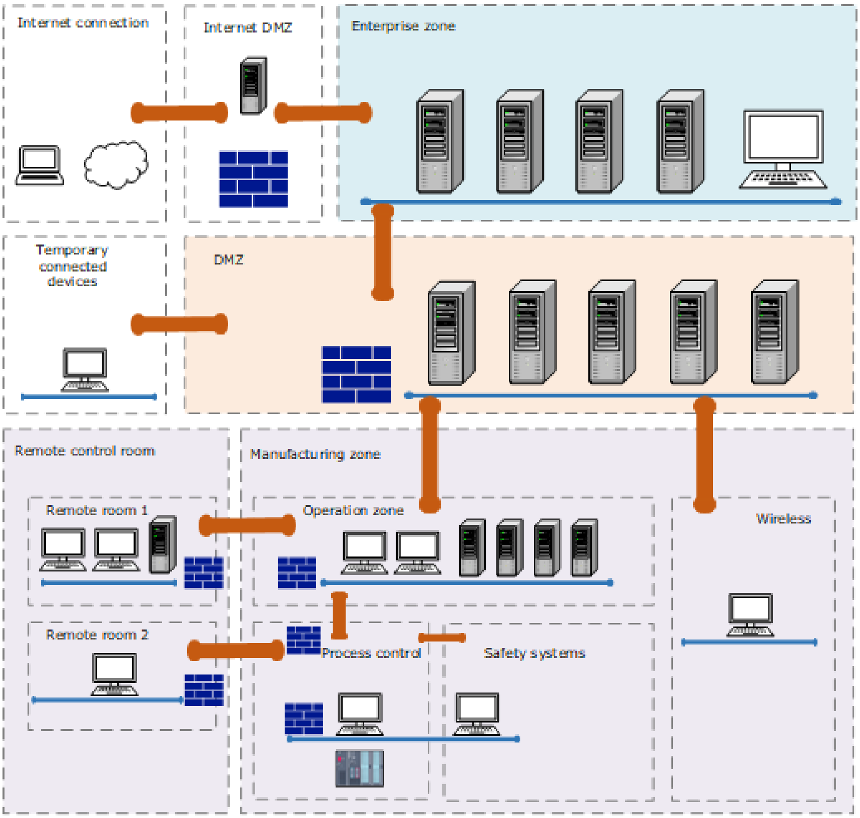


Figure 3.6: Example of zone and conduit partitioning, adapted from (DNV-GL, 2017).

Assess Security Level Target

Security Level (SL) is a categorization to determine demands for protection measures based on the level of threat. It consists of four SL levels ranging from SL 1 to SL 4. SL 1 corresponds to protection measures to handle simple digital threats and SL 4 for handling advanced threats from competent and resourceful threat actors. The Security Levels are categorized by IEC 62443-3-3 (IEC, 2020) into Security Level Target, shortened SL-T, Security Level Achieved, shortened SL-A and Security Level Capability, shortened SL-C.

SL-T, the Security Level Target, is in IEC (2020) defined as the desired level of security for a selected zone, conduit or IACS. The SL-T is usually assigned from a risk assessment, where the level is the needs of protection for the specific system or zone. Each SL-T is directly connected to and set according to the corresponding Security Level, as seen in Table 3.2.

Table 3.2: Security Level and Security Level Target.

Security Level	Description	Threat actor motivation	Security Level Target
SL 1	Protection against basic threats	-	SL-1
SL 2	Protection against moderate threats	Low	SL-2
SL 3	Protection against sophisticated IACS specific threats	Moderate	SL-3
SL 4	Protection against highly advanced IACS specific threats	High	SL-4

The SL-As check if a specific system meets the requirements set by the SL-Ts, and are the actual level of security that is achieved. The SL-Cs show the Security Level a specific, well configured system or component provides. It also shows if a specific system or component is able to achieve the SL-T without supplementary measures. As SL-As and SL-Cs are outside of the scope in this thesis, they are only described briefly. SL-T is covered more detailed below and applied in the risk and vulnerability assessment in chapter 5.

Every zone or conduits should be assigned a SL-T. According to IEC 62443-3-2 there exists no standard method for assigning the SL-T, so how the SL-T is established is up to each organization. Some organizations assign SL-T based on a risk matrix from likelihood and severity, and others establish the SL-T based on the security level description in Table 3.2. Another method is to choose SL-T by comparing the initial risk from the high level risk assessment and the tolerable risk set by the asset owner (IEC, 2020).

Note that there is a connection between the SL-T and the solution itself in IEC 62443-3 and IEC 62443-4. In the latter part one has concrete answers for what can be achieved by a SL-T. Another remark is that the overall security is not only implementation of systems and components, but also the maturity of the organisation. The overall security can be seen as a combination of system and component implementation and the maturity of the organisation. In chapter 5 we will see an application of the guidelines from IEC 62443-3-2 in a risk and vulnerability assessment for manufacturing plants.

4

Cyber attacks targeted against OT

This chapter will focus on cyber attacks from the last decades, targeted against OT systems. First a timeline of cyber attacks targeted against OT, from 1982 to 2021 is presented. Then the mindset and types of threat actors will be considered, as well as the type of targets they approach. Then we will have a closer look at some of the major known attacks. At the end we will have a look at the countermeasures, mitigations and what we can learn from these attacks. This chapter considers cyber attacks against OT system, and not specifically for manufacturing plants. The structure of different industrial control systems are similar, and the attacker strategies follow the same logic, almost regardless of type of industrial system. Therefore it is reasonable to draw lines from OT attacks to manufacturing plants, even though the majority of the events covered in this chapter is targeted againt other types of industries.

4.1 Attack overview and attacker approach

4.1.1 Timeline

Figure 4.1 is a timeline that combines OT related cyber attack from 1982-2020, from Iaiani et al. (2021) and Miller et al. (2021) and attacks from 2021 from Dragos (2022b). The events highlighten in yellow will be coveren more detailed in section 4.2. Figure 4.2 shows increasing number of public exploits in OT, which also means that the number of cyber attacks against also has an increasing trend. The reason for the low number for 2021 is that the Dragos report the figure is based on is published early in 2021, so all attacks from 2021 could not be included (Baines, 2021).

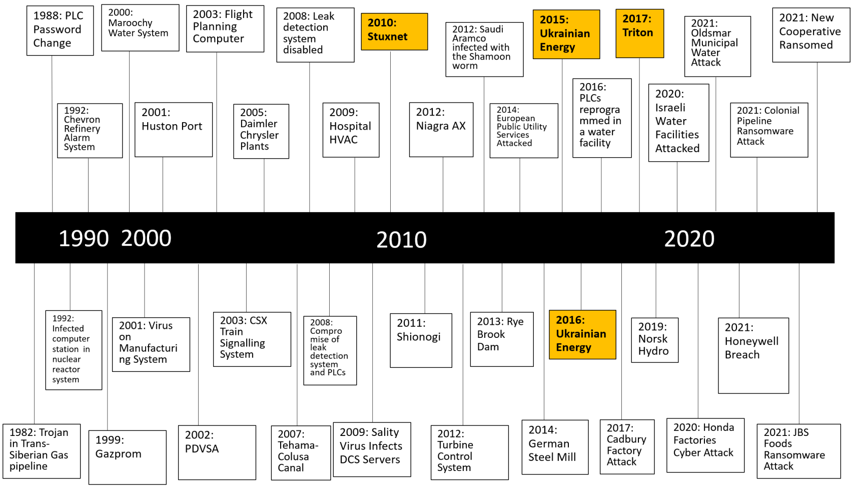

1988: PLC Password Change
2000: Maroochy Water System
2003: Flight Planning Computer
2008: Leak detection system disabled
2010: Stuxnet
2012: Saudi Aramco infected with the Shamoon worm
2015: Ukrainian Energy
2017: Triton
2021: Oldsmar Municipal Water Attack
2021: New Cooperative Ransomed
1992: Chevron Refinery Alarm System
2001: Huston Port
2005: Daimler Chrysler Plants
2009: Hospital HVAC
2012: Niagra AX
2014: European Public Utility Services Attacked
2016: PLCs reprogrammed in a water facility
2020: Israeli Water Facilities Attacked
2021: Colonial Pipeline Ransomware Attack
1990
2000
2010
2020
1992: Infected computer station in nuclear reactor system
2001: Virus on Manufacturing System
2003: CSX Train Signalling System
2008: Compromise of leak detection system and PLCs
2011: Shionogi
2013: Rye Brook Dam
2016: Ukrainian Energy
2019: Norsk Hydro
2021: Honeywell Breach
1982: Trojan in Trans-Siberian Gas pipeline
1999: Gazprom
2002: PDVSA
2007: Tehama-Colusa Canal
2009: Sality Virus Infects DCS Servers
2012: Turbine Control System
2014: German Steel Mill
2017: Cadbury Factory Attack
2020: Honda Factories Cyber Attack
2021: JBS Foods Ransomware Attack

Figure 4.1: Timeline of cyber events from Iaiani et al. (2021), Miller et al. (2021) and Dragos (2022b).

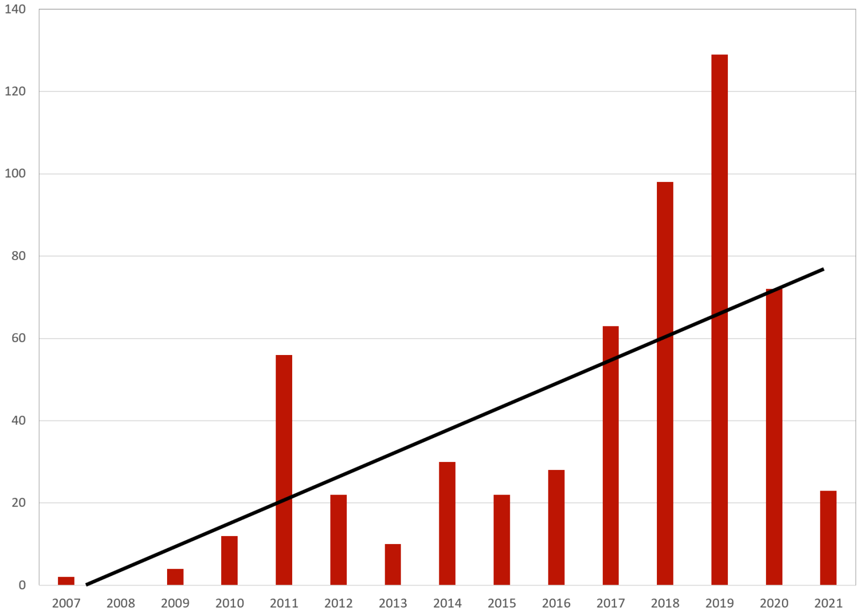


Figure 4.2: Evolution of public OT exploits, adapted from Baines (2021).

4.1.2 Attacker types, motivation and resources

According to the NIS Threat Actor Taxonomy, the attackers are often divided into the types insiders, professionals, hactivists, nation states and crime facilitators (Miller et al., 2021). The definition and strategies of the attackers are shown in Table 4.1.

Table 4.1: Hacker types and their strategies.

Type	Definition	Strategies
Insider	Ex-employee or unfaithful employee with inside accesses	Attack their company's systems by using internal knowledge
Professional	Hacker with high skills	Advanced attacks with customized code, and they cover their tracks
Hacktivist	Technical person who uses technical skills to front political agendas	Exploiting misconfigurations in web servers and public services and similar
Nation State	Skilled and well trained hacker, working for a government	Highly advanced attacks with multiple stages, where typically malware is installed, data is ex-filtrated and they stay in the network for a long time. These hackers often work in specialized groups
Crime facilitator	Hacker with access to hacking tools that knows cyber criminals are willing to use their tools	Selling or renting their exploitable code as a service

The motivations for insiders are typically revenge, or to inflict financial loss to the company. Professionals often seek financial gain or revenge and hacktivists typically wants to affect a company's reputation. Nation State actors will often want to destroy an adversary's infrastructure or ex-filtrate information, while crime facilitators mostly get motivated by money.

Another important aspect of attackers are their resources. Nation State actors sometimes have almost unlimited resources if the target is important, which makes them a dangerous threat for OT systems. Because of this nation state actors are often considered a bigger threat than other attackers with limited resources.

4.1.3 Attacker strategies

Figure 4.3 is further developed from Assante and Lee (2021) to connect the attacker objectives to the Purdue model. To the right one can see the most critical effects of a cyber attack for the corresponding Purdue level in the middle. Downwards to the left the degree of intrusion. This means that the most critical effects are in the lowest Purdue levels, where attackers can manipulate physical operational processes. The shape of the triangle corresponds to the surface of exposure, meaning that the wider surface, the higher degree of exposure. In context to the Purdue model this sounds reasonable, as most external attacks against the lower OT levels, must go through level 4/5 first, before propagating further down the levels. Remark that there in practise will be some overlap for the critical effects and Purdue level, especially for denial and manipulation for the lowest Purdue levels.

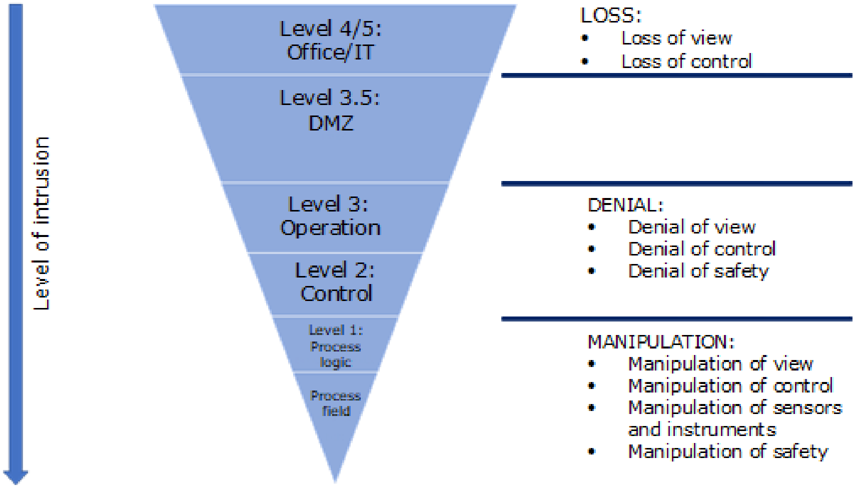
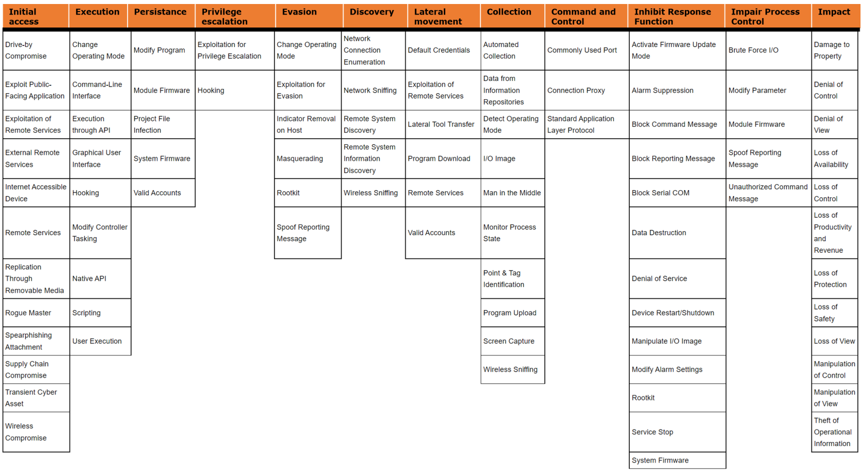


Figure 4.3: Attacker objectives corresponding to OT depth, further developed from Assante and Lee (2021).

MITRE, which is an ideal American organization that supports knowledge acquisition, do research and analyze cyber security incidents in both IT and OT systems. MITRE's ATT@CK for ICS is a knowledge base in the form of a website with associated sub-pages to explain which actions an attacker can do within an OT network. Figure 4.4 shows each main step and corresponding compromises for each row in a column. Each main step is described below the figure. By visiting the official MITRE ATT@CK for ICS website (MITRE, 2022), each step with corresponding techniques can be explored dynamically.



Initial access	Execution	Persistance	Privilege escalation	Evasion	Discovery	Lateral movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Figure 4.4: MITRE ATT&CK for ICS, adapted from MITRE (2022).

1. **Initial Access**: Gain a foothold inside the OT system. This could compromise IT resources and OT resources in the network and also external services and websites.

2. **Execution**: Infect the resources that have been accessed, so that the behavior of this equipment can be modified.

3. **Persistence**: Enable access and rights (privileges) that is obtained from equipment in the IT and OT system. It is not disrupted when, for example, new configurations, password updates etc. occur.

4. **Privilege Escalation**: Techniques that allow attackers to escalate their privileges and gain access to and control multiple systems and resources. Often necessary when access is protected through various layers of protection. Often achieves this by looking for exploitable vulnerabilities and misconfigurations in the systems.

5. **Evasion**: Remove or circumvent the possibility to be discovered. This can happen by compromising the system that is supposed to monitor and detect abnormal traffic and software changes.

6. **Discovery**: Try to map internal networks within the OT systems, the controllers that operate the processes and how they interact.

7. **Lateral movement**: Establish a connection between the OT network and itself, via equipment that has the functionality to connect externally through a firewall.

8. **Collection**: Overlaps in part with the purpose of step 6 (discovery), but here the attacker has created a better connection to extract data from step 7.

9. **Command and control**: Put the attackers in a position to communicate and manage compromised devices in the OT network, as an engineering workstation. Here the attacker has the option to start a download of new software or change data that is sent or displayed on the operator screen, or a combination of these.

10. **Inhibit response function**: Ensure that step 9 was successful without defensive countermeasures limiting the attack. This can propagate to block possibilities to carry out actions and prevent alarms from being given.

11. **Impair process control**: Allow attackers to directly change inputs and outputs on I/O cards, change parameters and inject malware in hardware updates for the controllers. I/O cards are devices that bridge a computer to another device, with input and output capabilities.

12. **Impact**: Disrupt, manipulate and destroy the functionality and integrity of processes and data so that the objective of the attack is achieved. In some contexts, such a goal can be to create confusion as a technique to hide the digital attack.

Traditional military kill chains show the structure of military missions for an aggressor, which consist of four steps, a) identify the target, b) dispatch forces to the target, c) initiate the attack on the target and d) destruct the target. The Cyber Kill Chain is an adaption of the military kill chains, but specified for digital cyber attack against IT systems. The method has been further evolved to consider digital cyber attacks against OT systems, namely The Industrial Control System Cyber Kill Chain. SANS has published a report describing typical steps in the latter (Assante and Lee, 2021). Industrial Control System, shortened ICS, is a term also used for an OT system. The report shows a systematic identification of how the attackers approach ICS systems, step by step, similar as for the military kill chains.

The Industrial Control System Cyber Kill Chain is divided into two stages, where stage 1 handles preparations for the cyber intrusion and stage 2 considers the development of the ICS attack. Each stage is presented in detail below, to a corresponding figure, as shown i Figure 4.5 and Figure 4.6.

This is also a useful method for defenders. By knowing the attacker steps as a defender, it is easier to identify and implement preventing countermeasures.

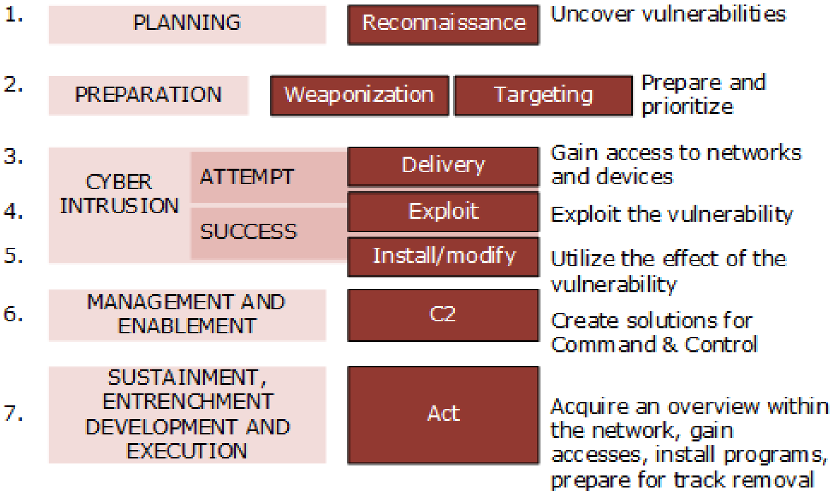

1.
PLANNING
Reconnaissance
Uncover vulnerabilities
2.
PREPARATION
Weaponization
Targeting
Prepare and prioritize
3.
4.
5.
CYBER INTRUSION
ATTEMPT
SUCCESS
Delivery
Gain access to networks and devices
Exploit
Exploit the vulnerability
Install/modify
Utilize the effect of the vulnerability
6.
MANAGEMENT AND ENABLEMENT
C2
Create solutions for Command & Control
7.
SUSTAINMENT, ENTRENCHMENT DEVELOPMENT AND EXECUTION
Act
Acquire an overview within the network, gain accesses, install programs, prepare for track removal

Figure 4.5: Cyber Kill Chain, stage 1: Preparing the cyber intrusion, adapted from Assante and Lee (2021).

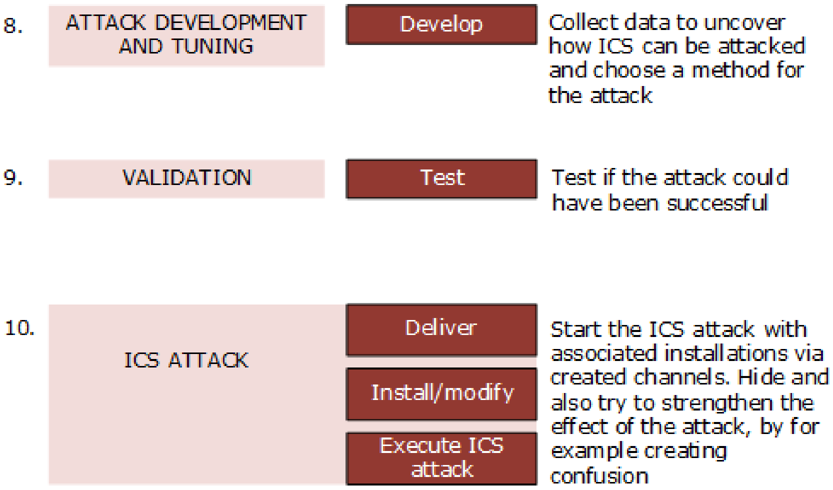

8.
ATTACK DEVELOPMENT AND TUNING
Develop
Collect data to uncover how ICS can be attacked and choose a method for the attack
9.
VALIDATION
Test
Test if the attack could have been successful
10.
ICS ATTACK
Deliver
Install/modify
Execute ICS attack
Start the ICS attack with associated installations via created channels. Hide and also try to strengthen the effect of the attack, by for example creating confusion

Figure 4.6: Cyber Kill Chain, stage 2: Developing the ICS attack, adapted from Assante and Lee (2021).

The OT related cyber attacks that is shown in Figure 4.1 are described in detail in their papers (Iaiani et al., 2021; Miller et al., 2021; Dragos, 2022b). These events will not be covered in detail here, so to get a deeper understanding of the events it is recommended to read these papers. I have analyzed the events by classifying each attack's main target and the attacker type, which is shown in Figure 4.7. The figure is briefly discussed below.

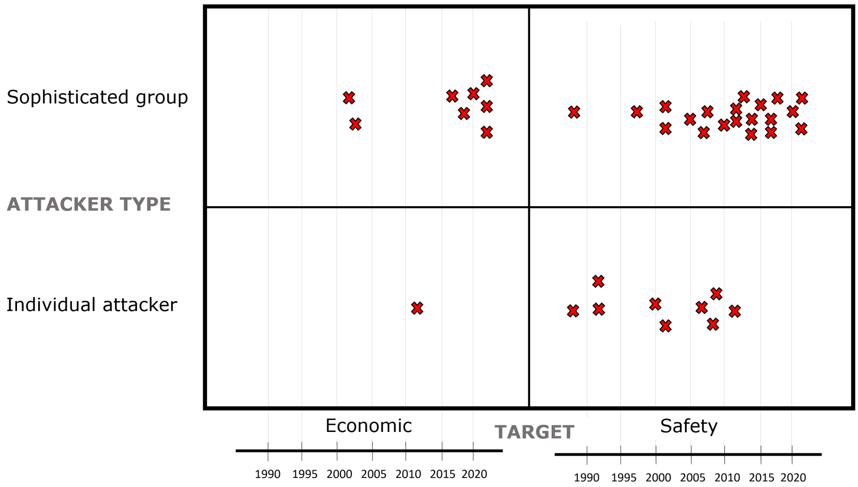


Figure 4.7: Classification of the cyber attacks targeted against OT.

The total number of classified attacks is 38, where the attacks span from 1982 to 2021. As the attacks have evolved over decades, so has the target and type of attackers. From 2010 one can see a clear increase in the number of attacks from sophisticated groups, especially those with safety as the target. This can probably draw parallels to the known massive attacks, like Stuxnet, the attacks against the Ukrainian energy and Triton. The degree of sophistication for sophisticated group varies, as both nation-state actors and creators of comprehensive OT related malware, are classified in this category. As comprehensive malware for advanced OT attacks needs year of expertise and experience to plan, develop and execute, it was decided reasonable to categorize these attackers as a sophisticated group as well.

In total, 9 of the attacks were classified as individual attackers with the target safety. In 100% of these the attacker was either an insider or a disgruntled employee. As success attacks against safety systems need prior knowledge of the systems, this result sounds reasonable, because it would have been unrealistic if a high number of external, individual attackers were able to damage the safety systems. Insiders or disgruntled employees have access to or prior knowledge about the systems.

One can see clearly that the number of attacks done by sophisticated groups have drastically increased from the early 1980s until today. Between 1982 and 2000 33.3% of the attacks were done by a sophisticated group, between 2000 and 2010 46% and between 2010 and 2020 93%. In 2021 100% of the considered attacks were done by a sophisticated group. As sophisticated groups have big resources, high motivation and high level of expertise, this means a higher threat level for OT system defenders. There is no longer enough for defenders to defend against basic threats and assume that threat actors can't penetrate their OT system. In 2022 you can't say that a digital system is ”unhackable”, because it should be assumed that highly advanced threat actors with unlimited resources and high motivation, may be able to break into any system. Therefore the question is how much resources defenders are willing to use to make it as hard as possible for attackers to break in.

4.2 Selection of major influential attacks

This section will now have a closer look at the events Stuxnet, the attacks against the Ukrainian Energy and Triton. Every attack is structure in four parts: Overview, figure, Step by step and recommendations. The first part is an overview of the attack, which is followed by a figure visualizing the attack. In all figures the red arrows and circular numbering represents the attack in chronological order. The black arrows are possible side effects of the attack, and the levels on the right are corresponding to the Purdue levels. BE in the figure for the Ukrainian energy, is shortened for BlackEnergy, the malware for the attack. After the figure, each step of the attack is listed and recommendations from the attack are briefly discussed. At the end some countermeasures, mitigations and lessons learned are considered for all of the three attacks. In order to understand some mechanisms mentioned in the selected attacks below, some terminology is described first.

Zero-day vulnerability: Vulnerability that is unknown to the organization, that has not been mitigated.

Rootkit: A system that is installed on the victim's computer to have full access to the system, without authorization.

SIS (Safety Instrumented System): .

SIS (Social engineering): A system to ensure that safety is preserved if an incident occurs. It makes sure the system goes to a safe state if something is not as intended within the system.

Remote access trojan (RAT): A remotely controlled malware that lets attackers have access to the victim's computer.

Remote code execution: A type of attack where commands on the victim's computer can be forced remotely by an attacker.

DLL file: Executable file, which can be used for modular processes.

Link file: A file that is a Windows shortcut for another program.

Dropper: A type of malware that install other malware.

P2P: Peer-to-peer a way to organise resources in a network.

Trojan: A type of malware that pretends to be something legitimate.

Botnet: A large number of computers cooperating to typically participate in a major attack. They are often used for denial of service attacks.

OLE loader: A system that loads objects into the memory of a computer.

CVE code: A code for a vulnerability that has been patched after it has been discovered.

Man-in-the-middle attack: Attack where an attacker can intercept the communication between two parties.

4.2.1 Stuxnet

Overview

Stuxnet is considered to be the world's first publicity digital weapon and is a standalone computer worm that requires no Internet access to propagate. It attacked Iran's nuclear facilities in 2010 and the malware's main target was to control the industrial system by infecting specific models of Siemens PLCs to make them deviate from their normal activity.

The computer worm initially spread via Microsoft Windows, where Siemens industrial software and equipment were targets. The malware checked the connection to specific models of Siemens PLC's, altered several copies and did some PLC programming. This resulted in centrifuges spinning too quick and too long, and the equipment was damaged or destroyed. False signals were also sent to the HMI, and for a substantial period no one saw anything suspicious and thought the system was running as normal.

Stuxnet exploited several remote code execution vulnerabilities in Windows where at least three of them were zero-day. Use of a self-launching zero-day vulnerability made the fast distribution of the malware in the targeted region possible (Firoozjaei et al., 2021). Significant autonomy was demonstrated and became a good example of a "fire and forget" type of malware (Kumar et al., 2022).

Stuxnet controls the worm with a large DLL file that replaces a Step 7 DLL file. Step 7 is a Siemens program on engineering workstations used to program and organize executable programs for Siemens PLCs. It also needs resources like rootkit drivers and an USB loader DLL file. Within the large DLL file the files are delivered by the Stuxnet dropper. The worm is a link file (.LNK) and a rootkit that works together to run the malware. For propagations and execution, the worm exploits vulnerabilities. The link file (.LNK) propagates the worm to automatically create several copies and makes the Stuxnet rootkit avoid detection. This is done by hiding all malicious files and processes. It also has root modules as a user mode and a kernel mode (Firoozjaei et al., 2021).

During the first loading of the malware's dropper, the victim's evaluation and compatibility like Windows and antivirus version, determines and checks the possibilities for the machine to be infected, and if it has been infected. The injection method is based on the antivirus version number. The injection process stops if the security product can't be bypassed. It injects the DLL files, which are lsass.exe, winlogon.exe and svchost.exe, into the chosen process. Without the administrator rights on the infected machine, a zero-day privilege escalation attack is executed. The Stuxnet malware alters security mechanisms to evade detection on the victim's system. By creating a rootkit specialized for Siemens PLCs, the modified code on the PLCs was hidden and the data sent from the PLC and HMI displayed incorrect information for the operator.

The Siemens Step 7 software uses the DLL file 7otbxdx.dll by hiding the file for communication with the PLCs when it is installed and executed. The original 7obxdx.dll file renames the file to s7obxsx.dll with its own version and the PLC rootkit code contained entirely in the fake DLL file. Without the PLC's operator realizing it, the Stuxnet malware modifies transmitted data and intercepts the communication between the controller and the PLC. Adversarial techniques like rootkit, PLC rootkit, masquerading, antivirus tricking, zero-day exploits, network discovery and P2P updates, process injection and Command & Control connections were used in the Stuxnet attack (Firoozjaei et al., 2021). Figure 4.8 shows the steps of the attack which are also described below.

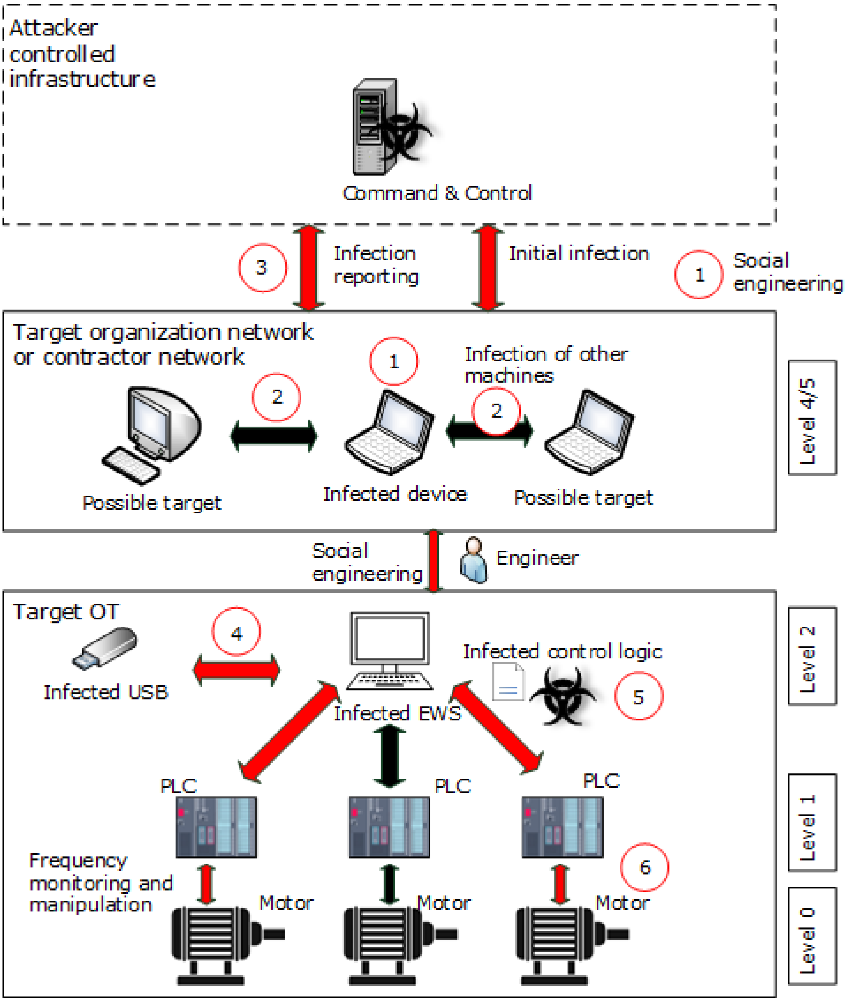


Figure 4.8: Stuxnet, step by step, adapted from Makrakis et al. (2021).

Step by step

- Since there is no consensus how attackers gained access to the restricted area of the ICSs, it is believed that the access was possible by insiders or through snooping (Kumar et al., 2022).
- Initiated through a corrupted USB drive targeting the Windows operating system the attack exploited the LNK/PIF (MS10-046) zero-day vulnerability (replication through removable media). It then exploited a windows server service (MS08-067). To evade automated detection, two stolen digital certificates were used.
- Privilege escalation was obtained by the MS10-073 and MS10-092 vulnerabilities.

Then the characteristics and model of the control systems for Siemens' WinCC/PCS7 (Remote System Information Discovery) were determined. With the correctly identified targets, the attack then attempted to gain access to download the most recent version of the malware on the internet.

- With the malware in the right machine, the WinCC DLL drivers for the vendor replaced files (especially the s7otbxdx.dll file), WinCC software and the targeted PLC device through a malicious communication. The PLCs were reprogrammed so the rouge code was injected into the controller.
- While taking occasional control (man-in-the-middle) to avoid detection, the malware permitted the controller to run the legitimate code and open Step 7 PLC program files.
- At last, to fake the signals of the industrial process control sensors, the installation of an industrial rootkit was utilized. Despite the abnormal behavior, no alarm or no shutdown were triggered thanks to this step.

Recommendations

A based line protection like regular software updates, application whitelisting, intrusion detection systems, antivirus, firewalls, strong passwords, network segmentation etc. of enterprise-based security measures, should be used.

The malware was allowed to modify the control parameters of the centrifuges because of the lack of encryption between the PLC and SCADA systems. SCADA, supervisory control and acquisition, is an architecture for control system s with a graphical interface. If the use of selected protocols were monitored, forbidden communication and use of network scanning would have been detected. One of the critical social engineering mechanisms is the corrupted external removable drivers gaining a foothold inside the organization. Regular cyber security drills and training sessions are important to be aware against social engineering attacks (Kumar et al., 2022).

4.2.2 Ukrainian Energy (Crashoverride/Industroyer)

Overview

BlackEnergy is a malware that was first acknowledged in 2007 and started as a web-based Distributed Denial of Service (DDoS) trojan. It was designed to automate criminal activities and evolved over the years to undermine system resources. Later it evolved into a sophisticated malware with various supporting plugins. In December 2015 a noteworthy attack using BlackEnergy, was discovered in the electric power grid of Ukraine, where several electric substations from the main power grid were targeted and disconnected. For several hours 225 000 people in three regional power distributions were missing electricity (Kumar et al., 2022).

BlackEnergy is a malware family and an HTTP-based botnet for DDoS attacks with three currently known versions (Firoozjaei et al., 2021). BlackEnergy-1, the first version is used for DDoS attacks, and is HTTP-based. BlackEnergy-2, the second version is used to set up a C&C server and modern rootkit and process injection techniques with server-side scripts. This version also consists of different components and is modular where the primary motivation is data theft. By exploiting vulnerabilities in the internet connected ICS devices, the malware gained access to networks, specifically to HMI products from various vendors, like GE Cimplicity and Siemens SIMATIC WinCC. BlackEnergy-3, the third version, affects a system with a spear phishing attachment resource. It was implemented in the power grid attack against Ukraine in 2015, where various plugins were allowed in their systems. Phishing attacks were probably the initial method to install the malware, either as an attached, infected document in an e-mail or as a link. Later it pivoted into the SCADA networks.

In December 2016, exactly one year later, after the attack with BlackEnergy-3, the whole city of Kiev was left in darkness, and once again the Ukrainian power grid was suspected of being hacked. It was the attack called Crashoverride/Industroyer that targeted a new cyber attack against the Ukrainian power grid, causing massive damage in Kiev. The damaged equipment was mainly the electric circuit breakers and underlying hardware, with communication protocols that controlled the electricity substation's switches. It had no zero-day exploited, and relied on existing Microsoft Windows with built-in tools as PowerShell. This means that it intruded into the ICS network, downloaded other parts of malware and targeted libraries and configuration files of the HMI to further understand its operating environment. The malware's backdoor is the main part, which consists of supporting payloads for mapping the network.

When the ICS network has been accessed, and the targeted system has been deployed as a system service by the launcher, the malware's abilities remains after the system reboots. The payload modules to target RTUs (remote terminal units) and toggle related values were then loading. A RTU is an electrical unit connecting objects to a SCADA system. These modules made it possible for the malware to find RTUs in the network, and to communicate with devices and make the circuit breaker status change. To get a substation to de-energize, circuit breakers on RTUs are forced to open an infinite loop, and still keep it open if the grid operators attempt to shut them down. The malware then used the issue of valid commands through selected industrial control devices. To open the circuit breakers these commands were sent directly to RTUs over the ICS communication protocol. To keep the circuit breakers open, an infinite loop was created. The wiper module manipulated registered values in the final stage of the attack, and made it difficult to recover. Registry entries were replaced with empty strings to make the operating system unbootable. The filename haslo.dat or haslo.exe of the component was executed by the launcher (Firoozjaei et al., 2021).

The core and the common part of this malware family is the dropper. Via different payloads with the file extensions of Microsoft documents, e.g docx, xls, or ppt, Java update scams, backdoor files, the malware can be delivered as a fake document on the victim's machine. In the power outage attack in Ukraine, the delivery of the dropper happened by a spear-phishing e-mail that contained an XLS attachment with a malicious macro inside. Macros are additional functionality within documents that allows programming, which can be manipulated to include malicious scripts.

The malware file was attached to weaponize a Microsoft Excel worksheet that contained the dropper of the malware. Once it was executed, it downloaded the malware files. Files located in the folder Windows/System32/drivers required root privileges for execution, but the main target were HMI workstations in the industrial control networks. Different vendors of HMI products were infected and targeted to deliver the malware payload named General Electric Cimplicity, Advantech/Broadwin WebAccess and Siemens WinCC. Modules that scan any network connected files and removable media are typical BlackEnergy infections, that propagates the malware laterally. To interact between the C&C server and the infected host, the malware has a remote procedure communication module. Months before the event, around 6 months or more, the payload was delivered to the host machine. It performed basic reconnaissance operations and was harmless for the entire period, but delivered the payload and wiped disks on the date of the attack. The BlackEnergy-3 is written in Visual C++ with over 309 functions, where 140 variables were found in reverse analysis. Payloads in the script are the vulnerable host support such as Visual Basic Advanced Macros for Microsoft Word and OLE loaders for Microsoft PowerPoint.

Windows-based machines that were used as HMI and power administration servers were the main target in the BlackEnergy-3 attack. By a reconnaissance attack with the ability to access and control field devices and equipment configurations, network discovery was performed to detect an internal server or HMI device. Where the internal server or HMI had the most controlled flexibility, the dropper was implanted. To gain complete control of a VirtualBox privilege escalation vulnerability, the attackers used BlackEnergy with one or more plugins for network scanning, keylogging, network discovery, remote execution, password stealer, and remote desktop.

With a stolen account, the attackers logged in to the VPN network and the VBoxDrv.sys service in the domain controller was installed. This vulnerability (CVE-2008-

3431) made it possible for the attackers to execute malware components by virtualizing the guest Windows operating system and to bypass the driver signature enforcement. By a user with administrator privileges, the SCADA system was remotely controlled and configured in the case of the power cut to remain switched off. By listening on port 6789, an SSH backdoor in the HMI was opened by the BlackEnergy malware, which altered configurations of inverters. To make the restore of the power system problematic, and destroying the entire file system, disks on the control server and HMI were wiped out and the master boot record destroyed by the KillDisk component of the malware. KillDisk a software to erase hard drives. Without manual intervention, forensic evidence made it possible for the systems to be restored.

The attackers also disrupted a call center service for the power company's center with a DoS attack. A DoS attack is an attack where services are sent a huge load of traffic so can't operate as intended. The blackout in the Ivano-Frankivsk regions of Ukraine was the most visible impact attack where at least 30 substations were opened. It took more than six hours to restore and more than 225 000 people were affected. Several techniques were used to deliver the dropper, replace the malicious drivers, manipulate service status, and connect to the C&C server (Firoozjaei et al., 2021).

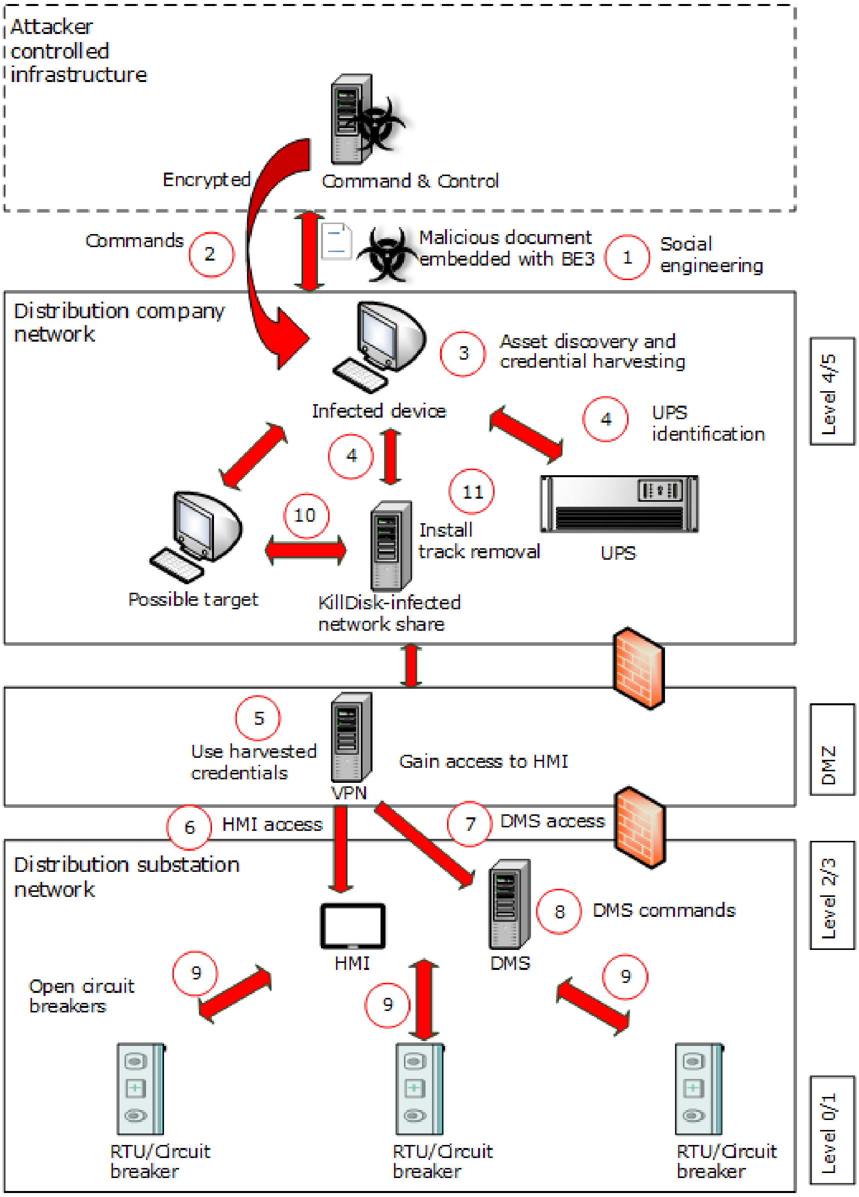


Figure 4.9: Ukrainian energy attack, step by step, adapted from Makrakis et al. (2021).

Step by step

- To target system administrators at local utility companies, the attack launched through a spear-phishing campaign, targeted against the system administrator. By impersonating government employees the attackers pretended to be legitimate vendors. E-mails with Microsoft Word (CVE-2014-1761) and Microsoft PowerPoints attachments (CVE-2014-4114) were embedded from the malware (Kumar et al., 2022).

- A malicious program was installed in the local application data to deliver the malware, once the endpoints were compromised. All the drivers, including the malicious one, caused a system restart when the program enumerated.
- By self-signature, the malware elevated its privileges to administrate the use of the "TESTSIGNING" feature by Microsoft. To bypass the cautionary test watermark, this was removed.
- To create a backdoor to the system when the malware had gained access, it installed a remote access tool. To enumerate the network and maintain persistence, the attackers did lateral movement in the IT environment, where they gathered credentials and communicated with the C&C.
- The malware called "KillDisk" that was installed on the infected endpoints could overwrite most of the files. To make the system unbootable, the malware could then corrupt the master boot record.
- To allow the malware to access workstations, servers and HMIs, it obtained the VPN credentials and gained access the remote system in the OT environments.
- The attackers carefully planned and coordinated a wide-scale attack, after penetrating the OT layer on all the infected power stations where they additionally launched a DDoS attack on the telephone system to delay reporting in the region.
- At last, the attackers disabled the back-up power supply, applied firmware updates to disable communication and a complete remote access were gained by the attackers.

Recommendations

It is recommended to use strong password and MFA for VPN connections and do regular monitoring of user accounts to prevent privilege escalation (Kumar et al., 2022).

4.2.3 Triton

Overview

In 2017 the control system of an oil and gas plant in Saudi Arabia was detected as the Triton (also known as TRISIS or Hatman) malware. Schneider Electrics' Safety Instrumented System (SIS), called the Triconex safety controller was the target. A SIS was specifically targeted for the attack and was monitoring the status process of the autonomous control system. To obtain a process where parameters define a hazardous state, the SIS attempts to get back to a safe state or automatically perform a safe process and a safe shutdown whenever a parameter value exceeds a threshold. Triconex are used as safety controllers in 18000 plants in various industry sectors. In the Triton attack, the Tristation communication protocol is used by a Triton SIS to change the logical final control element and to insert malicious firmware to affect all safety controllers running this protocol (Firoozjaei et al., 2021).

Like Stuxnet, a DLL replaced a malicious one in the Triton attack (Kumar et al., 2022). Files related to safety PLCs and binary components on a workstation can appear and might mimic legitimate Tristation software path filenames. The malware in Triton consists of the components trilog.exe, libraries.zip, inject.bin and imain.bin.

The trilog.exe is the Triton malware's dropper, which legitimates the Triconex SIS and is used to masquerade the controller's management software. Trilog is a Tristation application that is used to review logs on running workstations, which typically has the Windows operating system. The libraries.zip file contains a generated number of compiled Python modules (.pyc files). The compiled module is for malware obfuscation where the source code is used instead. inject.bin contains a code that exploits a zero-day and executes the malware. imain.bin contains the final code that allows a remote user to gain full control of the SIS device. The imain.bin is used to read and write memory on the safety controller and execute code at an arbitrary address within the firmware.

The Triton malware identifies the system's communication and identifies its targeted SIS device after loading on the workstation. It also loads the builds loader for core payloads (inject.bin and imain.bin.) and transfers the Triton malware to the loader module and the target. The Triton malware executes a running file to identify the memory locations and uses embedded binaries on the controller for replacement. A dummy program is uploaded to hide the core payload, that is a malicious ladder diagrams for the PLCs (Firoozjaei et al., 2021).

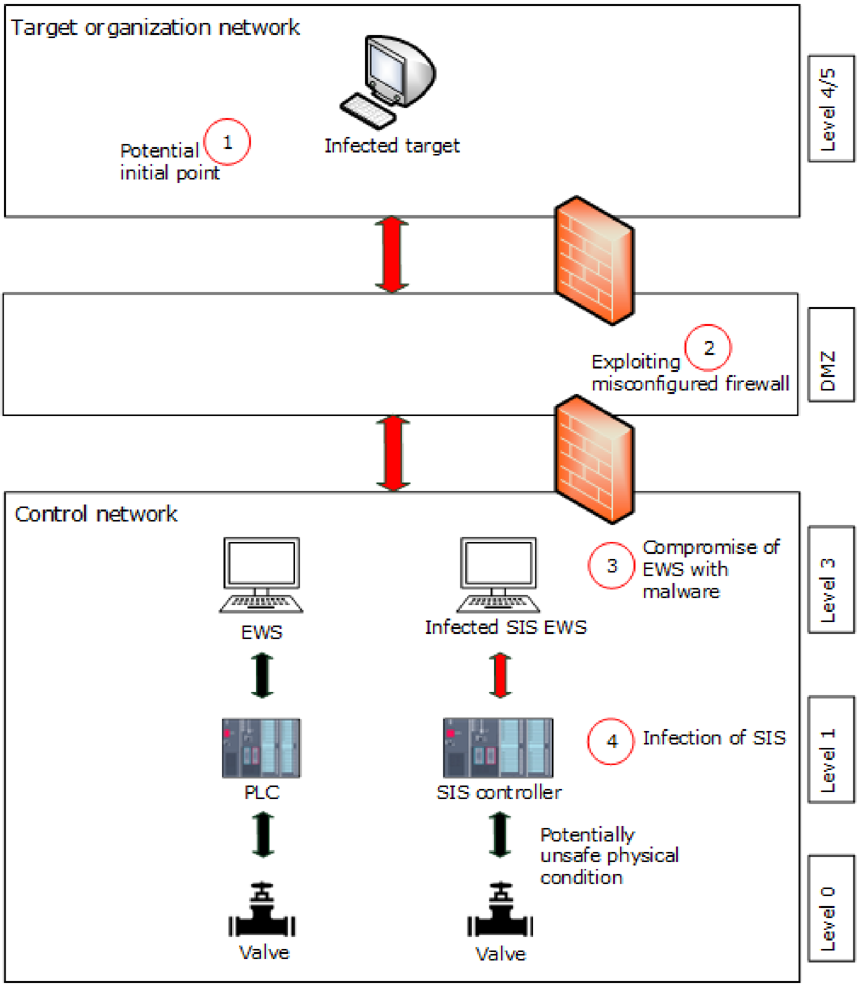


Figure 4.10: Triton, step by step, adapted from Makrakis et al. (2021).

- Through social engineering techniques, the malware established its foothold into the OT system. Removable drivers may have been used with malicious software alleged in the IT network(Kumar et al., 2022).

- The legitimate filename “trilogy.exe” was disguised by itself to deliver the payload, by a malicious dropper.

- A malicious payload delivered to the Triconex SIS controller contained the dropper file.

- The two files inject.bin and main.bin consisted in the payload. The targeted version 10.0-10.4 Triconex MP3008 was the main processor of the targeted SIS running the firmware. A more genetic code handles the payload injection into the running firmware. It performs additional malicious functionalities and is the payload.

- To communicate with the controller, the Tristation protocol (Schneider Electrics proprietary protocol) was used by the malware. If the Triconex SIS Controller during operation, is configured with the physical key that switch into 'program mode', it can modify code.
- A Python script capable of sending a specific UDP broadcast packet over port 1502 and detecting the Triconex controllers on the network is used by Triton. By using an encrypted SSH-based tunnel, the attack payload was delivered, and remotely execution of the program happened.
- To escalate privileges to maintain persistence of the malware and to write onto the firmware memory of the controller, the attackers exploited a zero-day vulnerability.
- At last, by pivoting the malware in the network communication of the malicious SIS, the payload of the malware was able to be called before the normal and legitimate Triconex communications.

Recommendations

A triple redundancy mechanism made the SIS system do a safe shutdown, so this limited the potential damage. IT-based defenses with stateful detection methods are not sufficient to protect against these types of attacks. Critical changes need to be authenticated before authorizing access to the device, where modifications on the state or logic is possible. By checking that the executable files are what they pretend to be and has its correct filename, masquerade attacks can be prevented (Kumar et al., 2022).

4.3 Countermeasures, mitigations and lessons learned

To defend against cyber security attacks like the Stuxnet attack, there are many articles in the literature that recommend proactive security measures and risk assessments methods based on scenario analysis. Simple IT security mechanisms are insufficient and dynamic physical systems can be defensive strategies. Stuxnet has also been used as a case study to find countermeasures against other attacks from highly sophisticated attackers. BlackEnergy has been a state-sponsored malware and a go-to tool for fraud and other state-sponsored attacks. It is also possible to find a timeline of the malware, and many detailed analyses in whitepapers and research blogs (Kumar et al., 2022).

Most of the existing literature on Triton is non-peer-review literature like vendor-specific videos, blogs, and presentations from security conferences, where the authors have presented the attack propagation paths for Triton. There is also a git repository hosting the malware samples, and a detailed forensic analysis provided by the US-CERT (United States Computer Emergency Readiness Team). To be better prepared for future attacks like Stuxnet, Crashoverride and Triton, threat modelling and massive database collection of known attacks, are pointed out as suggested defensive solutions by Kumar et al. (2022).

Visibility of data flow is important to be able to detect if the attacker has native system tools and in-memory execution at the early stage. These attacks are difficult to detect and are officially invisible before the target is activated. By monitoring communications in OT systems, defenders can acquire knowledge so that they can act and reduce the threats and prevent such attacks. It is therefore important to acquire more resources to improve visibility in OT systems (Slowik, 2018).

Slowik (2018) points out that suppliers of OT equipment and devices are encouraged to provide critical infrastructure products that monitors more operational data in order to detect when deviations occur. The fact that an attack is detected at an early stage increases the likelihood that the attack can be countered. Detecting attacks when it happens is better than reacting after it has happened. This provides the possibility to avoid and mitigate the attack.

Security recommendations beyond typical solutions like as MFA and backup should focus on detection and monitoring strategies. Examples include identifying new executable files in the control system network, detecting unsigned binaries from untrusted locations, and monitoring user logon behavior.

This is demanding and will involve resources in research, finance and collaboration to increase competence and support transfer towards a defense practice aimed at ICS networks and critical infrastructure in particular. This will also support a more robust IT defense.

Attacks on OT have changed over the last five years without the defender having kept up with the evolution of the attackers. Defenders have continued to focus on software updates, patch management, identifying malware, securing weak elements, and sharing observations. Attackers have been working to obtain necessary information about potential targets, and vulnerabilities to develop new Cyber Kill Chain tools. The threat landscape is constantly evolving. Individual organizations, national and international defense actors must continuously keep analyzing attack strategies and together prepare recommendations and resources to monitor the development of the attackers.

From Dragos' Year in review report for 2021 they recommend focusing on a few important security checks rather than many. They have five recommendations to provide the best effect, with regard to cyber threats for OT networks (Dragos, 2022a):

1. **A defensible architecture**: A defensible architecture must involve people in addition to the traditional technical ones. Data collection and infrastructure preparations are core requirements in defending networks.
2. **OT network monitoring**: Visibility that emerges from monitoring industrial devices validates the security checks implemented in a defensible architecture. Visible threats can be handled effectively, and making it easier to uncover and manage vulnerabilities. Network monitoring of traffic inside the OT network according to the industrial protocols, makes it possible to understand what is happening. Monitoring OT networks and endpoints is important wherever possible, but OT networks should be emphasized more than endpoint monitoring.
3. **Remote access authentication**: In remote access authentication MFA is still important. Where implementation is not possible, the focus should be on monitoring the data traffic in and out of the OT network.
4. **Key vulnerability management**: A defensible architecture solves most security vulnerabilities today. It is recommended that defenders prioritize those who bridge IT and OT rather than those only deep in the OT network.
5. **OT incident response plan (IRP)**: It is recommended that industry organizations have an IRP they are regularly trained for. This together with interdisciplinary teams (IT, OT, managers, etc.).

5

Managing cyber security risks

The entire IEC 62443 is about implementing barriers. This chapter is about barriers and the execution of a risk and vulnerability assessment. First some basic theory about barriers for the petroleum sector is presented and adapted to cyber security of industrial facilities. The next part covers the process and execution of a risk assessment for food safety in manufacturing plants, that is based on the risk assessment part of IEC 62443-3-2. Different security zones and levels can restrict threats, targets and reduce the risks of cyber attack as much as possible. Cyber security barriers, cyber risks and suggested technical measures will be covered. Chapter 6, which is a penetration test, can be seen as an extension of this chapter and covers the vulnerability assment part of the risk and vulnerability assessment.

5.1 Cyber security barriers

Barriers are actions intended to either identify conditions or limit damage. Conditions to be identified are the ones that can lead to errors, hazards and accidental situations, prevent a specific course of events from occurring or develop or influence a course of events in an intentional direction. The damages to limit are the ones that can lead to losses (Petroleumstilsynet, 2017). These types of barriers are from the petroleum sector, but are also transferable to cyber security in any industrial systems.

Risk should primarily be managed by having safe and robust solutions, and even if robust solutions have been established, they are also dependent on barriers. The purpose of barrier management is to establish and maintain barriers to manage the risks one faces at all times. The goal of barrier management is risk reduction, and the main points of barrier management are:

1. Identify fault, hazard and accident situations

2. Identify barrier functions

3. Identify barrier elements

4. Establish performance requirements

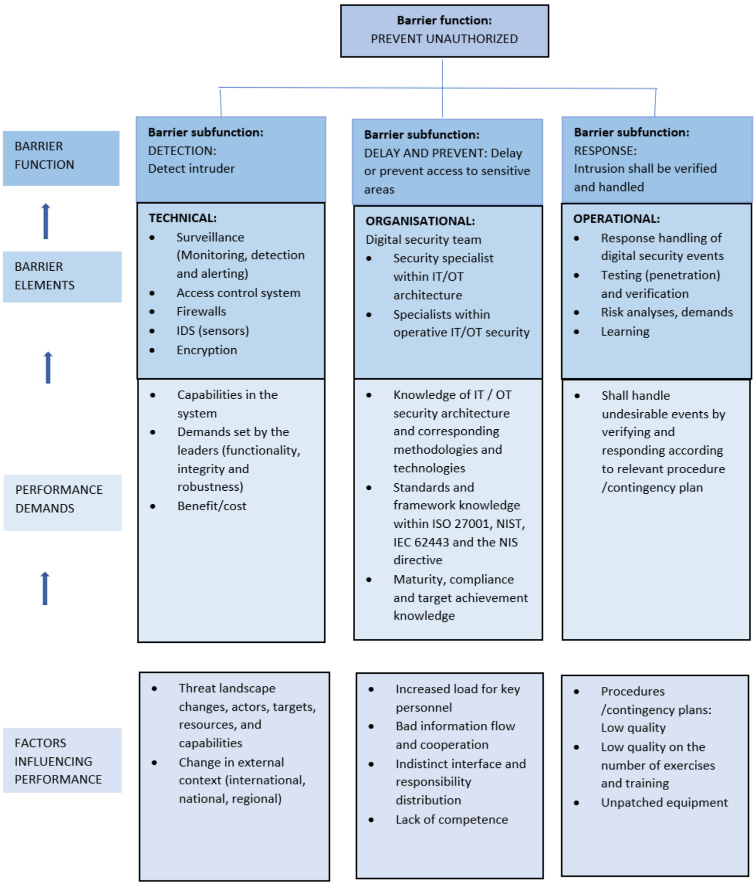
5. Follow up on the sufficiency of the barriers

The barrier hierarchy starts with a barrier function, i.e. what we want the barrier to do. To ensure that the function is taken care of, we use barrier elements (technical-, organizational- and operational barrier elements). Furthermore, the performance demands are imposed on the barrier element, the factors influencing performance and the element's ability to operate as intended. The barrier element is the requirements for the barrier element's properties to ensure that it performs as intended. The factors influencing performance are the factors that are important for functioning.

Technical barrier element deals with the technical equipment and systems that are part of the realization of the barrier function. Organizational barrier elements deal with personnel related to roles, functions and specific competence in order to realize a barrier function. Operational barrier elements set the safety-critical tasks that must be carried out in order for the barrier function to work.

The boundaries between which functions are added to the technical systems and which are added by humans have changed over the years and will also change in the future. Technical systems and human systems have their different strengths and weaknesses. The interaction between technical, organizational and operational barrier elements is important.

The same principles for barrier management in the petroleum activities have good transfer value for work on cyber security. I have illustrated this in an example of a barrier function shown in Figure 5.1, which is further from (Petroleumstilsynet, 2017) to be relevant for cyber security. The illustration is intended only to illustrate the transfer value from barrier management from the petroleum activities to cybersecurity activities. The barrier function is accomplished in interaction between technical, organizational and operational barrier elements, with associated barrier function, barrier element, performance requirements for the elements and factors influencing performance.



Barrier function:
PREVENT UNAUTHORIZED

BARRIER FUNCTION	**Barrier subfunction:** DETECTION: Detect intruder	**Barrier subfunction:** DELAY AND PREVENT: Delay or prevent access to sensitive areas	**Barrier subfunction:** RESPONSE: Intrusion shall be verified and handled
BARRIER ELEMENTS	**TECHNICAL:** • Surveillance (Monitoring, detection and alerting) • Access control system • Firewalls • IDS (sensors) • Encryption	**ORGANISATIONAL:** Digital security team • Security specialist within IT/OT architecture • Specialists within operative IT/OT security	**OPERATIONAL:** • Response handling of digital security events • Testing (penetration) and verification • Risk analyses, demands • Learning
PERFORMANCE DEMANDS	• Capabilities in the system • Demands set by the leaders (functionality, integrity and robustness) • Benefit/cost	• Knowledge of IT / OT security architecture and corresponding methodologies and technologies • Standards and framework knowledge within ISO 27001, NIST, IEC 62443 and the NIS directive • Maturity, compliance and target achievement knowledge	• Shall handle undesirable events by verifying and responding according to relevant procedure /contingency plan
FACTORS INFLUENCING PERFORMANCE	• Threat landscape changes, actors, targets, resources, and capabilities • Change in external context (international, national, regional)	• Increased load for key personnel • Bad information flow and cooperation • Indistinct interface and responsibility distribution • Lack of competence	• Procedures /contingency plans: Low quality • Low quality on the number of exercises and training • Unpatched equipment

Figure 5.1: Structure of barrier functions and subfunctions, further developed from Petroleumstilsynet (2017) to consider cyber security.

5.2 Risk and vulnerability assessment approach

NAMUR, ISA TR and DNVGL RP G108 are all applications of IEC 62443-3-2 and IEC 62443-3-3. The documents have the same main objectives, which is a) Identifying the risks, b) analyzing and evaluating the risks and c) Assigning a security level target to each zone and system involved. As none of these methods are suitable for a risk assessment for food safety, the chosen method was to follow IEC 62443-3-2 directly.

First a risk and vulnerability assessment is made, which consists of a risk assessment to set the Security Level Targets and a vulnerability assessment, that is a penetration test for discovering vulnerabilities. The penetration test can be seen as a vulnerability scan connected to the risk assessment.

Risk assessment vs. vulnerability assessment

A risk assessment identifies threats and assesses impact and likelihood and a vulnerability assessment tries to find secuirty holes that can be exploited.

The risk and vulnerability assessment is dived into three parts: Initial risk assessment, detailed risk assessment and vulnerability assessment. The vulnerability assessment is a vulnerability scan that is connected to the risk assessment in this chapter, and will be covered in detail in chapter 6.

The focus in this risk assessment is loss of food safety. For food and drink factories, food safety is safety in the context of ingredients, cleanliness and other relevant processes during the production phase. This means that the products shall be delivered without being health hazardous. Allergy-friendly products shall not have allergens, no products shall contain toxic substances, the products shall only contain the ingredients labeled on the packaging and the products shall have the expected content, texture and taste.

5.3 Risk and vulnerability assessment

Initial risk assessment

The starting point for the risk assessment is the generic Purdue model for a manufacturing plant, which is reproduced in Figure 5.2 and shown below.

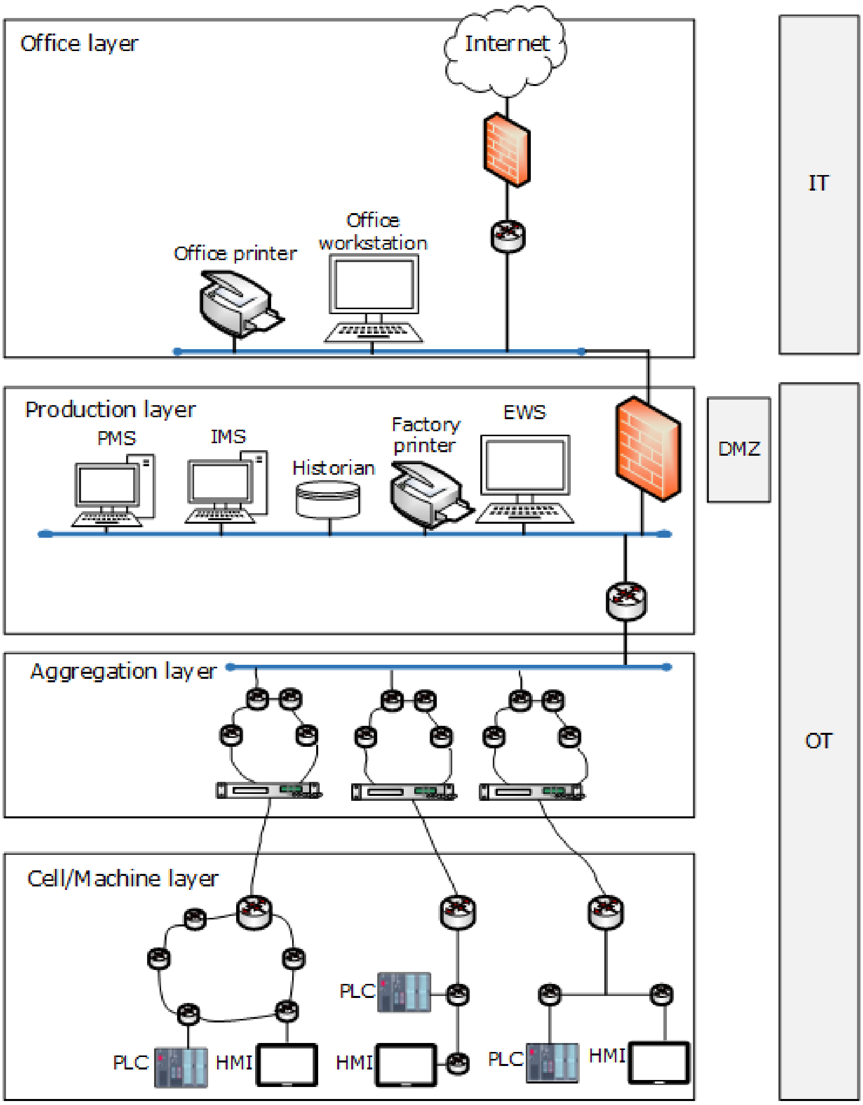


Figure 5.2: Reproduced generic Purdue model for a manufacturing plant

Identifying the SuC

Remark that this still is a simplified setup for an industrial facility, so more systems and devices will typically also be present in a system like this. As Figure 5.2 is simple, some more devices and systems exist. These plus the one included in the figure can be divided into these systems with corresponding devices and subsystems:

- Office system

  - Office workstation
  - Office printer
  - Historian
- Control system
  - Engineering workstation (EWS)
  - PLC
  - HMI
- Safety system
  - System to force a safe state (Safe State System, SSS)
  - Redundant takeover system (Takeover System, TS)
  - Production shutdown system (Shutdown System, SS)
- Remote access system
  - Remote access firewall
  - VPN system (VPN)
  - Remote access server (RAS)
- Information system
  - Backup server
  - Monitoring workstation with monitoring software (MWS)
  - Patch Management System with updating software (PMS)
  - Information Management System (IMS)

The entire system consisting of these subsystems is considered the system under consideration, shortened SuC. The office system consists of devices in the enterprise network for the office workers in the IT environment, which are not directly involved in the OT environment, unlike all the other systems. The control systems are the systems controlling the processes within the factory, e.g. controlling temperature, assembly line speed, concentration of ingredients etc.

The safety systems are responsible for safe production and taking actions if something goes wrong or if process field devices exceed their boundaries, e.g. if the temperature is too high, the assembly line speed is too high, the mixture of ingredients is unexpected etc. The remote access system is the system used for workers to connect to the IT and OT network if they are not physically at the factory. The information system lies within the OT network and is responsible for monitoring the network traffic, updating software and having an updated backup of the factory system data.

Within the SuC, the control and safety systems are the systems directly involved in the context of food safety. Regarding cyber security and food safety, the other zones and systems are relevant too, as attackers need to pass other zones to gain access to the control and safety systems. This step will focus on the food safety related subsystems within the control and safety systems. The following systems are involved in the case of food safety:

- Control system
  - Ingredient mixture system
  - System for adding allergens, e.g. nuts
  - Boiling system
  - Equipment cleaning system
- Safety system
  - Detection of ingredient amount deviation
  - Detection of temperature boundary deviation
  - System for handling deviations

Initial risk for the compromise effect and corresponding system

To be able to cause loss of food safety in a cyber attack, the attackers need to directly target the control and safety systems.

The major threats for a manufacturing plant is, based on the publicly known cyber attacks, are sophisticated groups that tries to access the OT systems through the IT infrastructure or by exploiting a vulnerability within a remote access solution. Based on the subchapter 5.1, one can say that the vulnerabilities lies within the barrier elements technical, organizational and operational, which is covered in the table in subchapter 5.1.

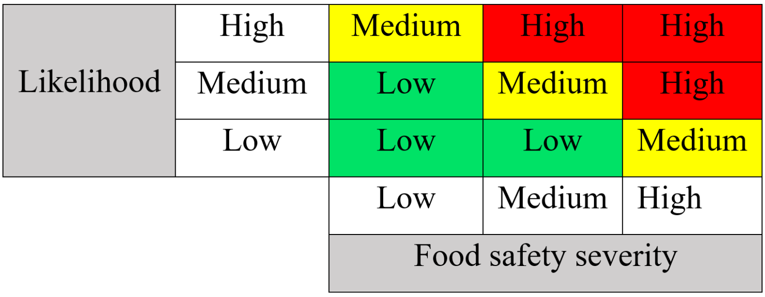
Every control and safety system listed above is considered in Table 5.1 to assess the initial risk in the case of a cyber compromise. An initial assessment based on Table 5.1 and Table 5.2 gives the likelihood and the severity respectively. Regarding the likelihood, it is in this case assumed that attackers already have access to the OT network. The likelihood is then assessed as a combination of the attackers' motivation and their ease of execution. Digital manipulation of boundary values is for instance assumed easier than modifying the ingredient mixture, hence is has a higher likelihood. A risk matrix is shown in Figure 5.3, where the initial risk is chosen as the intersection between the likelihood and severity. Table 4 shows the initial risk for the compromise effect and corresponding system.

Table 5.1: Likelihood level and description

Likelihood	Likelihood description
Low	Very unlikely, not expected to occur
Medium	Quite possible, may occur
High	Almost certain, expected to occur

Table 5.2: Level of food safety severity and corresponding product changes definition and description

Food safety severity	Description of product changes
Low	Minor changes to color, texture or taste
Medium	Major changes to color, texture or taste
High	Contains toxic ingredients or allergens



Likelihood	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		Food safety severity		

Figure 5.3: Risk matrix based on the likelihood and severity from Table 5.1 and Table 5.2.

Table 5.3: Initial risk for the compromise effect and corresponding system.

System	Example of compromise effect	Likelihood	Severity	Initial risk
Control system	Wrong ingredients added by the ingredient mixture system	Low	Low	Low
Control system	Allergens added to allergen-free product	Low	High	Medium
Control system	Manipulated temperature in boiling system	Medium	Medium	Medium
Control system	High concentration of dishwashing liquid in equipment cleaning system	Low	High	Medium
Safety system	Detection system for ingredient amount deviation disabled	Medium	Medium	Medium
Safety system	Detection system for temperature boundary deviation disabled	Medium	Medium	Medium
Safety system	System for handling deviations disabled	Medium	High	High

As can be seen in Table 5.3, the initial risk is mostly not higher than Medium for any of the compromise effects and systems. This may be because the most destroying cyber attacks are a combination of attacking both the control and safety systems. An attack on the control system but not on the safety system may lead to a deviation, and should be detected by the safety system. An attack on the safety system but not on the control system may cause a deviation not to be detected and handled, but without the control system being attacked, the deviations will most likely not occur. Therefore the possibility of cyber attacks against both the control and safety systems, need to be considered when partitioning the SuC into zones and conduits and when the Security Level Target is set.

Partitioning into zones and conduits

The last step of the initial risk assessment is the partitioning into zones and conduits. This is a rule-based approach, where it is common to follow the recommendations in IEC 62443-3-2. By following the proposals from IEC 62443-3-2, given in section 3.3 under ”Partitioning into zones and conduits”, one can see a suggestion of partitioning into zones and conduits in Figure 5.4.

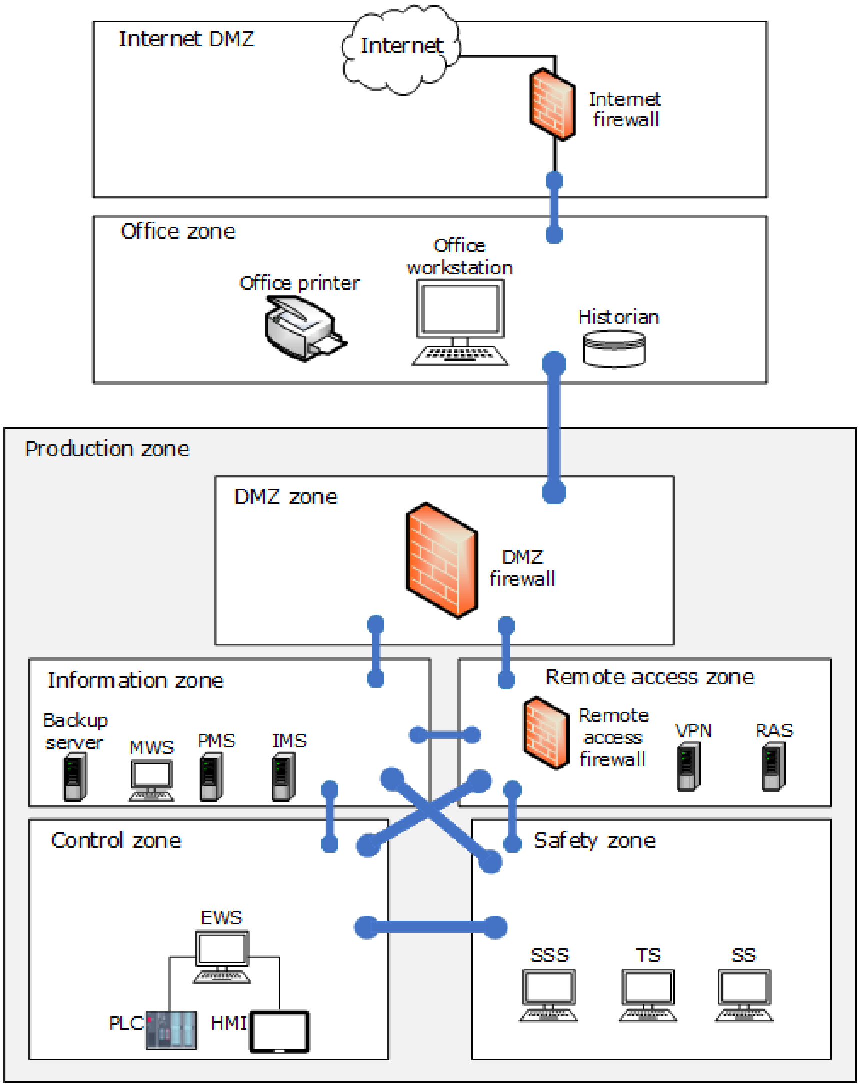


Figure 5.4: Partitioning into zones and conduits.

In the detailed risk assessment the zones and conduit drawing in Figure 5.4 is used to determine which zones and equipment have the highest threats. The Security Level Target and some measures are included in Figure 5.5, which is an improved and more detailed version of Figure 5.4.

Detailed risk assessment

The threat is highest for the zones and equipment with the easiest accessibility. External threat actors typically have two ways to gains access to the production network within the OT network, i.e. by a) exploiting a vulnerability in the remote access solution or b) installing malware on an office computer in the office network. The former is often done by using publicly known vulnerabilities in a combination of scientific research, to develop exploits specified for the vulnerable remote access solution. The latter is typically done by sending a spear-phishing email with a malicious attachment, to one of the office workers.

After gaining access to either the office network or the remote access solution, attackers will try to escalate their privileges and move downwards to the control and safety systems. This means that it is important to especially have increased security in the Internet DMZ zone, which is the connection between the office network and the Internet, and the Remote access zone, which connects external users to the control and safety systems. Since all connections from the office zone to the production zone must go through the DMZ zone, it is necessary to implement high security demands for the DMZ zone as well. In addition to the tiny discussion in the detailed risk assessment, some other considerations must be in place to conclude the Security Level Target for each zone.

Security Level Target

In Table 5.4, each zone has been assigned a SL-T based on the risk assessment and additional considerations regarding operability, accessibility and need for real-time transmissions. The starting point for the SL-Ts is Table 3.2 from chapter 3. Higher SL-Ts means better security protection but may affect the latter additional considerations.

Table 5.4: Security Level Target suggestions for the zones.

Zone	Security Level Target	Comment
Internet DMZ	SL-4	Continuously exposed to external threats
Office zone	SL-2	Not very critical and protected by the Internet DMZ
Production zone	SL-2	All zones within the Production zone must at least have SL-2
DMZ zone	SL-4	Critical zone that gain access to the lower OT zones
Information zone	SL-2	Not critical for control and safety and protected by the DMZ
Remote access zone	SL-4	Continuously a target for external threats
Control zone	SL-3	Very critical zone, but SL-4 may affect the accessibility
Safety zone	SL-3	Very critical zone, but SL-4 may affect the accessibility

Based on the Security Level Target, necessary measures need to be implemented to restrict the threats as much as possible. The goal of the measures is to reduce the likelihood or severity, and thereby reducing the risk. Some suggested measures for each zone which are based on the risk assessment, is listed in Table 5.5 below. It is divided into technical measures and policies.

Table 5.5: Suggested technical measures and policies for each zone.

Zone	Suggested technical measures	Suggested policies
Internet DMZ	• Strong anti-malware system (AMS) • Whitelisting firewall rules rather than blacklisting	• Update firewall rules regularly
Office zone	• Multi-factor authentication (MFA) • User lockout after multiple failed login attempts	• Increased security awareness • Strong password demands for all users • Regularly spear-phishing training • Principle of least privilege
Production zone		• All access to the Production zone must go through the DMZ zone • Regularly try to crack user password with brute forcing methods
DMZ zone	• Strong anti-malware system (AMS) • Whitelisting firewall rules rather than blacklisting • Only allow access to OT authorized users	• Update firewall rules regularly

Zone	Suggested technical measures	Suggested policies
Information zone	• Multi-factor authentication (MFA) • Strong encryption mechanisms for access to the Remote access zone, Control zone and Safety zone • User lockout after multiple failed login attempts	• Principle of least privilege
Remote access zone	• Multi-factor authentication (MFA) • Whitelisting firewall rules rather than blacklisting • Strong encryption mechanisms for access to the Information zone, Control zone and Safety zone	• Principle of least privilege • Access to the Remote access zone must go through the Internet DMZ, Office zone and DMZ zone
Control zone	• Add a separate Control zone firewall • Only allow access to users authorized for the Control zone • Use wired signals rather than wireless	• Principle of least privilege
Safety zone	• Add a separate Safety zone firewall • Only allow access to users authorized for the Safety zone • Use wired signals rather than wireless	• Principle of least privilege

Figure 5.5 shows an improved sketch of the devices, zones, conduits, SL-T and suggested measures for a generic manufacturing plant. The equipment and components with a green border are suggested measures. The blue light blue conduits marks increased encryption as a suggested measure.

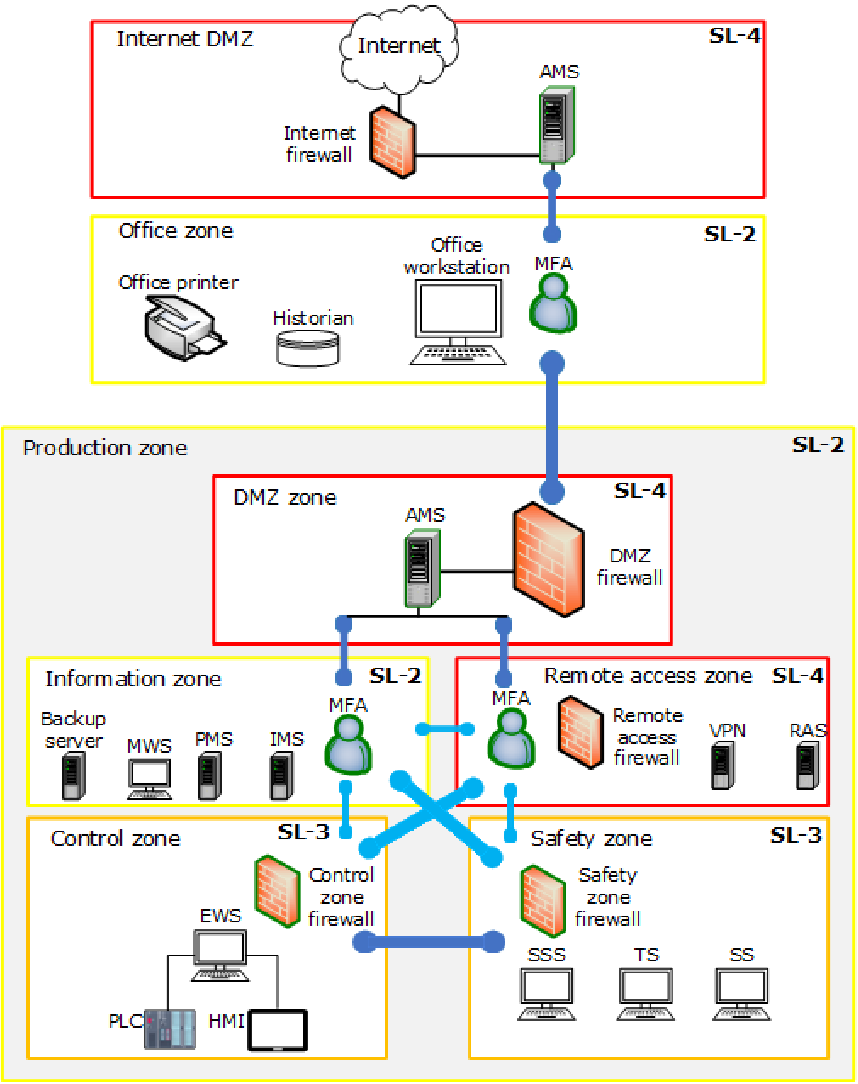


Figure 5.5: Improved topology for a generic manufacturing plant

6

Penetration test of a physical manufacturing plant

This chapter is about penetration testing of physical industrial facilities. A penetration test is a process where employees in an organization try to break into their own system to uncover vulnerabilities that later can be mitigated. First in this chapter tools for penetration testing in OT environments will be presented. The next part is about a penetration test that was physically executed at one of Orkla's factories. The plan, preparations and execution for this penetration test is then considered. At the end, the results will be presented and interpreted.

6.1 Tools for penetration testing in OT environments

In a paper from Permann and Rohde, they present commercial and open source tools for penetration testing in OT environments (Permann and Rohde, 2005). Permann and Rohde point out that these tools only should be utilized by professionals, as some computer skills are required. During the preparations for the penetration test on a physical manufacturing plant, some open source system specific tools were found on the Internet, mostly in GitHub repositories. All the tools are listed and briefly described below, and the system specific tools found during the preparations are marked with an asterisk, (*). Each tool is categorized to its corresponding phase of the penetration testing process in Figure 6.1. A dark red arrow in the figure means that the connected tool on the OT side is developed from the tool on the IT side to be customized for OT. The grey connction for Modbus PTF illustrates that Modbus PTF is applicable for two penetration testing phases.

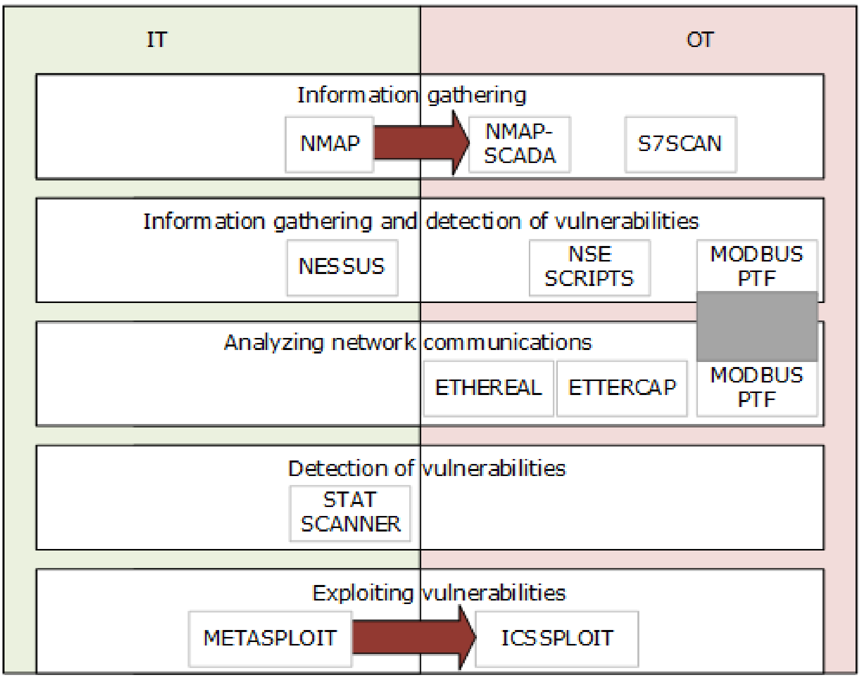

IT
OT
Information gathering
NMAP
NMAP-SCADA
S7SCAN
Information gathering and detection of vulnerabilities
NESSUS
NSE SCRIPTS
MODBUS PTF
Analyzing network communications
ETHEREAL
ETTERCAP
MODBUS PTF
Detection of vulnerabilities
STAT SCANNER
Exploiting vulnerabilities
METASPLOIT
ICSSPLOIT

Figure 6.1: Categorization of penetration testing tools categorized to the phase of penetration testing

NMAP

Nmap is network scanning tool used to map ports. Every port on every machine is identified, and from here each running service on each port is found. For every machine the open ports found are the starting point to test if there exists open access points to the OT system. ”Unknown ports” found by Nmap should be queried and deeper analysis should be made to verify the results from the scan (Lyon, 1997).

NMAP-SCADA (*)

Nmap-scada is a Nmap equivalent for identifying Siemens devices and other OT devices (jpalanco, 2013).

NESSUS

Nessus is a multi-purpose security scanner that runs through about 6 000 security checks to a) identify which services are vulnerable, b) assess a level of warning for each service and c) suggest mitigations for the vulnerabilities. The scan can be applied as an initial system assessment, to identify vulnerabilities that can be exploited later. Note that all vulnerabilities might not be detected by Nessus. For instance software on a local computer is not checked by Nessus, but tools like STAT Scanner be applicable for this (Tenable, 2005).

STAT SCANNER

STAT Scanner is used to detect vulnerabilities specifically for Microsoft components, applications and operating systems (Harris, 2004).

NSE SCRIPTS (*)

NSE Scripts is a tool to check if publicly known vulnerabilities are present in the OT devices (claroty, 2020).

MODBUS PENETRATION TESTING FRAMEWORK (*)

This tool is a implementation of the Modbus protocol and a framework for penetration testing the protocol. It is modular and is used for offensive features and diagnostics within the Modbus protocol (0x0mar, 2015).

S7SCAN (*)

S7scan is a network scanning tool for identifying all active Siemens PLCs and collect information about each PLC. The S7 protocol, which is the protocol many Siemens PLCs apply, is used to connect and communicate to the PLCs within the network. For each PLC the tool is able to gather information like the type of PLC, the hardware and software version, its network configuration and protection settings, which are the read and write access rights and key positions (klsecservices, 2018).

ETHEREAL

Ethereal analyses network protocol communication and is able to monitor the communication between individual OT components. It detects which components communicate, if encryption is enabled and the information sent in plain text, which can include passwords and usernames (Flylib, 2005).

ETTERCAP

Ettercap is a network sniffing tool for switched networks, used for man-in-the-middle attacks. It can sniff and filter the connections live and for some applications grab passwords. Communications between OT components and Ethereal or Ettercap can be viewed by a man-in-the-middle attack, where systems can be tested for other Ettercap attack functionality (Ettercap, 2005).

METASPLOIT

Metasploit is an open source framework used for exploiting systems, by development, testing and use of code. It is also applied for research work on vulnerabilities. The exploit code is automated, so it is relatively easy to use. A few OT related exploits exists, but it is not specialized for OT, as it mostly contains IT related exploits (Metasploit, 2005).

ICSSPLOIT, INDUSTRIAL EXPLOITATION FRAMEWORK (*)

Icssploit, also called the Industrial Exploitation Framework, is a Metasploit equivalent for OT. Among other features it includes exploits for specific PLCs from the vendors Siemens and Schneider, which are some of the biggest PLC vendors in industrial control systems today (dark lbp, 2017).

PUBLICLY AVAILABLE EXPLOITS

Many publicly known exploits for specific OT components are published online, often as executable scripts from source code. Typically these exploits are available on the repository website GitHub, where they are easy to download and run, to test for the target system.

6.2 Plan, preparations and execution

As this penetration test has been conducted at one of Orkla's factories that is in production today, the next three subchapters will not contain technical details about the process or results of the penetration test. This is for confidentiality and security reasons. What is presented here is therefore a generalization of the actual process and the actual findings, but it will nevertheless provide the correct methodology for what has been carried out.

Setup and planning

Penetration test in two parts, both of which run in parallel (focus of the task: Test system):

- Penetration test of the entire factory – security experts in Orkla, Sander observe

- OT penetration test for a test system - Sander, with help from security experts in Orkla

The planning, setup and execution of this penetration test has been a thorough process, as a result of constructive cooperation between Sander, supervisor from NTNU, co-supervisor from Orkla, security experts from Orkla and the contact person at the factory. In addition, I have received valueable input and considerations from Kenneth Titlestad and Einar Færaas, who are cyber security experts in OT for the industry. The design of the framework for the test system and the penetration test has followed these steps, and is thus quality assured before the penetration test was implemented:

1. Sander drafted an overall plan for the penetration test

2. The draft was presented to the supervisor, and was revised on the advice and input of the supervisor

3. The draft was presented to Orkla and the contact person at the actual factory, and adapted according to feedback

4. The contact person for the actual factory set up a test system, based on the final plan determined in step 3

5. The penetration test was carried out physically at the factory, for the test system set up in step 4

Figure 6.2 shows a simplified figure, intended to show the devices involved and the connection between them, without being too detailed. It can be seen in the context of the figures from the risk assessment in Chapter 5.

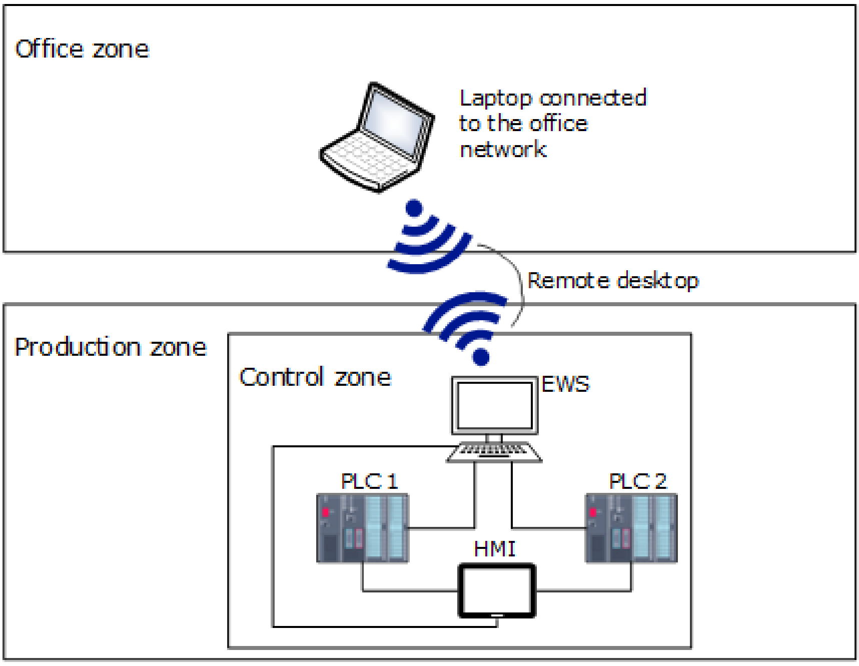


Figure 6.2: Test system set up by the contact person at the factory

Description: The system is an isolated test system in the OT network, consisting of an engineering workstation, two PLCs and an HMI device, where all these devices are connected to the same internal network inside the OT network. All devices and machines in the test system are located on a specific IP range, which was given before the penetration test began. The engineering workstation has the possibility of connecting through Remote Desktop from any machine connected to the office network of the IT network, in this case, Sander's computer. What is displayed on the HMI is set through PLC 1 and PLC 2. The data flow goes from the engineering workstation, then to PLC 1 or PLC 2 and then to the HMI. The values displayed on the HMI are sent to the Engineering workstation and can be read from there as a simulation of what is displayed on the HMI screen. PLC 1 cannot communicate with PLC 2 and vice versa.

Clarifications and simplifications: The penetration test starts by connecting a computer to the office network located on the IT side of the factory's network structure. It was decided that the necessary documentation on networks, devices and communication was provided in advance of the execution, which makes the penetration test a whitebox penetration test. If limited information about networks and systems had been provided, the penetration test would have been a graybox penetration test, and if minimal or no documentation had been provided, the test would have been a blackbox penetration test. This is a choice made in consultation with Orkla based on time, resources and relevance related to the scope of the penetration test.

The functionality around connecting to the engineering workstation through Remote Desktop is assumed to be working and will not be described in detail here. The firewalls and the DMZ are not considered between a machine on the IT network and the engineering workstation, as the engineering workstation will be accessed through username and password. Switches in the network of the test system are not included in the figure, but they exist in the network, as shown in the Purdue figure for a factory in Chapter 3.1. The test system is completely isolated from the actual production network, which means that any change and action within the test system, which does not concern machines outside the given IP range, will not be able to have any impact on the actual production.

Process

The penetration test process is based on Appendix A, and the final process is presented below. As a result of the limited time frame for the penetration test, one can see that the actual process is a simplification of the original plan, but the essence remains the same. The overall goals with the penetration test are listed below and Figure 6.3 shows a general approach for achieving the overall goals. Most of the steps from the figure will be covered in detail in the process of the executed penetration test.

Overall goals:

1. Aquire access to the OT network from the IT network

2. Aquire access to an engineering workstation on the OT network

3. Modify how processes are controlled as a proof-of-concept, by making changes to a PLC from the engineering workstation. A proof-of-concept in this context is to show through testing that it is possible to change the PLCs if one has access to an engineering workstation.

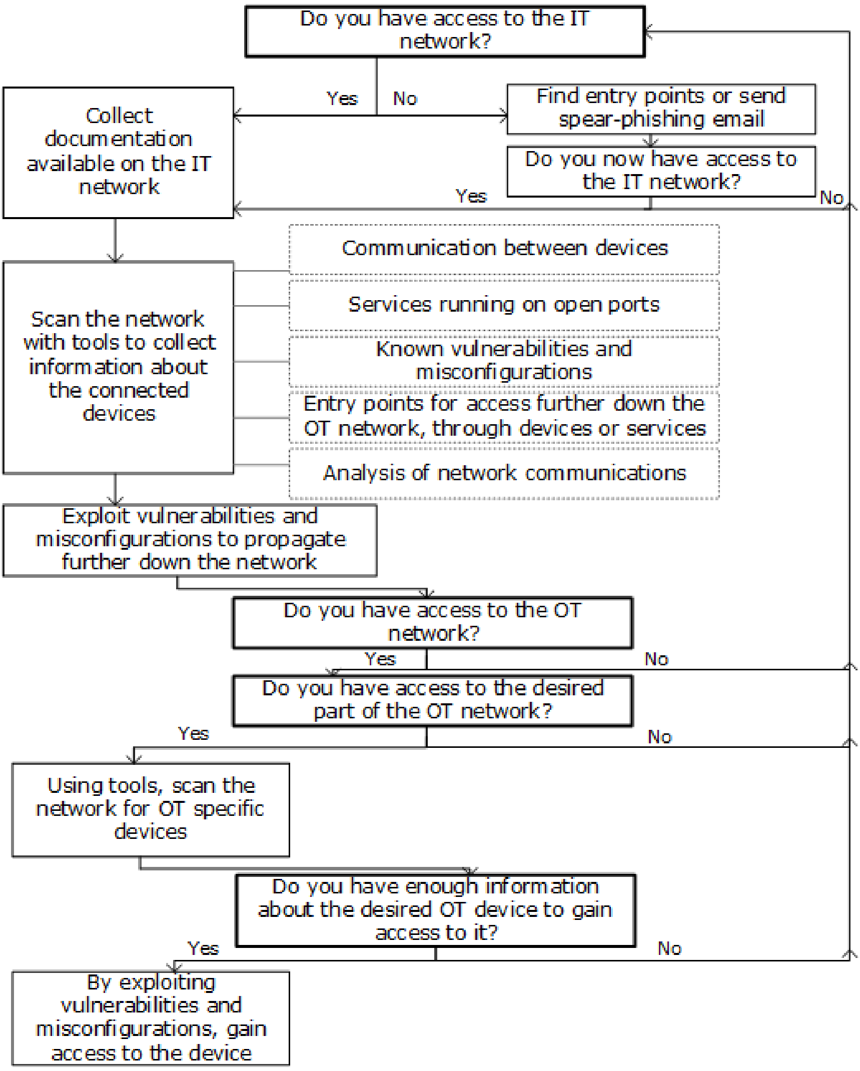

Do you have access to the IT network?
Yes
No
Collect documentation available on the IT network
Find entry points or send spear-phishing email
Do you now have access to the IT network?
Yes
No
Communication between devices
Services running on open ports
Known vulnerabilities and misconfigurations
Entry points for access further down the OT network, through devices or services
Analysis of network communications
Scan the network with tools to collect information about the connected devices
Exploit vulnerabilities and misconfigurations to propagate further down the network
Do you have access to the OT network?
Yes
No
Do you have access to the desired part of the OT network?
Yes
No
Using tools, scan the network for OT specific devices
Do you have enough information about the desired OT device to gain access to it?
Yes
No
By exploiting vulnerabilities and misconfigurations, gain access to the device

Figure 6.3: General approach for achieving the overall goals

General process for achieving the overall goals:

1. **Information collection and vulnerabilities**
   By being connected to the IT network, search for available documentation located within the IT network, or gain access to this from the factory, depending on the type of penetration test to be carried out. Specifically, look for shared folders and network files on the IT network and intranet, if you can access it, and otherwise randomly search for information. If you have physical access to the factory, search

drawers and shelves for available documentation, as more information makes it easier to break into the systems. Below is the information you want to look for, listed by category.

Devices & Communications

- Which different networks the factory consists of
- How the communication in each network is and how the communication is between the different networks
- Which network protocols that are used
- What types of devices that exist in the IT and OT networks and their IP addresses
- Which vendor and version number each device has
- Which devices in the IT network that can communicate with other devices in the IT and OT network

The OT network

- Usernames and passwords in plain text
- The extent to which simple standard credentials are used for devices in OT
- Which entry points exist from IT to OT and where they are located
- Firewall rules between IT and OT
- How DMZ and firewall rules are set up between different zones in the OT network
- Which devices belong to the different parts of the factory
- Which devices inside the OT network can communicate with other devices on the OT network
- Which devices have high privileges and can control other devices
- Which switches each device is connected to

Remote access

- How remote access is configured
- Which types of accesses that exist for remote access
- The extent to which one can gain access to an engineering workstation inside the OT network, through remote access
- If in use, how VPN is configured and what accesses one can achieve through VPN

Computers and services running on open ports and also are connected to the OT network

Use documentation and open sources on the internet to learn how to connect to these machines:

- Look for ”low-hanging fruits” based on the documentation accessed, which are accesses and services that require minimal effort to achieve, which can lead to more accesses
- Use automated or customized tools to scan the IT network for machines and services that use open ports
- For each machine and service found, check if it is connected or can be connected to the OT network
- Use tools and publicly available information on the Internet to check for known vulnerabilities associated with each machine or service
- For each vulnerability found, use tools and public information on the Internet to find out how to exploit the vulnerability, to gain access to the machine or service

2. **Given that an engineering workstation can be found on the OT network, gain access to this**

   - By utilizing tools and available documentation, find which services the engineering workstation uses and how it communicates with the IT network
   - Connect to the engineering workstation through one of the services it runs, using available documentation, information on the Internet and relevant tools
   - If the engineering workstation cannot be accessed directly, use the Internet to look for actual vulnerabilities for the given machine or service
   - If connecting to the engineering workstation requires a username and password, look for this in the available documentation
   - Brute force credentials using tools and customized password lists, if credentials are not found in the available documentation

3. **By having access to an engineering workstation, make changes to the behavior of a PLC**

   - Once inside the engineering workstation, look for programs, documents, network logs, users, credentials in clear text and similar

- Scan the network of the engineering workstation for which devices and machines it can access
- Scan the devices and machines to find as much information as possible, such as the vendor, version number and similar
- Use the information from the previous point and tools to scan the devices and machines for known vulnerabilities and how to exploit these vulnerabilities
- If available, use tools to exploit the vulnerabilities of the PLCs, to affect the behavior of the production devices
- If programs that directly can modify the control mechanisms of PLCs are found on the engineering workstation, try to tamper with these values and connect the modified program to the PLC, to verify on the physical equipment if the modification was successful

For step 3, it may also be useful to look for other types of information on the engineering workstation, which may be information or credentials that is reused in other parts of the OT system. Here, the structure of folders on the machine, with associated storage media, can be explored to look for information about installed programs, saved files, documentation for programs, files and users and credentials in plain text. There is also a lot of information in the web browser, and one can use this to read Internet web logs and stored usernames and passwords. One can also look for credit card information and sensitive personal information, which potentially could be used by real attackers as extortion in a future attack.

Relevant types of tools and systems for the steps in the general process

See Figure 6.1 for relevant tools used for each step above. In addition to these tools, it may also be useful to utilize the following types of tools for each associated part:

1. **Collection of information and vulnerabilities**
   - Scanning IP addresses on the network, for which services they are running and which ports they are connected to
   - Detecting known vulnerabilities associated with the machines and services found in the previous bullet point

2. **Given that an engineering workstation can be found on the OT network, gain access to this**
   - Equivalent tools as for step 1
   - Actively exploit the vulnerabilities to access the machine on the OT network

- Password brute forcing

3. **By having access to an engineering workstation, make changes to the behavior of a PLC**

    - Scanning PLCs for known vulnerabilities related to specific version numbers and specific vendors
    - Exploits for specific version numbers of PLCs, from specific vendors
    - Pre-installed software on the engineering workstation to connect modified executable program to the PLCs

Executed process for this penetration test

Due to a limited time frame, there was not enough time to complete all the steps in the general process and utilize all the tools. Since it is important that this penetration test shall not disclose detailed information about vulnerabilities or be recreated by malicious actors, it will not be clarified which tools have been used. Similar tools as those mentioned in subchapter 6.2 have been used.

The actual executed process was the steps described below, referring to the steps from the general process:

1. **Collection of information and vulnerabilities**

    Documentation: Information was obtained for network structure, devices, communication and remote access, both for IT and OT. This was done in accordance with step 1 in the general process. As this was a whitebox penetration test, all available documentation was provided by our contact person at the factory, so that time could be more efficiently spent understanding the systems and devices, rather than finding this documentation.

    Obtaining information about machines on the OT network: The machines included in the test system for this penetration test were located in a given range of IP addresses in the factory's OT network. For this given IP range for the test system, the machines and devices were scanned to see how they were connected to the OT network and if any of them were running on open ports, by following step 1 for the general process. When it was known from the documentation which IP address belonged to the engineering workstation in the test system, and this was the device we wanted access to, no more machines were scanned for vulnerabilities.

2. **Given that an engineering workstation can be found on the OT network, access this**

During the scanning of the network in the previous step, which services the engineering station used for communication between the OT and the IT network and for remote access, were also scanned. A finding was that the machine used the Remote Desktop Protocol (RDP), and thus that one could connect remotely to it from any machine connected to the IT network, both wired and wireless. For this penetration test, wired connection was used from Sander's test computer to the IT network.

When trying to connect through RDP to the engineering workstation one was met with a username and password login screen. The username for the machine was found in available documentation, but no password was available. It was first tested for some default passwords, but it didn't work, so the next step was to try to brute force the password using publicly known and self-made password lists and combinations of Norwegian and English letters, words and characters. Automated tools were used to try to crack the password. This is a time-consuming process with no prior information about any part of the password.

As the time frame of the penetration test was limited, and an important goal was to show that one could modify the PLC behavior from the engineering workstation, the password was eventually given by our contact person at the factory. Then one was able to log in with the known username and the password. Remote access to the engineering workstation was now achieved from the test computer. Now everything one could do from the engineering workstation, could now be done from the test computer.

3. **By having access to an engineering workstation, make changes to the behavior of a PLC**

   First, the folder structure within the engineering workstation was explored manually to map which programs were installed and whether there were any interesting documents or information about users or systems there. What is meant by manually in this context is to click through all the folders located in the folder structure of the engineering workstation. Furthermore, tools were used to scan the test system's network that the engineering workstation was connected to, to find as much information as possible about its connected PLCs. This tool was the same as used earlier, but the input to the tool had to be modified to see information about the OT-related devices.

   The software Wireshark was used to listen on the network traffic in the test system's network, to take a closer look at the data flow between the devices in the network (Wireshark, 2022). Wireshark is particularly suitable for this purpose, as it supports several industrial and non-industrial protocols, used both for OT and IT, and has good opportunities to filter data traffic on parameters such as sender/receiver and protocol. Furthermore, each installed program was run to see which PLCs the engineering workstation was connected to. The engineering workstation can configure software and download new versions of executable programs to these PLCs.

6.3 Results

1. **Collection of information and vulnerabilities**

   Documentation:
   Under the *Devices and Communications* category it was found information about the network structure for the IT and OT network, functional description for each network, IP addresses for computers and devices in the IT network and vendor and version number of devices in the IT and OT network. Specifically for the *OT network*, the documentation covered IP addresses and network locations for computers and devices, the communication between devices in the IT and OT networks, overview of switches, PLCs, HMIs, Engineering workstations, label printers, firewalls, firewall rules, DMZ firewall rules and the communication protocols used for the various networks inside OT. For *remote access*, some information were found about selected devices that can be accessed remotely and some information about VPN usage. Other interesting documentation found were contact information of technical personnel at the factory and the name and contact information of those responsible for third-party network systems.

   Obtaining information about computers on the OT network:
   The machines and devices in the test system were found during the scan. According to the documentation, all these machines and devices were part of the OT network. The information about the machines and devices included type of operating system, which for the engineering workstation was Windows, product version of the operating system, target name, NetBIOS Domain name, NetBIOS Computer name, DNS Domain name, and DNS Computer name.

   During the scanning of the engineering workstation, a service for one of the PLCs was running openly through HTTP on port 80. By accessing this service by connecting to the IP address in a web browser, the following information was displayed about the PLC: name, type, vendor, hardware and firmware version number, software used to control the PLC, operating state, serial number, date of manufacture, order number and vendor certificate MD5. It was also found that the engineering workstation was running remote desktop and that it was possible to connect remotely to this machine through Windows' remote desktop protocol, RDP.

2. **Given that an engineering workstation can be found on the OT network, gain access to this**

   Remote access to the engineering workstation was obtained through RDP, known usernames available from the documentation and passwords provided by the contact person at the factory.

3. **By having access to an engineering workstation, make changes to the behavior of a PLC**

   The information uncovered through scanning of the network matched what was found in step 1. A significant additional information found after accessing the engineering workstation was that PLC 1 and PLC 2 were from various suppliers. From pre-installed software, two different programs were found to transfer the executable program from the engineering workstation to the PLC, for PLC 1 and PLC 2 respectively. The engineering workstation is directly connected to physical PLCs in the factory, which means that if you transfer an executable program on a PLC, then this executable program will be run on the PLC.

   From the engineering workstation you were logged in as a local administrator, which means that you can do whatever you want inside the machine. Antivirus was turned off, which allowed programs, scripts and malware to be downloaded directly on the engineering workstation, from the engineering workstation, and external software could also be run. Through the software listening on the network traffic, the types of switches on the network were found as well.

   A proof-of-concept was carried out to show that from the engineering station one can send modified executable programs to a PLC, thereby changing the behavior of actual production processes. This was done by modifying an executable program to display a specified numerical value, and uploading that program to one of the PLCs. The new number value was then displayed on the HMI screen, showing that it was a successful proof-of-concept.

6.4 Interpretation of results

Documentation is critical information worthwhile for attackers to obtain, and accessing the right information can sometimes be enough to gain access to systems. There will typically be several levels of information according to how valuable it is and how accessible it is, and it is often distributed among several different sources with different degrees of protection. Information about employees at a factory and their responsibilities is often publicly available and may be easily found on social media on the Internet. This will be an easy way to point out selected targets for a spear-phishing attack. Otherwise, it may vary from factory to factory how accessible the information for the IT system and OT system is. If the documentation for the OT system is separated from the IT system documentation, and is only available in physical and digital access-restricted parts of the factory, it will be more difficult to obtain this information. In other words, it should not be possible to obtain documentation about the OT system if a machine on the IT network has been accessed.

An example of the importance of securing documentation is if you have a well-secured machine on a secured network that is very difficult to access, but that the documentation for this machine, which contains usernames, passwords, security policies and user manuals for the system, is located on a less secure network. If attackers then gain access to this documentation, they will effectively be able to have full access to the machine without having to pay attention to the secured network around the machine. A known strategy for attackers is to gain access to a network and extract as much documentation and information as possible, and then stay hidden in the network for an extended period before a potential attack is carried out. This underlines the importance of securing documentation and not taking the security of documentation for granted.

A blackbox or graybox penetration test will give a more realistic picture of how actual attackers are advancing and what information and accesses they can gain. As it requires time and resources to map the networks, systems and devices, this was considered unsuitable for the purpose of this penetration test. For more realistic testing, one would like to spend more time mapping the devices associated with the IT and OT system, especially for vulnerabilities related to specific version numbers of specific equipment and software. From open sources on the Internet there are many programs available to test for vulnerabilities for devices in OT networks. On a later occasion, it has thus been desirable to test out these programs to a greater extent.

RDP and other remote access services are controversial services in the security environment, as it is user-friendly and makes remote access more accessible, but at the same time can pose a threat to security. For these services, the default security configuration is often to let users have a large number or unlimited attempts to enter the correct password to log in, which makes them vulnerable. If attackers find usernames through documentation or other methods, they will then be able to run brute force attacks on the passwords of selected users. While this can be a time consuming process, attackers often have unlimited time and can run automatic scripts consistently for days to crack passwords.

An easy way to prevent password brute force attacks for RDP is to set a limit on the number of failed logins attempts before the user gets locked and no longer can brute force passwords. One can also change the time it takes from the time the user has been locked until it is opened again. Both can be done by changing the registry for the machine. An attacker could also intentionally lock users to prevent individual users from logging in to their own office computer. This can also be done targeting many users in the same network in a company to prevent them from doing their work, thereby indirectly leading to production downtime and financial loss for the company. In addition, MFA can be added as an authentication step for RDP connections, which will make these systems much more secure. This is not the default RDP configuration setting and is a comprehensive process that requires technical expertise, but it is certainly a recommended measure to make RDP more secure.

If you are connected to the OT network it is also possible to create your own engineering workstation, instead of connecting to an already existing one. Then you can set up communication to this engineering workstation on the OT network.

Parallels to a real OT system
In this test system, the output of a modified executable program sent to a PLC will only appear on a screen on the HMI, but in an actual production line one would have been able to control live processes in the factory. For a real production line, the HMI would have been replaced by a device that has an actual production operation, which can typically be an engine, industrial robot, assembly line, heating or cooling element or a device that adds raw materials, dishwashing liquid or equivalent. By having control of the engineering workstation and thus being able to control PLCs from it, one will then in practice have control over all the control systems associated with this engineering workstation. One can then potentially, directly influence and tamper with a live production line in the factory, by modifying the control system processes, turning off the control systems, doing DoS attacks or other types of damage.

7

Discussion

This chapter will look at the connection between the other chapters and set the basis to draw the conclusion. Cyber security in OT systems is directly transferable from other critical infrastructure industries to manufacturing plants. This is the baseline of this discussion.

Dragos' Year in review report for 2021 is one of the latest reports to review an entire year (Dragos, 2022a). This makes their findings highly relevant for the cyber security considerations in 2022. As Dragos' five recommendation points are so transferable to the other chapters in this thesis and so up to date, it will make the starting point of this discussion. For convenience the recommendations are again given shortly below and will be discussed in detail.

1. **A defensible architecture**
2. **OT network monitoring**
3. **Remote access authentication**
4. **Key vulnerability management**
5. **OT incident response plan (IRP)**

A defensive architecture involving people is a crucial part of the IEC 62443 series of standards, where the overall security for an organization can be seen as a combination of the maturity of the organization and the technical implementation of systems and devices. As people are a major part of determining the maturity of the organization, it is important to implement necessary and reasonable security policies and have well trained personnel if security incidents would occur. One have seen that the initial access method for both Stuxnet, the Ukrainian energy attacks and Triton, was a variant of social engineering, which involves people.

OT network monitoring points out the importance of monitoring the data flow within the OT networks and at its endpoints. If this kind of monitoring would have been implemented, the Stuxnet attack would have been detected. The privilege escalation in the Ukrainian Energy attack would also have been prevented if the user accounts' actions in the OT network were monitored. Slowik (2018) highlights OT network monitoring as a preventive measure to reduce the threats, as defenders can act at an early stage if attempts of attacks are discovered.

Remote access authentication needs to be implemented in order to avoid unauthorized remote connections. Both from the risk assessment and the penetration test, remote access solutions can be vulnerable access points. MFA is suggested as a measure for the remote access zone from the risk assessment, and as a method to improve the RDP security from the penetration test. This is also a recommendation from IEC 62443 for any remote connections to the production network. In the Ukrainian Energy attack, MFA is explicitly proposed as a countermeasure, and for Triton, authentication procedures in general are recommended when critical changes is about to be made for the control and safety devices.

Key vulnerability management is essential for managing the vulnerabilities that are present in the OT system. As OT and IT systems have become more connected over time, the vulnerabilities within IT also introduce new vulnerabilities in OT. In most attacks targeted against OT, the attackers gain their initial access through the IT infrastructure. Many of the OT systems and devices are designed to have a long lifetime, and some of them can't be patched and updated regularly. This introduces a major cyber security weakness in the OT system once attackers are inside the system. Because there are a lot of vulnerabilities within OT that can't be fixed, one needs to implement effective and robust measures in the entry points and IT systems.

The Purdue model seems like an effective measure for an initial cyber security defence. A reasonable partitioning into zones and conduits will make it harder for attackers to gain access to the OT system, as systems with different criticality is not directly connected. A concern about the Purdue model itself is the lack of one-way transmission of data, as the data can flow both directions during transmissions. A solution to this problem is to introduce Zero Trust, which follows the slogan "trust nothing, verify everything". This is a strategy where one always assumes that attackers already are inside the network and validates all communication for each device, to eliminate trust. This concept was also a topic on CDS-forum in May 2022, which means that it is highly relevant today. The question is how this could be implemented reasonable. A proposal is to have the Purdue model as a baseline for cyber security and implement Zero Trust elements to the entry points of the networks and for the conduits between zones. In general each device should also follow the principle of least privilege to restrict the attack surface if attackers gain access to the OT systems, which also corresponds to the mindset of Zero Trust.

OT incident response plan (IRP) is a measure that needs to be in place to ensure that the personnel are well trained to act if a cyber incident occurs. This is also a step to improve the maturity of the organization, which also will improve the overall security in compliance to IEC 62443.

Penetration testing, vulnerabilities and cyber security barriers

The results of the penetration test show the importance of keeping documentation secured and limiting the link between IT and OT as much as possible. Inside the OT network, it is important to limit the functionality and capabilities of all machines, especially engineering workstations and other machines in the control zone and safety zone. Regarding security, this should be an absolute minimum of what is necessary to manage the production processes. This was also mentioned in the ROSS seminar ”Basic principles for ICT security in industrial ICT systems” in December 2021, with the example that there is no reason for an engineering workstation to have an e-mail service, as this has nothing to do with the management of production processes. From here, a parallel can be drawn to the RDP, which is not necessarily always needed for production operations, and one can question the extent to which such machines should use these services.

In some cases, remote access to the engineering workstation will be convenient, for example, if the machine is attacked or if it is updating software or similar. Security-wise, such services will most often provide attackers with multiple entry points to exploit vulnerabilities, rather than being useful. From an accessibility and functionality perspective, such services will also be useful for remotely making changes to the machine. This includes patching systems quickly if vulnerabilities are detected, improving security mechanisms, reconfiguring firewall rules, and quickly limiting or preventing damage if an attacker has gained access to the machine.

In order to detect anomalies inside the OT network, it is desirable to be able to monitor data traffic and modifications for individual devices. It also reasonable to utilize tools that track the version of individual devices, traffic between devices, whether there are known vulnerabilities related to specific devices in the system, and notify if attackers try to exploit vulnerabilities in the system. Dragos, a company with expertise in cyber security for OT, has developed such a platform, which provides a good overview of the devices and communications in the OT network. It can thus be recommended that factories use such services as a security measure to prevent and detect anomalies.

To be a efficient security measure the zones need to have reasonable Security Level Targets. A challenging question is how these security levels should be set. As IEC 62443 doesn't have an explicit procedure for setting the SL-T, it is common to do a risk assessment and set the SL-T according to this. It is important to reflect on which procedure or risk assessment that has been done, to conclude on a SL-T for each zone. Different procedures will probably result in different SL-Ts, which could be influential for the overall security of the organization, as other security aspects rely on the SL-T according to IEC 62443.

It is a hard task to set the SL-T, as one needs to consider many security aspects. One need to consider the risk from threats and vulnerabilities and maintain the demands for accessibility, to have a stable operation. Zones exposed to high risks need a high SL-T

During the CDS-forum seminar in the fall 2021, there were discussions between oil and gas operators, vendors and government authorities on which SL-Ts different zones should have. With this in mind one can ask if the SL-Ts set in the risk assessment in chapter 5 are correct or if they should have been changed.

It is known from earlier events that cyber attacks against OT often start as a cyber attack against IT to gain a foothold inside the organization's network. One can say that the human is the weakest joint in a cyber security defense. This is seen from earlier attacks, where the initial access to the systems often is done through a variant of social engineering. It is usually easier for attackers to trick a unaware employee to install malware rather than doing it themselves. According to Miller et al. (2021) there is an increase in the number of spear-phishing attacks, which means that personnel need regular training for handling these. This is a step in the way of improving the maturity of the organization.

Since the Stuxnet attack was known in 2010 one can see an increased number of cyber attacks targeted against OT, and the evolution doesn't seem to stop. Attackers have become more devious and often find new vulnerabilities and approaches, but it seems like the defenders can't keep up with their pace. From the most damaging cyber attacks targeted against OT, nation-state actors are probably responsible for the attack. They are often a highly skilled group with big resources and high motivation. According to Miller et al. (2021) insiders are an undefeated problem in OT. These are have knowledge about the systems and may stay hidden for a long time. To reduce the threats from insiders and at the same time improve the maturity of the organization, it is recommended security measures when new employees start, during their time at the organization and when they leave the organization.

Miller et al. (2021) points out that BlackEnergy, the malware used in the attacks against the Ukrainian Energy, shows how one type of malware can be reused in later attacks and still be relevant years after it was discovered.

Miller et al. (2021) conclude their report by some recommendations against specific threats. The table shown in Table 7.1 is an adaption from their report, which summarized some recommendations against these threats.

Table 7.1: Recommendations corresponding to threats.

Threat	Recommendation
Insiders	Implementation of fundamental security measures, like access control
Sophisticated group	Threat intelligence exchange with national organizations within cyber security
Social engineering	Train employees to have a strong security culture
Techniques for post-access	Monitor vulnerability databases regularly and use techniques for assurance, like penetration testing
IT attacks pivoting to OT	Critical networks segmentation according to the Purdue model
Comprehensive reconnaissance	Preparations against a follow-up attack
Attacks of high impact	Establish compliant response plans according to standards and guideline, like IEC 62443

For earlier cyber attacks one can see a clear trend for the most advanced attacks targeted against OT. They consist of specialized parts, from reconnaissance, construction of malicious code, delivery of malicious code and malicious code exploitation. This can be seen in the context of the Cyber Kill Chain for industrial control systems, and shows that the attackers probably are sophisticated with big resources and experts for each part of the attack. To be able to do massive damage against safety, downtime or economy, it is crucial to have deep knowledge of the control systems and the connection between the control systems and the other data systems.

For an organization to be mature it needs to have strong technical, organizational and operational barrier elements

To close security holes it is in general important to patch and update the systems as vulnerabilities are known in the systems. For many OT systems, patching is a challenge, because some systems needs to be run to not stop a live production. As it is common for OT systems to have a lifetime over 10 to 15 year, there is almost certain that vulnerabilities exist in these systems. It is then crucial to have a solid layer of protection above the OT systems, because once attackers are inside the OT systems, it is easy to exploit these vulnerabilities. The entry points to the IT network and remote access solutions are exposed to a large number of attack attempts. This also corresponds to the risk assessment and the penetration test. From the risk assessment these zones, in addition to the DMZ zone, had the highest SL-T. In the penetration test the remote access solution RDP was the entry point to the OT network.

8 Conclusion

This is the conclusion of the thesis, which will answer the problems introduced in chapter 1. The conclusion is also the results of the other chapters, and is based on the discussion in chapter 7.

Cyber security handling in manufacturing plants is directly transferable from cyber security handling in other OT systems, because the structure of industrial facilities and its systems are similar. This way, historical cyber attacks targeted against OT systems are relevant for manufacturing plants as well. The overall cyber security of a manufacturing plant is a combination of technical implementation of security measures in systems and devices, and the maturity of the organization. Some of the most important measures are a defensible architecture, OT network monitoring, remote access authentication, key vulnerability management and an OT incident response plan. Also, penetration testing is a valuable tool to strengthen the cyber security barriers, as the discovery of new vulnerabilities from the penetration test means that a barrier doesn't work as intended, and needs to be improved. In addition testing and training of personnel is an important measure to increase the maturity of the organization and thereby improving the overall cyber security.

8.1 Further work

It would have been interesting to see greybox or black penetration test of the same manufacturing plant to see if the same or new vulnerabilities were discovered. A risk assessment with another procedure could also be of interest to see if new vulnerabilities would have been found.

Bibliography

0x0mar, 2015. Modbus Penetration testing Framework. 0x0mar, https://github.com/0x0mar/smod (accessed 24th July 2022.

Assante, M., Lee, R., 2021. The Industrial Control System Cyber Kill Chain. SANS Institute, p. 1-13.

Baines, J., 2021. Examining ICS/OT exploits: Findings from more than a decade of data. Dragos, p. 8.

claroty, 2020. NSE Scripts. claroty, https://github.com/claroty/ICSSecurityTools/tree/master/nse_scripts (accessed 24th July 2022).

DNV-GL, 2017. *Cyber security in the oil and gas industry based on IEC 62443*. DNV-GL-RP-G108, p. 15-26. Available from https://rules.dnv.com/docs/pdf/DNV/rp/2017-09/dnvgl-rp-g108.pdf (accessed July 24th 2022).

Dragos, 2022a. ICS/OT Cybersecurity year in review 2021. Dragos, p. 64-65.

Dragos, 2022b. Timeline of ICS threat activity in 2021. Dragos, available from https://www.dragos.com/year-in-review/#section-timeline (accessed April 23rd 2022).

Endresen, S., 2021. Cyber security implications of introducing 5G in industrial control and automation systems. Norwegian University of Science and Technology, Department of Engineering Cybernetics, p. 26-29.

Ettercap, P., 2005. Ettercap. Ettecap Project, https://www.ettercap-project.org/ (accessed 24th July 2022).

Firoozjaei, M., Mahmoudyar, N., Baseri, Y., Ghorbani, A., 2021. An evaluation framework for industrial control system cyber incidents. Canadian Institute for Cybersecurity, University of New Brunswick, p. 3-8.

Flylib, 2005. ETHEREAL. , https://flylib.com/books/en/3.84.1.95/1/ (accessed 24th July 2022).

Harris, 2004. STAT SCANNER. Harris Corporation, https://www.helpnetsecurity.com/2004/04/21/stat-scanner-527/ (accessed 24th July 2022.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021. Analysis of Cybersecurity-related Incidents in the Process Industry. Dipartimento di Ingegneria Civile, Universita ‘ di Bologna, p. 1-20.

IEC, 2020. Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. NEK IEC 62443-3-2:2020, p. 6-30.

Jaatun, M.G., Wille, E., Bernsmed, K., Kilskar, S., 2021. *Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer*. SINTEF 2021:00055, IKT-sikkerhet - Robusthet i petroleumssektoren 2020, p. 5-11.

jpalanco, 2013. nmap-scada. jpalanco, `https://github.com/jpalanco/nmap-scada` (accessed 24th July 2022).

klsecservices, 2018. s7scan. klsecservices, `https://github.com/klsecservices/s7scan` (accessed 24th July 2022).

Kumar, R., Kela, R., Singh, S., Trujillo-Rasua, R., 2022. APT attacks on industrial control systems: A tale of three incidents. Department of Computer Science and Information systems, Birla Institute of Technology and Science, p. 3-10.

dark lbp, 2017. Industrial Exploitation Framework. dark-lbp, `https://github.com/dark-lbp/isf` (accessed 24th July 2022).

Lyon, G., 1997. NMAP. NMAP.org, `https://nmap.org/` (accessed 24th July 2022).

Makrakis, G., Kolias, C., Kambourakis, G., Rieger, C., Benjamin, J., 2021. Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. IEEE Access, p. 9, 12-13.

Metasploit, R., 2005. Metasploit. Rapid Metasploit, `https://www.metasploit.com/` (accessed 24th July 2022).

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. Lancaster University, p. 1-14.

MITRE, 2022. ATT&CK for Industrial Control Systems. MITRE, available from `https://collaborate.mitre.org/attackics/index.php/Main_Page` (accessed 24th July 2022).

Permann, M., Rohde, K., 2005. Cyber Assessment Methods for SCADA Security. ISA - The Instrumentation, Systems and Automation Society, p. 7-12.

Petroleumstilsynet, 2017. Prinsipper for barrierestyring i petroleumsvirksomheten - Barrierenotat 2017. Petroleumstilsynet, p. 1-16, 34-35.

Slowik, J., 2018. Evolution of ICS Attacks and the Prospects for Future Disruptive Events. Dragos, p. 10-12.

Tenable, 2005. NESSUS. Tenable, `https://www.tenable.com/products/nessus` (accessed 24th July 2022).

Williams, T., 1989. *A Reference Model For Computer Integrated Manufacturing (CIM)*. Available from `http://www.pera.net/Pera/PurdueReferenceModel/TOC&Intro.pdf`, p.1-11 (accessed: June 21th 2022).

Wireshark, 2022. Wireshark. Wireshark, `https://www.wireshark.org/` (accessed 24th July 2022).

Appendix

A Initial plan for penetration testing

Scope for penetration testing

Background

Sander Endresen will do a penetration testing in conjunction with his master's thesis about cyber security in manufacturing plants. The focus of the assignment is the OT systems of the manufacturing plants, which are the parts of the network structure containing control and safety systems. It is known in the industry that today's OT systems suffer from unpatched and expired software, where also old equipment are still in use, which will have vulnerabilities. It is within the OT system the critical control devices are, so a successful, sophisticated attack against OT can have fatal consequences like modification of the manufacturing plant's production, production downtime, equipment damage, harm to people and death. By gaining access to an engineering workstation it is straightforward to reprogram the instructions to a PLC, which leads to undesired behavior. The attackers responsible for the most catastrophic and successful cyber attacks against OT, are often nation state actors having in-depth knowledge of the technical components within the OT system and how they communicate. These attacks are targeted against specific versions of components from specific vendors, with known vulnerabilities. As different industrial facilities mostly consist of the same types of PLCs from a short list of vendors, it is relatively easy to exploit these vulnerabilities once one has access to the devices. This penetration testing will consider how to gain access to the OT system from the IT system, how far within the OT system one can get and how to gain access to an engineering workstation to potentially do massive damage to the manufacturing plant. Finally it is desirable to do mitigations on some selected vulnerabilities uncovered.

Main objectives

Point 1, 2 and 4 are the most important points from this list:

1. How to gain access to the OT network, given access to the IT network
2. How to gain access to an engineering workstation
3. Consider the messages sent as data packets in the system and modify them
4. Describe the entire penetration testing process. Include a step-by-step brief overview of what Sander has been a part of, that is not the focus for the test system. Cover which types of tools are relevant for the different phases of the penetration testing

Clarifications

For the penetration testing a new test system will be set up. This is a “secured, isolated system”, that is not directly connected to any live production line in the manufacturing plant. There is a distinction between this penetration testing for the test system and Orkla’s penetration testing of the entire manufacturing plant. In advance, it is important to clarify with the technical personnel at the manufacturing plant which machines can be tested and which must not be touched, as they are directly or indirectly part of a live production line.

Goals

- Show how far one can get within the OT system through the IT system
- Present the amount of information one can collect and which types of accesses can be obtained without prior knowledge of the IT system
- Present the amount of information one can collect and which types of accesses can be obtained with prior knowledge of the IT system

- Present the amount of information one can collect and which types of accesses can be obtained with prior knowledge of the OT system
- Given access to the OT system, show that it is possible to gain access to an engineering workstation
- Mitigate some selected vulnerabilities detected
- Connect the findings from the penetration testing to the known cyber attacks against OT, attacker strategies, OT challenges today and Cyber Kill Chain for OT

Devices to be included in the test system (changes may occur)

- PLC
- HMI station
- Engineering workstation
- Historian server
- Switch
- DMZ

Desirable mitigations (if found and if time)

- Patch devices' software
- Update admin password on switches, if weak
- Suggest network configuration changes
- Suggest component upgrades
- Suggest systems for monitoring and detection of anomalies in OT activities
- Suggests security policy changes

Main topics for the penetration testing and corresponding execution plan

What	Day	Time
ENTRY POINTS AND PROTOCOLS	Tuesday	Before lunch
PROTOCOLS, DEVICES AND COMMUNICATION	Tuesday	Before lunch
DEVICE INFORMATION, VULNERABILITIES AND MISCONFIGURATIONS	Tuesday	After lunch
DATA TRAFFIC AND NETWORK LOGS	Tuesday	After lunch
MODIFICATION OF DATA PACKETS	Wednesday	Before lunch
ACCESS TO ENGINEERING WORKSTATION	Wednesday	Before lunch and after lunch
MITIGATIONS	Thursday	Before lunch and after lunch
COLLECTION OF THE MAIN FINDINGS	Thursday	After lunch
(IF TIME) TEST IF ONE CAN GET ACCESS TO THE OT SYSTEMS FROM THE PARKING LOT	Thursday	After lunch
PRESENT THE FINDINGS FOR THE MANUFACTURING PLANT PERSONNEL	Friday	Before lunch
DOCUMENT THE FINDINGS IN A REPORT	-	-

Description of each step from the table

ENTRY POINTS AND PROTOCOLS:

Find entry points to the OT network from the IT network and look for vulnerabilities in every entry point.

PROTOCOLS, DEVICES AND COMMUNICATION:

Find which protocols the manufacturing plant use, which devices exist in the system and how devices communicate. Do this by scanning the network with general tools without knowing which protocols are in use and reading documentation on network configurations.

DEVICE INFORMATION, VULNERABILITIES AND MISCONFIGURATIONS:

Gather as much information as possible on the following devices: PLCs, HMIs and engineering workstations. To do this use tools specialized for scanning the network for PLCs with known vulnerabilities and tools that exploit these vulnerabilities. When inside the network, look for vulnerabilities and misconfigurations by scanning the ports, IP ranges and hosts and use tools for brute forcing PLC credentials.

DATA TRAFFIC AND NETWORK LOGS:

By having access to a switch, listen to the network traffic and identify how normal network traffic looks and which communication protocols are in use. Gain access to network logs through a historian server to find out how the data packets for normal network traffic look. Do this by sorting logs on protocol, so every protocol used will have their own logs.

MODIFICATION OF DATA PACKETS:

Modify selected data packets to se how these are logged and detected in the system.

ACCESS TO ENGINEERING WORKSTATION:

Modify data packets to gain access to an engineering workstation or gain access in another way, to understand how to communicate to a PLC on the network and which OT specific vulnerabilities can be exploited. The goal is to show how to gain access to the engineering workstation, not necessarily send a malicious payload to a PLC, which should be straightforward once inside the engineering workstation.

MITIGATIONS:

If time, from the findings in the earlier steps, do as many mitigations as possible from the vulnerabilities detected.

COLLECTION OF THE MAIN FINDINGS:

Summarize the main findings from the penetration testing, and if time look at which penetration testing activities are detected and which aren’t.

(IF TIME) TEST IF ONE CAN GET ACCESS TO THE OT SYSTEMS FROM THE PARKING LOT:

Do a blackbox penetration testing from the parking lot outside of the manufacturing plant, to check whether it is possible gain access to the OT network from the outside of the manufacturing plant.

PRESENT THE FINDINGS FOR THE MANUFACTURING PLANT PERSONNEL.

Present the findings from the penetration testing to the technical personnel at the manufacturing plant.

DOCUMENT THE FINDINGS IN A REPORT:

Write a report with the findings and information about the vulnerabilities found.

NTNU

Norwegian University of
Science and Technology