Bachelor Degree Project


UNIVERSITY OF SKÖVDE

# OPERATIONAL TECHNOLOGY DEFINITION AND DIFFERENTIATION

In the context of operational systems in Sweden

Bachelor Degree Project in Information Technology with a Specialisation in Network and System Administration Level ECTS, 22.5 credits, IT610G Spring term 2020

Jennifer Nyquist
a17jenny@student.his.se
2020-06-15

Supervisor: Thomas Fischer
Examiner: Jianguo Ding

# Contents

## Appendices

# Abstract

ICS, short for Industrial Control Systems, can be a part of the electrical and water supplies among others, which are important instances for society. This all resides in the realm of Operational technology, abbreviation OT. Due to technological development, Information Technology i.e. IT is introduced and merged into the realm of industrial systems, because of society's increasing dependencies on digital infrastructures and services.

ICS and Supervisory Control and Data Acquisition (SCADA) systems are rather well known and reputable. In the realm of OT, there's a range of different systems, and ICS itself encompasses a range of process automation technologies, such as SCADA systems and Distributed Control Systems (DCS) among others.

This paper aims to try to define and differentiate a distinct boundary of systems without any connection to IT and can be considered purely OT, if they exist at all. This by conducting an interview with people working for governmental agencies with an eminent amount of experience in the realm of OT. What kind of systems are currently in operation today that don't fit into the realm of ICS, do they exist at all and how do they work?

The definition and differentiation of OT may indicate a subset of systems and components, and terminologies of systems in the OT-realm are misused, indicating a lack of insight in this realm of industrial systems.

Keywords: industrial systems, operational technology, SCADA, ICS, digitalization

# 1. Introduction

According to the technologist Spacey (2017), the terminology of Operational Technology i.e. OT has roots in business operations that extend back to the 1950s. OT is a big domain of systems and components that can be found in many industries, many of those which are important to society. Electricity and water supply functions are some examples of necessities that society is dependent on, if there would be disruptions or mishaps, could have serious consequences for society (MSB, 2014).

The method of this study is mainly based on interviews with participants, with a lot of experience in the realm of operational technology. In this study, four participants were interviewed, their occupation resides in MSB and FOI, and these participants have a lot of experience in the realm of industrial control systems.

The study aims to contribute and widen the awareness about these supposed OT-systems, by answering questions such as:

- Are there any OT-systems in Sweden and how do they work?
- Would you say that the OT-systems in general (such as ICS, SCADA, et al) are well known and reputable?
- What do these systems do and are they vital for society?
- What protection is there for these systems?

The basis of this study lies in a thorough literature search with the focus of; giving insight in the realm of; how do properly find literature, explain the fundamentals of OT and the systems which reside in the OT-realm, how do properly conduct an interview.

The interview questions could then be based on a theoretical understanding of the subject.

## 1.1. List of Abbreviations

- UAS – Unmanned Aerial Vehicle System
- IT – Information Technology
- OT – Operational Technology
- ICS – Industrial Control System
- PLC – Programmable Logic Controller
- DPC – Discrete Process Control
- SCADA – Supervisory Control and Data Acquisition
- PCS – Process Control Systems
- RTU – Remote Terminal Unit
- MSB – Myndigheten för samhällsskydd och beredskap | Swedish Civil Contingencies Agency (MSB, u.d.)
- NCS3 – Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet | National Centre for the Security in Control Systems for Critical Infrastructure
- FOI – Totalförsvarets forskningsinstitut | Swedish Defence Research Agency (FOI, u.d.)
- CHP – Combined Heat and Power, e.g. A power plant using a heat engine to generate electricity and useful heat simultaneously.
- A/D – analog-to-digital converter
- V2X – Vehicle-to-everything communication, is the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa (Wikipedia, u.d.).
- HMI - Human-Machine Interface

# 2. Background

OT is the abbreviation of Operational Technology, which refers to industrial systems and operations such as monitoring and controlling physical processes (Hahn, 2016). In the domain of OT, there are multiple factors included in the term of OT as mentioned in a report called *Industrial Control Systems: Getting a Grip on OT Cyber Security* by Williamson (2015), such as industrial control systems (ICS), programmable logic controllers (PLCs), discrete process control systems (DPC), and Supervisory Control and Data Acquisition (SCADA). DPC, DCS, and PLC is a part of SCADA, and those are part of ICS, as seen in the figure below (see figure 2-1).

While searching for information and relevant literature for this study, it became clear that there is a lack of information regarding operational technologies beyond ICS and SCADA with their potential respective controllers; thus, the definition of what OT systems are and if they exist at all will be further discussed in this paper. The aim is to explore and find systems that reside in the OT realm without making use of PLCs, DPCs, or SCADA.

Following in this chapter is a description of the elements of OT which explain the different systems. Further, the systems referenced in the figure below (see figure 2-1), will be highlighted for explanatory purposes, and other elements that are not relevant to this study will be excluded, as it is out of scope for this thesis, such as Discrete process control systems (DPC) hardware, which is managed by SCADA systems or Remote Terminal Unit (RTU), which is a digital control system component that interacts with physical processes, this by reading or controlling it, often associated with SCADA (MSB, 2014).

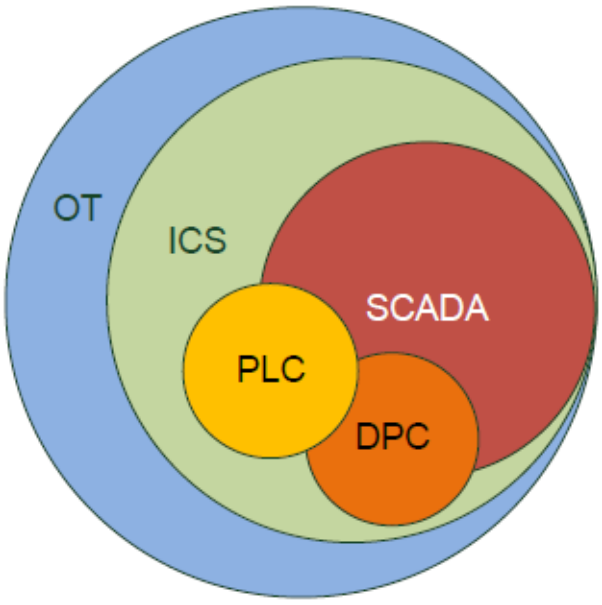


*Figure 2–1. Williamson, Graham (2015) Industrial Control Systems: Getting a Grip on OT Cyber Security (Report No: 71110). Wiesbaden: Kuppinger Cole Ltd.*

## 2.1. What is OT

A further description of OT according to Sarkar et al, (2018):

> "An OT network consists of hardware devices and software that monitors hardware devices and control operations of hardware devices. Unlike IT, OT used for operations and controls in ICSs is isolated as most of those OT network tools for monitoring and operations are mechanical and proprietary in nature. Nowadays, however, OT consists of smart devices to monitor, operate, and control equipment used in power stations, water treatment plants, etc." (Sarkar, et al. 2018).

According to Hahn (2016) who describes the difference between IT and OT in chapter 4 called *Operational Technology and Information Technology in Industrial Control Systems,* the clear difference between IT and OT is that OT focuses on the monitoring and control of physical processes, in contrast of IT which is commonly used in the development of e.g. software, maintenance, and networks to distribute data. In this thesis, IT will reference systems that by default make use of an IP address.

In the following headers in this chapter, a summary of different systems in the OT realm is presented, some of which is ICS, PCS, DCS, PLCs, and SCADA, as mentioned in *Cyber-security of SCADA and Other Industrial Control Systems* (Sullivan, et al., 2016). This does provide some insight into the different elements of OT systems.

### *2.1.1. What is ICS*

ICS is usually more associated with physical environments, some of which are transportation networks, Unmanned Aerial Vehicle Systems (UASs), nuclear power generation, electric power distribution networks, water and gas distribution networks, and advanced communication systems. Key segments of ICS can consist of thousands of different components worldwide and ISC systems are in the definition of the OT realm (Sullivan, et al., 2016). SCADA, PCS, PLC and DCS systems are a part of ICS while as everything is part of OT, as seen in figure 2–1.

Industrial Control Systems i.e. ICS differs from typical Information Technology systems i.e. IT. For example, a reboot of a typical IT system would be acceptable whereas a reboot e.g. outage for an ICS may not be acceptable, due to process availability requirements, meaning that outages must be planned and scheduled days/weeks in advance. Furthermore, in means of change management, a typical IT system may make use of software changes, which can be applied in a timely fashion and sometimes in automated procedures. Whereas in regards to ICS, software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained.

Furthermore, typical IT components have a lifetime in the range of 3 to 5 years, due to the evolution of technological development. Whereas today's ICS is often a combination of legacy systems, often with a planned life span of 20-30 years, and typical ICS component has a life span in the range of 15-20 years (Stouffer, et al., 2011).

### *2.1.2. What is PCS*

PCS stands for Process Control Systems. These systems control automation processes in a manufacturing environment, such as typical ICSs processes. PCSs usually monitors and controls these ICS processes commonly found in factories and industries. A Supervisory Control and Data Acquisition i.e. SCADA system may supervise one or more DCSs or PCSs at distant geographic locations and the SCADA system may poll information such as; when an alarm or event occurs, from the controllers less frequently than a DCS or PCS (Hahn, 2016).

### *2.1.3. What is DCS*

Distributed Control Systems controls automation processes at a single site, were it may monitor and supervise server PCS (Hahn, 2016), as mentioned above. Examples of DCS processes would be; control processes at oil refineries, drinking water, and wastewater treatment plants, and car assembly lines.

Supervisory Control and Data Acquisition i.e. SCADA and DCS resemble each other, as both are a software package that performs communication with control hardware and presents it in a Human-Machine Interface i.e. HMI. A subtle difference between DCS and SCADA is that DCSs are process-driven and they generally focus on presenting a steady stream of process information. The DCSs may for the most part pull information from a controller, regardless of the quality of the data, without maintaining records of all last known data values. These values are retrieved from control hardware that consists of PLCs (Galloway & P. Hancke, 2013).

### *2.1.4. What is PLC*

Programmable Logic Controller can be described as a microprocessor-controlled electronic device that reads input signals from sensors e.g. flow control, temperature measurement, and executes programmed instructions in ICS (Hahn, 2016).

PLCs are computer-based, solid-state electronic devices that form the core of industrial control networks and were first used to replace hard-wired i.e. relay-based logic circuits. A PLC has a power supply, central processing unit (CPU), communications interface, and input/output (I/O) module(s). An I/O module can either be digital or analog (Sullivan, et al., 2016).

Modern PLCs have the ability to perform both binary and analog input and output, this to operate within a plant and communicate with central data collection (Galloway & P. Hancke, 2013), such as a DCS and SCADA systems.

### *2.1.5. What is SCADA*

Supervisory Control and Data Acquisition is a type of ICS that collects data and monitors automation, which can be thousands of miles apart, and a SCADA system may supervise one or more DCSs or PCSs. SCADA systems can provide a graphical user interface for operators to easily observe the status of a system, receive any alarms indicating out-of-band operation, or enter system adjustments to manage the processes (Williamson, 2015).

As mentioned earlier, SCADA and Distributed Control Systems i.e. DCS resembles each other, as both are a software package that performs communication with control hardware and presents it in a Human-Machine Interface i.e. HMI. Whereas the DCS is process-driven, SCADA is event-driven and do not perform any control, but rather function in a supervisory fashion with a focus on reporting only changes in the state of the monitored systems (Galloway & P. Hancke, 2013).

## 2.2. Related Research

Similarly to this thesis, an acknowledgment of the importance of terminology is mentioned by Hasselbring (1999), thus, the problem resides in the realm of computer science terminology is that some terms are often used for different concepts and that the same concepts are denoted by different terms. In this paper, Hasselbring (1999) highlights the issues of terminology in regards to health care information systems, as opposed to this thesis which aims to define and differentiate the operational technology i.e. OT.

# 3. Problem

The definition of Operational Technology according to the sources mentioned in previous sections, has one thing in common and that is the amount of information of ICS systems and controllers, and a noticeable lack of information regarding systems that are not included in the ICS realm, if any exists at all. If there were to be existing systems that are not dependent of different controllers such as those described in heading 2.1 *What is OT*.

The lack of information emphases that further research on the topic is relevant. As industrial systems encounter more challenges in regards to a rapidly evolving area of information, supervision and data acquisition (Hedtjärn, et al., 2016), Sweden is going through a digital transformation (Ingemarsdotter, et al., 2020) which can indicate and point to older OT-systems that do not make use of ICS or sequential systems i.e. PLCs, SCADA, et al.

## 3.1. Research Questions

Research topics with questions regarding different aspects of this thesis have been established, aiming to answer the following questions:

- Are there currently any systems in Sweden considered purely OT, and if they exist, is the separation in the OT-realm self-evident?
- How do they work?
- Are some systems such as e.g. SCADA and ICS more reputable, and are the terminology of these systems being used correctly?

Due to the risk of insufficient information, i.e. if there's no such systems and the research questions cannot be answered, more questions were added to broaden the perspective into the realm of OT.

These additional questions aim to get an insight into; how many potential OT-systems are in operation currently in Sweden, what they do in society, how these are protected, and what's currently being researched in the area.

In total there are 7 questions, these have been divided into two Topics; Main and Subsidiary Topic. This to make a separation of the main questions, and the questions to broaden the subject if insufficient data was retrieved, this also facilitated the structure of this thesis.

### *3.1.1. Main Topic*

This section contains the main questions of this thesis, intending to answer the following:

1. **Are there any OT-systems in Sweden that do not fit into the ICS-realm and other components, such as SCADA, PLC, and others?**
   This question is based on establishing the fact of whether or not these OT-systems exists at all. If there's any separation between the layers as seen in figure 2-1.

2. **What are they, and how do they work?**
   How do these systems work and what do they do? This to get an insight into these systems from an experienced person's point of view.

3. **Would you say that the OT-systems in general (such as ICS, SCADA, et al) are well known and reputable?**
   Do people know about these systems and is the terminology used correctly? Is the realm of OT a Gray zone, even for people in the industry?

### *3.1.2. Subsidiary Topic*

This section is an extension of the topic, this can result in a broader discussion and aspire for future work based on this thesis.

4. **Approximately, how many OT-systems (e.g. Relay based and/or mechanical) of your knowledge are in operation in Sweden currently?**
   Try to get an insight into how many systems currently exist in Sweden.

5. **What do they do in society (due to delimitation, single down the question to a specific system and/or aspect that may be vital in society)?**
   Highlighting systems to get a societal perspective of why we need them. What do the interviewees consider important?

6. **What protection is there for them (e.g. aging/degeneration)?**
   How can systems experiencing aging and degeneration be protected?

7. **What is currently researched in this area (Important systems vital for society)?**
   What is one of the current topics at these instances, what's being researched, and why? This question is meant to give insight into current topics of what FOI and MSB as government

agencies are currently researching. Targeting subjects that can be associated, but not limited to, the OT-realm.

Both subjects include 7 questions in total, all of which aim to give a broad insight into the OT-realm and highlight the importance of what these potential systems may have in society. This with the insight of knowledgeable people who has years of experience in the area.

## 3.2. Delimitation

The realm of OT overall is a large subject, limitations needed to be established. This due to lack of time and the aim to focus on the main subject to conduct a successful study. Meaning that OT-systems described in the background section is from literature not restricted to Swedish origins, rather, that most of the publications are international. The interview study aims to interview people regarding OT systems that are located in Sweden.

The research is restricted in such a way that the information gained will not be presented in such a way that it could lead to potential exploitation of these systems. Rather give an overview of these the functionality and importance of these systems. Furthermore, this study aims to try to define, differentiate, and explore if there’s a distinct boundary of systems that can be defined as purely OT. Thus, the aspect of the security of OT is an interesting topic, it is out of scope and not the aim of this thesis. Thus, all security-related topics brought up by the participants in regards to the interview study, will be discussed and presented in the analysis and conclusion section.

# 4. Methodology

A qualitative study is chosen as a suitable method to answer the research questions, this by conducting an interview study. The methodology for this paper is based on literature, this to explain and define the terminology of Operational Technology, in the hopes of perhaps finding an OT system that does not fit into the realm of ICS. Furthermore, how to conduct an interview study as adequately and accurately as possible. The following chapter covers a description of the method used to conclude this thesis, which includes the selection of literature, interview study, ethical aspects, and validity factors.

## 4.1. Literature

By using literature in conjunction with an interview study made it possible to fill the gaps. To find relevant literature, a systematic approach needs to be used. Berndtsson (2008) emphasizes to analyze published sources with a specific purpose in mind and to do a careful interpretation and systematic analysis from each source. It's vital to identifying relevant sources, which can be retrieved from bibliographic databases, journals, and conference proceedings. Further, the research of OT i.e. industrial systems is a bit of a stretch from a typical subject associated with the NSA-programme, meaning that the method in the search for relevant literature didn't include a step-by-step guide of which databases to look into.

The literature used in this research made it possible to get an insight into the realm of OT and made it possible to establish the questions asked to the participants of the interview.

### *4.1.1. Selection of Literature*

The selection of literature has been for the most part retrieved from databases such as; ACM, Science Direct, Google Scholar, and SpringerLink. This by searching for relevant literature with the terms presented in table 4.1, and that resulted in excluding databases when no relevant literature would be found upon research.

The guidelines used in searching in databases and selecting relevant literature for the research questions were influenced by Kitchenham and Charters (2007) and are presented in the following chapters (see 4.2. Search of Databases and Terms and chapter 4.3. Selection Criteria). However, as mentioned above, the literature search operation was not strictly met by this guide. Further in this chapter, a description of how this literature was retrieved for this thesis is presented in the following sections.

### *4.1.2. Search of Databases and Terms*

In means of finding relevant literature for this study, search terms in the databases mentioned earlier were established in means of finding information about OT and other aspects in the same area. The search strings (see table 4.1) were assembled by using Booleans such as ANDs an ORs.

| |
|---|
| ‘Operational technology’ ‘OT’ ‘control systems’ ‘Industrial Control Systems’ ‘SCADA’ ‘Security’ ‘Terminology’ ‘Computer science’ |

*Table 4.1. Search Terms*

Finding relevant literature with information of OT systems where the terminology could differ, an OR-operator can be used to increase the chance of finding information and narrow down the search results (Berndtsson, et al., 2008). An example of this would be*; OT OR Operational technology OR Operative technology*.

### *4.1.3. Selection Criteria*

In the search for finding relevant literature, some criteria had to be established, to exclude irrelevant information regarding the research questions for this thesis. The following criteria were the baseline of the search process:

- The literature needs to provide relevance and evidence in means of answer the research questions in this thesis.
- It needs to be available in a language that’s either English or Swedish.
- A certain number of pages is necessary with the reasoning that sufficient information is needed.
- The publication needs to be open access, i.e. free.

In the search of literature and publications that would provide general information of OT systems outside ICS and its potential components, it was very important to find literature that would contain the basics of the OT realm instead of extensive information into e.g. PLCs and DCSs and other systems. This because this thesis aims to try to find and define OT-systems that do not fit into the other realms as mentioned.

The literature needs to be in a language that’s understandable from a personal point of view, either by being written in Swedish or English. This to lessen the risk of misinterpretations and eliminating the burden of translation which can be time-consuming.

Literature that consist of five pages or less was excluded due to lack of information and substance.

The publications used in this thesis needs to be free and open access, this due to financial aspects as a student.

## 4.2. Interview Study

This thesis contains an interview study, with the purpose of interviewing people who have knowledge and experience of working with these systems, to try and get answers for the research questions. The book called *Intervjuteknik* written by Häger (2007), and guidelines suggested by Berndtsson et al. (2008) has been used to properly conduct and prepare a successful interview.

Some of the guidelines according to Häger (2007) is; *Agree on the premise of the question*, which means to reflect the structure of the questions in such a manner that the person being interviewed will accept and be able to comfortably answer the questions, e.g. some topics may be restricted due to confidentiality. The next tip is *Use open questions*, this implies that the questions asked should open for discussion, to avoid closed ones, i.e. questions that can be answered with yes or no. The last tip being used is *Plan the interview*, as stated, the questions asked should be planned and perhaps answered in chronological order. It's vital to have in mind the logical reasoning, this to build a basis for further questioning. Residual questions could be asked at the end of the interview.

The structure of the interview used in this project has been influenced by Berndtsson et al. (2008) in regards to preparation and methodology, they present two different styles, open and closed interviews, which are presented in the bullet points below.

- Open Interviews is a commonly used form of an interview where the researcher has limited control over the interview, or no control at all. This implies that even though the purpose of the interview is clear for the researcher, the session is not planned in advance and aims to direct the session in a way that the interviewees would find important. In summary, an open interview can be characterized in a way that the "control" is very much in the hands of the interviewee.
- Closed interviews can be characterized as an interview with fixed questions, also referred to as a pre-structured interview. By using this type of method, it implies that it's not allowed to add or delete questions depending on the replies from the interviewees.

To answer the research questions in this study, a mixed variant of both open and closed interviews seems like an appropriate method. This by giving the interviewees a specific set of questions, but still let the interviewees have the control and talk freely, as Berndtsson et al. (2008) mentions, a compromise may be found between these two methods.

Berndtsson et al. (2008) emphasize that taking notes can be difficult during an interview, especially with the open interview method. Therefore, it may be preferable to record the session so that the interview can be accurately transcribed.

Transcriptions of the final result of the interviews can take a lot of time, and a lot can be said during an interview session. Hedin (1996) mentions different aspects of how to systematically process the

interview data, such as finding keywords; Reduce the text and analyze it to find out what it's really about. By reading the interview text a couple of times and extracting keywords relevant to the participant and the research question. Then the next step is to find themes in the keywords, meaning that the initial review of the interview session can contain many keywords and need to see which ones "fit together".

Furthermore, the result of each answered question of the interview study was then analyzed (see chapter 7 Analysis), to summarize and reduce the text from the result section. By doing this it was possible to determine what was said and argue what the result is about (Hedin, 1996).

### *4.2.1. Selection of Participants*

The selection of interviewees was based on the purpose of the research questions in this thesis. A qualitative study means to get as broad and accurate a description of the phenomenon as possible (Hedin, 1996), therefore, choosing the participants was based on the fact that they are very knowledgeable in the area. Even though the participants are few, this due to lack of time, the result of a conducted interview session aims at getting answers to the research questions, this by knowledgeable people working in the realm of Operational Technology.

In this study, four people were interviewed, all of which has a lot of experience in the field of industrial control systems. Three of which works for MSB, and the fourth for FOI. All participants remained anonymous in this study and therefore the participants are referred to as; MSB-1, MSB-2, MSB-3, and FOI-1. This to separate the participants in means of their occupation. For a further description of the participant's current occupation and experience in the field, see Appendix B.

### *4.2.2. Ethical Aspects*

By conducting and preparing a proper interview, it's important to establish trust and boundary's between the interviewee and the interviewer, otherwise, the results can be of limited value (Berndtsson, et al., 2008). Further aspects to consider according to Hedin (1996) is to be open and honest about the intension of the research and that the participants are well informed about the idea of the interview. The participants will decide for themselves whether or not to participate in the interview. Furthermore, the participants and their statements will include the option of being anonymized in this study, i.e. with their role as the only thing distinguishable about their identities.

The interview will be recorded with the participant's knowledge, this to facilitate the transcription process. The recorded session will be stored locally and not shared in any means, such as with other parties or in a cloud setup. The material will only be used for the motive of this thesis.

## 4.3. Validity and Reliability

It's important to have in mind the aspects of how the study is managed. The sought-after results need to be valid and reliable, meaning that in the search for answers for this study, some things need to be considered. This section presents a summary that applies to the interview study.

Berndtsson et al. (2008) mention various aspects to have in mind while concluding a reliable and valid study, one of those regard personal bias due to potential pre-conceptions. This implies that doing a project, collect data, and use literature from an organization or company can be a threat against validity. The literature used to answer the research questions is not from one single organization or company. The publications used in this thesis are thoroughly selected due to their scientific value and retrieved from reliable sources and databases.

As for the interview study which includes a self-developed questionnaire, it's vital that the participants have fully understood the questions. This to lessen the risk of misinterpretation which could lead to implying that the study probably is less credible and not a useful analysis. Therefore, all participants were thoroughly informed about the subject and research questions. The concluded transcript will be approved by the participants, and only then the results of the questionnaire will be presented.

# 5. Conduct of interviews

The participants were first contacted through email, where follow-ups consisted of a phone call with the intent of concluding the date and time for the interview. This communication occurred at the beginning of May and lasted until the beginning of June. Furthermore, the conversations included a description and motive of the thesis, including the figure presented in the background section (see figure 2-1). Each participant has been informed about the structure of the interview, such as:

- The interview is being recorded
- Each participant has the option of being anonymous
- The person being interviewed can stop and pause the session at any moment

An interview guide was used as a template of the interview (See Appendix A).

The interviews were conducted via a video call through a web interface and a phone call that lasted approximately 60-120 minutes, it was later transcribed and shared with the participants, this to ensure that there weren't any misinterpretations. The participant's approval of the finalized transcription needs to be established before applying it to this thesis.

The transcript of interviews will be summarized in the means of systematic processes, this to find keywords, and analyze the responses, aiming to answer the research questions. The summarized answers will be presented in a more elaborated manner in the results chapter. The participants of the interview are presented with a description of their current occupation and experience in the field (see Appendix B). The full transcript will be presented in Appendixes C and D.

# 6. Results

In this chapter, a summary of the conducted interviews in the means of answering the research questions is presented. This by analyzing the transcripts and summarize the responses in a systematic manner. The answers of the participants i.e. MSB-1, MSB-2, and MSB-3 are presented in the order of who and when the participants answered the questions, rather than the numeric value of the alias used by the participants. Since the interview session with the participant from FOI was conducted at a later moment, most of the statements from FOI-1 are presented at the end of each result question. The full transcript of interviews can be seen in Appendix C-D. Furthermore, a brief presentation of the literature mentioned by the participants, which can answer the research question in this thesis.

## 6.1. Result of the Main Topic

This section presents the answers from the Main Topic, and the answers from the participants will be presented. The material that is the basis for this summary can be found in Appendix C.

### *6.1.1. Result Question 1*

Are there any OT-systems in Sweden that do not fit into the ICS-realm and other components, such as SCADA, PLC, and others?

MSB-2 implies that there's no clear distinction between the different aspects of OT, meaning that OT itself is more of a concept of typical control systems, such as SCADA, PLC, et al. Including components such as hardware, cables, and SCADA software among others. The terminology of OT originates from the USA. The term OT got it's footing in Sweden later and may originate due to the evolution of IT security in control systems e.g. how they are connected to the Internet/IT.

MSB-1 implies that concepts such as IT and OT may exist to make distinctions, meaning that the "OT-world" does not want to be included in the IT and vice versa. Perhaps the term OT implies less of a division between software and hardware. There can also be organizational and cultural aspects in means of usages of the term OT.

FOI-1 does not fully agree with a separation of OT, as seen in the figure (see figure 1-6). Thus, implying that there are systems that partially reside outside the ICS realm. Such as old relay-based systems, which do not have any data monitoring, there may be a few of these still in operation today. The PLC was introduced for approx. 50 years ago, which replaced the old relay components in means of computerizing the systems. The PLCs a kind of computer, managed with a programmable language, similar to which the electricians used to manage the relay-based components.

### *6.1.2. Result Question 2*

What are they, and how do they work?

In regards to answering this question, SCADA, ICS et al, which makes use of IT has been excluded, but rather highlighting systems that do not fit into the realm of ICS et al.

MSB-2 mentions systems that do not make use of IT (Meaning that these systems per default do not make use of an IP-address) exist and are currently in operation today. Many of those are very old and completely mechanical and relay-based. They exist in nuclear, water, and heating industry's and some security features in wind turbines are also purely mechanical. MSB-2 implies that these old components may not be purely ICS, this due to the lack of IT involved and can therefore be separated in the form of layers, referencing the Purdue model (see figure 6-1). Thus, due to the technical development, the line between these layers is starting to experience erosion, as an example; sensors nowadays may be directly connected to the internet, and old systems that make use of hydraulics can be directly connected to an (A/D) i.e. analog-to-digital converter to obtain a digital signal.

FOI-1 also refers to the Purdue model (see figure 6-1), and emphasizes that layer 0 is the industrial process, layer 1 contains sensors, motors, eyes, ears, and hands in the system which listens and controls what happens. Layer 2 has direct control and automation to make sure that things go as planned, a PLC would probably reside in this layer. An example of layer 2 could be that the PLC listens to a sensor and control an engine, which in turn controls a pump. Then we have layer 3 which would probably contain a SCADA server. It is in layer 3 that there would be people analyzing and monitoring the industrial environment, making optimizations of the production. Everything from layer 0-3 can be defined as OT, it symbolizes production.

Furthermore, FOI-1 implies that there are probably still old relay-based systems currently in operation today in Sweden. FOI-1 have no personal experience working with these potential systems, but have heard about them. Something that's often associated with OT systems. OT supervises and controls systems, which have a long operational lifetime. The production system may have an operational lifetime of 20-40 years, some times longer than that. During that lifetime, some of the OT-components will be exchanged, but it is common with a long lifespan, especially compared to traditional office IT.

FOI-1 also mentions that OT systems are built to have a long life span, meaning that a system should be able to properly function for a long time without shutting them down in order to repair them. In comparison with typical IT systems, which have an estimated life span for approx. 2-3 years and can switch out e.g. cables, RAM among others and is easy to shut down, repair and restart again.

### *6.1.3. Result Question 3*

Would you say that some the OT-systems in general (such as ICS, SCADA, et al.) are more well-known and reputable than others?

MSB-3 mentions an example of how SCADA can be used as a mere subset of what's become a synonym for a whole area; the American vacuum cleaner manufacturers called Hover dominated the electric vacuum cleaner industry, to the point where the Hoover brand name became synonymous with vacuum cleaners and vacuuming overall.

MSB-2 mentions that due to his role in means of security in the operative area, it has led to encounters with people from the outside who work as IT-security consultants and pen-testers. While these people dive into the operative area with the sense of SCADA as a synonym, as mentioned earlier, even though the subject in question can be a PLC, as an example. MSB-2 reckons that due to the increased attention of the subject in media, there's a lot of confusion in that regard.

MSB-1 Agrees with the previous statements and finds that the term SCADA has become a synonym with a lot of different things.

FOI-1 implies that there's a lot of terms and concepts floating around, and they are depending on which industry you are talking about, but technically you are still talking about the same thing. FOI- 1 implies that SCADA is something specific, but the term is generally used incorrectly. ICS and SCADA are somewhat well-known concepts, and people who work with these systems, know the correct terminology for these systems and components. ICS is an overall term that includes e.g. SCADA and distributed control systems (DCS) and defined as stand-alone systems. Whereas PLC is a component that can be used in these stand-alone systems.

FOI-1 also emphasizes that some time ago, there was a clear separation between these systems, i.e. SCADA and DCS for example, but nowadays it has grown closer together.

## 6.2. Result of the Subsidiary Topic

This section presents the answers from the Subsidiary Topic. Material that is the basis for this summary can be found in Appendix D.

### *6.2.1. Result Question 4*

(Approx.) How many OT-systems (e.g. Relay based and/or mechanical) of your knowledge are in operation in Sweden currently?

MSB-2 implies that if the question suggests components that are relay-based or purely mechanical, i.e. without any connection to the Internet, and go through a digital converter that sends the signal to a PLC? Then we are talking about millions of OT systems.

MSB-2 mentions that the motorway tunnel called Southern Link (Södra länken) in Stockholm contains approx. 30 thousand measurement components that measure temperature and such, and they respectively send out a 20-volt signal to a PLC which in turn converts and gives it an IP-address and sends it to a SCADA system.

FOI-1 emphasizes that anything that blinks, moves, etc. in society, can be considered as OT systems, which implies that there's a lot. Not everyone is critical of society.

### *6.2.2. Result Question 5*

What do they do, how vital are they for society? (due to delimitation, single down the question to a specific system and/or aspect that may be vital in society)?

MSB-2 implies that there are multiple factors in regard of answering this question, would these systems affect society locally or throughout the country? But also mentions one of the most vital instances for society, and that would be the electrical supply, also called "Spindeln i nätet" i.e. Spider in the web. Which consists of electricity supply i.e. electricity grids, in means of production, distribution and transmission. If we would lose the transmission part of things, then the whole country would be affected. The consequences can be vital. Some aspects may stop working immediately, and some may have reserve resources, such as hospitals and such, but it's just a matter of time before the reserve resources are exhausted.

MSB-2 adds that the electricity supply is very important for society and a lot, if not all instances would probably not suffice without it. If the heating plant would stop working during a time period around June, while the temperature lies around 30 degrees Celsius, there wouldn't be a major problem. However, would that same scenario apply in January with -25 degrees Celsius it would be a very critical problem for society, people wouldn't be able to heat their homes for example.

FOI-1 emphasizes that electricity is the basis of everything, there are not many things that would function and our modern civilization ceases to function without electricity. FOI-1 also mentions the importance of computers, without these, it would be very hard to monitor, control, and produce electricity. The production of electricity is in symbiosis with computers. Furthermore, electricity production is not something that secluded in Sweden, rather than it's connected to a European network. Meaning that there are multiple electricity production companies here in Sweden, thus that they are probably connected to foreign countries and do not work entirely alone. Would Germany for example require more electricity, then Sweden would be able to assist in that matter.

FOI-1 also mentions that the water supply is also very important to society. Access to purified water is critical for people. Water treatment facilities and distribution are often local; Thus, the loss of a single facility would probably not affect the whole country. If the loss occurs in a heavily populated area, however, lots of people will be affected by this. Supplying water to a village or a city without using the regular distribution system is a difficult task.

### *6.2.3. Result Question 6*

What protection is there for them (Against e.g. aging/degeneration)?

MSB-2 implies that old systems are continually upgraded to counter aging. In regards to old systems that require components, that's no longer manufactured, either there are continuous stages of upgrades of these systems, this to keep up with technological developments, or the old components and spare parts are bought in large quantities and stored somewhere.

MSB-2 mentions a recollection of a very old gas turbine, located in the southern part of Stockholm, that's currently not in use anymore. This gas turbine was used to operate the subway and there were only approx. two people in the entire world who knew how it worked. These people didn't live in Sweden, meaning that to operate this turbine it was necessary to fly these people to Sweden from far, far away.

FOI-1 Mentions that on the IT side of things, it's very common to update the systems in means of security, thus in the OT realm containing these old systems, that's not always possible to do. Either you can't update these systems due to that there are no updates available anymore, or you're not allowed to due to the risk of failure and stopping production. Some systems that cannot update due to e.g. age, are segmented and put behind firewalls in means of isolating these systems. Segmentation is the main approach in means of securing old systems. This to lessen the risk of exposing them outwards on the internet.

FOI-1 mentions the increase of ransomware being used nowadays, implying that it is very important to educate people who are responsible for production technology and to realize that almost everything in

the OT-realm can be considered as a computer. Such as a PLC or the monitors on the train tracks that display arriving trains, those are basically a computer. Ransomware doesn't care what or where they end up, as long as there's a possibility to exploit these systems. FOI-1 Mentions a list of 3 things to be aware of:

1. Have a thorough knowledge of the inventory of all systems, components and units you have
2. When you know that, perform a risk analysis of the whole inventory; what can be exploited? Which of these things should be able to talk to each other? If they shouldn't be able to talk to other systems, separate and segment them, can these be updated?
3. Educate personnel, follow guidelines and continuous risk analysis needs to be done.

FOI-1 also emphasizes to keep an inventory of critical components. This in regards to older systems, i.e. those that are in the risk of e.g. aging/degeneration, which may use old components that are not being manufactured anymore.

### *6.2.4. Result Question 7*

What is currently researched in this area (Important systems vital for society)?

MSB-1 mentions that the first thing that comes to mind is the importance of the educational aspects in the supply chains. Meaning that the need for knowledgeable personnel who should have the right prerequisites to be able to manage these systems. This subject is something that has been researched and appeared in recent studies.

FOI-1 emphasizes that there's a lot of courses and education in regards to IT, but a noticeable lack of education that covers the OT side. FOI has for the last ten years held courses, in the security aspect of OT, which is connected to one of their first courses that were held around 2009. At the same time as this course started, Stuxnet became known, which was a waking call for people in the process control realm. FOI-1 also mentions that for the last three years, there has been a lot of education and courses regarding ransomware, which affected a lot of productions.

### 6.2.5. *Literature*

The following section provides some insight into relevant literature, mentioned by the participants in the interview. Material that is the basis for this summary can be found in Appendix C. This to present the layers between OT, ICS SCADA et al. Literature mentioned from the interviewees which emphasize the different layers in industrial control systems, i.e. the Purdue model (see figure 6-1).

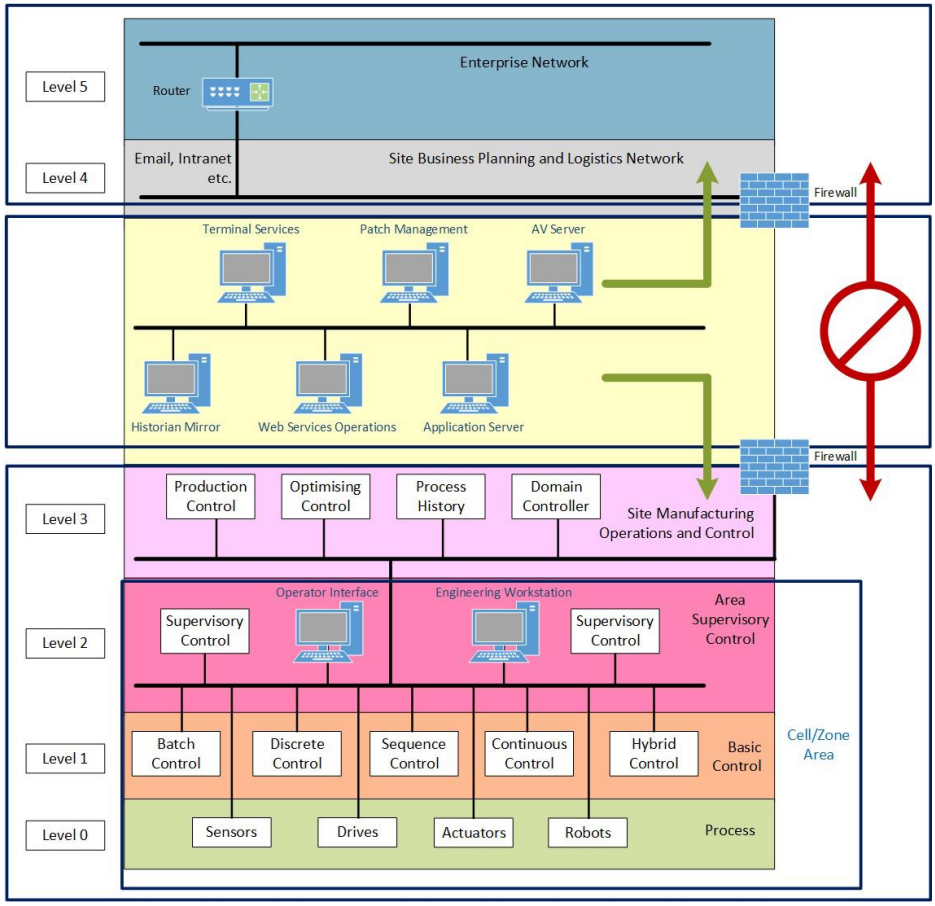


*Figure 6–1* (Cook, et al., 2016) *Purdue Model for Control Hierarchy. Attribution of Cyber Attacks on Industrial Control Systems. Volume 3, pp. 1-15.*

This can be used as a reference in means of explaining the architecture for control hierarchy that has become the standard within ICS, which includes 5 levels according to Cook, et al., (2016):

- Level 5 covers the corporate/enterprise network of an organization's applications and services.
- Level 4 includes the services to manage the planning, scheduling, and logistics of the operations.
- Level 3 management of the day-to-day industrial operations, such as; production scheduling, quality assurance, process optimization et al. SCADA system with the purpose of monitoring would occur in this layer.
- Level 2 provides supervisory control of the equipment involved in the overall industrial process.
- Level 1 encapsulates the control of individual devices and equipment involved in discrete elements of the overall process, such as PLCs.
- Layer 0 includes the devices, sensors, and associated equipment performing the industrial processes.

# 7. Analysis

The following section of this chapter finalizes and analyses the responses from the participants in order to answer the research questions for this thesis. This to summarize and reduce the text from the result section and draw conclusions from the statements of the participants from the interviews.

## 7.1. Main Topic

This section contains the is the main focus of this thesis, with the aim of answering the question; Are there systems in the OT-realm that's purely OT and does not have any connection to ICS? If so, attempt to explain what kind of systems they are and if they are well known and reputable.

### *7.1.1. Analysis Question 1*

The first question asked to the participants was: Are there any OT-systems in Sweden that do not fit into the ICS-realm and other components, such as SCADA, PLC and others?

The answers from all of the participants of the interview, with many years of experience in the field, points to the same conclusion; The depiction between OT and ICS, SCADA et al. are not evident. When talking about OT, there was a common understanding that the terminology is more of a concept that covers all the aspects of control systems. Rather than separated systems. Thus, all participants emphasized that there are systems that partially reside outside the ICS realm. Such as old relay-based systems, which do not have any data monitoring, there may be a few of these still in operation today. Some time ago, there was a clear separation between these systems, i.e. SCADA and DCS for example, but nowadays it has grown closer together. This due to technological development, e.g. the PLC was introduced for approx. 50 years ago, which replaced the old relay components in means of computerizing the systems.

Furthermore, the participants from MSB emphasizes that the term information technology (IT) is a globalized term that represents a lot of things, such as software, hardware et al. regardless of where in the world it can may be located, it's still considered IT. In contrast with the terminology of OT, which can vary depending on the industry. MSB-2 mention that the terminology of OT originates from the USA, it is not very long since the term began to be used in Sweden.

MSB-2 argue that the industrial market is more separated per sector, and that industrial control systems have existed for a longer period of time. Due to the terminology of OT does not originate from Sweden, the concept may recently take it's footing in Sweden, this to make distinctions and to imply less of a division between software and hardware. Meaning that the "OT-world" is less likely to be included in the realm of IT and vice versa.

### *7.1.2. Analysis Question 2*

The next question asked was: What are they, and how do they work?

During the interview, the meaning of the term OT became less cohesive as a distinctive system, rather than that it can be associated with components of control systems, such as all mechanical and relay-based components that manage logical operations. While these components may reside in very old systems, such as in the nuclear, water, and heating industries. This delimitation points to the fact that components without IT (Meaning that these systems per default do not make use of an IP-address) may reside outside the ICS realm. Though as the interviewees state; these components can be connected to some kind of digital converters, this to detect and report positions of the regulators, in the form of a signal. That signal can then be connected to a PLC and displayed on a screen. Implying that it is less likely that "OT-systems" today are stand-alone systems, rather, these are a part of ICS in the form of different layers.

To put the layers mentioned in a perspective, both the participants from MSB and FOI referred to the Purdue model (see figure 6-1) as a way to differentiate the components of a typical control system. In this example, layer 0 could represent these relay-based and mechanical components discussed earlier. layer 1 contains sensors, motors, eyes, ears, and hands in the system which listens and controls what happens. Layer 2 has direct control and automation to make sure that things go as planned, a PLC would probably reside in this layer. Then we have layer 3 which would probably contain a SCADA server. FOI-1 emphasizes it is in layer 3 that there would be people analyzing and monitoring the industrial environment, making optimizations of the production and that everything from layer 0-3 can be defined as systems in the OT-realm.

Furthermore, FOI-1 emphasizes that systems and components in the OT-realm are built to have a longer life span than typical IT systems. A typical OT system may have an operational lifetime of 20-40 years, some times longer than that.

### *7.1.3. Analysis Question 3*

In the next question, the participants of the interview answered the following question: Would you say that the OT-systems in general (such as ICS, SCADA, et al) are well known and reputable?

FOI-1 implies that ICS and SCADA are somewhat well-known concepts. All the participants mutually emphasize that the terminology of OT-systems (i.e. SCADA, ICS, et al.) is often used incorrectly. The participants from MSB share occasions where they themselves experienced that of the term SCADA has been used incorrectly, by e.g. people from the outside who work as IT-security consultants and pentesters. thus, that people who work with these systems know the correct terminology. This indicates

that the term SCADA for example, is being used as merely a subset of what's become a synonym for a whole area for outsiders who do not work with these systems.

## 7.2. Subsidiary Topic

This is an extension of this topic, aiming to broaden the discussion and mention relevant parts of the OT-realm which can be vital for society.

### *7.2.1. Analysis Question 4*

The respondents answered the following question: Approximately, how many OT-systems (e.g. Relay based and/or mechanical) of your knowledge are in operation in Sweden currently?

All participants imply that if the components, such as sensors in an OT-system is relay-based or purely mechanical, i.e. Without any connection to the Internet. And these at some point go through a digital converter that sends the signal to a PLC, then we're are talking millions of OT systems in Sweden.

This question was aiming to get a brief overview of the number of possible components of the OT-realm; thus, all the participants imply that in most cases these components are connected to a PLC. The reasoning behind this is due to the technical development, the line between layers of the control systems which uses these relay-based and mechanical components is starting to experience erosion. Sensors nowadays may be directly connected to the internet.

### *7.2.2. Analysis Question 5*

The respondents answered the following question: What do they do in society (due to delimitation, single down the question to a specific system and/or aspect that may be vital in society)?

All the participants highlighted that the electricity supply i.e. electricity grids are one of the most important instances for society, society would probably not suffice without it. MSB-2 mentions the term "Spindeln i nätet" i.e. Spider in the web represents; production, distribution and transmission. If we would lose the transmission part of things, then the whole country would be affected.

The participants note that these electrical supply instances aka Spider in the web is a big topic in regards to their occupation and if the transmission of the electricity supply fails, the consequences can be vital and affect the whole country. Furthermore, FOI-1 emphasizes that the water supply i.e. access to purified water, is also very important to society, thus, the loss of a single facility would probably not affect the whole country.

### *7.2.3. Analysis Question 6*

The respondents answered the following question: What protection is there for them (e.g. aging/degeneration)?

All the participants state that old systems which require components that are no longer manufactured, usually experience continuous stages of gradual upgrades. This to keep up with technological developments. Another solution would be to buy large quantities of critical components and spare parts used in these systems.

FOI-1 mentions a solution where the systems that cannot update due to e.g. age, are segmented and put behind firewalls in means of isolating these systems. Segmentation is the main approach in means of securing old systems. This to lessen the risk of exposing them outwards on the internet.

Another aspect brought up by the participants from MSB is the risk of limited knowledge in how to operate old systems. This implies that systems that don't undergo upgrades may be difficult to manage due to the lack of people that know how these systems work, and that there's probably no current education in how to manage very old systems.

FOI-1 mentions the increase of ransomware, and it's important to have in consideration that due to technological development, almost everything in the OT-realm can be considered as a computer and can be affected by these types of malware. Implying that it's just as important to apply the same security aspects and policies to the OT-realm as in the IT-realm.

Furthermore, FOI-1 mentions an approach to consider in means of protection of systems in the OT-realm; Have a thorough knowledge of the inventory of all systems, components and units, perform a risk analysis of the whole inventory and educate personnel, follow guidelines and perform continuous risk analysis.

### *7.2.4. Analysis Question 7*

The respondents answered the following question: What is currently researched in this area (Important systems vital for society)?

The participants from MSB mention that the supply chain is something that's currently a big subject in means of their occupation, and has appeared in recent studies. These studies aim to research the importance of how the personnel working within the supply chain needs to have the right prerequisites and knowledge.

FOI-1 emphasizes that FOI as a government agency has no operational responsibility, but rather that FOI acts and researches on behalf of other government agencies, such as e.g. MSB. Thus, mentions that FOI has for the last ten years held courses, in the security aspect of OT, which involves security courses

regarding ransomware. FOI-1 also points out that there are fewer courses regarding OT security, in comparison with courses regarding IT security.

This question i.e. 7, wasn't necessarily important in means of answering the research questions, but rather a means of broadening the topic. The topic itself is very interesting and gave insight into what MSB and FOI are currently working on and what's being researched.

# 8. Conclusion

The purpose of this study was to try and define and differentiate the terminology of operative technology, OT for short. This by diving into literature explaining the subject and get a greater understanding of what OT is. The following step to try to answer the research question was an interview study. The interview study resulted in interviewing people who have many years of experience working in the realm of OT. A brief summary of the result of this thesis would be:

- The definition and differentiation of OT may indicate a subset of systems and components, rather than a separate system.
- There are very old systems using these components, still in operation to this day which is vital for society
- Terminologies of OT-systems are misused, indicating a lack of knowledge in this realm
- There are millions of systems in Sweden that can be considered OT
- Upgrading old systems may be a proper way of protecting these systems against aging and degeneration. If upgrades are not an option, segmentation and isolation of these systems may be a proper solution of protection.

In regards to question 1 (Are there any OT-systems in Sweden that do not fit into the ICS-realm and other components, such as SCADA, PLC and others?): Terminology of OT may be applicable as a definition of a whole set of systems and components. The research question aims to establish a border in the OT-realm, meaning, if any separate systems can be considered purely OT. By analyzing the responses from the interviewees, it's clear that all of the participants unanimously agree that the OT-realm is a subset of systems and components. Thus, there are still very old systems in operation today that make use of components with characteristic features of OT e.g. relay-based. But for the most part, there's an interconnection between these systems to properly monitor and control them.

In regards to question 2 (Who are they, and how do they work?): The responses imply that there are still systems in operation today that make use of mechanical and relay-based components. Thus, these are somewhat connected to other instances in the ICS realm, e.g. PLCs. They exist in the nuclear, water, and electricity industries, and a lot of these systems are vital for society. Highlighting the importance of correctly managing and prioritize these potentially old systems.

Furthermore, in regards to question 3 (Would you say that the OT-systems in general (such as ICS, SCADA, et al) are well known and reputable?): all the participants of the interview mutually agree that terminology is often used incorrectly. The use of terminology sometimes differs depending on the type of industry. Furthermore, the term SCADA and ICS are more well-known concepts.

In regards to question 4 ((Approx.) How many OT-systems (e.g. Relay based and/or mechanical) of your knowledge are in operation in Sweden currently?): The interviewee's statements in this regard, suggests that there are millions of systems in Sweden to this day that is considered OT. Not all of these are critical to society. The question aimed to give the readers a brief understanding of how many of these systems exist.

In regards to question 5 (What do they do in society (due to delimitation, single down the question to a specific system and/or aspect that may be vital in society)?): This question aims to get an insight into the different OT related aspects in society, which the interviewees from different government agencies would consider crucial. The participants of the interviews all agree that the electricity supply is something that society is heavily dependent on. Some of these instances which produce electricity and heating may consist of very old systems. Another aspect mentioned by FOI-1 is the importance of clean drinking water. Thus, water treatment plants are found in most cities, and if one of these plants would cease to function, it wouldn't affect the whole country. On the other hand, if there would be an electricity transmission failure, it would affect the whole country, including water treatment plants. Highlighting that these systems are vital for society, and continuous risk analysis should be prioritized.

In regards to question 6 (What protection is there for them (e.g. aging/degeneration)?): This question aims to give insight into how to protect potential old OT systems. There are multiple things to consider according to the participants, e.g. if the systems in question are very old for instance; a possible security measure would be to continually upgrade these systems if possible, this to counter aging and degeneration. This also empathizes to make use of available updates and to buy replacement parts that are still being manufactured. If there were to be impossible to upgrade these systems, other measures have to be considered, such as segmentation, isolation, and proper documentation. As stated in the previous question, continuous risk analysis should be implemented and conducted regularly. Furthermore, systems that cannot be upgraded and that make use of rare components could keep an inventory of critical components.

Regarding question 7 (What is currently researched in this area (Important systems vital for society)?): This question is meant to give insight into current topics of what FOI and MSB as government agencies are currently researching. Targeting subjects that can be associated with the OT-realm, but other topics as well, mentioned by the participants. The participants from MSB mentions the supply chain, highlighting the importance of knowledge and prerequisites needed in this realm. Implying that education and proper management should be prioritized.

FOI as a government agency has no operational responsibility, but rather that FOI acts and researches on behalf of other government agencies. FOI-1 emphasizes that there's a lot of courses and education in regards to IT, but a noticeable lack of education that covers the OT side, which includes industrial

control systems for example. Thus, FOI-1 mentions that for the last ten years, FOI has held courses regarding this topic. Furthermore, for the last three years, there has been a lot of education and courses regarding ransomware, which affected a lot of productions. Ransomware doesn't care where or what kind of systems they infect, as long as there's a possibility to exploit systems. This implies that it's necessary to consider OT-systems as important as IT-systems.

The aim for this thesis was from the start a somewhat naïve attempt of simply find, and define OT as a specific system. This idea that OT may be a separate entity had to shift due to the insight gained from the interviewees. In regards to their expertise in the field, applying their perception and professional statements to this thesis. During the interview, the participants had the opportunity to talk freely which led to very interesting discussions, and these discussions gave an insight into what the OT-realm encompasses. The participants gave an insight into the importance and meaning of the different systems in the OT-realm and what they do in society in Sweden. There's a consensus regarding what the literature represents and what the participants described from their personal experience. This is clarified by the participants provided more elaborated examples of what a typical OT-system may consist of. Furthermore, the separation of the OT-realm has been more evident a long time ago, but that due to the technological development, the separation is getting less evident.

# 9. Discussion

This chapter includes a discussion regarding the choice of method, results, social and ethical aspects and future work.

## 9.1. Choice of Method

The choice of conducting an interview study was a suitable approach to answer the research questions for this thesis. In combination with literature that explains the subject and gives insight into the realm of industrial systems, the interview study added relevant information in order to complete the work. This by filling the gaps as the literature on its own couldn't answer the research questions.

This subject of OT itself is a very large area, and not something that's usually associated with the NSA-programme, which lean more into the realm of Information Technology. There was a shortage of similar reports from previous students who could inspired this subject in the form of future work.

The participants of the interview have a great amount of experience in the field and their contribution to this thesis was very useful in means of giving insight into the realm of OT and its systems.

## 9.2. Results

Due to the risk of insufficient information and participants willing to partake in an interview in regards of answering the research questions, the result wasn't evident. That resulted in more questions aiming to broader the subject. The participants of the interview were very open and gave many interesting discussions which also lead to answering all of the research questions.

The participants of the interview have a lot of experience in the realm of OT, i.e. Industrial systems such as ICS and PLCs. However, having more interviews with other instances would've been more insightful for this topic, both in regards of validity and reliability. The research question could probably be more specific and delimited if there would be numerous of participants, thus due to the lack of time and resources, the subject of this thesis was then broadened and included other interesting subjects.

## 9.3. Social Aspects

This work may open up the discussion of OT-systems and highlight their importance in society. As there has been a noticeable lack of information and wrongfully labeling e.g. SCADA systems being portrayed as a mere synonym for a whole area.

In society, we're dependent on heat, water and electricity, those things are a part of the necessities as human amenities, and e.g. hospitals and other instances need these to properly function.

Due to technological development, it can be without saying that older systems, which consist of non-IT related mechanical and/or all relay-based components are easily forgotten and overlooked. There are vital systems in operation to this day.

## 9.4. Ethical Aspects

The participants of this interview study were fully informed of the subject and goal of this thesis. The guidelines mentioned in section 4.2.2 was implemented, which narrates that the interview was conducted in the following manner:

- The interview session was recorded
- The participants have the option of being anonymous.
- The material is stored locally and not distributed in any shape or form.
- The material gathered from the interview session will only be used in means of this thesis, and as the work is concluded, the material will then be deleted.

The structure of this thesis aims to give insight in the realm of industrial systems, with the delimitation of what can be considered OT. The systems mentioned, including a brief explanation of how they work, do not instill sufficient information which can lead to exploitation or misuse of these systems.

## 9.5. Future Work

As the study mentions systems that use IT to properly function, such as ICSs and PLCs. There is increasing use of IoT systems that don't employ classical ICS environments or use PLCs. An example of that would be an e.g. Fitbit, smartwatches, etc. Considering such an application in terms of an ICS is useful. The Fitbit device for example has inbuilt functionality to collect the information from the sensors (e.g. pulse, accelerometer, etc.) and display the results on the screen as well as transmit them to a smartphone app. Considering the Fitbit device as the controller and the smartphone as the SCADA device is useful because it gets us to answer questions regarding the device identifier i.e. ensuring the right device is being monitored and the security of the communications between the device and smartphone application.

Another example is vehicle automation. The sensors and actuators in a car communicate with various controllers that are making autonomous decisions. Considering the security around this communication is important. The Vehicle-to-everything (V2X) comms should also be treated as part of and ICS ensuring identification of devices and appropriate encryption is put in place.

So, by employing the design severity of an ICS to any OT application may be an interesting topic to research on.

Furthermore, a continuation of this research would include interviews with more instances, such as; NIST, FRA, et al. Questions asked to the participants would be similar to the ones used in this thesis.

# References


Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B., 2008. *Thesis Projects A Guide for Students in Computer Science and Information Systems,* London: Springer.

Cook, A. et al., 2016. Attribution of Cyber Attacks on Industrial Control Systems. *EAI Transactions on Industrial Networks and Intelligent Systems,* Volume 3, pp. 1-15.

FOI, n.d. *Totalförsvarets forskningsinstitut.* [Online]
Available at: https://www.foi.se/
[Accessed 08 05 2020].

Galloway, B. & P. Hancke, G., 2013. *Introduction to Industrial Control Networks,* s.l.: IEEE Communications Surveys & Tutorials.

Hahn, A., 2016. *Cyber-security of SCADA and Other Industrial Control Systems Chapter 4.* Fairfax, VA, USA: Springer International Publishing Switzerland 2016.

Hasselbring, W., 1999. Technical opinion: On defining computer science terminology. In: Tilburg: ACM, pp. 42(2), 88-91.

Hedin, A., 1996. *En liten lathund om kvalitativ metod med tonvikt på intervju.* [Online]
Available at: https://studentportalen.uu.se/uusp-filearea-tool/download.action?nodeId=459535&toolAttachmentId=108197
[Accessed 07 05 2020].

Hedtjärn, S. V., Malmberg, A. F. & Clausen, M. J., 2016. *NCS3 – Gammalt är inte äldst,* Stockholm: FOI.

Häger, B., 2007. *Intervjuteknik.* Stockholm: Liber.

Ingemarsdotter, J., Eidenskog, D. & Hedtjärn, S. V., 2020. *Vilse i lasagnen? En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur,* Stockholm: FOI.

Kitchenham, B. & Charters, S., 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering,* Durham: Kitchenham.

MSB, 2014. *Vägledning till ökad säkerhet i industriella informationsoch styrsystem,* Stockholm: MSB.

MSB, n.d. *Myndigheten för sammhällsskydd och beredskap.* [Online]
Available at: https://www.msb.se/
[Accessed 08 05 2020].

Sarkar, S., Agrawal, A., Teo, Y. M. & Chang, E.-C., 2018. *VOTNET: HYBRID SIMULATION OF VIRTUAL OPERATIONAL TECHNOLOGY NETWORK.* Gothenburg, Sweden, IEEE Press, p. 1170.

Spacey, J., 2017. *8 Examples of Operational Technology.* [Online]
Available at: https://simplicable.com/new/operational-technology

Stouffer, K. et al., 2011. *Guide to Industrial Control Systems (ICS) Security,* Gaithersburg: NIST special publication, 800(82), 16-16.

Sullivan, D., Luiijf, E. & Colbert, E. J., 2016. *Cyber-security of SCADA and Other Industrial Control Systems Chapter 2.* Switzerland: Springer International Publishing Switzerland 2016.

Wikipedia, n.d. *Vehicle-to-everything.* [Online]
Available at: https://en.wikipedia.org/wiki/Vehicle-to-everything
[Accessed 31 05 2020].

Williamson, G., 2015. *Industrial Control Systems: Getting a Grip on OT Cyber Security,* Wiesbaden: Kuppinger Cole Ltd.

Williamson, G., 2015. *OT, ICS, SCADA – What's the difference?.* [Online]
Available at: https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

# Appendix A – Interview Guide

## Introduction

The subject and reasoning of the thesis are explained to the people being interviewed including a short introduction of myself. The interview is recorded and will be deleted as the study is concluded.

## Brief description of the participant(s) being interviewed

Questions such as;

- Briefly describe your occupation
- Describe your role | institution
- What is your role in the business? How long?

As the interview starts, ask for ambiguity and to speak clearly.

## Get an insight into the current and operational OT-systems in Sweden.

Questions asked to participants:

**Main Topic**:

**2.** Are there any OT-systems in Sweden that do not fit into the ICS-realm and other components, such as SCADA, PLC and others?

**3.** Who are they, and how do they work?

**4.** Would you say that the OT-systems in general (such as ICS, SCADA, et al) are well known and reputable?

**Subsidiary Topic**

**5.** (Approx.) How many OT-systems (e.g. Relay based and/or mechanical) of your knowledge are in operation in Sweden currently What research is done on them?

**6.** What do they do in society (due to delimitation, single down the question to a specific system and/or aspect that may be vital in society)?

**7.** What protection is there for them (e.g. aging/degeneration)?

**8.** What is currently researched in this area (Important systems vital for society)?

At the end of the session, the interviewees are encouraged to talk freely, and if they feel like adding something to the topic.

# Appendix B – The Interviewees

**Brief description of the participant(s) being interviewed from MSB:**

Interview MSB - 2020-05-15
Finalized 2020-05-19

**MSB-1 -** Officer at MSB (2020):

- Working for MSB for 1 ½ years
- Has worked with industrial IT (Information systems i.e. ICS) in the energy sector for approx. 15-16 years before started working for MSB.

**MSB-2 -** IT security specialist at MSB (2020):

- IT security specialist working with ICSs for approx. 2 years
- Has worked with ICS in means of programming PLCs before started working for MSB.

**MSB-3 -** Executive Officer at MSB (2020):

- Working for MSB since 2013
- Current role as a bureaucrat, which includes being a specialist in his field and other aspects, such as; administer course activities, track investigations and studies et al.
- Over 20 years of experience in the defense and security industry, mainly in development and research, including border control and protection of critical infrastructure.

**Brief description of the participant(s) being interviewed from FOI:**

Interview FOI - 2020-06-04
Finalized – 2020-06-08

**FOI-1** - Researcher in information security:

- Working for FOI since 2001, i.e. 19 years.
- Involved in several research projects, studying authentication, authorization, access control, and secure information sharing between countries in a coalition.
- For the past five years, FOI-1 has mainly worked with security issues within critical infrastructure, for instance, electricity, purified water distribution, and large-scale supervision. This work is a program funded by MSB and contains several projects. Within the program, FOI conducts studies, gives courses and exercises.

# Appendix C – Main Topic

The Main Topic is the primary focus of this thesis, intending to answer the question; do these systems exist at all?

**9. Are there any OT-systems in Sweden that do not fit into the ICS-realm and other components, such as SCADA, PLC and others?**

**MSB-2**:

- Implies that there is not a clear depiction between SCADA, ICS and automation, if it exists at all.
- MSB-2 interprets OT as more of a concept that covers all the aspects of control systems. That includes SCADA, PLCs, et al.
- IT is also a concept that covers hardware and software, including cables, therefore the same interpretation would apply for the term OT, meaning that OT includes:
    - PLCs
    - SCADA software
    - Hardware components
    - RTUs et al.
- MSB-2 mentions that the origin of the terminology of OT comes from the USA. The term OT got it's footing in Sweden later and may originated due to the evolution of IT security in control systems i.e. how they are connected to the Internet/IT.
- IT is more of a globalized term, meaning that a lot of things (e.g. software, hardware et al.) are considered as IT, regardless of where in the world it can may be located.
- The ICS market has existed longer, and is separated per sector, meaning for example; water purification plants, Heating facilities et a. While these different sectors use their own hardware and software brands.

**MSB-1**:

- When thinking about IT and OT, those concepts may exist to make distinctions, meaning that the "OT-world" does not want to be included in the IT and vice versa.
- Perhaps the term OT implies less of a division between software and hardware. There can also be organizational and cultural aspects in means of usages of the term OT.

**FOI-1:**

- Does not fully agree with a separation of OT, as seen in the figure (see figure 1-6). Thus, implying that there are systems that partially reside outside the ICS realm. Such as old relay-based systems,

which do not have any data monitoring, there may be a few of these still in operation today. The PLC was introduced for approx. 50 years ago, which replaced the old relay components in means

**10. What are they, and how do they work?**

**MSB-2**:

- There are very old systems still in operation today that's all relay-based, such as the cogeneration power plant (CHP) in Stockholm called Värtanverket, which uses coal-fired boilers such as KVV1. It is all relay-based with thousands of relays that handles all logical operations and has no association with IT at all. This supplies heating for a large part of Stockholm.

- Other examples of systems which do not make use of IT (Meaning that these systems per default do not make use of an IP-address):
    - In the nuclear industry, there's a lot of relay-based systems.
    - Water industries with regulators which is purely mechanical and hydraulic.

  However, there can be some kind of digital converters for these systems, this due to power conversion and to detect and report positions of the regulators, in the form of a signal. That signal can then be connected to a PLC and displayed on a screen. Turbines are another example of systems that can disconnect from control systems as a safety function. If the system for example encounters over excess pressure, then it makes use of autonomous functions which is purely mechanical.

**MSB-1**:

- It doesn't get more OT than that.

**MSB-2**:

- Mentions the Purdue model which states that the different components in ICS belong to different layers, for example; Sensors belong to layer 0 while a PLC belongs to layer 1 and so on. Due to the technical development, the line between these layers is starting to experience erosion, as an example; sensors nowadays may be directly connected to the internet, and old systems that make use of hydraulics can be directly connected to an AD converter to obtain a digital signal.
- This Purdue model in means of tiering may be something useful for me as a researcher and can be applied to my research in means of defining terminologies.

**FOI-1:**

- Mentions the Purdue model (see figure 6-1), you could say that layer 0 is the industrial process, layer 1 contains sensors, motors, eyes, ears, and hands in the system which listens and controls what happens. Layer 2 has direct control and automation to make sure that things go as planned, a PLC would probably reside in this layer. An example of layer 2 could be that the PLC listens to a sensor and control an engine, which in turn controls a pump. Then we have layer 3 which would probably contain a SCADA server. It is in layer 3 that there would be people analyzing and monitoring the industrial environment, making optimizations of the production. Everything from layer 0-3 can be defined as OT, it symbolizes production.
- Implies that there are probably still old relay-based systems currently in operation today in Sweden, have no personal experience working with these potential systems, but have heard about them. Something that's often associated with OT systems. OT supervises and controls systems, which have a long operational lifetime. The production system may have an operational lifetime of 20-40 years, some times longer than that. During that lifetime, some of the OT-components will be exchanged, but it is common with a long lifespan, especially compared to traditional office IT.
- OT systems are built to have a long life span, meaning that a system should be able to properly function for a long time without shutting them down in order to repair them. In comparison with typical IT systems, which have an estimated life span for approx. 2-3 years and can switch out e.g. cables, RAM among others and is easy to shut down, repair and restart again.

**11. Would you say that the OT-systems in general (such as ICS, SCADA, et al) are well known and reputable?**

**MSB-3**:

- When I'm presenting the topic, I usually say that SCADA is merely a subset of what's become a synonym for a whole area. As for an example; the American vacuum cleaner manufacturers called Hover dominated the electric vacuum cleaner industry, to the point where the Hoover brand name became synonymous with vacuum cleaners and vacuuming overall.

**MSB-1**:

- Agrees with MSB-3 that SCADA has become a synonym with a lot of different things.

**MSB-2**:

- Due to my role in means of security in the operative area, has led to encounters with people from the outside who works as IT-security consultants and pentesters. These people dive into the

operative area with the sense of SCADA as a synonym, as mentioned earlier, even though the subject in question can be a PLC, as an example.

- MSB-2 reckons that due to the increased attention of the subject in media, there's a lot of confusion in that regard.

**MSB-1**:

- States that he feels the same way and agrees fully with MSB-2's statement.

**FOI-1:**

- There's a lot of terms and concepts floating around, and they are depending on which industry you are talking about, but technically you are still talking about the same thing.
- FOI- 1 implies that SCADA is something specific, but the term is generally used incorrectly. ICS and SCADA are somewhat well-known concepts. People who work with these systems, know the correct terminology for these systems and components.
- ICS is an overall term that includes i.e. SCADA and distributed control systems (DCS) and defined as stand-alone systems. Whereas PLC is a component that can be used in these stand-alone systems.
- Mentions that some time ago, there was a clear separation between these systems, i.e. SCADA and DCS for example, but nowadays it has grown closer together.

# Appendix D – Subsidiary Topic

Subsidiary Topic is an extension of the matter, this can result in a broader discussion and aspire for future work based on this thesis.

**12. Approximately, how many OT-systems (e.g. Relay based and/or mechanical) of your knowledge are in operation in Sweden currently?**

**MSB-2**:

- If the question suggests components that are relay-based or purely mechanical, e.g. Without any connection to the Internet, and they go through a digital converter that sends the signal to a PLC? Then we are talking about millions of OT systems.

**MSB-1**:

- It may be a good idea to delineate the question, as MSB-2 is implying.
- Regulators, for example, that does not classify as a classic ICS or SCADA system, in most cases, these are somehow connected to a PLC.

**MSB-2**:

- Let's imagine a component that does not have any IT connection whatsoever, such as houses and residential properties, there's a thing called ventilation ducks. These ducks control heating, ventilation and such. Then the question is, how many houses are there in Sweden?
- Another example would be the motorway tunnel called Southern Link (Södra länken) in Stockholm. That tunnel contains approx. 30 thousand measurement components that measure temperature and such, and they respectively send out a 20-volt signal to a PLC which in turn converts and gives it an IP-address and sends it to a SCADA system.

**FOI-1:**

- Anything that blinks, moves, etc. in society, can be considered as OT systems, which implies that there's a lot. Not everyone is critical of society.

**13. What do they do in society (due to delimitation, single down the question to a specific system and/or aspect that may be vital in society)?**

**MSB-2**:

- Mentions that there are multiple factors in regard of answering this question, would these systems affect society locally or throughout the country?
- "Spindeln i nätet" i.e. Spider in the web, which is electricity supply i.e. electricity grids, then we're talking production, distribution and transmission. If we would lose the transmission part of things, then the whole country would be affected.
- There have been instances where transmission of the electricity supply malfunctioned and resulted in large power outages. There's an electrical interconnection between Sweden and Denmark and because of this transmission shortcoming, there was a reconsideration as of cutting the electricity supply to Denmark completely.
- If the transmission of the electricity supply fails, the consequences can be vital. Some aspects may stop working immediately, and some may have reserve resources, such as hospitals and such, but it's just a matter of time before the reserve resources are exhausted.

**MSB-1**:

- The electrical supply is the "Spider in the web" and this is a big topic in our discussions in regards to our occupation.

**MSB-2**:

- The electricity supply is very important for society and a lot if not all instances would probably not suffice without it. E.g. If the heating plant would stop working during a time period around June, if the temperature lies around 30 degrees Celsius, there wouldn't be a major problem. However, would that same scenario apply in January with -25 degrees Celsius it would be a very critical problem for society, people wouldn't be able to heat their homes for example.

**FOI-1:**

- FOI-1 mentions that FOI as a government agency has no operational responsibility, but rather that FOI acts and researches on behalf of other government agencies, such as MSB. But FOI-1 emphasizes that electricity is the basis of everything, there are not many things that would function and our modern civilization ceases to function without electricity. FOI-1 also mentions the importance of computers, without these, it would be very hard to monitor, control and produce electricity. The production of electricity is in symbiosis with computers.
- FOI-1 mentions that electricity production is not something that secluded in Sweden, rather than it's connected to a European network. Meaning that there are multiple electricity production companies here in Sweden, thus that they are probably connected to foreign countries and do not

work entirely alone. Would Germany for example require more electricity, then Sweden would be able to assist in that matter.

- FOI-1 also mentions that the water supply is also very important to society. Access to purified water is critical for people. Water treatment facilities and distribution are often local; Thus, the loss of a single facility would probably not affect the whole country. If the loss occurs in a heavily populated area, however, lots of people will be affected by this. Supplying water to a village or a city without using the regular distribution system is a difficult task.

**14. What protection is there for them (e.g. aging/degeneration)?**

**MSB-2**:

- Old systems are continually upgraded to counter aging.
- In regards of old systems that require components, that's no longer manufactured, either there are continuous stages of upgrading of these systems, this to keep up with technological developments, or the old components and spare parts are bought in large quantities and stored somewhere.
- MSB-2 mentions a recollection of a very old gas turbine, located in the southern part of Stockholm, that's currently not in use anymore. This gas turbine was used to operate the subway and there were only approx. two people in the entire world who knew how it worked. These people didn't live in Sweden, meaning that to operate this turbine it was necessary to fly these people to Sweden from far, far away.

**FOI-1:**

- Mentions that on the IT side of things, it's very common to update the systems in means of security, thus in the OT realm containing these old systems, that's not always possible to do. Either you can't update these systems due to that there are no updates available anymore, or you're not allowed to due to the risk of failure and stopping production.
- Says that IT represents Information and you want to protect it against information loss, if there were any problem with the IT, you could probably shut it down, fix the problem and restart, as long that there's no information loss it's not a problem. If you're looking at OT and what's the most vital part in that realm, it would reside in the means of availability, these systems need to function continuously. If these OT systems stop, the production will come to a halt and can cost millions in losses. A short summary would be: OT is about availability; IT is about information and perhaps confidentiality.

- Some systems that cannot update due to e.g. age, are segmented and put behind firewalls in means of isolating these systems. Segmentation is the main approach in means of securing old systems. This to lessen the risk of exposing them outwards on the internet.
- In the aspect of antivirus and such, the antivirus may work in some cases. Would a control system get infected with some kind of virus that does not interfere with production, it is in most cases ignored and considered as not important.
- Mentions the increase of ransomware being used nowadays, implying that it is very important to educate people who are responsible for production technology, and to realize that almost everything in the OT-realm can be considered as a computer. Such as a PLC or the monitors on the train tracks that display arriving trains, those are basically a computer. Ransomware doesn't care what or where they end up, as long as there's a possibility to exploit these systems.
- Mentions a list of 3 things to be aware of:
    1. Have a thorough knowledge of the inventory of all systems, components and units you have
    2. When you know that, perform a risk analysis of the whole inventory; what can be exploited? Which of these things should be able to talk to each other? If they shouldn't be able to talk to other systems, separate and segment them, can these be updated?
    3. Educate personnel, follow guidelines and continuous risk analysis needs to be done. FOI-1 also refers to the life-cycle model.
- When it comes to secure older systems, meaning those that are in the risk of e.g. aging/degeneration, which may make use of old components that are not being manufactured anymore, FOI-1 emphasizes to keep an inventory of critical components.

**15. What is currently researched in this area (Important systems vital for society)?**

**MSB-1**:

- The first thing that comes to mind is the importance of the educational aspects in the supply chains. Meaning that the need for knowledgeable personnel who should have the right prerequisites to be able to manage these systems used. This subject is something that has been researched and appeared in recent studies.

**FOI-1:**

- As mentioned earlier, FOI as a government agency has no operational responsibility, but rather that FOI acts and researches on behalf of other government agencies.
- FOI-1 emphasizes that there's a lot of courses and education in regards to IT, but a noticeable lack of education that covers the OT side. FOI-1 mentions that FOI has for the last ten years held

courses, in the security aspect of OT, which is connected to one of their first courses that were held around 2009. At the same time as this course started, Stuxnet became known, which was a waking call for people in the process control realm.

- For the last three years, there has been a lot of education and courses regarding ransomware, which affected a lot of productions.