UNIVERSITY OF TWENTE.

KPMG

Business Information Technology

Dennis Waalewijn

Supervisors:
Prof. Dr. K. Sikkel
Prof. M. Junger
Dr. D. Hadžiosmanović
Ir. M.B. Paques CISSP CISA
J. Hogenboom MSc.

Cyber Security in the Supply Chain of Industrial Devices

December 9, 2014

Preface

The master thesis that is lying in front of you is the result of a 10 months research at KPMG, Information Protection Services to graduate from the University of Twente.

The writing of the report has gone through ups and downs. Especially in the beginning I experienced some troubles finding a research topic and defining a suitable research question. I was not familiar with the related topics therefore this period took quite some time. After numerous meetings with KPMG supervisors, a client's problem was introduced that got my attention. It was important for me to carry out a research that really interests me. Performing something for a client at KPMG would definitely get my interest as it serves a better cause than just a scientific one. Next to that, I wanted to specify a research question on which I am curious to find an answer. In my opinion, I succeeded in this. My first word of thanks goes to Dina Hadžiosmanović for helping me defining my research question. Additionally I would like to thank her for helping me finding the research direction as a whole and supporting me throughout the research with her scientific knowledge.

What was really unfortunate is that the client of KPMG eventually did not have the time and energy to help me with this research after all. After 4 months of working in literature to create the research this was really a great setback for me. The purpose of the research disappeared and it felt I lost a lot of work. After multiple meetings with University supervisors and KPMG supervisors, everyone did their best to find new sources to gather information from for this research. Eventually through my own and KPMG's network I have accomplished to gather three sources over the course of three months. Without the support and knowledge of Jip Hogenboom and Matthieu Paques I would have never been able to achieve this, therefore my second word of thanks goes to them for helping me find sources for the research and supporting me with a lot of knowledge on the topic. Also, I would like to thank Marianne Junger, my second examiner to provide a lot of insights from different angles to continue the research.

Furthermore, I would like to give a special thanks to my dad René Waalewijn and a close friend Eelco van Ruiten who referred me to the right persons to interviews. Without them I would have never gotten the information sources.

This period of finding new information sources was a really tough period for me because I had lost the purpose to finish the research. After conducting a few interviews however, my first examiner Klaas Sikkel never lost trust in this research and he often shared that opinion during the meetings. My last but certainly not the least word of thanks therefore goes out to him for supporting me mentally during this research. During the whole process, he was always there for me to support me.

Management summary

Cyber Security in the Supply Chain of Industrial Devices is vital to security of industries, countries and even the world, because when the energy, oil & gas, dairy, water management, beer and many more sectors are compromised in the supply chain a disaster that is not easy to prevent could be happening. It is important to secure the supply chain from cyber threats because this is an attack path that is hard to detect and very different from contemporary network-based attacks. An industrial device might be tampered with during shipment and after installation perform malicious actions in an industrial process. Such attacks are not uncommon at mobile embedded devices, therefore it is also likely industrial embedded devices are targeted too. However, because of the complex chain there is currently too little knowledge where in the supply chain may lie the possible threats. This knowledge is needed to be able to implement countermeasures where necessary in order to reduce the likelihood of attacks happening and to reduce the impact of an attack. A device lifecycle for industrial devices is used to create an overview of the stakeholders that are involved before the device is operational. The actors that perform actions in the lifecycle are identified. The relations between the actors make up the overview of the global supply chain of the above mentioned industrial devices. The supply chain is a complex globally dispersed web of many stakeholders. These stakeholders interact with the device which makes security in the supply chain of industrial devices an important aspect in the security of Industrial Control Sytems.

The goal of this research is to identify the threats that could be occurring in the supply chain. Ultimately to derive the current threat landscape of the supply chain that actors who operate in the supply chain need to become aware of. They can use this knowledge to improve their supply chain processes in order to increase the supply chain security and sustainability.

A 'threat model' is derived from a literature study and reported incidents on PLCs/PACs. How these incidents could be translated in the supply chain is then determined by modelling attack trees. The threats have been looked at from an threat actors' point of view and show what a threat actor could achieve by interfering with the supply chain of industrial embedded devices. Next to that, a taxonomy of threat actors is used in order to show who would be able to perform such threat. The result is 35 theoretical threat scenarios that could be occurring in the supply chain of industrial devices. The threat scenario's are categorised generically as hardware counterfeiting, firmware/software tampering, intellectual property theft and the installation of backdoors. The threat model is then tested in reality by interview sessions with three different stakeholders of the supply chain, an OEM, a Systems Integrator and an Asset Owner. The interview consisted of four groups of questions; general production process; supply chain related; incident report; controls and measures in place.

The OEM mainly performs plant security and does not take supply chain threats into account. Supplier selection criteria do not cover measures that can be met by third parties,

integrators and distributors to secure the supply chain. The people that are involved are trained and checked on knowledge of the products but it is unclear if they are checked any further. This leaves many opportunities during shipment for firmware/software tampering for OEM, especially with many collaborations with distributors all over the world. From the system integrator's point of view, the production process consists of creating software on top of the PLCs/PACs and providing a plant solution. Critical parts of the software is encrypted. However, a lot of parts regarding software and hardware are insourced that can be tampered with if no measures are taken. The interviewed system integrator totally handles transport by itself and does not collaborate with distributors at all, this gives a certain layer of security for their deliveries. The Asset Owner's perspective shows that they are only able to collaborate with a few suppliers, and where possible only one at the time for building a new factory. This is good because that leaves less room for tampering. Controls the Asset Owner has in place is secure environment for installation and maintenance, however sometimes third parties do the installation and updating.

Following from these interviews and the literary research, this thesis gives insight into the state of the supply chain and threats that the devices in the supply chain face. This knowledge could be used to offer KPMG's clients in the industrial sectors a new service. A new service to be involved in the process of either designing, acquiring or installing a new Industrial Control System with regards to:

- Critical success factors in supply chain security
- Maturity modelling for actors in the supply chain

Furthermore, the thesis is structured as follows: First, a literature research has been done and the relevant theories that support the rest of the thesis are described in this part. The second part of the thesis contains the the detailed threat analysis with the creation the threat model. Then, an analysis of the supply chain has been performed with a comparison with ICT supply chain as a preparation of the interviews. Followed by the part that contains the results of the interviews that have been performed at three stakeholders of supply chain. Finally, conclusions and recommendations that consist of the above mentioned extra knowledge

Contents

List of Figures

List of Tables

List of Acronyms

CIA	Confidentiality, Integrity, Availability
COTS	Commercial Off The Shelf
DCS	Distributed Control Systems
FAT	Factory Acceptance Test
FTP	File Transfer Protocol
ICS	Industrial Control Systems
MTU	Master Terminal Unit
OEM	Original Equipment Manufacturer
PAC	Process Automation Control
PCS	Process Control Systems
PLC	Programmable Logic Controllers
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
TCO	Total Costs of Ownership

Chapter 1

Introduction

The goal of this chapter is to introduce the thesis topic and the reason why this study will contribute to involved stakeholders.

1.1 Motivation

Recently, a company published a report about their corporate smart phones running Android OS were infected with a pre-installed malware (Webwereld, 2014). Analysis later revealed that this malware infection was widespread and that the malware sent credit card information to a server located in Russia. How could this happen? The manufacturer loaded the genuine firmware on the phone and the company thought it was buying genuine phones for its employees. Further investigation showed that the firmware was modified in the supply chain before it was actually shipped to the company. This incident highlights that many actors of different countries are involved in the global supply chain and shows the need to analyse the full chain in order to be able to implement adequate security measures to prevent such attack.

The reason why such malware in Industrial Control Systems (ICS) is unlikely to be seen in an industrial process is because no employee needs to use a creditcard. However, when an industrial process is disrupted by malware this could potentially have disastrous consequences. These consequences arise because many of the ICS are used in critical infrastructures of a country. Although not for creditcard phishing, but for other purposes ICS can be targeted with malwares in the supply chain. Reports by the pentagon state they are planning to spend an additional 500 Billion USD on security of supply chain of devices and systems that are used in critical infrastructures (Department of Defense, 2013).

Since the discovery and detection of ever more sophisticated attacks on ICS like Stuxnet, these systems are vulnerable and becoming an attractive target for hackers, cyber criminals. It is even suggested (given the size and complexity of Stuxnet) governments target ICS for cyber warfare (Zhu, Joseph, & Sastry, 2011). The embedded industrial devices of an ICS are the main target for such attacks because they are at the heart of a physical process. An attacker could possibly interfere with the supply chain of these devices to cause potential harm. Several possibilities could be installing backdoors, own root certificates of the firmware or installing malware. The actors are dependent on each other in the supply chain and therefore need to be aware of these threats in their processes to be able to take adequate actions against it.

1.2 Background

Back in 2000 the first cyber incident on an industrial control system was reported on an Australian waste water plant. A former employee of the waste water plant who was fired remembered the login code to access the water flow control and used it to release over one million liter of water on the streets. There are two interesting aspects to this story that hold true for many ICS. What is the reason that a control interface is connected to The Internet and why hasn't the login code changed. R. Turk reports to the US department of Homeland Security that in the years following the waste water incident that many more incidents where reported. Their reports are summarised in (Turk, 2005) and their estimates show that at least a ten fold of incidents actually happened but haven't been reported because of lack of good analysis. The move to more open protocols, interoperability and connectivity has the effect that hackers can take advantage of the industrial sectors more easily than companies are aware of. The result is that ICS has gained a lot of attention by both the people who try to protect it and also the people who try to interfere with it. As R. Turk reports in the year 2005, at least 42% of the reported incidents are from malware infection. The developments of malware infection attacks on ICS that have been reported to this day have seen a steep increase in sophistication and specialisation since the waste water incident. Stuxnet is the product and proof of such developments.

Water supply, energy and petrochemical sectors are amongst many utility's of ICS, which are most often critical for a country. Disruption of one or multiple of those sectors could potentially disable a full country in functioning properly and could cause public chaos. After the vulnerability of many ICS came to light this immediately became a high priority for national governments who wanted to improve security of their critical infrastructures. Also to support industrial companies to ward against potential harmful attacks. In the United States the National Institute of Standards and Technology(NIST) in conjunction with North American Electric Reliability Corporation(NERC) have made a lot of effort to create frameworks, standards and directives to secure their infra and the industrial sectors in general. In their special publication, a framework for assessing potential risks and mitigation strategies is presented as a guideline for the industrial sector and especially for the critical infrastructures of the US (NIST, 2013a). The EU has made directives for each of her member states to be followed as guideline's towards ICS security as well. The International Society of Automation in conjunction with International Electrotechnical Commission has created European standards that supports end-users, manufacturers and other actors in securing their industrial device and their environment. Domestic developments consist of the creation of a Cyber Emergency Response Team (CERT) and generally raising awareness of cyber security in both IT and ICS. CERT is an effort to obtain knowledge and to learn how to act against new incidents by collecting and maintaining a database of reported incidents and providing a central emergency unit to report incidents (ENISA, n.d.). Together these efforts need to ensure more security in the industrial sectors by supplying industry specific standards for communication and support. These standards are also benefiting manufacturers and integrators of the systems in the hope that they will design their industrial devices with respect to maintainability and reliability.

Despite the above mentioned efforts and the governmental developments in security, in the year 2010 the infamous Stuxnet malware was discovered. Stuxnet malware was specifically designed to seek and infect Iranian nuclear powerplants in order to sabotage, ultimately delaying the Iranian nuclear project by a few years. To this day Stuxnet is considered the most sophisticated piece of malware that has been discovered in the field of ICS. It works in three distinctive phases; namely propagation, distribution and sabotage. First, the malware needs to enter the designated system. Because in older ICS data transfer is mainly done through USB sticks and CD drives, the malware was first uploaded to an USB which got into the hands of an engineer at an Iranian nuclear plant. After the USB was used at one of the terminals inside, the malware could propagate onto the ICS. To be able to propagate malicious code like that, Stuxnet used a series of exploits called zero-day exploits. After distributing towards the real devices the malware began to work its so called 'payload', the piece of code which actually does the damage. The target was the nuclear centrifuges. It overrid the internal logic that control the speeds at which the centrifuges span. By making the limit higher and higher and at the same time send fake information to the control terminal, nobody in the power plant saw what was really happening. The centrifuges where spinning so hard that they eventually destroyed themselves. After reverse engineering it was discovered that Stuxnet used many unknown exploits and was estimated that development of such malware would have cost at least ten million USD (Kushner, 2013). From this attack we can learn a few things that are important in cyber security of ICS. From a safety perspective it became clear that outcomes of successful attacks can have disastrous consequences. From a security perspective it became clear that Stuxnet required much inside knowledge of the exact systems that were operative in Iranian nuclear power plants and that it is highly likely that governments can be behind these kind of attacks because of the immense amount of development costs. Furthermore, it became clear that industrial devices are increasingly becoming targeted by sophisticated malware.

As can be derived from the developments like the move towards interoperability and connectivity, ICS has changed from obscure environment with closed protocols to open protocols and standards that enable to interchange industrial devices from different vendors in one solution. Manufacturers of these industrial devices where required to no longer only offer full custom solutions but also industrial devices that could be used in any application of an ICS instead. Additionally, the end-users of such systems gained the ability to choose industrial devices from all different brands which has changed the demand and supply globally, introducing many more distribution channels for the interchangeable industrial devices. The industrial devices are therefore more widely available and the supply of the above mentioned industrial devices has rapidly become a globally dispersed supply chain. When industrial devices are more widely available more knowledge about the industrial devices can be acquired. This knowledge also gives more opportunity for an attacker to take advantage of it.

The lifespan of an ICS is usually much longer than a corporate information system and can range from ten to twenty years. Therefore it is common for the industrial devices of an ICS to be used and handled by many actors in it's device lifetime (Hristova, Obermeier, & Schlegel, 2013). It makes it important to not only look at the end user where the ICS is installed but also look at the supply chain of these devices. It might not be uncommon that current attacks target the supply chain of the industrial devices. Many actors are involved in the process of maintaining, updating, integrating and manufacturing all kinds of industrial devices which makes it imperative that the companies involved are prioritising security on their agenda.

1.3 Research

1.3.1 Problem Statement

ICS are more and more becoming targeted because of their inherited lack of security and potential disastrous consequences. The infamous attacks and the many other reported incidents have led to the categorisation of cyber attacks on ICS. Namely attacks by a network based approach like they are known in the traditional ICT domain. The vulnerabilities that are inherited in the network stack and communication protocols are widely reported and countermeasures that can be taken are mostly already known as well. Many ICS are now operative offline and are not reachable by outsiders anymore. The industrial devices of an ICS are a potential attractive target for cyber attacks. Next to that the supply of these devices has become a globally dispersed complex chain, together this gives reason to believe these devices are prone to be -or- already targeted in the supply chain. Actors in the supply chain have different responsibilities when it comes to manufacturing, delivering, installing and using an industrial device this is a complex system of actors. End-users want the industrial devicess they bought to be genuine and manufacturers don't want their device to be tampered with during transit. Because of the complex chain there is currently too little knowledge where in the supply chain may lie possible threats. This knowledge is needed to be able to implement countermeasures where necessary in order to reduce the likelihood of happening and reduce impact of an attack.

1.3.2 Goal

Before ICS devices find their industrial destination they have passed several production processes where a multitude of companies are involved in. From manufacturing and assembling to transportation and installation. Within the chain it is possible that attackers find the possibility to tamper with the device, where are the vulnerabilities and what should the stakeholders in the chain be aware of? Therefore the goal of this research is to gain knowledge of the global supply chain of industrial devices by identifying the weak spots in the supply chain and possible cyber threats that these industrial devices could face. The possible outcome can be used by KPMG to be able to advise on supply chain processes in order for better supply chain (cyber) security.

1.3.3 Research Questions

To address the above mentioned problem this thesis aims to answer the following central research question:

RQ: *What are the current cyber threats towards industrial embedded devices that could occur in the supply chain?*

Breaking down the central research question there are three central topics that needs to be answered. First, a comprehensive overview of the supply chain needs to be made and the different responsibilities that each actor has should become clear. Knowledge is required about the device, who interacts with it in the supply chain and the distribution channels that are used need to be discovered. To address this, the following sub question needs to be answered:

SQ1:How are actors and their responsibilities arranged in the supply chain of industrial embedded devices?

Second, after having an overview of the supply chain and their role in the supply of industrial embedded devices, a thorough research is needed to be able to find the possible threats that an industrial device can face. To get a complete view a threat will be described as detailed as possible in terms of origin and technical information. Additional knowledge about the device is required as well to understand where the possible threats can take place. The following sub question will be answered to address this sub problem:

SQ2: What are the possible cyber threats towards industrial embedded devices?

Finally, from the threat model that is derived at sub question two we can then argue what the possible entry points are in the supply chain for the found threats to happen. The weak spots in the supply chain need to be identified in order to get insight in where supply chain security will be most important. The following research question will be answered to gain that knowledge:

SQ3: What are the possible vulnerabilities in the supply chain of industrial embedded devices?

In the following section the method by which these above mentioned questions will be sought to answer is given.

1.4 Research Methodology

In order to answer these research questions the research will be split into four distinctive sections: a literature study, a threat analysis, a supply chain analysis and interviews with stakeholders.

1.4.1 Literature study

A literature study is performed on Industrial control systems, cyber security and the industrial device. Next to that, the complex supply chain with the stakeholders need to be identified and literature will be used for this too. Existing literature on supply chain risk management will be consulted and existing frameworks for assessing risks need to be selected to be used.

In order to create a threat model that consists of cyber threats, information from several sources need to be gathered. First, a general definition of a threat is required in order to combine the found information into an actual threat model and the definition serves as the main way to derive threats. Additional literature is required to identify threat actors and, where possible, the reported incidents and possibilities will be analysed to gain insight in the threat landscape.
There are many global supply chains existent where device security is an important aspect, usually where sensitive industrial devices are produced and delivered. This is also the case with industrial devices that are used in critical industrial processes. For the analysis several sources will be used to get a detailed picture what the supply chain looks like. First, the industrial devices need to be discussed and therefore from the market leaders in the automation industry some best selling industrial devices will be analysed and their developments highlighted. Followed by consulting scientific literature to gain knowledge about the device and its lifecycle to able to allocate stakeholders in the supply chain in the lifecycle. As most likely the supply chain of industrial devices to some extend will have similarities with a global ICT supply chain a comparison between actors and the lifecycle is required to learn about the striking differences that need to be taken into account to create a threat model.

1.4.2 Threat Analysis

From the literature study on the threats it is determined how these results can be translated to the supply chain. The threats are broken down into attack trees to find the root cause. It is then determined who can perform the found threats. A threat actor and attack tree of a threat make up the threat model.

1.4.3 Supply Chain Analysis

The resulting threat model is mapped on the supply chain. Next to that the supply chain of industrial devices is compared to traditional ICT supply chain to find similarities and differences. The comparison will be used to gain knowledge in the responsibilities of the stakeholders.

1.4.4 Interviews

To gain insight in the different perspectives of the supply chain of industrial devices three open interviews are performed. Beforehand an interview questionnaire is made however, the interview is done in open format and answers are filled in afterwards. An asset owner, a system integrator and an Original Equipment Manufacturer(OEM) are included in the interviews. These interviews have three goals: one is to gain practical knowledge about the supply chain and the supply chain specific processes that each stakeholder governs. The second goal is to challenge the threat model in order to find at these stakeholders what threats would be possible to happen. The third goal is to gain insight in any countermeasures these stakeholders have in place for security of supply. In Appendix A the structure of the interview can be found which is going to be used at the above mentioned stakeholders.

1.4.5 Validation

Several sections of the threat analysis have expert opinion as validation method. The creation of attack-trees, attack-trees requirements, threat actor capabilities are validated using this method. The outcomes of the interviews is used to validate the threat model as a whole.

1.5 Stakeholders of this study

KPMG KPMG is the main contractor of this study. Within the Information Protection Services department Process Control Domain is a topic which has received a lot of attention in the last few years and has proved to be very important for clients of KPMG. This study contributes to general knowledge about the complex supply chain of industrial devices.

University of Twente The educational institution at which the research is started and finished. This study contributes to cyber security possibilities of the University.

University of Delft The secondary educational institution that adds a lot of guidance and knowledge that is required. This study contributes to further investigation in cyber security of ICS.

Actors in the Supply Chain The central stakeholder where the study is about. This study contributes to general knowledge amongst the stakeholders to improve security throughout the whole supply chain.

1.6 Structure of Thesis

Part 1 First, a literature research on the related work has been done and the relevant theories that support the rest of the thesis are described in this part.

Part 2 The second part of the thesis contains the the detailed threat analysis with the creation the threat model.

Part 3 Then, an analysis of the supply chain has been performed with a comparison with ICT supply chain as a preparation of the interviews.

Part 4 The final part contains the results of the interviews that have been performed at three stakeholders of supply chain. After this part conclusions and recommendations have been given.

Chapter 2

Related Work

The goal is of this chapter is to show the basic principles of an industrial control system and belonging components, to highlight the cyber security aspects and to create an understanding about the differences between corporate IT and ICS. Next to that, the theories that are helpful to use to answer the research question are explained.

2.1 Industrial Control Systems

ICS is a system that controls, monitors and manages large physical industrial processes. Generally speaking, an ICS connects the physical with the cyber world in a way such that devices that are used in the physical process are operated from a distance over a distributed network. ICS gathers information from multiple endpoint instruments and sensors about the status of a process that can be fully or partially automated. The systems read the values of the endpoint devices and interacts based upon programmed internal logic and events that require action from an operator. Status updates about the system are reported to a central control room and where necessary an operator can also control the process from there. The process is usually reflected as an interactive graphical user interface which is referred to as the Human Machine Interface (HMI) that shows the system status in an organised manner. These systems can spread over large geographical areas or can be located in just one location. ICS can be distinguished by the terms Supervisory Control And Data Acquisition (SCADA), Distributed Control Sytems (DCS) and Process Control Systems (PCS) . Figure 2.1 shows how these four terms relate to each other. The main difference is the extent to which they are geographically distant (Macaulay & Singer, 2012).

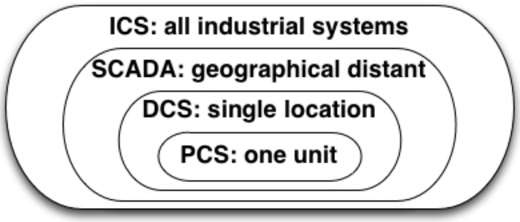


Figure 2.1: ICS, SCADA, DCS terminology.

Because processes can be partially or fully automated and an ICS can just be intended to function for monitoring, there exists many possibilities for implementation. ICS are used in a variety of industries and generally play a striking role in the facilitation of energy in water supply, oil and gas. Alternately, ICS are also present in amusement parks, production plants, bridges and traffic flow control. For instance at traffic flow control the information that the system gathers from the field devices at big traffic nodes is used for long term city planning. On the other hand, in a giant oil rig, the system is used to carry out automated tasks and respond to operator's actions. Therefore the many possibilities can either be relatively simple or very complex, which is highly dependent on the type of industry. The industries where ICS are used in are also very different from each other and therefore the architecture of the system is depending on the environment. Moreover, organizations that operate in the same sector have their own unique characteristics so really every ICS is unique of it's kind. On a technical level ICS can be described by network and communication topologies as the devices can be set up as a slave or as a master. On a physical level the control devices need to be custom configured for the process which they are destined for.

Continuing with the elements of an ICS, each system can be seen as it is made out of several layers. Each layer consists of several components, an example overview is shown in Figure 2.2 (Krotofil & Gollmann, 2013). All communication between devices and layers is done through a multitude of protocols, the most common are DNP3 and Modbus. On the top level resides the corporate network that connects with the ICS. Historical data like production amounts and status about the process can be obtained in that layer. In the process management layer the applications that support the functionality for the corporate layer are stored. Where the process is actually controlled from is called the supervisory control layer, ICS specific devices are installed in the network from that layer down. The Human Machine Interface is the graphical user interface that shows the process and it's industrial devices that can be changed and configured from there. Next is the control layer, the PLC devices are the main control devices that operate the field instrumentation and sensors on the bottom layer.

So, a key device is the Programmable Logic Controllers (PLCs) . The PLCs are at the heart of an ICS and the main control devices of the actual physical process, that is shown as level 1. Inside a PLC is a programmable logic circuit which holds various process specific parameters. PLCs also have a user- programmable memory for storing instructions for the purpose of among others, communication, arithmetic, and data and file processing. PLCs communicate through a network communication channel with a control room, or Remote Terminal Unit (RTU) at the Supervisory Control Layer in level 2. All RTU's communicate with a master control room called the Master Terminal Unit (MTU), also in level 2 . A PLC can also function like an RTU in some cases where geographical distance between the MTU and PLC is shorter, like in DCS. A MTU contains the control software and the Human Machine Interface (HMI) that is able to monitor and control the PLCs. All devices and the control room communicate with each other by the use of various open and closed protocols over a network (NIST, 2013a).

PLCs used to be designed for closed and trusted networks and with little attention to security. There are developments of using more open standards and networks like The Internet and TCP/IP and the heretofore mentioned Modbus and DNP3 protocols. Also, other developments in the PLCs technology is an embedded Operating System and other modules like File Transfer Protocol (FTP) are embedded which makes the devices more applicable in modern organizations. The long lasting idea of security by obscurity is no longer valid and this brings many new threats in ICS in general. As PLCs are virtually part of every ICS, when such embedded devices are compromised this could cause great damage financially as well as damage to equipment and environment or endanger public safety. More detail will be given on the industrial device in the following sections.

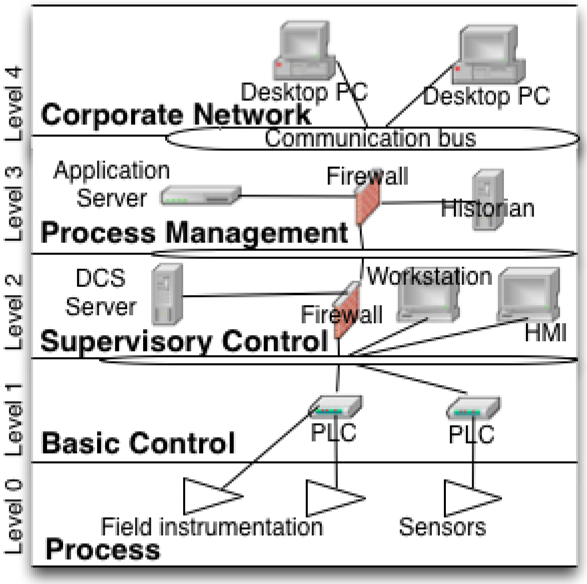


Figure 2.2: An example of different layers of an ICS architecture.

2.2 Cyber Security

In many countries and organisations cyber security is getting a lot of attention because of the increased connectivity and the many incidents that are reported. There are several key security properties that are used to describe security of an automation system (any system that is automated with the use of ICT). This is referred to as the CIA-model. CIA is an abbreviation for Confidentiality, Integrity, Availability. Confidentiality property means that information is only accessible with the right credentials and it should be prevented that unauthorized persons or systems can access (sensitive) information. This property can be ensured with secure encryption of information and communication channels and well established access control for example. However, security in this context is trivial because no security property can be fully ensured, instead it is matched to an acceptance/allowance level. On the other hand, if information is changed unknowingly by unauthorized persons or systems it is considered a breach of the Integrity property of a system. Integrity should be ensured when it is important that information that is processed remains the same and cannot be changed. To ensure this, preventions of message injection in the network and spoofing need to be in place. Next is Availability, which is rather straightforward, means that a service of the system should be available as much as required. When it is important for users to always receive email's of co-workers instantly, the mail-server should always work and have the least downtime as possible. To ensure this property, usually redundancy of servers are in place. The CIA-model provides a means to determine what security properties are most important and should have priority for a given system (Dzung, Naedele, Hoff, Crevatin, & Motivation, 2005).

For a corporate Information System that process sensitive client information and where collegues collaborate through corporate email, Confidentiality and Integrity and not so much Availability are the security properties that need to be ensured. In these traditional Information Systems where client, pay-roll, strategic plans are being processed, stored and shared among co-workers Confidentiality is a striking property because the above mentioned information is usually sensitive information that unauthorized persons or systems shouldn't have access to. In addition, Integrity of this information is equally important because the business should be able to use reliable data. Availability as mentioned above is not so much of importance because when a service like e-mail does not work for 10 minutes it is not a problem when the e-mail is sent after that period. However, this depends on the business and the services of such Information System. So, when comparing corporate IT with ICS security there are quite some similarities but some notable differences as well, which also has influence on the CIA model. The differences largely have to do with the continuous and physical nature of an ICS. The differences are summarised in the table 2.1 below (Kang, Lee, Kim, & Park, 2009).

Information System	**Control System**
Not real-time	Real-time basis
Correctness of Information	Response time is critical
Delay Allowed	Big problems caused by delay
Planned Tasks	Sequential Tasks
Data Integrity is important	User's security is important
Task loss by data corruption	Economic loss or casualties
Resoration by re-booting	Continuous operation required

Table 2.1: Information System and Control System differences

Mostly these differences are centred around a few principles, namely; Almost all ICS security failures have physical consequences and have direct impact on the environment; Often the security issues are manifest as maintenance failures and therefore anomalies more prevalent and that makes the failures more difficult to detect; ICS security can be more difficult to manage because of old systems, lack of test environment and assets can be dispersed over wide area; Lastly as Macaulay et al mentions, cyber threats to an ICS include many additional threat possibilities because of the non-typical network protocols and certain commands that can't be blocked due to safety issues like alarm event traffic (Macaulay & Singer, 2012). These principles and the differences shows there is another security property that is important to ICS, however not directly related to cyber but definitely to the process control domain. Safety is one of the most looked-after property that is required and in all ICS explicit safety regulations are applied. Sometimes this results in that security properties are not thought of. So next to the Confidentiality, Integrity, Availability, a fourth property can be added specifically for ICS: Safety. When potential threats can be allocated to these four properties it will become more clear what the impact can be and what kind of effect the threat could have.

Continuing with how organisations can be viewed according to their ability to secure their environments. Basically organisations have the choice to comply to developed security guidelines in order to be best prepared or protected against cyber threats. These organisations can be assessed based on their maturity in information security. The maturity model is a measure to what extent an organisation is pro-actively operating to guard their security in the broadest sense possible. In fact, the maturity model is a structured collection of elements that describe certain aspects of maturity in an organisation and the level of maturity indicates the degree and strength of the organisation's security measures. As Lessing describes in the study of maturity levels in information systems, an organisation with high maturity level is expected to be well responsive to security breaches in an appropriate manner. A generic maturity model is given in the figure 2.3. As is suggested by the figure, the maturity and the amount of risk is related to the amount of effort that is put in to security (Lessing, n.d.). Assessing maturity proves to be a good way to categorize organisations in their ability to ward against cyber attacks, although there are many different maturity models, they are all quite similar to each other. Karakola et al highlights the aspects and strengths and weaknesses of the most common models (Karokola, Kowalski, & Yngström, 2011). Of the many information security maturity models that are available none is specific to ICS or supply chains so a generic maturity model would be the best starting point to use such model.

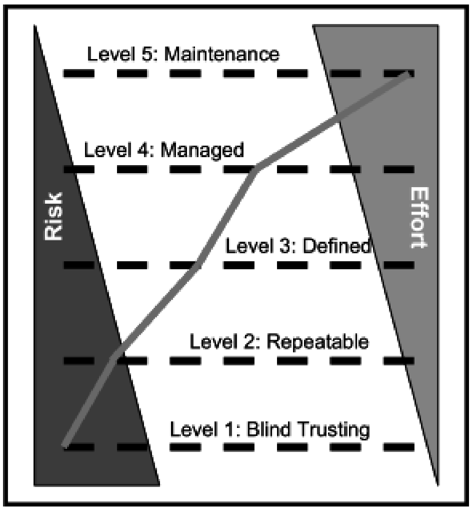


Figure 2.3: A generic maturity model for information security.

Furthermore, to be able to report and learn from discovered cyber attacks, these attacks are broken down into pieces to create an understandable structure. This structure of an attack against a system can be explained as an 'attack tree'. There is an ultimate goal and there are several ways to achieve the goal described by different paths along the tree (Schneier, 1999b). The cybercrime landscape used to be the landscape of 'hackers', 'hacktivists' and 'script-kiddies'but is increasingly becoming the landscape of organized crime and cyber warfare (NCSC, 2013). This is leading to 'attack-trees' of contemporary attacks being far more sophisticated and the targets are switching from 'target-of-opportunity' to 'target-of-choice' (Matthieu & Waalewijn, 2014). Targets-of-opportunity being fire and forget malware that was not pointed to a specific location as this information was not available but target-of-choice is in fact looking for a vulnerable system and point the attack towards that specific location. So, in cyber security terms we can describe the ability to withstand and react to attacks based on maturity and an attack can be described as an attack tree that has an impact on one or more security properties. This knowledge is used to perform a profound analysis on threats towards industrial devices and to be able to find security gaps that are necessary to be dealt with.

2.3 Cyber Security in Industrial Control Systems

Due to the continuous nature of an ICS, the priorities in the CIA-security properties change with respect to traditional information systems. For example when ICS have any downtime this could be very costly for the organization. Availability is therefore the most important property for ICS. Integrity on the other hand is also important because the control devices shouldn't be making process decisions based on information that is corrupt, this is also summarized by Zhu et al. As mentioned above, the added safety property is a high priority security property as well (Zhu et al., 2011).

Other than the security properties, the possible cyber attacks to ICS need to be taken into account. When a cyber attack is discovered and the impact can be estimated, it can then be linked with the security properties to calculate severity of the attack for that particular system. In recent research done by National institutes for standards and cyber security at both local and US governments they show that there is a trend of increasingly targeting ICS (NIST, 2013a) (NCSC, 2013). This raises concerns because many ICS are used in critical infrastructures of countries. That ICS are becoming more targets of choice however is also because ICS are currently getting more widely known for their vulnerabilities and the critical assets of industrial processes are getting more attractive than common targets as well. Additionally, openly available tools such as Shodan [1] make it very easy to search for open online interfaces anywhere in the world. These developments came to light after the discovery of a very sophisticated attack on an Iranian nuclear power plants back in the year 2010 called Stuxnet. After the reverse-engineering and examination of Stuxnet, it was considered the most technical complex malware ever created and it is an eye-opener for the ICS-field regarding cyber security. Next to that, Zhu et al (Zhu et al., 2011) shows a taxonomy of attacks that ICS could face, this is enumerated below. Also, Zhu et al take a view on ICS from an end-user perspective and look at what could happen in an operational system.

- Attacks on Hardware
- Attacks on Software
- Attacks on Communication Stack

An attacker could get unauthorised access to a physical location where devices of an ICS are located. The attacker could then change configurations or change thresholds that are on the outside of the devices. This could result in that operator display values are different without the operator being aware of it. This might jeopardise safety in an industrial environment when responses to alarms are delayed for example. In the devices an ICS consists of, there is a variety of software present. The specific software is installed at multiple levels, namely level 1, level 2 and level 3 (as in figure 2.2 to meet the functionality it requires for the given ICS. Moreover, several big databases that store historical data are also present, often containing confidential data about the process. The software in the different levels use the real-time data from the sensors and historical data to draw correct decisions to steer the progress of the processes. Because most of this software is written in C, the authors of (Zhu et al., 2011) highlight that with vulnerabilities on the software layer extra precaution should be taken. Among the attacks that should be taken with extra precaution on the software layer are: SQL-injection, no privilege separation of tasks and buffer overflow. Continuing with attacks on the communication stack, these happen in the communication protocols that are used in between devices and applications. The type of attacks are referred to as attacks on the layers in the OSI-model, namely the transport layer, network layer, application layer. Also, protocol vulnerabilities can be exploited when the implementation of a protocol fails due to segmentation faults or buffer overflows.

The research of Hadžiosmanović identifies methods to protect the process of ICS. To do this and to improve cyber security there are two general strategies, first strategy implies using best practices from IT in the ICS domain. The other strategy is an ICS specific

[1] http://www.shodanhq.com

strategy to improve cyber security. The first strategy means at the client-side of ICS, an defense-in-depth plan like National Institute of Standards and Technology created (NIST, 2013a), needs to be in place and users that interact with the system need to be aware of the possible threats. A defense-in-depth plan means several measures are present on every layer of the system and also contains measures at the personal psychology layer to improve awareness of people. These measures are mainly managerial measures like regular password changing by the control users and use Intrusion Detection (IDS) techniques. If these measures are met they also need to be implemented correctly and regularly tested for compliance before it will be very difficult to launch an attack from the outside of the ICS environment. As mentioned above, the second general strategy implies a more ICS-specific approach of security. An example of such strategy is researched by Hadžiosmanović where industrial specific log files are analysed on anomalies so that the process does not need to be interrupted.This research also highlights security of PLCs is critical for security of ICS (Hadžiosmanovic, 2014).

2.4 The industrial device

As mentioned in this chapter, ICS are increasingly becoming the target of cyber attacks (or the amount of attacks are the same but they are increasingly being monitored and reported) and the core control devices, the devices that directly control industrial processes, are at the heart of it (NCSC, 2013). In some cases up to a thousand control devices can be part of an ICS which makes it important these devices are looked after. Industrial control devices have been around for over 40 years and they have been developed from simple I/O devices towards intelligent embedded devices for their industry specific tasks. Each generation getting more sophisticated and more intelligent, reaching demand all over the world. To satisfy that global demand, a complex globally dispersed supply chain has emerged for the supply of these devices. The device' history and the associated components need to be well understood in order to understand the facets of this supply chain.

A typical ICS control layer can contain three different control devices, the Remote Terminal Unit (RTU), the Programmable Logic Controller (PLC) and the more recently developed Programmable Automation Controller (PAC), which has only been around for approximately 10 years as opposed to 40 years for RTU and PLC. All those devices are used to control industrial processes that are existent in sometimes harsh environments. They are built to last well over 10 years in such environments so their design is robust and simple.

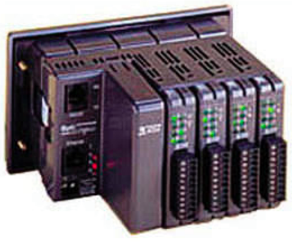


Figure 2.4: An example of a RTU

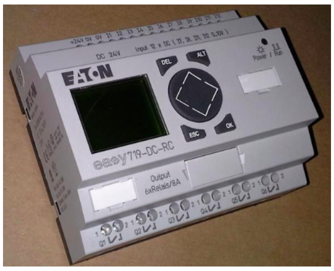


Figure 2.5: An example of a PLC

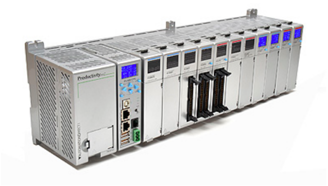


Figure 2.6: An example of a PAC

RTUs are mainly used to collect data from field devices and convert the analogue signals to digital signals to be used for transmission to the control room of a industrial process.

The transferred data is then used to display the information on operation terminals or stored in a server to acquire historical process data. RTUs are considered the simplest of all control devices used in ICS because they have very limited processing power and usually does not contain the control logic of the industrial process. Basically an RTU serves as a passage from the physical world to the cyber world, translating serial analog signals to digital ethernet messages. It communicates with a centralized control unit. The PLC devices can be used in conjunction with or are as replacement of a RTU. They are designed for real-time use in harsh industrial environments and they may contain control logic and programming to control their part of the process. The main difference with an RTU is that a PLC can work standalone due to its control logic and does not require input from a centralised control unit. Whenever contact is lost with the control room a PLC can continue to work. Like RTUs, PLCs were designed as simple devices with limited processing capability but emerging trends of today's suppliers show that the PLCs are being designed with more emphasis on their architecture. The renewed device architecture may also include a HMI, advanced reporting and ability to support more advanced process control features. Additionally, it includes an OS and network interface as opposed to the primitive I/O features and RTU functions it used to have. Next is the PAC, basically a name for an advanced PLC with, among others, even more functionalities, multiple processors and bigger memory. Figure 2.4, 2.5 and 2.6 show examples of respectively the RTU, PLC and PAC, the difference in sophistication can be clearly distinguished by its size and amount of ports that are visible for example. The size of the devices range from 20cm width(RTU) to up to a meter in width (PAC) (Macaulay & Singer, 2012).

To further highlight the striking differences between the industrial devices that are used in industrial control, please refer to table 2.2.

Aspect	**RTU**	**PLC**	**PAC**
Processors	Single	Single	Multiple
Programming Logic	None	Ladder Logic	Computer Programming Function Block Diagram Ladder Logic
Functionality	Collect and transmit data from I/O signals	Sequential scan of logic	Dual scan of logic Process control Motion control
Memory	Up to 64K	Up to 64K	64K and up
I/O modules	10	2	100's
Communication	Mostly WAN/GPRS	Mostly Proprietary & TCP/IP	Multiple protocols open standards
Automation	Not standalone	Can be standalone	Mostly Standalone

Table 2.2: Differences between RTU, PLC, PAC

Furthermore, different embedded devices can be distinguished by their applicability. Because the latest trend in ICS has been towards inter operability, this resulted in the increased use of Commercial Off The Shelf (COTS) devices. COTS devices are designed with open standards and well known Operating Systems (OS) for fast and easy installation and to be used in conjunction with many other devices because they work well together. The result of this is that these devices are widely available and require less specific knowledge to handle. Therefore, threat actors can take advantage more easily because of the well-known devices. There are also the industry specific devices, a custom made device specifically designed for the designated task or environment. In comparison with COTS devices these custom tailored devices are harder to take advantage of because of specific knowledge that is required. It's also less effective for an attacker to target because of the specialized devices are only used in one or a few applications. It's important we make this distinction because this difference is needed to take into account for the overall vulnerability of the device in the supply chain (Group, 2008).

2.4.1 Device Components Overview

In table 2.2 some of the device functionality is already shown. These functions are enabled by the associated devices the RTU, PLC and PAC are made of. To better understand device vulnerabilities, a comprehensive list of devices and their origin is required. Mulder et al and Mcminn highlight the components of such device and distinguishes them by their low level functionality. They have disassembled a PLC to gain a deeper understanding of device design. Because Mulder et al also highlight that their results can be used for other industrial embedded devices similar to PLCs, their results can be used perfectly to gain knowledge of these devices and where their vulnerabilities originate from (Mulder et al., 2012).

Next to the applicability that was just described above, another distinction can be made. Internally the device is made up of three operational layers. Mcminn et all distinguish these three layers of which an attacker could take advantage of (Mcminn & Butts, 2012). Delineated as degree of abstraction, these layers are hardware, firmware and programming/software layer. As Mcminn points out, the lower the abstraction level, the harder it is to modify and to verify it. Therefore as hardware is the lowest layer, to some extent hardware needs to be trusted because it is the hardest to verify. The firmware is considered the lowest electronically modifiable layer of a control device. In the same firmware layer the operating system of the device is also included. On top of that, is the programming layer which consists of the logic and the sequential steps to control a process. In the programming layer the functionality of the device can be modified. Later on we can use the operational layers to pinpoint what threats target which operational layers. The specific components in relation to the operational layers can be seen in figure 2.7 (Mulder et al., 2012).

2.4.2 Industrial Device Lifecycle

The different stakeholders that are involved in the supply chain of industrial devices can be identified when an understanding is made about the device lifecycle. It is then possible to allocate stakeholders to the different lifecycle stages of a typical industrial device to create a clear overview of the chain. Hristova et al identifies these typical engineering stages of the industrial device lifecycle (Hristova et al., 2013). This device lifecycle also helps to comprehend the complexity of the supply chain and the vulnerabilities of the control devices in the supply chain. In the many general product lifecycle models it is argued that before production there is also a concept and design phase, these phases however are not mentioned by Hristova et al because they are irrelevant for the transit of the device from manufacturer to where it will become operational. Although it is needed to mention that in these phases sub-assembly components are selected and insourced from different sources and therefore could pose a vulnerability as well.

Phase 1: Production The conception of the device is the production. This is where the hardware parts, modules and computer circuit boards are assembled and tested on correctness of assembly. After successful testing of the different modules the first firmware

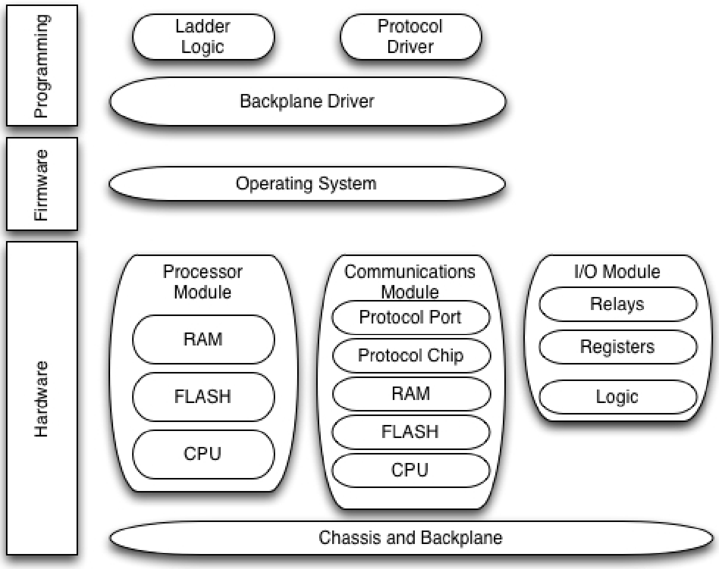


Figure 2.7: Generic PLC module overview

is loaded on the device for the later stages. The device has factory default settings so does not contain any control functionality yet but is ready to be designated for an industrial solution. In the production phase, the hardware, firmware and programming layers are finished and therefore many critical production processes are being executed. Some of the key processes in this phase are quality management that is used to validate if finished products maintain their certifications such as ISO 27001.

Phase 2: Shipment When the device finds a buyer, the device is shipped to that location. Logistic companies are involved in this phase. Marketing channels reach to distributors, integrators and asset owners so many stakeholders interfere with the product.

Phase 3: Engineering / Customization Every ICS is unique in it's kind and so is the physical process for the device is going to monitor and control. Before the device is actually going to be used, the modules that contain the control logic, the Operating System, the network segmentation need to be customized to the specific characteristics of the designated site. In this phase the device is engineered to match the requirements of the asset owner and the firmware and programming layers are altered here.

Phase 4: Factory Acceptance Test A typical lifespan is 10 to 20 years(Macaulay & Singer, 2012) for an ICS therefore the field devices need to be well-tested before their operation. First, the Factory Acceptance Test (FAT) is carried out to ensure the system itself works as promised. The device is tested on all fronts so on every operational layer tests are being carried out. When any tests fail the device is returned and repaired to work properly.

Phase 5: Installation / Commissioning After the device is working as required, it will be installed and commissioned in the intended industrial environment. All necessary connections with real control rooms, sensors, I/O modules are created in this phase.

Phase 6: Site Acceptance Test The Site Acceptance Test's (SAT) goal is to ensure that the device also works properly in the intended environment, the site. After the SAT it is ready for full operation. The device is tested on all layers for full functionality and the device is configured.

Phase 7: Operation In this phase the device is set up, installed and working properly in the intended industrial environment. The industrial process is operational.

Phase 8: Maintenance / Repair Like mentioned above the ICS differ much from each other, even the industrial process may need different control parameters in different seasons. Maintenance is done to change or repair the device as desired.

Phase 9: Decommissioning A device can be disregarded from operation, the device is then disposed or (parts of it) recycled as it reaches it's end of life.

A product lifecycle of a PLC is shown in Figure 2.8 (Hristova et al., 2013).

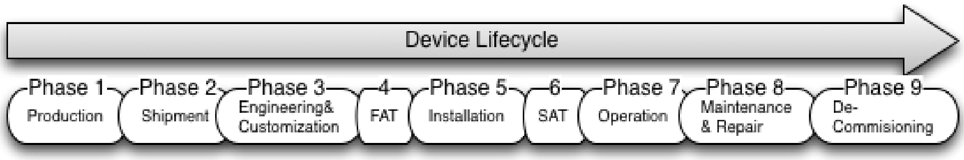


Figure 2.8: Device Lifecycle phases.

2.5 Supply Chain of Industrial Devices: Identification of Stakeholders & Roles

The supply chain is a globally dispersed complex system consisting of a network of entities that interact with the product. The entities include organisations, people and services that are derived from the product lifecycle described above. The key processes in the supply chain can be described as design, manufacturing, delivery, integration, testing, maintenance and disposal. From a thorough analysis on the product lifecycle and from the traditional ICT supply chain the following stakeholders are most likely present in the supply chain of embedded devices.

2.5.1 Device Critical Component Manufacturers & Suppliers

As with many products and as shown in the component overview section, the control device as a whole is made of multiple parts. The supply chain starts with the manufacturers of these sub-assembly components which are critical to the device. The memory chips, computer chips and circuit boards for example are generally engineered by the well-known organizations such as Intel, AMD(CPU) Asus, Nvidia(GPU), Corsair (Memory), Realtek, IBM, Gigabyte(Network & communication), ASML (Circuit boards). The components differ from traditional IT hardware because the industrial devices are used in rugged environments and have to withstand severe circumstances. Also, in many cases the Original Equipment Manufacturers (OEM) also design & engineer their own critical components. These stakeholders and their suppliers can be seen as phase 1 in the lifecycle.

2.5.2 Original Equipment Manufacturers

The OEMs are the companies that insource the critical components and other sub-assembly parts to create a working embedded device. The final product can be COTS-product or industry specific designed device that meets customers requirements. COTS products usually takes much less time to market and generally have a lower Total Cost of Ownership (TCO) which is the total costs involved in buying, operation and disposal. The key role the OEMs take is the design and manufacturing of the device.

According to a recent survey of controlglobal.com the top 10 PLC/PAC manufacturers by market share(descending order) are Siemens, ABB, Emerson, Schneider Electric, Rockwell Automation, Yokogawa Electric, Mitsubishi Electric, GE, Honeywell and Danaher (ControlGlobal, 2014), (Automation.com, 2014). These companies are active in phase 1 of the product lifecycle.

2.5.3 Device Wholesalers

To reach a broader market, manufacturers use several distribution channels to get their products to customers. Wholesalers act as intermediary between manufacturers and other business related users, connecting them globally. They buy in bulk and sell the products to retailers, resellers, institutional and industrial users or other wholesalers. These organisations reside in the phase 2, shipment and phase 3, engineering. They govern the distribution channels and can do a little customisation upon request.

2.5.4 Device Retailers & Resellers

Retailing is the sale of goods or services to the end-users or asset owners. Generally big market places with lots of different products. In some cases a retailer also replaces or install Operating System on the devices to match customers' needs before it is shipped. Big companies in this category are AutomationDirect and Acromag for example. More locally there are resellers of the products. These stakeholders also reside in phase 2 and 3, like the wholesalers.

2.5.5 Device Transportation & Shipment

Third party logistics play a role in every shipment, wether it is by sea, air or land. Products are stored in warehouses and delivered to major hubs in the region the product is destined to. In phase 2, shipment, these companies can be found.

2.5.6 System Integrators & Solution Providers

Because of the complexity and uniqueness of many of the ICS, some organisations offer complete solutions to custom fit the whole industrial process with the necessary devices and programming of the logic. They provide services to install, test and maintain the devices they provide. Usually these companies specialise in a certain industry. A few well-known companies are IS International Services, Data Centric Solutions. They often use high quality products of OEM's. Intgrators are active in engineering/customization, FAT, Installation and SAT phases in the lifecycle.

2.5.7 Third Party Software Developers

It is possible that OEM's or System Integrators decide to outsource their software development processes. In this case the third party software developers also supply an important component to the device in the supply chain. These actors play a role in phases 1 or 3.

2.5.8 Device End-users

The organisations that eventually use the products in their industrial environments are the asset-owners or end-users. They can choose to get their product from wholesale, retailer or reseller or get a complete solution. These are the customers of the ICS and reside at the end of chain. In the product life-cycle they can be grouped at phase 7, the operation.

2.5.9 Device Maintenance & FAT/SAT testing

During installation and operation at the industrial site these tests and maintenance activities can be carried out by several organisations. When an ICS is supplied and installed by a Solution provider or System Integrator the maintenance and testing is carried out by these companies. However, in some cases this could also be a 3rd party or the asset owner's own engineers. In phase 4, 6 or 8 we can find these companies.

2.6 Supply Chain of Industrial Devices: Overview

Given the identified distinct roles for multiple phases in the device lifecycle, a graphical overview can be made that represents the structure of the supply chain and how the stakeholders relate to each other. The lines between them represent flow of materials or products, this can be seen in Figure 2.9. The flow of materials or products up to the distributors and system integrators can be seen as the upstream of the supply chain. The downstream supply is from the integrators to the destination at the asset owner. However, it is possible that OEM's collaborate directly with asset owners and also directly perform the system integration. Moreover, asset owners can also decide to purchase directly from resellers locally because they have the knowledge in-house to configure the products for their environment.

2.6.1 Supply Chain (Risk Management)

Up until now ICS and cyber security has been viewed from an end-user perspective. In detail the elements of a installed, operative ICS have been discussed and the important aspects of cyber security and complications for ICS have been highlighted. As mentioned above, the main control device, the PLC is critical for the security of the process and the ICS in general. There are a lot of efforts in simulation environments (Chabukswar & Sin, 2010), (Davis et al., 2006), (Wang, Fang, & Dai, 2010) together with more and more research being done in how to mitigate the (found in simulation) common attacks on an operative ICS(Liu, Ten, Member, & Govindarasu, 2009), (Ten, Manimaran, & Liu, 2010). While these studies simulate common attacks and show how end-users could reach a higher level of maturity in their security, they all leave out the possibility that a product is faulty before it is operative. When looking from an attackers perspective, attacking an operative facility with an ICS would not be the only option to consider. The attacker could possibly tamper with devices before it is installed, making the efforts in securing an operative ICS not sufficient in optimally securing the process. Before the devices are

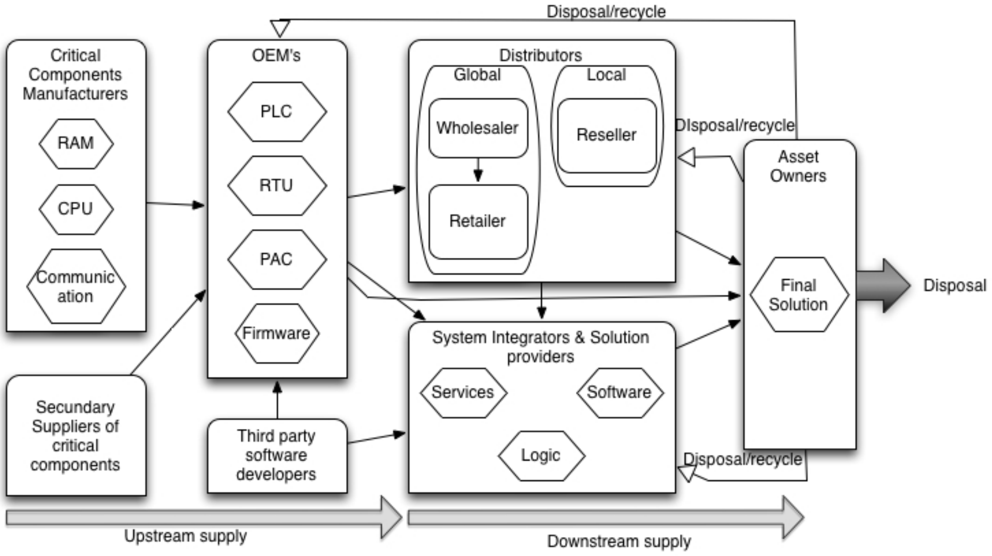


Figure 2.9: Supply Chain Overview

operative they traverse a whole chain in which the device is, among others manufactured and configured for example by many different actors. In information and communications technology the supply chain is a globally distributed system that is very complex by its geographically distant distribution routes and because at actors in the chain parts of the production process can be outsourced. The final product of the supply chain has been created by a large network of organisations, people, processes and products that are active somewhere in the lifecycle of the product. A comprehensive view on these aspects of supply chains is given by Zsidisin et al (Zsidisin & Ritchie, 2009).

In the field of logistics, supply chain is generally known as the path a product or service takes throughout it's lifecycle. The supply chain starts at initial raw material processing to the end consumer and everything that is in-between such as processing and transportation. Nowadays, Supply Chain Management (SCM) is the discipline that seeks to optimise and ultimately increase profitability of the supply chain by reducing waste, enable fast lead times to the end consumer, gain a more sustainable competitive advantage and become more agile and efficient at the same time. This is also known as Lean Six Sigma theory, a quality perspective. In addition, SCM is concerned with information sharing and communication as well as relationship development throughout the whole supply chain. In general, supply chain management can be viewed at two organizational levels, operational and strategic. The focus at the operational level would be towards effective and efficient production, insourcing of goods, stock control, warehousing and distribution of finished goods. From a strategic point of view, suppliers need to be chosen carefully and with whom the organization is going to work together and share information needs to be assessed. These examples above are mainly activities that seek to improve the organizations own processes and minimize disruption in the supply chain. For the ICS domain with respect to security of the devices in the supply chain, the strategic perspective on supplier selection and information sharing is useful because the cyber threats don't have the same origin as the qualitative risks like waste and therefore the origin will be more physically related to suppliers/other stakeholders.

SCM is now increasingly becoming a proactive activity with other stakeholders in the supply chain that try to collectively enhance the added value, agility and profitability of the chain. Additionally, this development introduces a multitude of involved risks that need to be dealt with, like risks that are associated with sharing information and the consequences of building a relationship across the supply network and establishing trust for example (Zsidisin & Ritchie, 2009). SCRM is a broad term that comprises of a set of activities in relation to the supply chain. Zsidisin et al report that these are the components of SCRM and also described as the SRCM-process:

1. Risk identification
2. Risk analysis, assessment and impact measurement
3. Risk management
4. Risk monitoring and evaluation

Although very general terms of a risk management process, it gives a view on supply chain risks and how these could be assessed. Because there is little known about the supply chain of devices that are used in ICS, the general components of SCRM would be a good starting point in understanding supply chain related threats. Starting at risk identification to get an understanding on type of risk, the authors of (Dittmann, Gaudenzi, Myers, & Stank, 2014) show a different perspective on risks which makes them easier to understand. They divide the risks into four categories, namely Supply Risk, Operational Risk, Demand Risk and Security Risk. Supply Risk evolves in the supply side, there is a lack of movement of insourced goods to the organization which results in the organization not being able to meet the customers demand. Operational Risk has to do with the organization's inability to create the products or services with the right quality and therefore not meeting the right productivity or loss of productivity occurs. On the other side of Supply Risk there is Demand Risk, which is associated with the losses that occur after variances in volume demanded by the customer's. Next to that is Security Risk in the categorization, this type of risk is the most relevant for security of supply chain of industrial devices because it is including adverse events where intellectual property and information are affected and count towards the incurred loss. Because many of the cyber security incidents in PLCs could be occurring in the supply chain, like in the example of the smartphones given in the motivation, the incidents can possibly be categorized in this risk category. These briefly explained theories on SCRM are mainly related to the logistic processes of products and services and they give a basic understanding of how risk is involved and how it can be addressed. However, cyber security in supply chains is very complex because of the fact when parts or devices are malware-infected and afterwards recycled/re-used this can become another problem. Therefore it is necessary to understand both supply chain risks and possible cyber threats in order to perform adequate risk management.

2.7 Definition of Threats and Vulnerabilities

In a recently published draft framework of the National Institute of Standards and Technology, the 800-161 publication, it is highlighted of what elements risk is made of. The framework is made to apply for ICT supply chain and because the supply chain of industrial devices have many things in common with corporate or traditional IT, it assumed the risk in the supply chain of industrial devices comprises of the same elements as well. Also, they show many of the aspects of the ICT supply chain that can contribute to a risk. As can be seen in figure 2.10, a supply chain risk consists of Threats, Vulnerabilities, Likelihood and Impact. When an attack source is capable of exploiting a vulnerability it becomes a threat, together with how likely it will happen and given the impact according to CIAS-model described above a detailed risk that can lead to a supply chain compromise. This framework is used to assess the supply chain of industrial devices and to gain knowledge about the risks that these devices face (NIST, 2013b).

First, definitions of the variables of a risk need to be defined and then to what extend we are able to determine these variables. Starting with the first variable, the threats. To be able to describe a threat, first an understanding is needed of the term threat. Because ISO 27001 standards are widely used in ICS domain, first the ISO 27001 definition of a threat is looked at. The definition is: *"A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system."* The definition does not contain the elements of an "event", which is needed to create a scope for researching threats. By the National Institute of Standards and Technology (NIST) such an event is translated to the "potential for a threat source to exercise a specific vulnerability" (NIST, 2002). Where the "potential" can be described as a combination of the "capability" and the "opportunity" to exercise a "vulnerability". Vulnerability will be described in the next paragraph. However, the threat source must also have an "intention". So, the term threat can be best defined as the following equation:

$$Threat = Capability * Intent * Opportunity \tag{2.1}$$

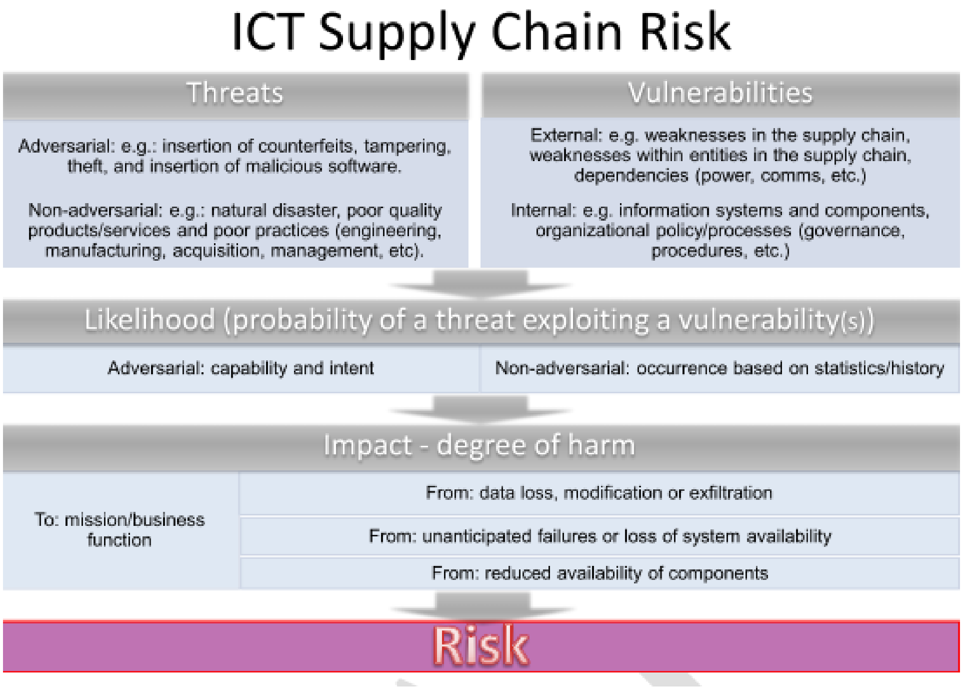
This equation means, as is described by Kang et al (Kang et al., 2009), that the source of a threat must have the following:

- an intention such as a clear goal or motivation;
- the capability in terms of financial or knowledge and;
- must be given the opportunity to form a threat such as having access to a location of a vulnerability.

The equation shows that a threat can only be existent if all three of the products is not zero. To be able to use the equation and to find threats in the supply chain, research is required in all three elements and find scenario's where all three elements are present. Since this all together will be an extensive research, it is helpful to simplify the equation. Intention and Capability will be the easiest to research because these can be generalised. Opportunity is dependent on the organisations that are involved and as was described above, all ICS are unique. Therefore researching opportunity will only be applicable to a specific context. So, in order to create a threat model it is assumed opportunity is equal to one. This way, the equation will only consist of Capability and Intent.

Next is vulnerability, by the ISO 27001 standard it is described as: *"A vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats."*

In more detail a vulnerability is described by the NIST as a "weakness in a system or it's security procedures, internal controls or implementation of the controls that could be exploited or triggered by a threat source. Moreover, it is any weakness in the system or component design, development, manufacturing, production, shipping and receiving, delivery or operation that can be exploited by a threat actor to degrade the performance of a system that supports the mission." (NIST, 2013b) This comes down to that supply chain vulnerabilities may be found in the development lifecycle of a device that traverses the supply chain. The likelihood of the threat being carried out can only be determined with a lot of knowledge about the organisation where the threats apply to, this also counts for the impact.



ICT Supply Chain Risk

Threats

Adversarial: e.g.: insertion of counterfeits, tampering, theft, and insertion of malicious software.

Non-adversarial: e.g.: natural disaster, poor quality products/services and poor practices (engineering, manufacturing, acquisition, management, etc).

Vulnerabilities

External: e.g. weaknesses in the supply chain, weaknesses within entities in the supply chain, dependencies (power, comms, etc.)

Internal: e.g. information systems and components, organizational policy/processes (governance, procedures, etc.)

Likelihood (probability of a threat exploiting a vulnerability(s))

Adversarial: capability and intent

Non-adversarial: occurrence based on statistics/history

Impact - degree of harm

To: mission/business function

From: data loss, modification or exfiltration

From: unanticipated failures or loss of system availability

From: reduced availability of components

Risk

Figure 2.10: ICT Supply Chain Risk

2.7.1 The use of attack trees

To assess the vulnerabilities in the supply chain, the supply chain and the lifecycle needs to be analysed. From there the weaknesses in the parts of the supply chain can be identified. However, these weaknesses, events or activities that lead to an undesired outcome of losses are not always to be pinpointed accurately. The potential weak spots, contributors to mishaps, failures or root causes of failure of these events or activities need to be searched for and several analytical techniques can be used to so. Fault Tree Analysis (FTA) is a top-down method that links undesired events to contributors and causes as leaves and nodes of a tree to systematically break down the loss event. Failure Mode Effect Analysis (FMEA) is similar to FTA as it also decomposes the possible failures to identify the root cause. Hazard & Operability Study (HAZOP) on the other hand is focused on the operability of a production site and mainly addresses safety problems in process control systems. HAZOP uses process descriptions and checklists and can be used to get a better understanding of the supply chain vulnerabilities (Clemens, 1993), (Dunjó, Fthenakis, Vílchez, & Arnaldos, 2010). For the determination of likelihood and impact only estimates can be made or specific knowledge need to be acquired.

The use of attack trees is much alike fault trees that is used in other disciplines, they function to find the root of a fault in a system that is described by failure scenarios. The purpose of an attack tree is to understand how a system can be compromised describes how the given failure propagates. Attack trees are used to model threats and vulnerabilities to find possible entry points for a threat to be executed. The top of an attack tree is the ultimate goal and the nodes that connect with the goal are the different paths of achieving that. The branches of the tree represent an "OR" relation, unless it is specifically stated that a combination of branches is an "AND" relation. So all branches from the root node are different activities that lead to the ultimate goal and don't have to happen or performed simultaneously (Byres, Franz, & Miller, 2004). The resulting tree and its branches represent the possibilities in a simplified way. The need for the use of attack trees is to understand what the attackers goals are, who the attackers are and what the entry points are in a given system. Generally attack trees are created in two steps, first, the goals need to be identified. That is just done above. Step two is to identify attacks against these goals and the possible ways to achieve the goal. This methodology is required to show attack possibilities and understanding the relationships.

Figure 2.11 shows an example of an attack tree to demonstrate how attack trees are created and used (Schneier, 1999a).

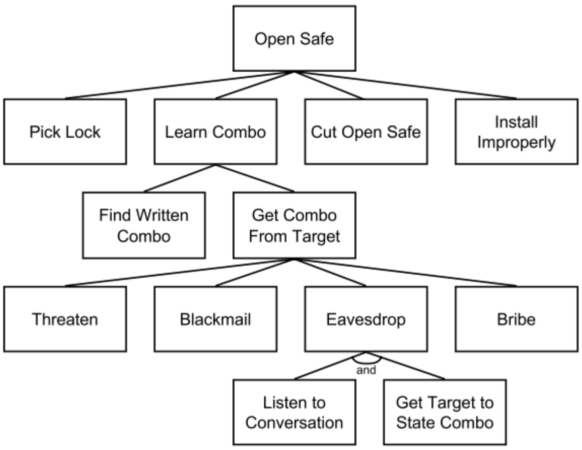


Figure 2.11: Example Attack Tree

This simplified tree can be read as follows: in order to Open the Safe, a few things are required. The lock can be picked, the combo can be learned, the safe may be cut open or the safe can be installed improperly. Learn Combo is then split up in a few extra possibilities. The combo can be learned to retrieve the written combo somewhere or to retrieve the combo from a target. This in term can be done in multiple ways, like blackmailing and bribing or even threaten. For the attacker to be able to open the safe by eavesdropping, the threat actor needs to listen to a conversation and make sure the conversation is about the combination of the safe. These are the possible paths to achieve the goal to open safe.

2.7.2 Criminal Behaviour

For the supply chain of industrial devices the found definitions of threat and vulnerability can be used to create a threat model. To asses the threats in the supply chain a profile of threat actors, capabilities and intent is needed. As interfering with products in the supply chain is considered a criminal act, the threat agents that propose a threat can be considered criminals. From crime science research, the intent of a criminal act can be explained to better understand the motives and how crime arises. Although crime science research is primarily focused on understanding what drives criminals and also contributes to the prevention, detection and reduction of crime in general. Everybody in the society has dealt with or is confronted with crime. Unfortunately, it's happening everywhere from the local streets to global minority groups around the world and of course there is terrorism. However very different from ordinary burglary and theft, executing a cyber attack on ICS is considered a crime as well and organizations are the victims. The criminals' behaviour behind cyber crime can be explained just as the criminals' behaviour for robbing a bank but instead of viewing this behaviour from the organisation's perspective, the behaviour can be explained as the rational choice of the criminal (Cornish & Clarke, 2008). Cornish et al report that the rational choice perspective offers a way of looking at offending from the attackers perspective and it's environment as a whole, the environment of every day life, lifestyle and instrumental action to achieve particular goals. Furthermore, the criminal behaviour is broken down into concepts to describe it. First, crimes are committed with a purpose and committed with an intention to benefit the attacker. Secondly, the crime is rational, which is means that the attacker will try to achieve the goal with the best available means available. Thirdly, the decision-making is crime specific in terms of motives for committing the crime, every single crime, may it be the same sort of crime can distinguished by the choices and decisions the attacker made. The other aspects are decision-making models. With the rational choice perspective it is possible to better understand what is required and what is possible or likely to happen for an attacker to possibly disrupt supply chains of industrial devices.

2.7.3 Threat Actors

Threats to the industrial devices can come from numerous sources. These sources include for example opposing governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders. It is important to distinguish these adversarial sources because they have different capabilities and sophistication. To do this, Fabro et al is consulted because his work resembles a very helpful taxonomy of a substantial amount of threat actors with their motivation. The list that is created by Fabro et al (Fabro, 2012) shows from an attackers point of view the possible threat actors and how they can be understood in groups. Because many threat actors are also double mentioned in different groups, a truncated version of this taxonomy can be seen in Appendix C. Fabro et al describes that for analysis of threats to ICS in general the taxonomy can be used to to help identify the origin of the threat. The taxonomy is a very exhaustive list of possible threat actors and threat origins which also include accidental sources for example. Because of the supply chain characteristics and the reasoning from criminology point of view that are explained above in this chapter. It is chosen to focus on the criminal intention of the threat actors because that is the easiest to comprehend. Therefore the list in Appendix C only contains the class "deliberate" to identify threat actors. When looking at the taxonomy of Fabro et al and leaving out the specific activity the relevant distinctive threat actors for embedded devices that traverses the supply chain can be grouped. These threat actors can all have a motive to target the supply chain to pursue their goal.

Military and Paramilitary An opposing government has motives that relate to cyber warfare to cause a threat. Their financial capability is great and their knowledge to cause a threat as well. However this category threat actor would be more of a concern for critical infrastructures instead of ICS in other sectors. Unless that country has special interest in the type of industry where an ICS is operative.

Hackers from a specific faction Hackers that are involved in a conflict and are part of a specific minority group or faction that operates from their beliefs and values can cause a threat to ICS. Their intention is probably triggered by activities that are against their values and beliefs, like when industrial operations touch ethical and environmental values. The knowledge required to cause a threat is present and financially they could be capable as well as having a clear goal. Activists also belong in this category.

Foreign Intelligence Services When an opposing government uses its intelligence agency to pursue valuable information about ICS this can form a threat in the supply chain. This adversarial group has a lot of financial capabilities and knowledge at their disposal.

State sponsored organisations Organizations that work together to gain a combined goal from the targeted ICS.

Companies that work with news media However controversial, news media and the companies that work together with news media can pose a threat as well. Either to highlight flaws that have been investigated for dishonest sales gains for the particular company in question or to gain confidential information. Or to just demonstrate vulnerabilities.

Other organisation/state or competitor In the same market a competitor has a motive to cause a threat by wanting to gain confidential information on the industrial process to use in their advantage.

Hacker groups/individuals Hacker groups can vary from small script kiddies towards organised hackers groups. A distinctive property would be the financial capabilities and knowledge to cause a threat. Also, organised hacker group have a more serious and persistent motive to cause a threat. So, this adversarial group can be further grouped into the extent to which they are capable to use sophisticated means. More sophisticated groups can also use 'automata', that are botnets of infected computers around the world that can perform several attacks.

Disgruntled employees After employees have lost their jobs or didn't get the promotion they were hoping for there could be a such a feeling of revenge. These employees have a great motive to either deliberately pose a threat themselves or get involved in something bigger and aid that with their inside knowledge. I terms of capabilities this threat actor mostly has inside knowledge and not the financial capabilities.

Insider. An insider is someone who is employed at the company that is targeted and has access to confidential information or perimeters that are needed to cause a threat. An insider can also be referred to as a disgruntled employee, their motives are generally less serious however they could be part of an organised group which would mean they are actually working for a competitor or organised group instead. Capabilities are similar to a disgruntled employee however financial capabilities are much bigger.

Outsider threat actors that are contracted to cause harm somewhere are referred to as outsiders.

Counterfeiters Criminal(or legal in certain places in the world) group or organisation that have the ultimate goal to steal intellectual property, reverse engineer and build a fake cheaper product.

2.7.4 Threat element: intention

As is explained above, one of the components of a threat is the intent. The intent is the ultimate desire of the threat actor and is the reason of performing one of the activities in the list above. For cybercrime against ICS we can define a few general but clear intentions the attackers can have. We can learn this from the reported incidents, the above mentioned activities and from infamous dossiers like Stuxnet and others.

Sabotage. After Stuxnet it really became clear that cybercrime is capable of actually destroying devices. Therefore this is the most severe type of disruption; sabotage. The goal of sabotage is known as deliberately destroy, damage, obstruct something, especially for political or military advantage. Other sub categories of intention that belong to sabotage could be the intention to delay production or to delay the creation of new factory. Decreasing the competitive advantage is another important intention to take into account with deliberately sabotaging. Sabotage can also be used to ultimately damage the reputation, both can be considered as decreasing competitive advantage.

Espionage. Other reported incidents have a different goal then Stuxnet. In Duqu, Flame and Red October it is found that they have at least one thing in common and that is that they are malware specifically designed to target ICS. Although not as sophisticated as Stuxnet, they are used to send gathered information about the infected ICS to the attackers, probably for industrial espionage. However can serve multiple purposes, some incidents reported key loggers which sent passwords that were used. Other incidents sent information about the production process or configuration of the process. The goal of these kind of attacks can be described as espionage, the information can be used in advantage of other businesses or governments. Espionage is known as the practice of spying or usage of spies. Typically done by the governments to obtain political and military information. Gaining competitive advantage by getting sensitive data is also part of this intention.

Financial Gain. What the two mentioned goals have in common is both specifically target an ICS. The knowledge that is required is dependent on the specific industrial process. The third goal does not share that characteristic and is independent of the target ICS. When attackers produce fake products that require less costs because the materials are of less quality or they steal intellectual property from circuit boards and software packages they are after financial gains. Furthermore it is possible to disrupt a device that is used to measure and report production quantities. This could be used to blackmail or illegally tap off water or oil and at the same time fake the production results so that it would take some time for this kind of theft to get noticed.

2.7.5 Threat element: capability

What we can learn of the reported incidents are the capabilities and means of the attackers to reach their goal. The specific goal of the attacker(s) also become more clear by analysing what has been reported and what is shown in literature about attacking PLCs/PACs. As mentioned above in this chapter the embedded device can be split up into 3 distinct categories. From a Software, Firmware and Hardware point of view the incidents and vulnerabilities are investigated. So for example, incidents that include a denial-of-service attack of the distributor's website so that it can't fulfil front-end order are out of the scope as the focus is on the embedded industrial device that traverses of the supply chain.

The literature and reported incidents describe five possibilities which are explained in detail below. It is structured in the order of abstraction: first from a software point of view, secondly from a firmware point of view and lastly from a hardware point of view.

Trojanized software. Recently an incident was reported about trojanized software or malware (Symantec, 2014). A group of attackers used legitimate software of several manufactures of PLCs and infected it with extra software packages. One of the packages that was identified installed a VPN client on the device which would make remote access possible. The trojanized software was made available for download as 'genuine software' on the manufacturers' own website. The manufacturers hosted the software that was originally intended to do software updates. However instead of performing a genuine update, the update would trojanize the devices which enabled unauthorised access. This can be certainly a supply chain threat because in the process of updating and maintaining the device the manufacturers' website could be used. The updating and maintaining is mostly done by manufacturers, solution providers, distributors and also asset owners. This particular incident has been reported to be carried out by a group of attackers called Dragonfly and shows a new attack vector of targeting PLCs. Depending on what the trojanized software could do, it can be said that the trojanized software could be used for either sabotage or espionage, and perhaps as a leverage for financial gains. It could be transferring incorrect data while sabotaging the process. Also, espionage could be reached in the same way such that the device that has been tampered transfers information to a malicious destination. Other motives to perform this kind of attack is to steal intellectual property of the current genuine software in order to create similar working software (Symantec, 2014).

Install or use backdoor. An other way to gain access to devices is to use hardcoded backdoors in the software that are used by developers to more easily gain access to the device during testing for example. As is thoroughly described by Santamarta (Santamarta, 2011), these hidden authorisations can be retrieved with the right know-how. When this is achieved attackers could gain access to the root of the device in order to change or insert software.

Firmware modification. Basnight et al shows the ease of retrieving and reverse engineering firmware, during the firmware loading process they use a packet sniffer to retrieve the versions. Then, by binary code inspection in multiple firmware versions available from the OEMs webpage, the most suitable version is selected and changed. Ultimately they show that they successfully load a modified firmware on the device (Basnight, Butts, Lopez, & Dube, 2013). Because this is relatively easy to achieve with tools that are also widely available it is therefore likely that threat actors are also capable to do this. The requirements to achieve this kind of tampering would be physical access to the device and time to figure out what version could be best modified by binary code inspection. Also, reverse engineering and modifying the firmware to reach one of the goals will take some time. The actual loading of the new firmware does not take as much time. The firmware is directly located on the device flash memory and is used to enable functionality of the device even when there is no Operating System present.

Hardware counterfeiting. Counterfeiting can be performed by recreation of the device or one of its components and replacing it with lower quality materials. It requires physical access to the device. When the threat actor knows the location and destination of a shipment it can insert counterfeited products that don't work properly or completely make a replica of the device and sell as genuine. The intention would then be sabotage. In many other cases hardware counterfeiting is done with the motive for financial gain, selling a cheaper alternative of the same product. Guin et al show the rising threat of counterfeiting semi-conductors parts in the global supply chain (Guin et al., 2014). As PLC/PAC have become sophisticated computers, this can be considered a threat.

Intellectual Property Theft Many companies protect their devices by registering Intellectual Property(IP) and patent parts that are genuinely innovative. When IP gets stolen it can damage the company financially. Intellectual property can be in the form of circuit boards, pieces of software or amongst others blueprints of a certain ICS solution. Whereas hardware counterfeiting is replacing an existing product with fake parts or a fake product, Intellectual Property theft on the other hand is the unauthorised use of protected parts or protected design of devices in new devices.

Stuxnet, Red October, Flame, Duqu Virvilis et at describe the advanced persistent threats that lure on ICS and they state that probably since years many systems have been infected with these malware. They also have been reverse engineered to find what their purpose is and for all but Stuxnet it is found that they only leak information to another destination, thus spying on in the industrial process. Stuxnet had the purpose of deliberately sabotaging the destined ICS as is described earlier in this chapter.

2.7.6 Possible Activities of Threat Actors

In section "Cyber Security" it is said that cyber security can be assessed based on the CIA model. That model was extended with the S: Confidentiality, Integrity, Availability and Safety. The possibilities that threat actors have to compromise the embedded device can be described in more detail as a breach in one or multiple of the security properties in the CAIS-model. OWASP, the free open software security community identifies five harmful activities that products in the supply chain face (Goertzel, 2010).

- Sabotage (building in malicious logic, backdoors, intentional vulnerabilities)
- Tampering (to add any or all of the above post-development)
- Counterfeiting, piracy (substitution of legitimate with illegitimate product)
- Theft (physical product, intellectual property, e.g., for reverse engineering)
- Destruction

In the supply chain context of industrial devices, a cyber threat for stakeholders in the supply chain does not occur after destruction of the device. It is a loss for the manufacturer but it does not have an impact which is cyber related. Therefore, destruction is not usable from this list. The other harmful activities can certainly end in cyber-related incidents, which leaves the list to sabotage, tampering, counterfeiting and theft. To further elaborate on the above list and to add the CIAS-model to it, the list has been broken down to activities on the industrial device. Sabotage can be translated to installing backdoors, tamper with firmware/software or OS. Tampering can be translated to tamper with sensitive data. Counterfeiting is straight forward, and theft can be translated to Intellectual Property theft.

Activities that breach Confidentiality:

- Install backdoor
- Tamper with sensitive data
- Intellectual Property Theft

Activities that breach Integrity:

- Tamper with firmware
- Tamper with software/Operating System
- Tamper with sensitive data

- Counterfeit hardware
- Intellectual Property Theft

Activities that breach Availability:

- Stop the internal logic
- Shutdown device

Activities that breach Safety:

- Counterfeit hardware
- Tamper with internal logic

This list shows from the knowledge of OWASP the possible actions that can be done to an industrial device. This list will be used in the next chapter to model threats using attack trees.

Chapter 3

Threat Analysis

In this chapter the focus is on the embedded industrial device that traverses the supply chain. The goal of this chapter is to describe the possible threats by its goals and origin. To do this, a threat model is created that represents what an attacker could accomplish in the supply chain. The knowledge required for that is obtained from the list of threat actors that is described in Chapter 2. Also, the use of attack trees is described in Chapter 2. This method is used to model four attack scenarios in the supply chain. Next to that, the possible attackers are analysed and grouped in terms of Knowledge, Financial Capabilities and Persistent intention. The modelled attack trees and the threat actors capabilities are validated by expert opinion. After which it can be assumed which actors is able to perform which attack tree. From the incidents and activities that are described in Chapter 2 it is looked at how these can be translated in the supply chain. These findings combine as the threat model and this chapter will answer *SQ2: What are the possible cyber threats towards industrial embedded devices?*.

3.1 Used definitions and methodology

What can be recalled from Chapter 2 is the definition of a threat. The definition that is used for this research is: ”the potential for a threat source to exercise a specific vulnerability” (NIST, 2002). Where the ”potential” can be described as a combination of the ”capability” and the ”opportunity” to exercise a ”vulnerability”. However, the threat source must also have an ”intention”. So, the term threat can be best defined as the following equation:

$$Threat = Capability * Intent * Opportunity \tag{3.1}$$

This equation means, as is described by Kang et al (Kang et al., 2009), that the source of a threat must have the following:

- an intention such as a clear goal or motivation;
- the capability in terms of financial or knowledge and;
- must be given the opportunity to form a threat such as having access to a location of a vulnerability.

What can be concluded from the definition above is that an understanding is needed of threat source. In this research it is referred to as threat actor. A comprehensive list can be found in Appendix C. Already in Chapter 2 this list was truncated to be used for this research. Next to threat source, the intention was described namely Sabotage, Espionage and Financial intention. In this chapter, the possibility for a threat source to cause a threat is researched as follows: First, the possible harmful actions toward an industrial device in the supply chain is modelled as attack trees, then actors are analysed on their capability to perform such action and together with the intention the threat actor has this will be combined as the threat model. Before the actual threat model is created, the modelled attack trees and the analysis of the capabilities of the threat actors is validated using a expert opinions. Interviews were performed for this. Additionally, in Chapter 2 the use of attack trees is explained, this methodology is used to draw the attack trees below.

3.2 Modelling of Attack Trees

3.2.1 Attack trees in supply chain context

In Chapter 2, the threat actors capabilities is described and further broken down to activities that can be performed on the industrial device. From this list of activities, four activities are selected on three criteria. The selection is based on distinctiveness, so that attacks that are almost the same won't be modelled twice. The selection is also based on difference in impact, so that each of the security properties is covered. Lastly the selection is based on the different device layers (hardware, firmware, software) The activities that meet these criteria are:

1. Tampering with firmware or software;
2. Install backdoor;
3. Hardware counterfeiting;
4. Intellectual Property theft.

3.2.2 Attack tree 1: Tamper with firmware

As can be seen in figure 3.1 to tamper with firmware/software three possibilities can be achieved by a threat actor, given the fact they have the knowledge and ability to modify the firmware. To then tamper with the firmware on the device physical access is required. This can be obtained by several ways, but it is required to infiltrate the loading process and/or the location where the devices are. Access to these locations could be obtained by working together with an insider, or to social engineer access to the location by pretending you are someone else. Also, at different actors it could be possible the threat actor is working together to gain access. Another way of achieving this as is described in Chapter 2, the 'Threat element: capability' section, is to make the malicious firmware available for download which requires certain credentials to achieve.

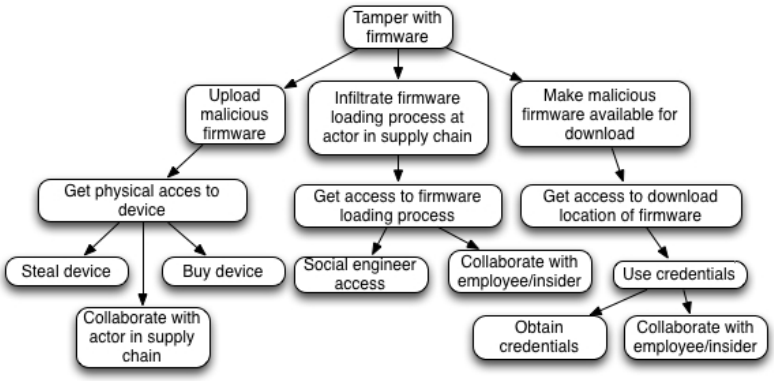

Tamper with firmware
Upload malicious firmware
Infiltrate firmware loading process at actor in supply chain
Make malicious firmware available for download
Get physical acces to device
Get access to firmware loading process
Get access to download location of firmware
Steal device
Buy device
Social engineer access
Collaborate with employee/insider
Use credentials
Collaborate with actor in supply chain
Obtain credentials
Collaborate with employee/insider

Figure 3.1: Attack Tree: Tamper with firmware/software

3.2.3 Attack tree 2: Use backdoor

In figure 3.2 the attack tree of using a backdoor can be seen. To achieve this it is required that either access to an existing backdoor or access to the firmware is required to program a new backdoor. To access an existing backdoor physical or logical access is needed to the device which can be obtained by either collaborating with an employee or to obtain the device by stealing or working together with an actor in the supply chain.

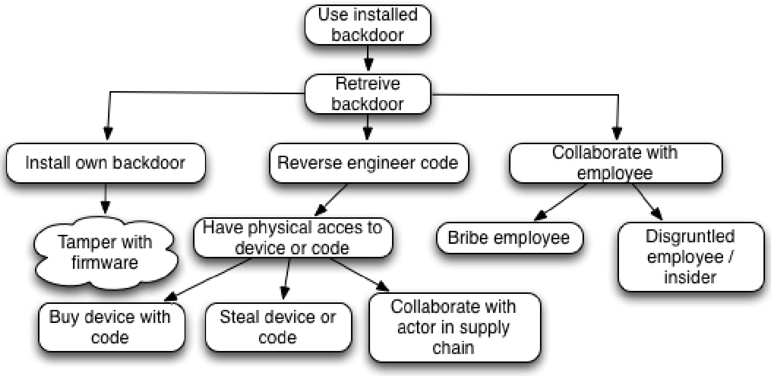


Figure 3.2: Attack tree: Use backdoor

3.2.4 Attack tree 3: counterfeit hardware

What can be seen in figure 3.3 is the attack tree to counterfeit with hardware. There are two possible ways to do this, namely to replace an existing device with a one or more counterfeited components or to fully make a valse replica of the device. The difference is in where this would take place, fake components will happen in upstream supply and fake replica's will happen in downstream supply. It is required for a threat actor to have access to the location of the shipment or act as a supplier/retailer/distributor in order to infiltrate the supply chain.

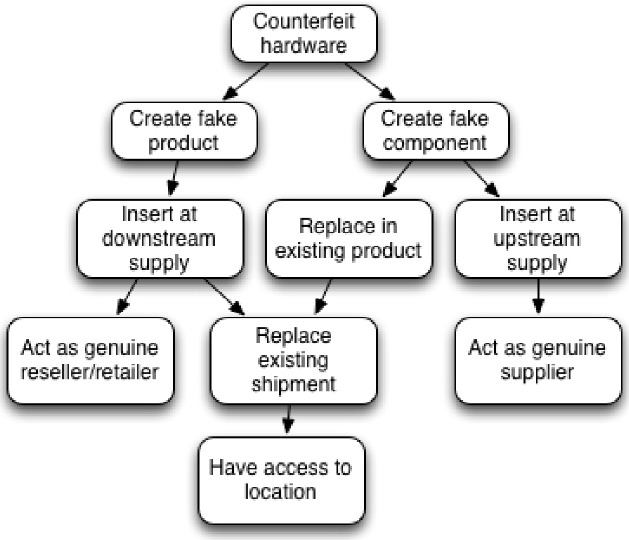

Counterfeit hardware
Create fake product
Create fake component
Insert at downstream supply
Replace in existing product
Insert at upstream supply
Act as genuine reseller/retailer
Replace existing shipment
Act as genuine supplier
Have access to location

Figure 3.3: Attack tree: Counterfeit hardware

3.2.5 Attack tree 4: Intellectual property theft

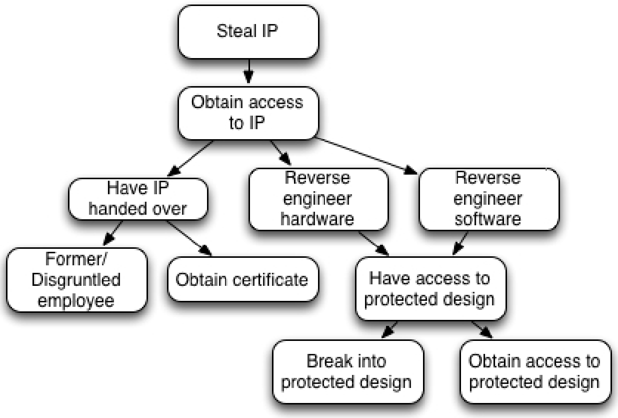

Steal IP
Obtain access to IP
Have IP handed over
Reverse engineer hardware
Reverse engineer software
Former/ Disgruntled employee
Obtain certificate
Have access to protected design
Break into protected design
Obtain access to protected design

Figure 3.4: Attack tree: Intellectual Property Theft

In figure 3.4 the attack tree of stealing intellectual property can be seen. The tree concludes as obtaining access to a protected piece or the whole device. Legally this can be done by getting a certificate to use a patent if that is possible but if you are a threat actor other means can be used to obtain the Intellectual Property. Either through former employees, insiders or perhaps disgruntled employees.

3.3 Analysis of attack tree requirements & threat actor capabilities

Based assumptions leading from the literature that explained the capabilities in Chapter 2, the attack trees are grouped into what would be required to exercise the attack. As firmware modification is shown to be done with relative ease, the knowledge required is medium, not low because there is some technical knowledge required. To actually modify the firmware and to perform such an attack in the supply chain the costs can rise because of required tools, programmers or bribing people for example. This isn't the case at Use backdoor, therefore the knowledge is medium and the financial requirement low. Hardware counterfeiting is considered as both high because of the materials that is needed and knowledge to actually replicate a device. Intellectual property theft is considered low on knowledge required and medium on financial. A brief summary of these assumptions and the rationale is given below in 3.1.

- The attack tree 'Tamper with firmware' could be achieved with rather simple organisation and also a low budget but with a lot of knowledge, depending on the severity that is intended. Really complex modifications for sabotaging through firmware will be more costly and requires more knowledge.
- The attack tree 'Use backdoor' does not require a lot of financial capability for an threat actor but it does require some knowledge.
- The attack tree 'Counterfeit hardware' requires well organisation and financial capabilities together with knowledge that is needed to create a replica. To replace fake components like connecting cables this would be less.
- The attack tree 'Intellectual Property theft' does require a lot of knowledge because no special skills are involved in obtaining the IP, to use it on the other hand would require more knowledge. The most striking requirement is persistent capability because if an threat actor doesn't have the goal to use the Intellectual Property it is not very attractive target.

3.3.1 Analysis capabilities of threat actors

A threat actor can be fully understood if their capabilities can be estimated. The capabilities can be separated in knowledge, financial capabilities and persistent intention. In Chapter 2 the whole list of threat actors is described, as the author of the report states the actors where analysed specifically for ICS domain, the list is used in this chapter too. After it is assumed which threat actor has what kind of capabilities, they can be mapped on the attack trees which will create Threat Model. The summary of these aspects can be found in table 3.2.

Attack tree	**Knowledge required**	**Financial requirement**
Tamper with firmware/software	Medium	Medium
Use backdoor	Medium	Low
Hardware counterfeiting	High	High
Intellectual Property Theft	Low	Medium

Table 3.1: Capability requirements for the attack trees

Threat actor	Knowledge	Financially capable	Persistent intention
Military or Paramilitary	High	High	High
Foreign Intelligence Services	High	High	High
State sponsored organisations	Medium	High	Medium
Other organization/state or competitor	High	Medium	Medium
Hacker groups	High	High	Medium
Hacker individuals	Medium	Low	Low
Companies that work with news media	Medium	Medium	Low
Disgruntled employees	Low	Low	Medium
Insider	High	Medium	Medium
Outsider	Medium	Medium	High
Activists	Medium	Low	High
Counterfeiters	High	Medium	High

Table 3.2: Differences in capability of threat actors

3.4 Expert Interviews

3.4.1 Interview Setup

Two professionals in the area of IT security and the ICS domain in The Netherlands were interviewed as part of the validation of the above mentioned attack trees and assumptions on capability of the different threat actors. The IT domain means expertise in IT in general, the security domain means expertise in IT Security topics like governance, risk and compliance and among others technical security reviews. The ICS domain and industrial device context means expertise in technical requirements to cause a threat, knowledge of threat actors and capabilities and furthermore knowledge and experience of the ICS domain in terms of trends, developments and current state. The IT professionals are both very experienced in the domain of IT security and ICS as they have a strong background in technical security reviews and have been involved in many project involving ICS.

The author of this research first introduced the threat analysis methodology to the interviewees, then explained the goal of the discussion. From there on, the attack trees were explained, and all the steps were showed. This was all done with the help of images and diagrams that can also be found in this research. In several occasions, the interviewer and interviewee elaborately discussed different topics and items that supported the research. Especially the different attack trees led to interesting questions of if they would work in reality like they are modelled. At the end of the interview, there was time to discuss whether or not the attack trees and table with capabilities would be representing a real case threat scenario. Furthermore, the usefulness of the mapping of the attack trees and actors' capabilities were discussed at length with these different interviewees.

3.4.2 Interview results

This section summarises the results of the expert discussion group. First, a general discussion on the selection of types of attack trees has taken place. After which each attack tree and the two tables with assumptions on requirements and capability are discussed. Finally, the discussion can be concluded in main improvement points which are processed after.

General discussion: At first the discussion started about the choice of the activities. The reaction from the expert group was that the activities chosen are common sense and should be chosen. There are more possibilities but based on what is applicable on supply chain context these activities should certainly be used. The group replied with another expert source: OWASP to rationale behind the activities.

Attack tree: Firmware tampering: Layer by layer the attack tree is discussed. On the first two layers no comments were made and they agreed on these possible branches. The main point of discussion at first was that in the nodes resulting from "Get access to download location of firmware" the "Obtain credentials" is too broad. It was suggested by the expert group to make it more clear that 'steal' or 'guess' would be added to that node. Furthermore, the "Get access to download location of firmware" node is not really from a threat actors point of view. In order to get access a threat actor needs to perform a hack or another type of activity. Next to that, the discussion went on about the node "Get access to firmware loading process" and the resulting nodes. The expert group shared the opinion that only the human-factor is taken into account and not the technical factor. A threat actor can also have technical access by a website or ftp service for example to access the firmware process. The expert group agreed on the other activities and nodes.

Attack tree: Install backdoor: First of all, the expert group shared their opinion about attack tree with 2 succeeding root nodes. That is not possible and not logical. Furthermore, it is ambiguous that to retrieve a backdoor, the threat actor first needs to install a backdoor. Next to that, with respect to the supply chain of industrial devices, the attack tree wouldn't be "Use installed backdoor" but rather be "Install backdoor" as the backdoor will probably be utilised after the device is operative and not directly in the supply chain. Finally, about the nodes resulting from "Collaborate with employee", it is inconsistent with the other attack tree: firmware tampering. It was advised by the expert group to use the same level of detail in the figures. The expert group further agreed on the other activities and nodes.

Attack tree: Hardware counterfeiting: The expert group noted that this was a straightforward attack tree and not much can be added or changed. The distinction between upstream and downstream supply was clear. The main point of discussion was that acting as somebody else can be said as 'social engineering', however it was clear the way it was written down in the first place. The expert group further agreed on the attack tree.

Attack tree: Intellectual Property Theft: First, the expert group noted that the root of the attack tree showed the same modelling fault as the attack tree: install backdoor. The ambiguous nodes in the top was advised to be changed by the expert group. Furthermore, the node "Obtain Certificate" was too vague to be meaningful in this context according to the expert group and lastly "Collaborate with employee" is not used consistently in this attack tree as well. The expert group advised to use the same layer of detail as the other attack trees. Next tot that the "Have access to protected design" nodes was unclear as well as being documentation in the opinion of the expert group. The expert group advised to be more clear on the part that means encrypted or safeguarded IP and further agreed on the other resulting nodes.

Table: Attack tree requirements: Continuing with the discussion to validate the tables with assumption on the requirements of the attack trees. The expert group immediately replied that, from their experience, it is very hard to estimate the financial requirements and they also noted that this is highly dependent on ICS sector and scale of the attack. The financial requirement cannot be generalised in this way. This results in only being able to allocate the threat actors based on knowledge required. Although, initially the method was to determine for both attack trees and threat actors the financial and knowledge requirement and capability and then match each other, this was strongly dissuaded by the expert group. The discussion led to the point where based on the expertise, knowledge and experience in IT security and the ICS domain of the expert group the threat actors could be allocated to the attack trees.

Table: Threat Actor capabilities: So, instead of discussing the capabilities belonging by the threat actors, the discussion was set forth the allocation of threat actors to the attack trees. The result was the following table which is now based on the experience and knowledge of the expert group. Furthermore, about the list of threat actors the expert group had one addition, that disgruntled employees, insider and outsider are actually the same and it was not necessary to separate them.

Final remarks on the models and tables: Finally the discussion of the expert group was brought to the intention of the threat actors. The expert group agreed on the what was initially assumed on the persistent intention of the threat actors. The validated intention

Improvement points The main improvement points that resulted from the expert interviews can be summarised in the list below. In the section succeeding that the improvement points are processed and the renewed figures and tables are shown on which the threat model is based.

- Don't use ambiguous double root node attack trees
- Use consistent level of detail with "Collaborate with employee" node
- Model from threat actor point of view and technical point of view
- Determine financial requirement too hard, allocate threat actors directly from experience and knowledge

3.4.3 Update of attack trees and tables

Below you can see the updated attack trees that resulted from the expert group opinions described above. The red text in the nodes is what has been changed according to the expert opinions and the red double lines is what have been removed according to the expert opinions.

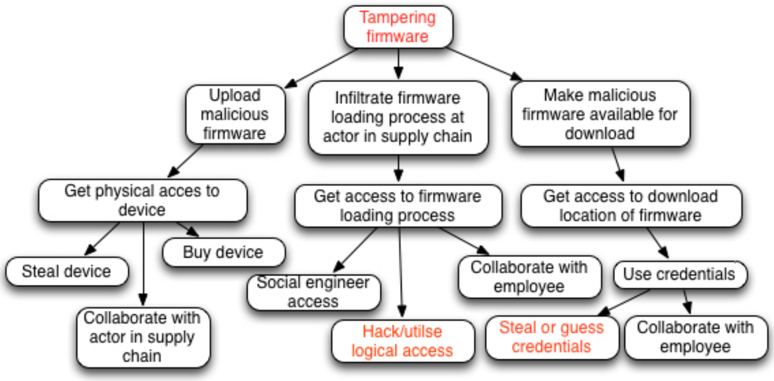

Tampering firmware
Upload malicious firmware
Infiltrate firmware loading process at actor in supply chain
Make malicious firmware available for download
Get physical acces to device
Get access to firmware loading process
Get access to download location of firmware
Steal device
Buy device
Collaborate with actor in supply chain
Social engineer access
Hack/utilse logical access
Collaborate with employee
Use credentials
Steal or guess credentials
Collaborate with employee

Figure 3.5: Attack Tree: Tampering firmware/software *revised*

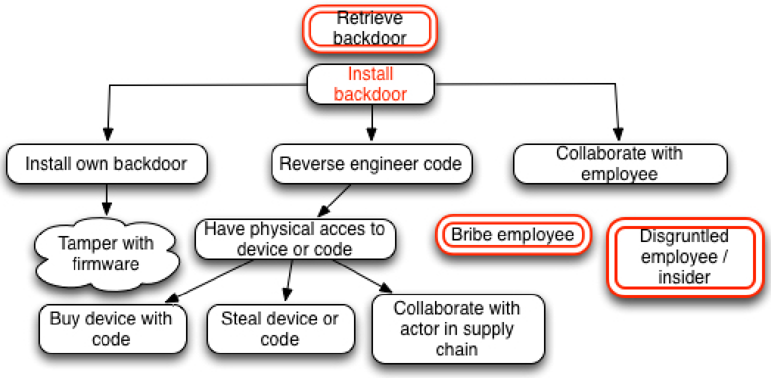


Figure 3.6: Attack tree: Install backdoor *revised*

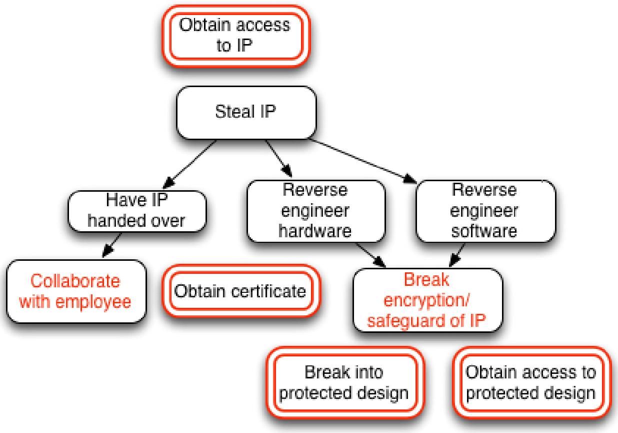

Obtain access to IP
Steal IP
Have IP handed over
Reverse engineer hardware
Reverse engineer software
Collaborate with employee
Obtain certificate
Break encryption/ safeguard of IP
Break into protected design
Obtain access to protected design

Figure 3.7: Attack tree: Intellectual Property Theft *revised*

Additionally, the table with requirements and capabilities have been discussed with the expert group. The resulting adjustments can be seen in table 3.3.

3.5 Concluded Threat Model containing scenario's and impact

When the equation is combined we can derive the threats that would be possible. So the expert opinions showed the capabilities of the threat actors and attack trees. Additionally, the second variable in the equation was intent, that was described as Sabotage, Espionage or Financial gain.

The persistent intention that can be read in the table 3.2, which was validated by the expert group, is taken into account as well. For example: counterfeiters wouldn't be persistent in installing backdoor because that requires a whole different operation than they are active in. These findings combine as the threat model and this will answer *SQ2:*

Threat actor	**Capable of performing which attack trees**
Military or Paramilitary	all modelled attack trees
Foreign Intelligence Services	all modelled attack trees
State sponsored organisations	all modelled attack trees
Other organization/state or competitor	all modelled attack trees
Hacker groups	Tampering with firmware, Install backdoor, IP Theft
Hacker individuals	Tampering with firmware, Install backdoor, IP Theft
Companies that work with news media	Install backdoor
Disgruntled employees	Tampering with firmware, Install backdoor, IP Theft
Activists	Install backdoor, IP Theft
Counterfeiters	Tampering with firmware, Hardware counterfeiting, IP Theft

Table 3.3: Differences in capability of threat actors, revised

What are the possible cyber threats towards industrial embedded devices?. The answer is provided in the mentioned table and can be seen below.

3.6 Summary

In order to fully understand the threats, the threat equation is used. A threat is the result of capability, intent and opportunity. Usage of the equation has to start with an understanding of what is possible to achieve on the devices in the first place. The found possibilities form the literary and incident research cover the three distinct layers of the device, hardware, firmware and software. On the lowest abstract layer it is possible to counterfeit parts of hardware or fully replicate a device, designs of circuits that are intellectual property may be stolen as well. On the firmware layer it would be possible to utilise a backdoor or tamper with firmware by modifying the firmware and load it on the device. On the software layer the software could be maliciously infected by malware, or parts of intellectual property may be stolen.

By using a narrowed down list of threat actors the most relevant threat actors are listed. Based on the literature and expert interviews their financial capability, intention and knowledge are validated. To further understand the threats the most intrusive possibilities are modelled as attack trees against the device that traverses the supply chain. Then, these attack trees are also investigated on what would be required to perform the attacks. The found capabilities and intention together make up the overview of the threats and who can perform it. The resulting threat model represents a theoretical model of the possibilities in the supply chain. The long list consists of all possible equations between opportunities, intention and capability. A total of 35 threats make up the theoretical list of threats.

Threat	**Attack tree**	**Intent**	**Threat actor**	**CAIS**
1	Tamper with firmware/software	Sabotage	Military	Availability, Integrity, Safety
2			Opposing Government	
3			Foreign Intelligence Service	
4			Hacker Group/faction	
5			Disgruntled employee	
6			Competitor/organisation	
7		Espionage	Opposing Government	Confidentiality, Integrity
8			Opposing Government	
9			Foreign Intelligence Service	
10			Hacker Group/faction	
11			Disgruntled employee	
12			Competitor	
13		Financial	Hacker group/faction	Confidentiality, Integrity
14			Disgruntled employee	Confidentiality, Integrity
15	Install backdoor	Sabotage	Military	Availability, Integrity, Safety
16			Opposing Government	
17			Foreign Intelligence Service	
18			Hacker Group/faction	
19			Disgruntled employee	
20			Competitor/organisation	
21			Activist	
22		Espionage	Opposing Government	Confidentiality, Integrity
23			Opposing Government	
24			Foreign Intelligence Service	
25			Hacker Group/faction	
26			Disgruntled employee	
27			Competitor	
28		Financial	News media	Confidentiality, Integrity
29	Hardware Counterfeiting	Financial	Counterfeiters	Availability, Integrity, Safety
30			Hacker Group/faction	
31			Competitor/organisation	
32	Intellectual Property Theft	Financial	Foreign Intelligence Service	Integrity, Safety
33			Hacker Group/faction	
34			Disgruntled employee	
35			Competitor/organisation	

Table 3.4: Threat Model

Chapter 4

Analysis of the Supply Chain of Industrial Devices

The goal of this chapter is to understand possible supply chain vulnerabilities and the supply chain of industrial devices in terms of differences with the traditional ICT supply chain. By mapping the threat model and attack trees on the supply chain overview, the location of vulnerabilities can be analysed. Also, the mapping will give an idea where the threats might be occurring and what the stakeholders of the supply chain should be aware of. The findings of the mapping will serve as input for the interviews that will be done to test the threat model in real cases. This chapter will answer *SQ3:What are the possible vulnerabilities in the supply chain of industrial embedded devices?*.

4.1 Used definitions and methodology

In Chapter 3 possible cyber threats are analysed, in this chapter the supply chain vulnerabilities are analysed. In this research the following definition for vulnerability is used: *"A weakness in a system or it's security procedures, internal controls or implementation of the controls that could be exploited or triggered by a threat source. Moreover, it is any weakness in the system or component design, development, manufacturing, production, shipping and receiving, delivery or operation that can be exploited by a threat actor to degrade the performance of a system that supports the mission."*

In Chapter 2 a literature study is performed on the lifecycle of the industrial device and the belonging stakeholders of the supply chain. The resulting list of stakeholders can be seen below.

- Device Critical Component Manufacturers & Suppliers
- Original Equipment Manufacturers
- Device Wholesalers
- Device Retailers & Resellers
- Device Transportation & Shipment
- System Integrators & Solution Providers
- Third Party Software Developers

- Device End-users
- Device Maintenance & FAT/SAT testing

These stakeholders together form a web of actors like a system that is described in the definition of a vulnerability. Therefore in the definition of NIST above it can be mapped on the definition as a system on a high level. It is high level because at every actor there are multiple processes in place that could be exploited separately by a threat source as well.

4.2 Comparing with ICT supply chain

The supply chain of embedded devices that are used in corporate IT systems and by consumers all over the world can be characterised by three key aspects. These aspects are discussed by Beamon as the key performance measures of a supply chain and are useful to create a comparison between corporate ICT supply chain and ICS supply chain. The first aspect is resources, which is the main driver of supply chain performance. The goal of every supply chain is to minimise resources in order to be the most efficient and cost-effective. Total costs, inventory cost and distribution cost are part of this performance measure. Second aspect is output. Output performance include customer responsiveness, product quality and also quantity of the final product produced. This results in the quantifiable measures such as sales, profit, on-time deliveries and customer-respond time. Last measure is the flexibility that represents the ability of a supply chain to adapt to changing demands therefore changing delivery dates and changing product offerings for example (Beamon, 2001). The evidence on supply chain performance can be used to understand the differences between the ICT supply chain and the supply chain of industrial embedded devices.

First of all the ICT supply chain can be seen as both business-to-consumer and business-to-business while the supply chain of embedded industrial devices is strictly business-to-business. When talking about the performance measure resources, the priority of the performance measures doesn't change because it can be concluded that in every supply chain the minimisation of resources is a key driver for performance. However, it can be argued that with products that are sensitive or destined in a critical environment, distribution costs shouldn't be sought to be reduced as much as possible. Continuing with the performance measure output, in business-to-consumer supply chains the most exposure to consumers as possible is important. Therefore quantity of final product and customer responsiveness is very important there.

In the supply chain of industrial embedded devices product quality is more important because the products are used in rugged environments for longer periods than other devices. Performance is therefore measured by more qualitative measures than quantitative measures when comparing traditional ICT supply chain with the supply chain of industrial devices. Finally, on flexibility aspect an important difference can be made in the flexibility of product mix. Because ICS in general have many different purposes even in the same sector, expertise and availability of many different products and solutions need to be present in order to meet that demand. Whereas in ICT supply chain, the newest model is usually the best choice which applies to many different solutions. These differences also come forward from the earlier mentioned comparison table 2.1. In other words, in ICT supply chain the focus lies on fast delivery and huge quantities because it is destined for the masses and at industrial devices supply chain the emphasis is on the quality of the product and quality of delivery because it is more specialised longer term business-to-business supply.

4.3 Supply Chain of Industrial Devices: Threats Overview

From Chapter 2 Hristova et al is looked at to identify the typical engineering stages of the industrial device lifecycle (Hristova et al., 2013). This device lifecycle helps to comprehend the complexity of the supply chain and the vulnerabilities of the control devices in the supply chain. In Chapter 3 possible cyber threats are analysed by modelling attack trees but how do they relate to the lifecycle phases of the industrial device? In order to map the attack trees to the different stages of the lifecycle the exact processes of the lifecycle as they are described in Chapter 2 need to be consulted. Then, letters will be assigned to each of the lifecycle phases that corresponds to the attack trees. This is marked as follows: Attack tree 1: Tampering with Firmware/software is marked as ”F”; Attack tree 2: Install backdoor is marked as ”BD”; Attack tree 3: Counterfeit Hardware is marked as ”CF”; Attack tree 4: Intellectual Property theft is marked as ”IP”.

The result of the mapping can be seen in Figure 4.1. Starting with attack tree 1: Tampering with firmware(”F”). Firmware can be tampered with during production as firmware creation and loading process is a part of the production process. It can also be tampered with during shipment because in distribution channels threat actors can interfere with the industrial devices. Furthermore, it can happen at Engineering & Customisation phase as the device is still being set up and employees, or 3rd party developers have access to the device, logically or physically. In the other phases, the question arises if tampering with firmware would be possible. It is unclear what these phases exactly are in terms of people involved and processes that are carried out. So, in the process of allocating attack tree 1: tampering with firmware to the device lifecycle phases I have encountered several questions that arise. During the literature study on the lifecycle it is shown that Factory Acceptance Test takes place after the engineering and customization phase. However, couldn’t it be in some cases the FAT is carried out by the OEM after production and before shipment? And what exactly is tested in the FAT, should it ensure that the firmware is genuine or not? These questions are valuable to ask to stakeholders of the supply chain to get more insight in this and are represented as blue ”F?” in Figure 4.1.

Continuing with attack tree 2: installing backdoor. A backdoor can be practically installed in the same phases as the firmware can be tampered with. Where there is a software or firmware development or loading involved there could be this threat occurring. The same questions arise with installing backdoors as with firmware tampering. More insight is required in the installation and testing phases of the device. For example, is software or firmware loaded during installation or during engineering or customisation? What kind of logic access is used during these phases? Also valuable questions to ask stakeholders. The blue ”BD?” represents this.

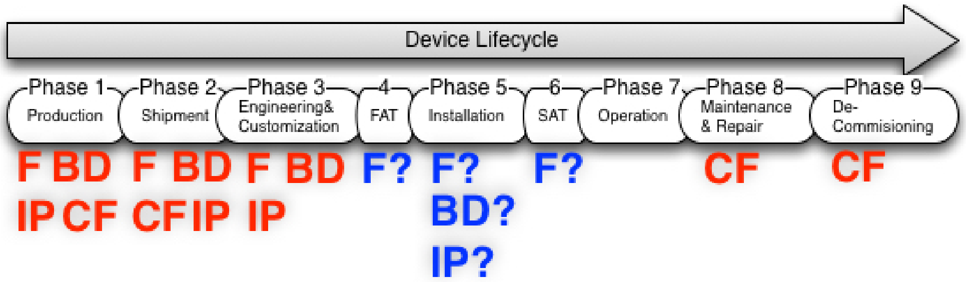


Figure 4.1: Device Lifecycle phases with mapped attack trees (F, BD, CF, IP)

Attack tree 3: Counterfeiting hardware is also mapped on the device lifecycle. In Chapter 3 a difference could be seen in upstream and downstream counterfeiting. This is resembled in the mapping on the lifecycle. Basically it can be said that in each phase where parts are insourced or in transit this could be happening. Production phase, shipment phase. Also, at maintenance & repair when parts are replaced or the whole device is replaced this could be happening.

Finally, attack tree 4: Intellectual Property theft is added to the lifecycle. This attack tree could be occurring in the production, shipment and engineering & customisation phases. The question that arises when allocating IP theft in the lifecycle is how exactly installation is performed with the industrial devices. Can 3rd parties also install solutions or separate devices in some cases? Then probably IP theft is a threat in that phase as well. The blue "IP?" represents this question that is valuable to ask.

The mapping of the attack trees can also be done on the stakeholders that have been modelled in an overview. The legend is the same as in the device lifecycle phases. The mapping of the stakeholders in the overview is a result of the mapping of the attack trees on the lifecycle phases. In Figure 4.2 two differences can be seen, one is allocation of attack trees to stakeholders directly, the other is on transitions between stakeholders.

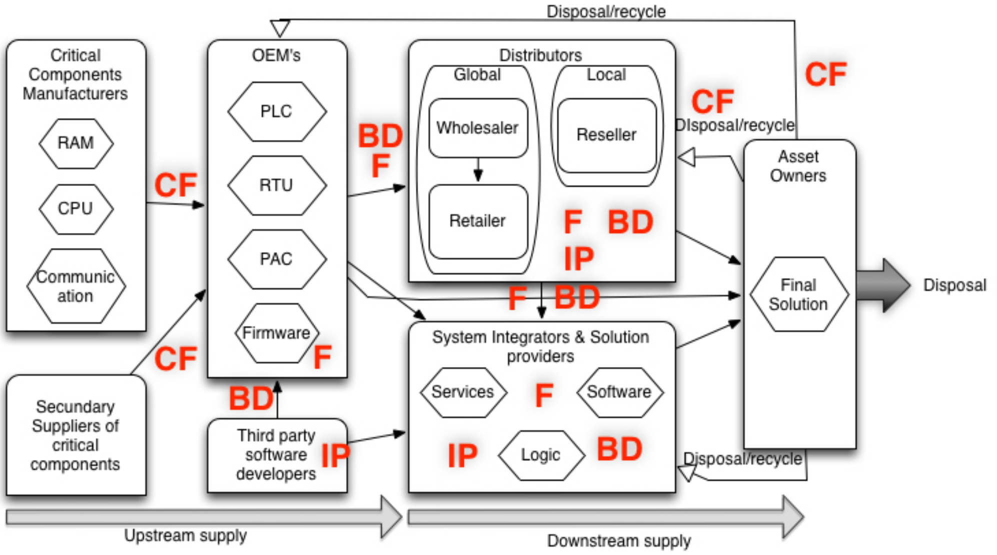


Figure 4.2: Supply Chain Overview with mapped attack trees (F, BD, CF, IP)

As is stated in the definition of vulnerability above, a vulnerability can be a weakness in a system or it's security procedures, internal controls or implementation of the controls that could be exploited or triggered by a threat source. In order to find these weaknesses in security procedures more insight knowledge is required on the different stakeholders procedures. In addition, when looking at the mapping of the attack trees on the device lifecycle and the supply chain overview it shows cyber security in the supply chain is very complex. Also, implementation of security procedures can be very costly for the stakeholders in the chain. At all phases of the product lifecycle special cyber security challenges arise (not only from the supply chain) and there are different measures that can be met in order to secure the product that passes the chain the best possible. It is possible that in one ore more phases of the lifecycle the supply chain is infiltrated with in-genuine parts or whole counterfeit products. This demonstrates that supply chain risk management is not only a matter of protecting intellectual property, customer relations, distribution and meeting the right demands with the right supply but in light of current and upcoming cyber-threats the problem might be much greater. Before the production and assembly phase, counterfeit circuit boards and memory chips might have been inserted. For example what happens when a shipment is delayed at the customs boarder? Or when it is stored in a distribution warehouse? In the engineering phase it is important to ensure the firmware and software that is loaded is actually genuine. In the FAT and SAT phases can the testers that also update the software or replace products be trusted that they use genuine parts as well? What rules apply when an asset owner disposes or returns products to its supplier? These are examples about cyber security challenges in the supply chain. It shows why cyber security is very complex and very costly for every stakeholder in the supply chain because many parties are dependent on each other and it imposes many different mitigation techniques.

4.3.1 Stakeholders' Responsibilities

When looking at the supply chain stakeholders' roles and their dependability it becomes clear that it is important to understand how collaboration takes place and under what circumstances collaboration is decided, to gain insight in supply chain security. Additionally, it is important to gain knowledge of the mitigation techniques that are already in use and if so where they are in use. It comes down to how a manufacturer chooses their distribution channels and supplier relations and for each stakeholder what they perform to mitigate cyber-threats in their development, production or shipping process. In terms of supply chain management that means it is required to gain insight in the supplier, distribution vetting process and in the measures that companies in the chain take themselves.

4.3.2 Preparing interviews with stakeholders

From the analysis of the supply chain vulnerabilities a couple of questions arise that are valuable to ask stakeholders in upcoming interviews. The questions were raised in the sections above and can be grouped as follows:

- what exactly the different lifecycle phases imply for the given stakeholder (e.g. what do you do exactly when you install devices)?
- how the given stakeholder secures production/customization/testing/installation processes of the device?
- on what basis is collaboration with suppliers/distributors decided?
- who do they think is responsible in case of an incident?

These questions will be added to the interview questionnaire in Appendix A. The questions are respectively listed as: 1.1 & 1.3(Part 1); 4.1 - 4.4(Part 4); 2.3 (Part 2); Part 3 & General Comments.

4.4 Summary

The core control devices are the RTU, PLC, PAC. The RTU is most simple device and the PAC the most sophisticated. With the added functionalities like Operating System, memory chips, improved ladder logic and more and more modules for digital I/O the devices have changed from simple obscure I/O devices towards widely available COTS-devices that use open standards. The mentioned control devices have become a much more attractive target for threat actors.

An overview is created in Chapter 2 that contains the actors that are involved before the device is operational, a device lifecycle is used and the actors that perform actions in the lifecycle are looked at. The relations between the actors make up the overview of the global supply chain of the above mentioned control devices. The supply chain is a complex globally dispersed web of all these actors. OEMs manufacture the device and supply this to distributors and resellers. The end product for the asset owner is a combination of components created by critical components supplier, 3rd party software developers, OEMs and systems integrators/solution providers. Many different parties interact with the device which makes security in the supply chain of industrial devices an important aspect in the cyber security of operative ICS.

Furthermore, the supply chain of industrial devices is compared versus a supply chain of other embedded devices. The main challenge of security of supply chains is the ability to ensure that the product that is delivered at the Asset Owner's site is genuine after it has traversed the supply chain. An important aspect that actors can take into account is how suppliers are selected. Next to that the figures above show where the threats could be occurring theoretically.

Chapter 5

Comparing with theoretical scenario's

Goal of this chapter is to show the results of the interviews which are performed at three stakeholders in the supply chain. The results are compared with the threat model of Chapter 3.

5.1 Interview questionnaire

As has been introduced in the previous chapter, the interview questions that arise from analysing the supply chain and threats. Therefore, each of the interviews is set up in multiple parts. The first part is to gain knowledge of the product and the general production process. The second part is focused on supply chain processes and relations with suppliers and transportation/warehousing. This part is necessary to get a better understanding of the PLCs that transit the supply chain. Next to that, information about reported incidents and control measures is asked in the questionnaire. In addition, criteria that the companies have with selecting new suppliers or collaborations is also an important question that is added. This question will give an idea to what extent the companies are aware of threats in the supply chain. The main interview questions are visible in Appendix A.

In total three interviews are done with three different stakeholders of the supply chain in an open format. The first stakeholder is an Original Equipment Manufacturer. The second is an solutions provider and the third is an asset owner. The biggest difference is that the OEM is active in many industries and there two stakeholders are active in only one. As some information might be too sensitive to be shared it is chosen to perform the interviews in a free format discussion, trying to cover all aspects of the questionnaire and to not increase the pressure by making the interview more like an interrogation. This way more honest and reliable answers will probably be given. The interviews serve as additional knowledge in the complex supply chain of industrial devices.

When describing the interviews, the finding or conclusion is made **bold** after which the reference from the interview is presented in *italic*. The **bold** text does not resemble interview questions.

5.2 Interview 1: An Original Equipment Manufacturer of PLCs/PACs

The first case study is from the perspective of an Original Equipment Manufacturer. They offer a wide range of electrical engineering- and electronics-related products and services. Its products can be broadly divided into the following categories: buildings-related products; drives, automation and industrial plant-related products; energy-related products; lighting; medical products; and transportation and logistics-related products. The OEM's drives, automation and industrial plant-related products include motors and drives for conveyor belts; pumps and compressors; heavy duty motors and drives for rolling steel mills; compressors for oil and gas pipelines; mechanical components including gears for wind turbines and cement mills; automation equipment and systems and controls for production machinery and machine tools; and industrial plant for water processing and raw material processing. Thus it can be said they have expertise in many sectors where ICS are used in and have a wide range of products they offer to their customers, therefore the OEM is one of the largest manufacturers of industrial equipment that is active in well over 100 countries.

In appendix D the interview is written down in the interview format. The interviewee is an employee of the OEM and as a Product Manager he is responsible for the supply of new products. The interview has taken place in the headquarters of the OEM, below are the most striking findings:

D1.1 **The products are indeed mostly COTS products, as for the customised products there is almost no demand.**
Interviewee: We mainly sell PLCs, and over the past few decades these products have been developed from very simple I/O devices towards much more sophisticated devices with numerous TCP/IP ports and Operating Systems. They are usually operative for at least 10 to 20 years. We also manufacture HMI's and the necessary measurement devices for a complete solution. The products are also mainly COTS products; as for very customised products there is almost no demand.

D2.3 **New collaborations are selected on quantitative criteria like delivery time and amounts of goods sold**

D2.3 **Collaboration with systems integrators however, the OEM can provide whole solutions to asset owner if demanded**
Interviewee: Of course not everyone is allowed to sell our products, the distributors who want to sell our products are selected and assessed based on some criteria. These criteria are mainly amount of goods sold, delivery times and if they have the required knowledge of our products to configure them for example. We have some regular collaboration with systems integrators. When they win a tender process for an industrial company and they want to use our products we work together in providing the solution. In some cases the asset owners specifically want our products and that's when we provide the solution our selves, although this does not happen very often. The systems integrators are also mainly selected on knowledge and experience with our products to ensure our products are programmed and used correctly.

D3.2 **The OEM is not aware of threats in the supply chain**
Interviewee: Actually we are not aware that these activities can be suspicious of that kind.

D3.3 **Hardware counterfeiting more present in connectivity components such as cables**

Interviewee: With our PLC products there hasn't been any of those incidents reported by the OEM itself, however what is more likely to happen is that cables and other equipment that are used to connect the components and systems with each other are of less quality than expected and probably are counterfeit products.

D4.2, D4.3, DGC **OEM performs plant security, not security of supply**

Interviewee: We do software integrity checks after delivery only if specifically asked for, usually with very complex and large destination plants like in the petrochemical plants where our products are going to be used and not with the smaller production plants. So this is application dependent.

Interviewee: We implement plant security that consist of perimeter security, access management and network segmentation.

Interviewee: The OEM does a lot when it comes to testing of the product before it leaves the production plant. When a product is in system-under-test phase the product is thoroughly tested on functionality and robustness to receive the "Achilles 2" certificates which means the industrial device works as required on a IP-level. Achilles 1 certificate is a certificate for quality of hardware however only the IP-level requirements are tested by the OEM. Additionally, the OEM believes the biggest threat to ICS and PLCs is human error and therefore they organize security awareness training in an existing factory. Several aspects of defence-in-depth are covered like access control and perimeter security. Also, they offer in depth Plant Security on physical, network and control level but these measures only are present in the industrial plant. As a side-note they always recruit an engineer with IT knowledge as security officer for the plant that does administrative security checks like password management.

5.2.1 Final remarks

The answers of the OEM show that indeed the products nowadays are mainly produced as COTS products. Furthermore, in the supply chain the OEM can take the role of a system integrator as well. The selection criteria also consist of knowledge and experience about the products. The OEM performs trainings for the people that are going to work with the industrial devices. However, what is interesting to note is that the OEM does not mention anything about the actual people that perform actions on the devices. It could be that these employees are not screened at all. When the OEM is presented with a summary of what can happen in the supply chain the threat scenario's are totally new for the OEM, so it could be assumed the OEM is not aware of the threats that might occur in the supply chain. In addition, only counterfeited cables has been reported as an incident to the knowledge of the interviewee.

The OEM thinks it is their responsibility when it comes to security of their product and therefore they give the awareness training to anyone who is responsible for configuring, updating, operating the devices in an industrial plant. However there is little awareness of supply chain threats and security in the supply chain. What happens to a product when its returned because of malfunction? There are two possibilities; either the product is at its end of life or the product needs to be repaired. In most cases the old product is destroyed completely and the new model in the same line is offered for replacement, this also happens to any product that is more than ten years old. When a specific product is returned under warranty but is not produced anymore the same product is revised and returned. That's how the end of the lifecycle looks like at the OEM's

Industrial Automation. Finally, about delivering products the OEM mentioned that in some countries delivery is not possible like in Iran because it is too high risk. To summarise, the OEM mainly performs plant security and does not take supply chain threats into account. Selection criteria do not cover security measures that could be met by third parties, integrators and distributors to secure the supply chain.

5.3 Interview 2: A Systems Integrator and Solutions Provider of ICS

The second case study is from the perspective of a Solutions Provider and Systems Integrator. They are providing a range of different packaging and processing solutions and consequently supplying complete systems of processing, packaging and distribution within fields as various as ice cream, cheese, fruit and vegetables and pet food. In addition, interviewed company provides integrated processing and distribution lines for different kinds of food manufacturing, including packaging machines and carton, equally providing distribution equipment like conveyors, tray packers, film wrappers, crates, straws and roll containers. The company additionally offers automated production solutions and technical service.

In appendix E the interview is written down in the interview format. The interviewee is an employee of the systems integrator and in the Automation Solutions department, below are the most striking findings:

E1.1 **Product is combination of insourced PLC/PAC with software on top it. The software is partially open source for customization**
Interviewee: The firm consist of several departments namely dairy, processing and packaging. The PLCs are in-sourced from suppliers, mainly from OEMs OEM and Rockwell. The firm develops software on top of the PLCs and it is built into the machines before it is shipped to the customer. However, some machines are also shipped without any PLCs. PLCs are grouped into three distinctive levels, distinguished by size of application. The first level are PLCs that reside in one unit, the 2nd level is in multiple units in a production line and the 3rd level is on plant level with multiple production lines and a central control room. Their machines' code is open and therefore customers can reprogram parts of the code that is standard delivered, this will void warranty but it enables more applicability for the customer, this is mainly the case in production line and plant wide solutions. These solutions are more open to integration. The firms' personnel is responsible to install machines after it gets thoroughly tested for acceptance. The final code gets deployed when the machine is staged at the customers' site.

E2.1 **Many (critical) parts are insourced, collaboration on basis of trust**
Interviewee: The firm is largely a mechanical company and therefore any form of electronics is in-sourced from several suppliers. Operator panels, GUI related software, windows-based programs and OS for integration are among the parts that are in-sourced.
Interviewee: We have contracts with many suppliers and they don't change often because we have built a relation of trust.

E2.3 **Selection criteria is quantitative and qualitative: qualitative on certifications, quantitative on financial capability.**

E2.3 **Collaboration with 3rd part integrators, software developers & criteria does not cover screening of personnel**
Interviewee: In some cases we hire 3rd party integrators to install machines for us at the customer site. These collaborations are chosen on criteria such as experience, financial capability, stability, appliance with ISO-certs. Basically same quality requirements that the firm itself adheres to. Moreover, they must come to the firm for special training to be able to install solutions at customer sites.

E2.4 **Handles transportation itself**
Interviewee: We don't act through retailers and we don't work together with 3rd party logistics. We do this ourselves.

E3.3 **Are partially aware of the threats in the supply chain and also take action against it.** *Interviewee: Our software development process and the loading of the software on the devices is a secure process that can only be done with certificates, so far we don't have any reports of malicious software. However, because a part of our code is also open code and it can be modified. Disgruntled employee or 3rd party integrator could install backdoors or modified firmware at the customers' site for example but no reported cases.*

E4.1 **Secure development, secure installation, code encryption**
Interviewee: In our code the critical parts are encrypted therefore only with special certificates this can be changed or obtained. Moreover, after installation on customer site the software is deployed so we try to have the critical process the latest as possible. We also have a mechanism for tamper proofing to protect our intellectual property. For hardware intrusion we don't have any mechanisms because our products are not resold or distributed.

5.3.1 Final remarks

The answers in the interview show the production processes of a systems integrator and their core business. As can be concluded, they only collaborate with a few suppliers of PLC/PACs. The open source code could leave a lot of opportunity to take advantage of but from the interview it didn't become clear to what extend functionality of the device can be altered with it. Third party software and many other parts are insourced to support their products. In addition, the selected suppliers are not assessed on anything security related, because of trust that is built over time the collaboration continues. While the exact purpose of the parts remains unanswered, it might be the most vulnerable process of the system integrator because this is the critical part of the industrial device to the integrator. Their software is the core business of the solution.

Furthermore, the system integrator also performs trainings for employees that are going to work with the devices. In some cases 3rd party integrators perform the task of installation of their solutions. However, the employees that are involved are not screened. A positive part is that collaboration is selected on qualitative requirements. Deliveries of new machines and factories is taken care of by the systems integrator themselves, no 3rd party is involved in the transportation. From a supply point of view this could be very beneficial for the security of the supply as it can be fully controlled, if sufficient measures are taken.

It can be said that the system integrator is aware of the threats in the supply chain relating to software and transportation. Also taking into account the secure installation and the transportation that is done by themselves. A lot of threats are mitigated by these activities. Although the integrator mentioned that anti-hardware counterfeiting is not necessary because their devices are not resold or distributed, judging on the many insourcing activities this could still remain a threat.

To summarise, the system integrator handles almost every step in the lifecycle of the industrial device. The devices are only insourced from OEMs and from there it is the firm's business. Quality is from utmost importance and that's what the delivering of the solution is about. No 3rd party logistics are involved and only certified 3rd party integrators may handle the devices for installation. This reduces the possibilities for attackers. For better integration in broad applications of their solutions some code is made open to changes, however there is only warranty on delivery of the solution. Their main concern is Intellectual Property theft, this is directly handled with use of encryption and certificates. Responsibilities are laid down in contracts with customers and other collaborations.

5.4 Interview 3: An End User of ICS

The third and last case study is about an end user at the end of the supply chain. The perspective is much different from the other interviewees because an asset owner does not produce the industrial equipment itself but choses the solution that is best suitable to the requirements of their business. In this case, the sector the interviewee is active in is beer brewing. They own many plants over the world and have a lot of experience in collaborations with system integrators.

In appendix F the full interview is written in the interview format. The interview took place over the telephone, the interviewee is Manager Global Process Control of the Supply Chain Services department. The striking findings of the interview are enumerated below:

F1.1 **Perspective of asset owner on acquiring a new ICS**

Interviewee: After the assignment is issued for an existing factory to be replaced or a new one to be built, the asset owner designs the factory and the negotiation with suppliers begin. At first the basic design features are discussed like surface area, number of processing, filling and packaging units for example. From the drawing board applicable suppliers are selected. In the past 30 years the asset owner has experienced that the components are far less obscure than they used to be. The components are now running mainly on Windows OS. The reason for this is that the production demand rose and at the same time extra efficiency in production was required. So more production with less people. All factories are 'Proleit' configured, that is a working program for all our factories and that's also where we train our employees for. The asset owner enforces to use ISA-99 standards for designing all process automation systems.

F2.1 **Collaborates with very few suppliers**

Interviewee: When a tender is set out for the designing of the new factory the asset owner seeks to only collaborate with one supplier or OEM. The collaborator needs to comply to the used standards. Usually, the OEM also assumes the role of systems integrator and provides the whole solution for the whole plant. Because there are not many integrators of the brewery factories the asset owner requires, the choice with who to collaborate is usually limited but easy to make. Because all factories are 'Proleit' process control technology configured, this actually leaves little to no space for OEMs for custom configuration.

Interviewee: Not always, It sometimes happens that it's not possible to collaborate with only one OEM or systems integrator. In this case an external relation is *entered into. However, because only 2 or 3 integrators are applicable in our sector the choice is limited.*

F2.3 **Suppliers are selected on qualitative and quantitative criteria.**
Interviewee: Mainly on performance criteria: how many process alarms can be configured, delivery time of the supplier and also how does the software behave on startup for example. Also, the collaborations need to comply with the same standards we operate in, namely ISA-99.
Interviewee: Asset owner demands a clean install of the integrator or OEM where the asset owner can load its own application for their factories.

F1.3 **Focus on plant security, not on security of supply**
Interviewee: With the creation of a new factory, the asset owner inherits IT security in the design of the new process automation domain. The roles and responsibilities are divided between process engineers and IT managers in order to fully utilise the factory. Every factory has its own IT service organization and awareness of cyber threats in the factory is well brought about to the engineers, IT service organization and other employees.
Interviewee: Measures that are used to secure the PLCs are two-factor-authentication for updating the devices and for installation too. Two-factor authentication is also used for maintenance on the PLC from the outside.

5.4.1 Final remarks

The systems are run on only Windows OS and the environments have seen a development into far less obscure. This confirms the developments mentioned in Chapter 2. 'Proleit' configuration is a piece of software that is specifically designed for the given industry. ISA-99 standards are used, however security of supply is not covered in that framework.

The answers show the relation between asset owner, systems integrators and OEMs. The direct relations between them in the supply chain are confirmed. Also, it can be said that because of the industry there is almost no room for new collaborations. The limitation in choice makes it either easier to select a supplier or on the contrary it can be harder when all available integrators/OEMs show little to no defence strategies for their products. Moreover, there is sought to collaborate with only one supplier which makes maintenance and delivery to the factories more secure than when collaboration is done with multiple suppliers, although sometimes more than supplier is collaborated with. Only some criteria is used for the selection of the supplier, however suppliers are not assessed on how they secure their deliveries. They only demand a clean install of the integrator/OEM. From the asset owners point of view they are not really concerned about threats in the supply chain but more on operational threats. Although the people involved are trained for awareness, this doesn't cancel the threats that might be happening in the supply chain. Interesting fact is that all changes and updates are done through two-factor-authentication. Two-factor authentication is a well established method.

To further summarise, the asset owner believes the greatest threat for the devices and the factory is probably old employees taking revenge. A big risk is that they are aware of is that some of the equipment is too old and no spare parts are available anymore. Deliveries of the equipment was never tampered with before. Although a good thing is that they only collaborate with a few suppliers, and where possible only one at the time for a new factory. The supply of the products is not thought of and the asset owner thinks it's the responsibility of the integrator/OEM to deliver properly.

5.5 Comparing with theoretical scenario's

The interviews give perspectives on the complexity of the supply chain and a perspective on supply chain (security) from three angles. The perspectives are summarised in the findings of the section above. Based on the findings we can compare the theoretical threat scenario's with the situation that are presented in the interviews. To do this, the interviews are analysed on the following aspects:

- how they secure their product;
- how suppliers are selected;
- to what extent they are aware of the possibilities in the supply chain.

Based on first aspect it can be assumed what threats firmware/software tampering could be occurring. The second aspect can show insight in where the threats could be occurring. The third aspect could show some insight in how stakeholders relate supply chain in terms of awareness.

5.5.1 Perspective of the OEM of PLCs/PACs

What became clear from the interview with the OEM is that they are not aware of the threats in the supply chain. Other than plant security, the OEM didn't mention any security for their devices. The devices receive two certificates but that is only on IP-functionality, not if basic security measures are met in production for example. Therefore, it can be assumed that firmware tampering is a threat to the OEM. Furthermore, two situations can be distinguished, the OEM takes the role of systems integrator or the OEM takes the role of supplier to system integrators or distributors. In both cases the OEM does only select on qualitative criteria. As transportation and collaboration with distributors is not controlled, it can be assumed that these collaborations would be most exposed to threats. For example, on a warehouse or distribution centre new backdoors could be installed because the collaboration is not checked on qualitative criteria if deliveries are protected. In the second situation, the amount of people involved in the product lifecycle increases because of the collaboration with wholesalers and retailers is included. These collaborations are only selected on knowledge with the product so it could be assumed that there exist more possibilities for tampering. It didn't became clear from the interviews if the people that perform the maintenance and SAT-test are screened on their background, if this is not the case this is a certainly a threat in the supply chain for the OEM.

Combining these findings the following threat model could apply to the OEM. The OEM is involved in basically all industries as a market leader therefore the threat actors identities cannot be determined specifically. Firmware modification and use backdoor are the threats that could be occurring together with hardware counterfeiting because of the insourcing of parts and low controllability of transport.

5.5.2 Perspective of A Systems Integrator and Solutions Provider of ICS

In the interview with the systems integrator and solutions provider it became clear that they are more aware of threats in the supply chain than the OEM. Several security measures are taken like code encryption and this would mostly mitigate tampering

Threat	Attack tree	Threat actors	Lifecycle phase
1	Firmware/software tampering	Military, Opposing government, Foreign Intelligence service, Hacker group, Disgruntled Employee, Competitor	Shipment, Engineering&Customization, SAT, Maintenance
2	Install backdoor	Military, Opposing government, Foreign Intelligence service, Hacker group, Disgruntled Employee, Competitor	Shipment, Engineering&Customization, SAT, Maintenace
3	Hardware counterfeiting	Counterfeiters, Hacker group/faction, Competitor/organisation	Production, Shipment, Decommissioning

Table 5.1: Threat model comparison OEM

Threat	Attack tree	threat actor	Lifecycle phase
1	Intellectual Property Theft	Disgruntled Employee, Competitor	Engineering&Customization, FAT, SAT
2	Install backdoor	Disgruntled Employee, Competitor/organisation	Engineering&Customization, FAT, SAT
3	Firmware/software tampering	Disgruntled Employee	Engineering&Customization, FAT, SAT

Table 5.2: Threat model comparison system integrator/solution provider

with firmware/software. However, an employee that has access to the encryption could still pose this threat. Furthermore, they show a way to mitigate threats by using own transportation and choosing not to collaborate with distributors or third party logistic providers. However they do insource almost all parts and only add own software to it, of which a parts is also insourced from third parties. Because of this, installing backdoors into insourced parts could be occurring. Hardware counterfeiting could take place before the system integrator produces their own product. The suppliers are usually the same and selected on qualitative criteria such as knowledge of the product. When third party integrators are asked to install solution for them, the people are also trained. As very few collaborations are chosen and transportation is performed by the system integrator itself, this mitigates most of the hardware counterfeiting threats. Because the software is of high importance to the system integrator, the biggest impact on the company would have Intellectual Property Theft as this damages the trademark. Although this part of the code is encrypted, it could be leaked by disgruntled employees.

Combining these findings the following threat model could apply to the systems integrator. The systems integrator is involved in only one industry, dairy processing, therefore the threat actors identities can be assumed as the target is most attractive to competitors, disgruntled employees

5.5.3 Perspective of an End User of ICS

What became clear from the interview with the asset owner is that by the design of the new factories a lot of security measures are already met. For example, they demand a

Threat	Attack tree	threat actor	Lifecycle phase
1	Firmware/software tampering	Disgruntled Employee, Competitor	Engineering&Customization, FAT, SAT
2	Install backdoor	Disgruntled Employee	Engineering&Customization, FAT, SAT
3	Hardware counterfeiting	Competitor/organisation	Production, Shipment

Table 5.3: Threat model comparison Asset Owner

clean install of their factories in order to load their own application in their breweries. All actions on the PLCs are done with two-factor-authentication for the testing, updating and maintaining. Only disgruntled employees would be able pose a threat by taking advantage of the installation process. Furthermore, they only work with a few suppliers, usually only one and they need to comply to a security baseline, therefore the suppliers are selected on a qualitative basis. However, sometimes external relations is entered into and collaborations of two or more integrators and OEM is required. In general the beer brewery industry only has a few integrators who can build beer-factories, which makes the possible threats less. However, because it is unclear what is done to prevent hardware counterfeiting by the asset owner or its suppliers, this could be a threat for the asset owner. Moreover, the above mentioned tasks that are performed on the PLCs/PACs may be secured but it is unclear if the employees are screened on their background before they are authorized to work with the control devices. The threats that this asset owner could be facing are disgruntled employees and competitors tampering with the devices before installation and operation in a new factory.

5.6 Summary

The threat model that is created in chapter 3 shows an overview of the threats that could be occurring in the supply chain of industrial devices. It's a theoretical model based on literature and reported incidents that needed to be tested in reality. The current situation of the supply chain is unknown and therefore if perspectives from stakeholders in the supply chain is looked at, the model can be compared with the actual situation. In this way the current situation can be understood and actual threats can be determined. This is helpful in order to mitigate the threats.

The theoretical model is tested against perspectives of an Original Equipment Manufacturer, System Integrator/Solution Provider and an Asset Owner. These stakeholders are interviewed to find out a the following: production process, suppler selection criteria, controls in place to secure the device, information on reported incidents. The production process is asked for because that shows the relation with other actors in the supply chain and it gives an understanding in what way the actors interfere with the device. Supplier selection criteria is helpful to understand how collaborations are started and on what base in-sourcing and supplying is decided. This criteria can help with determining if the actors are aware of the threats that could be happening in the supply chain. Furthermore, the controls and measures they already have or don't have in place to secure their product or production/transportation is important to be able to determine if the theoretical threats have already been mitigated or not. Information on reported incidents is necessary to be able to confirm the threats from literature and other reported incidents.

To summarise, the OEM mainly performs plant security and does not take supply chain threats into account. Supplier selection criteria do not cover measures that can be met by third parties, integrators and distributors to secure the supply chain. The people that are involved are trained and checked on knowledge of the products but it is unclear if they are checked further. This leaves opportunities during shipment for firmware tampering for OEM, especially with many collaborations with distributors all over the world.

From the system integrator's point of view, the production process consists of creating software on top of the PLCs/PACs and providing a plant solution. Critical parts of the software is encrypted however, a lot of parts regarding software, hardware are insourced which can be tampered with. The interviewed system integrator totally handles transport by itself and does not collaborate with distributors at all, this gives a certain layer of security for their deliveries. A part of their software is made open source which creates increased customisation abilities but also more opportunities to tamper with the software in a malicious way.

The asset owner's perspective shows that they are only able to collaborate with a few suppliers, and where possible only one at the time for building a new factory. This leaves less room for tampering. Their process is mainly negotiating with suppliers in building their factory, criteria is made according to the ISA-99 standard. For deliveries only a clean install on delivery is required with a specific type of program which is industry specific, in general this leaves little opportunity. Controls they have in place is secure environment for installation and maintenance, however sometimes third parties do the installation and updating. For the asset owner, the biggest threat would be to collaborate with more than one supplier. However their industry is not an attractive target due to the nature of the industry. The main threat actors that could have intention to exercise a threat would be either disgruntled employees, insiders and competitors.

Chapter 6

Conclusion & Discussion

The goal of this chapter is to conclude on the research questions bases on the previous chapters. The discussion will contain arguments under what circumstances this research generated the outcomes and how this could be different in other circumstances.

6.1 Conclusion

The main research question of this thesis is *"What are the current cyber threats towards industrial embedded devices that could occur in the supply chain?"*.

This question has been answered by the threat model in Chapter 3 and the interviews with stakeholders in Chapter 5. The threat model is derived from a literature study and reported incidents on PLCs/PACs. How these incidents could be translated in the supply chain is then determined by modelling attack trees. The threats have been looked at from an threat actors point of view and show what a threat actor could achieve by interfering with the supply chain of industrial embedded devices. Next to that a taxonomy of threat actors is used in order to show who would be able to perform such threat. The threat-equation that is mentioned in Chapter 1, is then used to form all possible threat scenario's that ultimately form the threat model. The result is 35 theoretical threat scenarios that could be occurring in the supply chain of industrial devices. The threat scenario's are categorised generically as hardware counterfeiting, firmware/software tampering, intellectual property theft and the installation of backdoors.

The threat model is then tested in reality by interview sessions with three different stakeholders of the supply chain, an OEM, a Systems Integrator and an Asset Owner. The interview consisted of four groups of questions; general production process; supply chain related; incident report; controls and measures in place. The interviews showed three perspectives of security in the supply chain of industrial devices and from these perspectives the actual possible threats from the threat model is determined. The perspectives showed that the three stakeholders have a different view on supplier/collaboration selection criteria. The OEM is concerned about quantitative criteria such as delivery times and amount of goods sold whereas the Systems Integrator and the Asset Owner are concerned about qualitative criteria such as compliancy to certifications and security baselines. Another difference that was shown in the interviews is the awareness about these threats occurring in the supply chain. The OEM is not really aware because little measures are taken, the systems integrator is aware and the asset owner is also aware because of, among other reasons, code encryption and secure delivery and installation. The threat model comparison with the three interviewed stakeholders showed which threats from the threat model could actually be occurring in the supply chain at these stakeholders.

The interviews also showed the relation between the different stakeholders in the supply chain. The OEM of the supply chain has the most important and the most complicated task when it comes to security of supply. The OEM strives to have the most sales and therefore the most distribution channels as possible is needed. The OEM can collaborate directly with the asset owner but also with distributors, integrators and solution providers. All relations are many to many and responsibility for the security of supply is hard to determine.

The OEM mainly performs plant security and does not take supply chain threats into account. Supplier selection criteria do not cover measures that can be met by third parties, integrators and distributors to secure the supply chain. The people that are involved are trained and checked on knowledge of the products but are not checked further. This leaves many opportunities during shipment for firmware/software tampering for OEM, especially with many collaborations with distributors all over the world. From the system integrator's point of view, the production process consists of creating software on top of the PLCs/PACs and providing a plant solution. Critical parts of the software is encrypted. However, a lot of parts regarding software and hardware are insourced that can be tampered with if no measures are taken. The interviewed system integrator totally handles transport by itself and does not collaborate with distributors at all, this gives a certain layer of security for their deliveries. The Asset Owner's perspective shows that they are only able to collaborate with a few suppliers, and where possible only one at the time for building a new factory. This is good because that leaves less room for tampering. Controls the Asset Owner has in place is secure environment for installation and maintenance, however sometimes third parties do the installation and updating.

6.1.1 Supply Chain Security Challenges

The biggest challenge or most critical part for better supply chain security can be viewed from the perspectives of the interviewees. These findings are based on the the interviews that are described in Chapter 5. For the OEM the biggest challenge would be to control the many collaborations with distributors across the globe and to sharpen selection criteria in order to secure transport and the device. For the system integrator the biggest challenge would be the controlling of insourcing of parts(software). This would be critical to secure the supply chain as the other production phases are well covered for this stakeholder. The biggest challenge for the asset owner would be the screening of the people that are involved in installation and configuration of the plants and selection criteria for suppliers. These factors will be beneficial for the asset owner to ensure better supply chain security of the products they buy.

6.2 Discussion

First of all the research examines the supply chain from a generic point of view. The actors are found based on a device lifecycle and literature only. If products in the actual supply chain from multiple OEM's to destination asset owners can be followed physically this would have created a much more detailed and accurate overview of the supply chain and its actors. Also, this would be helpful for determining the weak spots in the supply chain as then it can be experienced directly. Furthermore, the threat model is a theoretical representation of the threats occurring on the devices in the supply chain and is not based on industry specific context.

Moreover, sectors in which ICS are used are very different from each other. The interviews with the system integrator and asset owner only represent one specific sector. The OEM's point of view is of course applicable for multiple sectors. So, the conclusions of the interviews are based on one sector per interview. The dairy industry where the system integrator is active might not be as attractive as the energy sector for example. Additionally, the beer brewery where the asset owner is active only has a few integrators to work with and might not be as attractive as well. In order to generate a specific list of threats in the supply chain a thorough distinction between sectors need to be made. The intention of the threat actors would also be very different for each sector.

Finally, for a complete overview of the supply chain it would have been beneficial for this research to be able to get interviews from all different angels. Adding an interview from multiple sectors and with a reseller or distributor would have created a much broader picture.

Chapter 7

Recommendations

The goal of this chapter is to provide recommendations that follow from the conclusions. Next to that, a short summary of literature that could be useful look into for mitigation of threats in the supply chain is given.

7.1 Recommendations

This thesis gives insight into the state of the supply chain and threats that the devices in the supply chain face. This knowledge could be used to offer KPMG's clients in the industrial sectors a new service. A new service to be involved in the process of either designing, acquiring or installing a new Industrial Control System with regards to:

1. Critical success factors in supply chain security
2. Maturity modelling for actors in the supply chain.

Both are explained below.

7.1.1 Critical Success Factors

Although the results of the interviews are sector specific I think a lot can be learned about what can be applied in general. What makes a supply chain successful in mitigating threats? One of them can be learned from the interview with the system integrator. The collaborations that they have with the asset owner is pretty special in terms of transportation. If a company handles the whole transportation itself there is no chance that third parties can interfere with the devices and the only threat actor would be an insider. In other words, system integrators should be assessed based on how they do deliveries of equipment. If the deliveries are done in-house it would be an advantage to collaborate with that integrator. It is unsure if this is sector dependent but it at least is possible in the dairy industry. The second success factor can be learned from the interview with the asset owner. They only collaborate with one OEM or integrator and only exceptionally with multiple ones. As an asset owner you don't want a solution of more than one supplier to reduce the amount of people that have interfered with the product while it traversed the supply chain and to reduce maintenance of the companies later on. Furthermore, supplier selection criteria other than quantitative criteria and on one security framework would be necessary to check to ensure better security. Criteria such as if the supplier does screening of backgrounds of people that perform the critical processes in the installation and SAT phases. Together this can bring a few critical success factors where potential clients of KPMG can be checked upon.

7.1.2 Maturity Model

In Chapter 2 cyber security is also explained as the amount of awareness and activity a company performs in cyber security strategies. This extent to which a company is aware of the threats and acts against it in mitigation strategies is the maturity level of that company. This helps to determine logical and strategic steps to take in order to reach a high level of maturity. The sector and type of business can have an influence on the maturity level that is desired. The same kind of maturity model could be made up to be used for companies in the industrial sectors where ICS are installed. Also the companies that are involved in the supply chain of the industrial devices. Important factors to take into account for a maturity model of the supply chain would be compliance to standards and for example awareness of the threats in the supply chain. Furthermore, the critical success factors that are just described could also prove to be useful in order to determine the maturity level of companies. The result would be same kind of scale as described in Chapter 2 and would be helpful as a first step in bringing the discussion about supply chain security to the tables.

7.1.3 Possible Supply Chain Threat Mitigation Techniques

7.1.4 Secure production programming

In security of embedded devices it's crucial to protect the software against cloning, counterfeiting and unauthorized alterations. For example: sales of illegal copies of devices opposes a big threat for the manufacturers and industrial companies that are involved. Manufacturers lose sales and reputation by counterfeiting and the owners are facing unnecessary risks when using devices that are not genuine. In (Kjellsson & Torngren, 2011) the focus is on embedded devices that are based on microcontrollers which have onboard Random Acces Memorty (RAM) and Read Only Memory (ROM). As Kjellsson et al (Kjellsson & Torngren, 2011) argues, the system integration phase is most vulnerable phase for unauthorized production and counterfeiting. This is the phase where the firmware is loaded on the device. In this study a proof of concept is presented that should mitigate these risks by using a pre-programmed boot loader which only accepts firmware images encrypted with a certain key. Furthermore, this study focuses on secure production of new products and leaves out how existing field devices can be securely upgraded.

7.1.5 Hardware anti-counterfeiting

Concerns about hardware security have increased with the wide availability of sophisticated tools and invasive techniques to discover the secrets and keys that traditionally protect devices from counterfeiting and tampering. Malicious attacks on hardware are increasing in scale and sophistication, and, if successful, can cost electronics companies millions in revenue and endanger company as well as brand reputations. Hardware security systems aim to protect intellectual property (such as designs, software, etc.) and preserve revenues by preventing counterfeiting, tampering, theft-of-service and reverse-engineering attacks on electronic devices, this is discussed by Tuyls et al. Traditionally, hardware is protected by cryptographic means and the necessary secret keys are hidden somewhere in the actual hardware. The confidentiality of the secret key is therefore the critical factor for the security of the entire device or system. Because of the fact that devices that can reveal the hidden keys are widespread nowadays, this proposes a serious security threat. The authors of (Tuyls, 2010) propose a way to counter these threats by means of not storing the key on the hardware but use a small RAM unit. That unit generates an activation code with a given secret key and after which it will return the key when the code is queried to check for validity.

7.1.6 Management of certificates

Generally speaking, certificates bind a public key to an identity of a certain authority. This key can then be used to achieve mutual authentication of the authorities in order to ensure authenticity of the product that is being used. The heretofore mentioned device lifecycle introduces many stakeholders and therefore multiple certificate signers or Certificate Authorities(CA). Usually they are not involved throughout the whole lifecycle as well which makes management of certificates an important issue. In Stuxnet-like attacks attackers were able to retrieve valid root certificates and were able to alter the device. In (Obermeier et al., 2012) such attack vectors are discussed. The vectors are attacks during production, shipping or operation of the embedded device where attackers manage to compromise the root key. Their proposed solution is to install a private key, default device certificate and a root certificate of the manufacturer in a trusted environment. By allowing only one root certificate on the device a malicious root key can be identified before it is integrated in the system for usage. Additionally, two ways of establishing a trust relationship between the manufacturer, system integrator and plant operator is presented. Face-to-face meeting and out-of-band communication using PGP wordlist can be used to ensure the verification of certificates(Obermeier et al., 2012). Important aspect that is left out in this research is the revocation and replacement of the certificates when the devices are already in operation.

7.1.7 Secure Acquisition

According to a recent document published by the Department of Defense, changing the behaviour of program managers and acquisition decision managers would be the key actions to enable secure acquisition.(Department of Defense, 2013).

7.1.8 Verification of PLC firmware

Verification of firmware could be done by passively tap the line from where the firmware is loaded on the device, the tap could then be verified with a checksum algorithm. This paper shows how validating could be done for device firmware and even without a PLC by emulation (Mcminn & Butts, 2012).

Bibliography

Automation.com. (2014, May). *Process control & instrumentation product suppliers & manufacturers.* http://www.automation.com/suppliers/automation-product-manufacturers.

Basnight, Z., Butts, J., Lopez, J., & Dube, T. (2013, June). Firmware modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, *6*(2), 76–84. Retrieved from http://linkinghub.elsevier.com/retrieve/pii/S1874548213000231 doi: 10.1016/j.ijcip.2013.04.004

Beamon, B. M. (2001). Measuring supply chain performance.

Byres, E. J., Franz, M., & Miller, D. (2004). The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems.

Chabukswar, R., & Sin, B. (2010). Simulation of Network Attacks on SCADA Systems.

Clemens, P. L. (1993). Fault Tree Anlysis. (May).

ControlGlobal. (2014, May). *Directory.* http://www.controlglobal.com/articles/2012/boyes-clayton-serene-economic-recovery/?start=1.

Cornish, D. B., & Clarke, R. V. (2008). The rational choice perspective. In *Environmental criminology and crime analysis* (pp. 21–45).

Davis, C. M., Tate, J. E., Okhravi, H., Grier, C., Overbye, T. J., & Nicol, D. (2006, September). SCADA Cyber Security Testbed Development. *2006 38th North American Power Symposium*, 483–488. Retrieved from http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4201358 doi: 10.1109/NAPS.2006.359615

Department of Defense. (2013). *Improving Cybersecurity and Resilience Through Acquisition.*

Dittmann, J. P., Gaudenzi, B., Myers, M. B., & Stank, T. P. (2014). Handbook of Global Supply Chain Management Risk Management. , 319–337.

Dunjó, J., Fthenakis, V., Vílchez, J. a., & Arnaldos, J. (2010, January). Hazard and operability (HAZOP) analysis. A literature review. *Journal of hazardous materials*, *173*(1-3), 19–32. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/19733970 doi: 10.1016/j.jhazmat.2009.08.076

Dzung, D., Naedele, M., Hoff, T. P. V. O. N., Crevatin, M., & Motivation, A. (2005). Security for Industrial Communication Systems. , *93*(6).

ENISA. (n.d.). The Netherlands Country Report.

Fabro, M. (2012). Study on Cyber Security and Threat Evaluation in SCADA Systems. (March).

Goertzel, K. M. (2010). Supply Chain Risk Management and the Software Supply Chain.

Group, A. A. (2008). Custom controller or cots?

Guin, B. U., Huang, K., Dimase, D., Carulli, J. M., Tehranipoor, M., & Makris, Y. (2014). Counterfeit Integrated Circuits : A Rising Threat in the Global Semiconductor Supply Chain.

Hadžiosmanovic, D. (2014). *Process matters: cyber security in industrial control systems.* Enschede, The Netherlands. Retrieved from `http://purl.org/utwente/doi/10.3990/1.9789036536042` doi: 10.3990/1.9789036536042

Hristova, A., Obermeier, S., & Schlegel, R. (2013, July). Secure design of engineering software tools in Industrial Automation and Control Systems. *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 695–700. Retrieved from `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6622968` doi: 10.1109/INDIN.2013.6622968

Kang, D.-J. K. D.-J., Lee, J.-J. L. J.-J., Kim, S.-J. K. S.-J., & Park, J.-H. P. J.-H. (2009). Analysis on cyber threats to SCADA systems. *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific*, 1–4.

Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services : A Stakeholders View.

Kjellsson, J., & Torngren, M. (2011, July). A Concept for Secure Production Programming of Embedded Industrial Field Devices. *2011 IEEE 35th Annual Computer Software and Applications Conference*, 176–181. Retrieved from `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6032339` doi: 10.1109/COMPSAC.2011.30

Krotofil, M., & Gollmann, D. (2013). Industrial Control Systems Security : What is happening ?

Kushner, D. (2013). The real story of Stuxnet. , 48–53.

Lessing, M. M. (n.d.). Best practices show the way to Information Security Maturity.

Liu, C.-c., Ten, C.-w., Member, S., & Govindarasu, M. (2009). Cybersecurity of SCADA Systems: Vulnerability Assessment & Mitigation. , 2–4.

Macaulay, T., & Singer, B. (2012). *Cybersecurity for industrial control systems: Scada, dcs, plc, hmi, and sis.* Taylor & Francis. Retrieved from `http://books.google.nl/books?id=YBM3cwTNwj0C`

Matthieu, P., & Waalewijn, D. (2014). Digitale spionage en cyber criminaliteit groeiende dreiging voor de energiesector. *Compact*, 40–49.

Mcminn, L., & Butts, J. (2012). A Firmware Verification Tool For Programmable Logic Controllers. In *Critical infrastructure vi* (pp. 66–77).

Mulder, J., Schwartz, M., Berg, M., Houten, J. V., Urrea, J. M., & Pease, A. (2012). Analysis of Field Devices Used In Industrial Control Systems. *Critical Infrastructure VI*(January 2012), 56–67.

NCSC. (2013). Cybersecuritybeeld Nederland. (3).

NIST. (2002). NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology. , *30*(July).

NIST. (2013a). *NIST Special Publication 800-82 Guide to Industrial Control Systems Security* (Tech. Rep.).

NIST. (2013b). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *800-161 special publication*(August).

Obermeier, S., Schierholz, R., Hadeli, H., Enderlein, R. R., Hristova, A., & Locher, T. (2012). Secure Management of Certificates for Industrial Control Systems.

Santamarta, R. (2011, December). *Reversing industrial firmware for fun and backdoors i.* `http://www.reversemode.com/index.php?option=com_content&task=view&id=80&Itemid=1`.

Schneier, B. (1999a). Attack Trees.

Schneier, B. (1999b, December). *Modelling security threats.* `https://www.schneier.com/paper-attacktrees-ddj-ft.html`.

Symantec. (2014, June). *Dragonfly: Western energy companies under sabotage threat.* `http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat`.

Ten, C.-W. T. C.-W., Manimaran, G., & Liu, C.-C. L. C.-C. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *40*(4), 853–865.

Turk, R. J. (2005). Cyber Incidents Involving Control Systems. *US-CERT Control Systems Security Center*(October).

Tuyls, P. (2010). Conquering Copycats : Attacks Fail Against Hardware Intrinsic Security.

Wang, C., Fang, L., & Dai, Y. (2010, March). A Simulation Environment for SCADA Security Analysis and Assessment. *2010 International Conference on Measuring Technology and Mechatronics Automation*, 342–347. Retrieved from `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5459612` doi: 10.1109/ICMTMA.2010.603

Webwereld. (2014, February). *Pre-installed malware found on new android phones.* `http://www.computerworld.com/s/article/9246764/Pre_installed_malware_found_on_new_Android_phones`.

Zhu, B., Joseph, A., & Sastry, S. (2011, October). A Taxonomy of Cyber Attacks on SCADA Systems. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. Retrieved from `http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6142258` doi: 10.1109/iThings/CPSCom.2011.34

Zsidisin, G. A., & Ritchie, B. (Eds.). (2009). *Supply Chain Risk. A handbook of Assessment, Management and Performance.* Springer.

Appendix A

Interview Questionnaire

Part 1: General questions

1.1 Can you describe your products(technical specifications)?

1.2 What do you think is the greatest threat for your product?

1.3 Can you describe your production process in general steps?

Part 2: Supply chain

2.1 Do you insource any parts from suppliers? If yes, what kind of parts?

2.2 Are they always the same suppliers? If no why?

2.3 How do you choose new suppliers or new distributors or other collaborations?

2.4 How is transportation/warehousing to your customers arranged?

2.5 Can you give an indication of the lead-time of your product to your customer?

Part 3: Incident report

3.1 Has there been any incident reported with your product with respect to insourcing, transportation/warehousing, delivery at customer, product usage, production?

3.2 What do you do when such thing happens? It could be the device that is being shipped is first being tampered with before it is delivered at destination.

3.3 Has there been any incident reported regarding software/hardware counterfeiting, malicious code infection, installed backdoors and such?

3.4 Any other incidents reported regarding cyber security?

Part 4: Controls and measures in place

4.1 What controls do you have in place to secure your product and production process?

4.2 What controls do you have in place to secure transportation/warehousing?

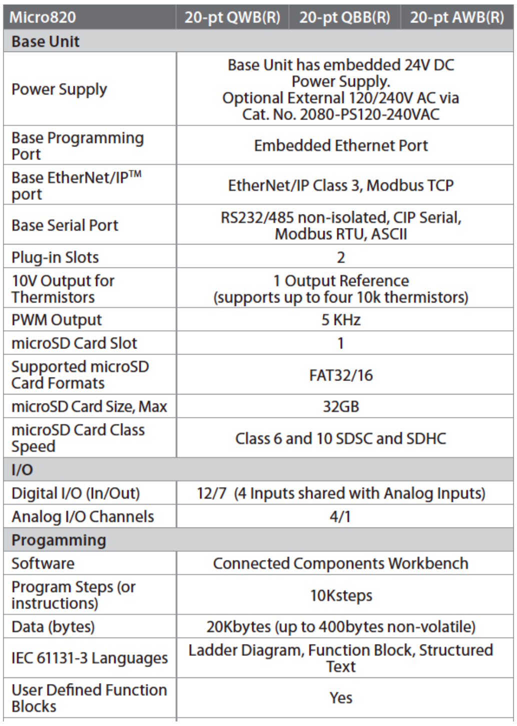
4.3 What controls do you have in place to secure the product after it is in use by your customer?

4.4 How do you secure your product?

General Comments

Appendix B

PLC/PAC Product specification label



Micro820	20-pt QWB(R)	20-pt QBB(R)	20-pt AWB(R)
Base Unit			
Power Supply	Base Unit has embedded 24V DC Power Supply. Optional External 120/240V AC via Cat. No. 2080-PS120-240VAC		
Base Programming Port	Embedded Ethernet Port		
Base EtherNet/IP™ port	EtherNet/IP Class 3, Modbus TCP		
Base Serial Port	RS232/485 non-isolated, CIP Serial, Modbus RTU, ASCII		
Plug-in Slots	2		
10V Output for Thermistors	1 Output Reference (supports up to four 10k thermistors)		
PWM Output	5 KHz		
microSD Card Slot	1		
Supported microSD Card Formats	FAT32/16		
microSD Card Size, Max	32GB		
microSD Card Class Speed	Class 6 and 10 SDSC and SDHC		
I/O			
Digital I/O (In/Out)	12/7 (4 Inputs shared with Analog Inputs)		
Analog I/O Channels	4/1		
Progamming			
Software	Connected Components Workbench		
Program Steps (or instructions)	10Ksteps		
Data (bytes)	20Kbytes (up to 400bytes non-volatile)		
IEC 61131-3 Languages	Ladder Diagram, Function Block, Structured Text		
User Defined Function Blocks	Yes		

Figure B.1: Specifiacations of Allen Bradley's best sold product

Appendix C

Taxonomy of Adversarial Sources

Table C.1: Taxonomy of Adversaries against ICS

Class	**Activity**	**Category**	**Adversary**
Deliberate	War	Nation States	Military and Paramilitary
	Civil Conflict	Faction	Hackers
	Espionage	Foreign Intelligence Service	Services
		Other State Sponsored	Organizations
		News Media	Companies
		Industrial Espionage	Companies/States
		Hackers	Groups
			Individuals
		Organized Crime	Groups
	Sabotage		Organizations
		Vendor	OEM
			Outsources Software Developer
			Systems Integrator
			Manufacturer
		Competitor	Organizations
		Disgruntled Employees	Groups/Individuals
		Activists	Radical Groups
		Hackers	Casual
			Automata
			Targeted Attacks
			APT
	Subversion		
		Political Activists	Groups
		Compitors	Organizations
		Labour Unrest	Groups
		Hackers	Script Kiddies
			Fully Capable
			Elite Hackers
	Criminal Acts	Insiders	Employees
			Temporary Help

			Subcontractors
			Service Staff
			Security Guards
		Outsiders	Clients
			Contractors
		Organized Crime	Groups

Appendix D

Interview Original Equipment Manufacturer

Interviewee role within organization: Product Manager Industrial Automation

Part 1 General questions

D1.1 Can you describe your products(technical specifications)?

Interviewee: We mainly sell PLCs, and over the past few decades these products have been developed from very simple I/O devices towards much more sophisticated devices with numerous TCP/IP ports and Operating Systems. They are usually operative for at least 10 to 20 years.

We also manufacture HMI's and the necessary measurement devices for a complete solution. The products are also mainly COTS products; as for very customised products there is almost no demand.

D1.2 What do you think is the greatest threat for your product?

Interviewee: Human errors are still the most common that can be in the form of incorrect configuration of the product or incorrect usage, which leads to disruption of the industrial process or in the worst case, physical damage or injury.

D1.2 Can you describe your production process in general steps?

Interviewee: Basically the systems design cycle.

Part 2: Supply chain

D2.1 Do you insource any parts from suppliers? If yes, what kind of parts?

Interviewee: Some components are in-sourced like some communication ports and antenna's and some circuit boards, but mainly we produce everything ourselves.

D2.2 Are they always the same suppliers? If no why?

Interviewee: Mostly they are from the same suppliers, sometimes the delivery times of our own product is delayed because a component we need to insource from a supplier is delayed as well and we don't switch to another supplier in that case.

D2.3 How do you choose new suppliers or new distributors or other collaborations?

Interviewee: Of course not everyone is allowed to sell our products, the distributors who want to sell our products are selected and assessed based on some criteria. These criteria are mainly amount of goods sold, delivery times and if they have the required knowledge of our products to configure them for example.

We have some regular collaboration with systems integrators. When they win a tender process for some industrial company and they want to use our products we work together in providing the solution. In some cases the asset owners specifically want our products and that's when we provide the solution our selves, although this does not happen very often. The systems integrators are also mainly selected on knowledge and experience with our products to ensure our products are programmed and used correctly.

D2.4 How is transportation/warehousing to your customers arranged?
Interviewee: Usually through the same distribution channels to either an asset owner, systems integrator or distributor which is done by local offices.

D2.5 Can you give an indication of the lead-time of your product to your customer?
Interviewee: This highly depends on the availability of the parts that are needed to assemble the products. Sometimes this delays the lead-time. But overall the COTS products are widely available.

Part 3: Incident report

D3.1 Has there been any incident reported with your product with respect to insourcing, transportation/warehousing, delivery at customer, product usage, production?
Interviewee: Not to my knowledge but it can happen a delivery of a distributor or systems integrator we work together is delayed.

D3.2 What do you do when such thing happens? It could be the device that is being shipped is first being tampered with before it is delivered at destination.
Interviewee: Actually we are not aware that these activities can be suspicious of that kind.

D3.3 Has there been any incident reported regarding software/hardware counterfeiting, malicious code infection, installed backdoors and such?
Interviewee: With our PLC products there hasn't been any of those incidents reported by the OEM itself, however what is more likely to happen is that cables and other equipment that are used to connect the components and systems with each other are of less quality than expected and probably are counterfeit products.

D3.4 Any other incidents reported regarding cyber security?

Part 4: Controls and measures in place

D4.1 What controls do you have in place to secure your product and production process?
Interviewee: The OEM does a lot when it comes to testing of the product before it leaves the production plant. When a product is in system-under-test phase the product is thoroughly tested on functionality and robustness to receive the Achilles 2 certificates which means the product's works as required on IP-level. Achilles 1 certificate is certificate for quality of hardware however only the IP-level requirements are tested by the OEM and all products have Achilles 2 certificate.

Additionally, the OEM believes the biggest threat to ICS and PLCs is human error and therefore they organize security awareness training in an existing factory. Several aspects of defence-in-depth are covered like access control and perimeter security. Also, they offer in depth Plant Security on physical, network and control level but these measures only are present in the industrial plant. As a side-note they always recruit an engineer with IT knowledge as security officer for the plant that does administrative security checks like password management.

D4.2 What controls do you have in place to secure transportation/warehousing?
Interviewee: I can't answer that with my knowledge.

D4.3 What controls do you have in place to secure the product after it is in use by your customer?

Interviewee: We do software integrity checks after delivery only if specifically asked for, usually with very complex and large destination plants like in the petrochemical plants where our products are going to be used and not with the smaller production plants. So this is application dependent.

D4.3 How do you secure your product?

Interviewee: We implement plant security that consist of perimeter security, access management and network segmentation.

General Comments

DGC **Interviewee:** The OEM thinks it is their responsibility when it comes to security of their product and therefore they give the awareness training to anyone who is responsible for configuring, updating, operating the devices in an industrial plant. However there is little awareness of supply chain threats and security in the supply chain.

Furthermore, the most vulnerable processes for the OEM would be the firmware/software loading and updating on the devices.

Next to that what happens to a product when its returned because of malfunction. There are two possibilities; either the product is at its end of life or the product needs to be repaired. In most cases the old product is destroyed completely and the new model in the same line is offered for replacement, this also happens to any product that is more than ten years old. When a specific product is returned under warranty but is not produced anymore the same product is revised and returned. That's how the end of the lifecycle looks like at the OEM's Industrial Automation.

Finally, about delivering products the interviewee also mentioned that in some countries delivery is not even possible like in Iran.

Appendix E

Interview with a Systems Integrator/Solution Provider

Interviewee role within organization: Process Automation Solutions

Part 1 General questions

E1.1 Can you describe your products(technical specifications)?

Interviewee: The firm consist of several departments namely diary, processing and packaging. The PLCs are in-sourced from suppliers, mainly from OEMs mentioned in Chapter 2. The firm develops software on top of the PLCs and it is built into the machines before it is shipped to the customer. However, some machines are also shipped without any PLCs. PLCs are grouped into three distinctive levels, distinguished by size of application. The first level are PLCs that reside in one unit, the 2nd level is in multiple units in a production line and the 3rd level is on plant level with multiple production lines and a central control room.

Their machines' code is open and therefore customers can reprogram parts of the code that is standard delivered, this will void warranty but it enables more applicability for the customer, this is mainly the case in production line and plant wide solutions. These solutions are more open to integration. The personnel is responsible to install machines after it gets thoroughly tested for acceptance. The final code gets deployed when the machine is staged at the customers' site.

E1.2 What do you think is the greatest threat for your product?

Interviewee: To be honest there are not much threats to our PLCs we think but we are mostly concerned about Intellectual Property. When our code gets tampered with it might damage the trademark, which is really important for us.

Also, when firmware is changed the machine needs to be revalidated because our code only works with a particular firmware version of OEM. The machine is validated together with firmware. Furthermore revalidation is 2-years process so it would not be effective as a threat.

However, in quite some existing machines Windows NT is present that has some known vulnerabilities inherited.

E1.3 Can you describe your production process in general steps?

Interviewee: Insource plc, develop software, create solution, and configure software to specific environment, delivery, installation & code deployment, acceptance test.

Part 2: Supply chain

E2.1 Do you insource any parts from suppliers? If yes, what kind of parts?
Interviewee: The firm is largely a mechanical company and therefore any form of electronics is in-sourced from several suppliers. Operator panels, GUI related software, windows-based programs and OS for integration are among the parts that are in-sourced.

E2.2 Are they always the same suppliers? If no why?
Interviewee: We have contracts with many suppliers and they don't change often because we have built a relation of trust.

E2.3 How do you choose new suppliers or new distributors or other collaborations?
Interviewee: This is mainly a customer demand to have a solution based from a specific vendor. We don't collaborate with distributors.

In some cases we hire 3rd party integrators to install machines for us at the customer site. These collaborations are chosen on criteria such as experience, financial capability, stability, appliance with ISO-certs. Basically same quality requirements that the firm itself adheres to. Moreover, they must come to the firm for special training to be able to install solutions at customer sites.

E2.4 How is transportation/warehousing to your customers arranged?
Interviewee: We don't act through retailers and we don't work together with 3rd party logistics. We do this ourselves.

E2.5 Can you give an indication of the lead-time of your product to your customer?
Interviewee: Can't give an approximation.

Part 3: Incident report

E3.1 Has there been any incident reported with your product with respect to insourcing, transportation/warehousing, delivery at customer, product usage, production?
Interviewee: Nothing cyber threat related.

E3.2 What do you do when such thing happens? It could be the device that is being shipped is first being tampered with before it is delivered at destination.
Interviewee: We deploy software after installation and with that we haven't experienced this yet.

E3.3 Has there been any incident reported regarding software/hardware counterfeiting, malicious code infection, installed backdoors and such?
Interviewee: Our software development process and the loading of the software on the devices is a secure process that can only be done in a certain way with certificates, so far we don't have any reports of malicious software. However, because a part of our code is also open code and it can be modified anywhere. Disgruntled employee or 3rd party integrator could install backdoors or modified firmware at the customers' site for example but no reported cases.

E3.4 Any other incidents reported regarding cyber security?
Interviewee: We did a survey on the market about this and we found 1 case: not to PLCs but the systems got infected by a USB device. This was due a customer operator. All actions are logged and from there the root could be found.

Part 4: Controls and measures in place

E4.1 What controls do you have in place to secure your product and production process?
Interviewee: In our code the critical parts are encrypted therefore only with special certificates this can be changed or obtained. Moreover, after installation on customer site the software is deployed so we try to have the critical process

the latest as possible. We also have a mechanism for tamper proofing to protect our intellectual property. For hardware intrusion we don't have any mechanisms because our products are not resold or distributed.

E4.2 What controls do you have in place to secure transportation/warehousing?
Interviewee: The firm itself does transportation warehousing; there is a level of trust involved.

E4.3 What controls do you have in place to secure the product after it is in use by your customer?
Interviewee: We don't spend effort in securing the information the machine is producing once it is operative. After the installation and configuration the machines belong to the customer. We don't do audits on delivery afterwards, beyond what we legally can do. After customers sign it's their equipment.

E4.4 How do you secure your product?
Interviewee: With the encryption that is just mentioned.

General Comments

EGC **Interviewee:** In general the firm handles almost every step in the lifecycle of the industrial device. The devices are in-sourced from OEMs and from there it is the firm's business. Quality is from utmost importance and that?s what the delivering of the solution is about. No 3rd party logistics are involved and only certified 3rd party integrators may handle the devices for installation. This drastically reduces the possibilities for attackers. For better integration in broad applications of their solutions some code is made open to changes, however there is no warranty for changes, only warranty on delivery of the solution. The main concern is Intellectual Property theft, this is directly handled with use of encryption, certificates. Responsibilities are laid down in contracts with customers and other collaborations.

Appendix F

Interview with an End User of an ICS

Interviewee role within organization: Manager Global Process Control & Utilities
Note: the interview questions are slightly different as an asset owner does not produce any products itself but is at the end of the supply chain. The perspective of an Asset Owner has therefore a different set up in the questions asked.

Part 1 General questions

F1.1 Can you describe your how you acquire an ICS? How is this changed over the years?

Interviewee: After the assignment is issued for an existing factory to be replaced or a new one to be built, the asset owner designs the factory and the negotiation with suppliers begin. At first the basic design features are discussed like surface area, number of processing, filling and packaging units for example. From the drawing board applicable suppliers are selected.

In the past 30 years the asset owner has experienced that the components are far less obscure than they used to be. The components are now running mainly on Windows OS. The reason for this is that the production demand rose and at the same time extra efficiency in production was required. So more production with less people.

All factories are 'Proleit' configured, that is a working program for all our factories and that's also where we train our employees for. The asset owner enforces to use ISA-99 standards for designing all process automation systems.

F1.2 What do you think is the greatest threat for your environments?

Interviewee: Greatest risk for the devices and the factory in general is old employees taking revenge. Another risk that they are aware of is that some of the equipment is too old and no spare parts are available anymore. Deliveries of the equipment was never tampered with before.

F1.3 Can you describe the configuration/installation of your assets in general steps?

Interviewee: With the creation of a new factory, the asset owner inherits IT security in the design of the new process automation domain. The roles and responsibilities are divided between process engineers and IT managers in order to fully utilize the factory. Every factory has its own IT service organization and awareness of cyber threats in the factory is well brought about to the engineers, IT service organization and other employees.

Part 2: Supply chain

F2.1 How do you select new collaborations?
Interviewee: When a tender is set out for the designing of the new factory the asset owner seeks to only collaborate with one supplier or OEM. The collaborator needs to comply to the used standards. Usually, the OEM also assumes the role of systems integrator and provides the whole solution for the whole plant. Because there are not many integrators of the brewery factories the asset owner requires, the choice with who to collaborate is usually limited but easy to make. Because all factories are 'Proleit' process control technology configured, this actually leaves little to no space for OEMs for custom configuration.

F2.2 Are they always the same suppliers? If no why?
Interviewee: No not always, It sometimes happens that it's not possible to collaborate with only one OEM or systems integrator. In this case an external relation is entered into. However, because only 2 or 3 integrators are applicable in our sector the choice is limited.

F2.3 How do you choose new suppliers or new distributors or other collaborations?
Interviewee: Mainly on performance criteria: how many process alarms can be configured, delivery time of the supplier and also how does the software behave on startup for example. Also, the collaborations need to comply with the same standards we operate in, namely ISA-99.

F2.4How is transportation/warehousing to your customers arranged?
Interviewee: This is done by the integrators and OEM's we work together with.

Part 3: Incident report

F3.1 Has there been any incident reported with your product with respect to insourcing, transportation/warehousing, delivery at customer, product usage, production?
Interviewee: We never had any reported problems regarding a delivery of equipment of a new factory. Also, i think PLCs are generally not being targeted in the supply chain.

F3.2 What do you do when such thing happens? It could be the device that is being shipped is first being tampered with before it is delivered at destination.
Interviewee:

F3.3 Has there been any incident reported regarding software/hardware counterfeiting, malicious code infection, installed backdoors and such?
Interviewee:

F3.4 Any other incidents reported regarding cyber security?
Interviewee: No not at all.

Part 4: Controls and measures in place

F4.1 What controls do you have in place to secure your factories?
Interviewee: The risk management process of the asset owner consist of a very detailed analysis of what equipment is in use with their inherited vulnerabilities. They estimate the possibilities for attackers to exploit the vulnerabilities and determine critical processes. There are systems that still run on Windows NT, they are vulnerable. It happens that the IT manager is not certified and capable enough for the security task.

F4.2 What controls do you have in place to secure transportation/warehousing?
Interviewee: Asset owner demands a clean install of the Integrator or OEM where the asset owner can load its own application for their factories.

F4.3 What controls do you have in place to secure the product after it is in use?

Interviewee: Measures that are used to secure the PLCs are two-factor-authentication for updating the devices and for installation too. Two-factor authentication is also used for maintenance on the PLC from the outside.

F4.4 How do you secure your product in the future?

Interviewee: The asset owner strives towards shifting the responsibility of the supply chain towards the IT organisation