Universiteit Leiden

ICT in Business

Cyber Security in the Supply Chain

Name: B.(Boudewijn) M.C.S. Middendorf
Student-no: 1314661

Date: 14/04/15

1.1 *1st supervisor: Prof. dr. J.N. Kok*

1.2 2nd supervisor: Prof . dr. H.J. van den Herik

Abstract

The focus of this Master thesis is Cyber Security in the Supply Chain. We will take a closer look at current methods and models that are used to achieve Cyber Security in the Supply Chain (CSSC). We will provide the central question: ‘Can we achieve and guarantee a certain percentage of Cyber Security in the Supply Chain?’

Currently, only standards like the International Organization for Standardization (ISO) 27036 and 28000, International Society of Automation (ISA)/ International Electrotechnical Commission (IEC) 62443 series and the national standards like the US National Institute of Standards and Technology (NIST), are used to perform CSSC. These standards ensure that the procedures within suppliers of products or key-components (ICT-hardware, software and firmware) are based on the same standards. When analyzing these standards it is remarkable that they are mainly focused on ‘trust’ between suppliers and acquirers. And they do not run a check on key-components other then acceptance and release tests. There is currently no method or model that checks the key-components on their Cyber security.

Therefore we have developed the Six-step method. This method will help the acquirer and supplier to check the key-components of their product or products. This check uses the method for information security, which focuses on three parts: confidentiality, integrity and availability abbreviated CIA. For high-tech products with a high number of key-components it is difficult and impossible to guarantee a complete 100 percentage of CSSC. The Six-step method determines what is relevant to analyze, as in key-components and their backgrounds. The Six-step method helps the acquirer and suppliers to check a new and high-tech product on CSSC and gives an advantage when there is an update of a key-component within a product. The benefit of the Six-step method is to reduce the time to perform a CSSC check on an acceptable level. Together, with the current standards that are used and our Six-step method, it is possible to create an even higher percentage of CSSC. After writing the thesis we will test our method on a high-tech product. This test will be performed by using a syllabus to test the product which is added to this thesis as appendix 1. With the outcome of the check in the use case we have adjusted the Six-step method. The improved Six-step method is created into an improved syllabus which will be used for CSSC-checks and is added to this thesis as appendix 2.

Table of Contents

1 Introduction

The central question that we will answer is:

Can we achieve and guarantee a certain percentage of Cyber Security in the Supply Chain?

We start by showing that the statement ‘Cyber Security in the Supply Chain (CSSC) is not guaranteed’ is well substantiated with several articles in the media. A product consists of many different components from different suppliers and sub-suppliers or sub-contractors. Many products that are developed and produced, are not made by one single supplier. In the process of making the product many sub-contractors are involved in producing small parts that are used later on in many different products. This process with the different components from suppliers is the supply chain. Sometimes a product contains components from three or more different suppliers. Because there are so many suppliers and sub-suppliers, it is impossible for us to be familiar with all these different supplier and sub-suppliers and to check whether their components could be manipulated.

To answer the central question, we divide the central question into three main research questions. These questions are:

1. What is the State of Art in CSSC:
    a. What is written in the literature about components and Cyber Security in the Supply Chain?
    b. Is there currently a model or method for cyber security checks in the supply chain?

If the answer on the first question is negative, then we will answer the second question.

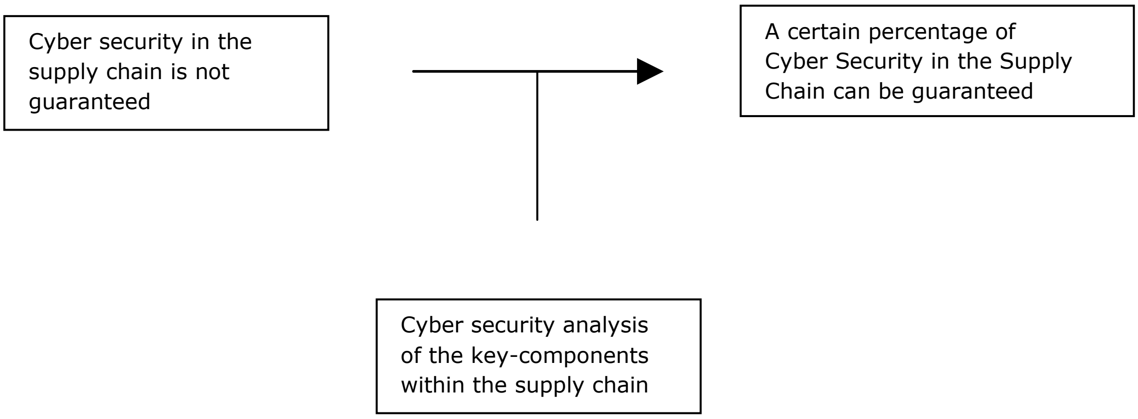
2. Can we develop a model or method for CSSC?

3. Can we evaluate our developed model or method by checking a use case on Security in the Supply Chain?

A related question to the central question is: ‘how the optimal Cyber Security in the Supply Chain can be achieved with as little effort as possible?’ Within a supply chain there are many different suppliers. This makes it possible to provide CSSC and especially to guarantee security. More and more products have ICT components and therefore need to be checked on Cyber Security. Robert J. Bowman (2013) writes in the article “Why Cybersecurity is a Supply-Chain Problem” when a business case is created the senior-management needs to be helped to make sure that a basic plan of action of CSSC is part of such a business case. He also states that like any good internal review, it also involves asking the right questions: Which products, components or raw materials are we outsourcing? To whom? David Inserra and Steven P. Bucci (2014) write in their article “Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace” that Cyber Security in the Supply Chain is too important to be ignored. High technological products gives the users of these products a lot of advantages. The global marketplace makes products cheaper but this increases the risk of compromised ICT-hardware, firmware and software. These risks should be taken seriously.

We want to find the vulnerabilities that comes with the use of more ICT-hardware, firmware and software in products. One of the largest threats of the vulnerabilities are Zero days. Zero days are vulnerabilities in software that are not yet known to the public or the developer. With Zero days there has not yet been an update of software or ICT-hardware with an improvement code which will tackle this vulnerability. These vulnerabilities are often used by hackers for Cyber-attacks. Mainly countries pay for the knowledge of these vulnerabilities to find a way to attack other countries. Abhay Joshi (2004) elaborates in the article “How to protect your company from 'Zero-day' exploits” on www.computerworld.com upon a few examples are mentioned of Zero–days. It is likely that in firmware or in software malicious codes are inserted in components of products during the assembly of another product. The aim of our research is to ensure more Cyber Security in the Supply Chain in the future and to prevent those codes. We will use literature and interview people who are now part of Cyber Security in the Supply Chain (CSSC) sector. For testing our theory we will use as a use case, a high tech product from the organization in The Netherlands Toegepast-Natuurwetenschappelijk Onderzoek (TNO). More information can be found on their website at www.tno.nl.

If we are unable to answer the first research question whether there is currently a model or method to achieve CSSC, we will develop our own method or model. Here below we discuss the conceptual model which helps us to develop a model which supports us to answer the second question. When we have to answer the second research question the conceptual model helps us to develop a model in a later stadium of the master thesis.


Cyber security in the supply chain is not guaranteed
A certain percentage of Cyber Security in the Supply Chain can be guaranteed
Cyber security analysis of the key-components within the supply chain

The conceptual model above shows a predictive argument. Which means that by analyzing the key-components within a product, the prediction is that a product will be more cyber secure. A guided model is used to identify the key-components and to analyze them so that a certain percentage of Cybersecurity can be guaranteed. The analysis of the key-components will be explained by means of a use case which will help to clarify why certain components are essential for CSSC.

This thesis is based on a literature study in combination with interviews for the use case. The thesis starts by the introduction with a motivation for the thesis with the central question and the conceptual model. In the next section we will explain some background terms. We show different types of method about how ‘trust’ within companies within their supply chain is described. The section Six-step method explains the new method about security in the components of the product. The last section contains the conclusion of the two described methods at section 4 and 5. In section 6 we use a high tech product to check a method and where needed the method will be improved. After this use case there is a section 7 with the conclusion of the development and the use of the method.

2 Background

This section gives some background information relating to Cyber Security in the Supply Chain (CSSC), including definitions and explanations of components, and about the security for CSSC. Countries and organizations which value security, vary in the definitions of what and where CSSC stands for. There are multiple definitions available of terms related to this thesis therefore we made some choices to define the basic terms that are related to CSSC. The basic terms and definitions we defined are:

Cybersecurity

The National Coordinator for Security and Counterterrorism states that “Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems."

Supply chain management
The Council of Supply Chain Management Professionals (CSCMP) states on their website (http://cscmp.org/) that "Supply Chain Management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third-party service providers, and customers. In essence, Supply Chain Management integrates supply and demand management within and across companies. Supply Chain Management is an integrating function with primary responsibility for linking major business functions and business processes within and across companies into a cohesive and high-performing business model. It includes all of the logistics management activities noted above, as well as manufacturing operations, and it is leading coordination of processes and activities with and across marketing, sales, product design, finance and information technology."

Component
The Dictionary of technical terms describes a component as "Computers are made up of many different parts, such as a motherboard, CPU, RAM, etc. Each of these parts consists of smaller parts, called components. For example, a motherboard includes electrical connectors, a printed circuit board (PCB), capacitors, resistors, and transformers. All these components work together to make the motherboard function with the other parts of the computer. The CPU includes components such as integrated circuits, switches, and extremely small transistors. These components process information and perform calculations.

Generally speaking, a component is an element of a larger group. Therefore, the larger parts of a computer, such as the CPU and hard drive, can also be referred to as computer components. However technically, the components are the smaller parts that makes up these devices." In this thesis we say that all the small parts are seen as components as well. All the components are all the parts of a product.

We state that the key-components are the ICT-hardware, firmware and software of the product unless stated otherwise.

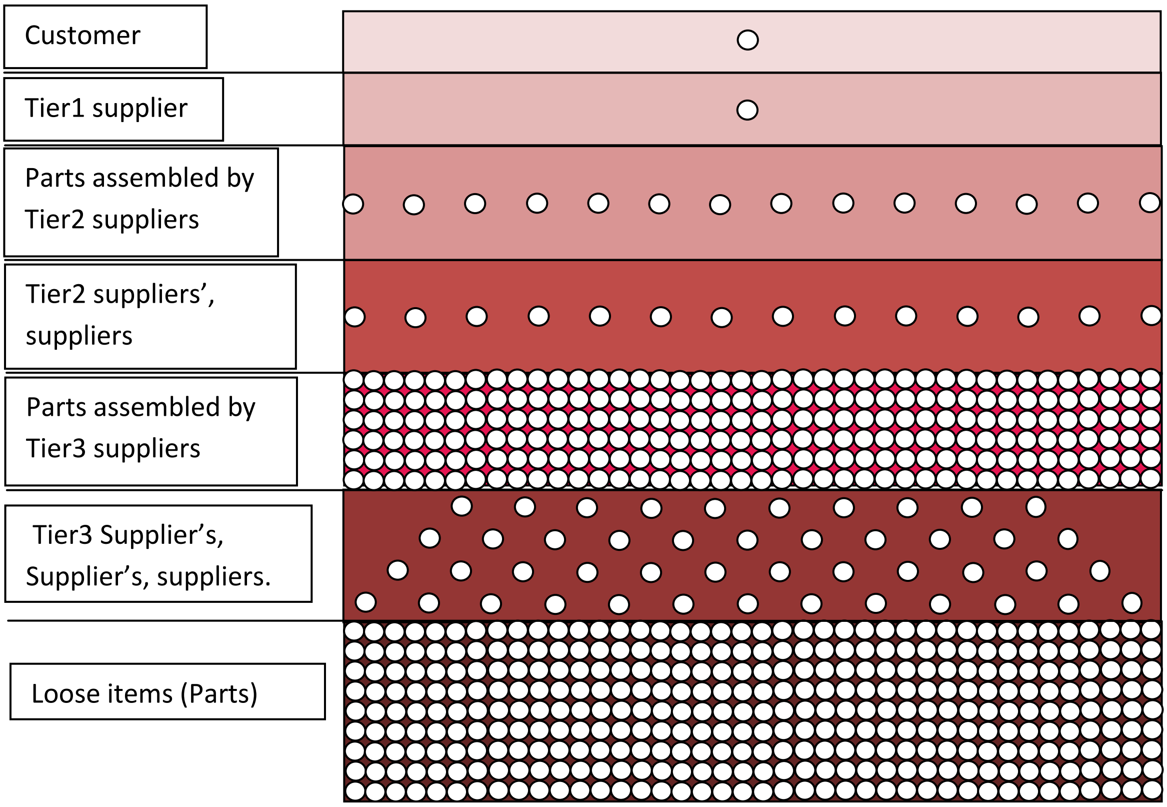
ICT-hardware
ICT-hardware includes the computer chips, which process and complete the work needed to perform a given task. Multiple components may form ICT-hardware. ICT-hardware can also be seen as a component by itself.

Firmware
Firmware is embedded software which is needed for basic ICT-hardware operation and is essential for a computer chip to operate properly.

Software
Software is being used in computer programs that tasks the ICT-hardware with specific activities and tells how to complete those activities in order to obtain a certain result.

3 Current methods for Cyber Security in the Supply Chain

In this section we will start with describing current methods and models used for Cyber Security in the Supply Chain (CSSC). Here we illustrate the complexity of how a product is produced and built by all the different suppliers and sub suppliers/sub contractors in the following sub-sections. There are different methods of achieving CSSC. One option is to focus on the companies and the security within that company. This is called defense in depth and will be explained in section 3.1. To achieve defense in depth there are many different ways. Companies have for their methods of working certificates and because of that they use audits. Therefore they can be checked. Another possibility is the focus by studying and analyzing a product. As we described earlier in this Thesis a product is produced by many different suppliers and has a lot of components, and it is not clear for the customers to know who is the supplier of the suppliers. We have visualized this below in figure


Customer
Tier1 supplier
Parts assembled by Tier2 suppliers
Tier2 suppliers', suppliers
Parts assembled by Tier3 suppliers
Tier3 Supplier's, Supplier's, suppliers.
Loose items (Parts)

1.

Figure 1: A product with all the supplier, suppliers from the suppliers and the different parts (components).

Next we will zoom in on "Defense in depth", because security is a layered defense of physical and technological security. Then we will present ISO and ISA methods that are connected to the topic of this master thesis. We will also spend a part of this thesis on standards used by countries. These different standards give an overview of 'trust' that the standards create between suppliers and countries. Please note that these standards are not used by us to create our method, it only serves as background information to the subject.

3.1 Defense in depth

In this subsection “Defense in depth” we will show that security or defense within a company needs to be implemented in different layers within organizations. With defense we do not mean the military term. Therefore the first option to achieve CSSC is by checking the procedures of “Defense in depth” at the contracted companies. This type of defense provides security on different levels within the contracted companies. This can be a physical security at the gates to regulate the security of the key-components with which the company is working with. There are multiple articles written about “Defense in depth” and how to implement this within companies.

For example Miller, Vandome en McBrewster (2010) describes that “Defence in Depth” is also known as “Elastic Defence” or “Deep Defence”. This last type of defense, is a chain of security on different levels within the organization. And there are more views on “Defense in depth”. Barnum (2005) writes that the world of ICT “Defence in Depth” also works, because by a layered defense in software the change the success factor of an attack from outside reduces.

Smith (2003) writes in his article, that the “Defence in Depth” (layered defence) strategy is a fundamental principal of physical security of the different parts of an organization. In the article of Jon Ringler on www.tech-wonders.com “How Cyber Attackers and Criminals Use Defense in Depth Against IT Professionals”, he explains that ‘defense’ states that Defense in Depth at its inception was a military strategy originally defined by the National Security Agency (NSA). The goal of this Defense in Depth strategy was to elongate and delay rather than prevent the success of an attacker therefore exhausting their resources and causing them to diminish their forces while buying time and keeping attackers at bay. Instead of defeating an attacker and defending their territory with a single, strong defensive mechanism, Defense in Depth relied on the tendency of an attack to lose momentum over time as resources were consumed over a period of time. This would allow a defender to give up lightly defended grounds in an effort to use an attacker's logistics to consume its own resources, rendering them susceptible to a counterstrike. As attackers' resources are consumed and they have begun to lose momentum and cover more ground, a counter strike could be launched on the attacker's weak points in an attempt to cripple the attacker or cause them to fall back to their original positions.
The following figure 2 depicts a basic visual representation of Defense in Depth as it was designed.

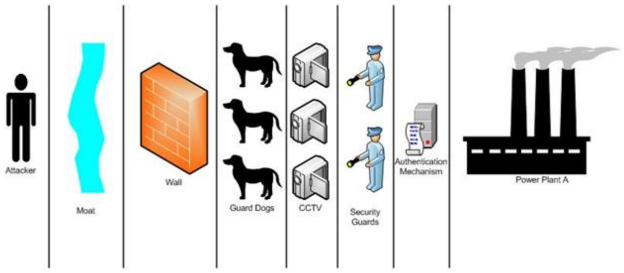


Figure 2: Defense in depth

Each one of the lines above illustrates different Defense in Depth mechanisms for which the concept was initially designed. The major differentiator is that Defense in Depth was designed for a physical real world application.

Defense in Depth for IT Professionals is an Information Assurance (IA) concept in which multiple layers of security controls are placed throughout an IT system. Defense in Depth for the IT world layers people, processes and technologies, with the intention to provide additional security controls if the primary security control fails or have a vulnerability which is exploited to circumvent the primary control. Defense in Depth comes down to having multiple defensive mechanisms, at multiple layers and performing different tasks.

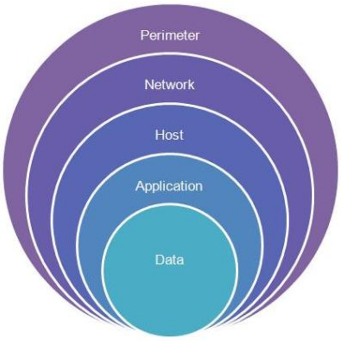


Figure 3: IT Defense in Depth is better defined as a Layered Defense Model.

An example of this Defense in Depth or Layered Defense is the use of a Network Based Intrusion Prevention System (NIPS) and a Host Based Intrusion Prevention System (HIPS). The NIPS operates at the Network Layer and provides a defensive mechanism inspecting traffic as it traverses the network. If the network traffic can pass through the NIPS, the HIPS can provide another mechanism for inspection and protection."

We will not go further into detail about "Defense in Depth". It is important to understand that many different standards are mostly based on a certain level of "Defense in Depth". Because these standards are mostly focused on "Defense in Depth" the mutual confidence between suppliers, the acquirer or customer and the manufacturer should grow. This mutual confidence is a kind of 'trust' between the manufacturer and the customer of the product.

3.2 Standards

In this sub-section we will highlight several standards that are currently used to provide Cyber Security in the Supply Chain (CSSC). The standards we describe in this sub-section have the characteristics of building a relationship of 'trust' between the supplier and the final customer. These initiatives of standards can be found in civil standards or standards for doing business with state institutions. There are different civil standards, in the next sections we will focus on two standards that are close to the subject of this master thesis. These two standards are the ISO-standards and the ISA-standards. When an involved product has specific military purposes there are different standards for state institutions. Those standards often contain a combination of multiple ISO and ISA standards.

ISO Standards

The first standard that we describe in this sub-section is from the ISO organization. The ISO organization describes on her website what ISO means and what it stands for. "ISO stands for International Organization for Standardization which is an independent, non-governmental membership organization and also the world's largest developer of voluntary International Standards. The organization is made up of 165 member countries which are the national standards bodies around the world, with a Central Secretariat that is based in Geneva, Switzerland.
ISO gives world-class specifications for products, services and systems, to ensure quality, safety and efficiency. They play an instrumental role in facilitating international trade. In total they have published more than 19 500 International Standards covering almost every industry, from technology, to food safety, agriculture and healthcare. ISO International Standards affects almost every supply chain. In 1946 ISO was founded by delegates from 25 countries, they met at the Institute of Civil Engineers in London and decided to create a new international organization 'to facilitate the international coordination and unification of industrial standards'. In February 1947 the new organization, ISO, officially began operations. Since then there have been published over 19 500 International Standards covering almost all aspects of technology and manufacturing.

The current amount of 165 member countries and 3368 technical bodies take care of standard development. 'International Organization for Standardization' would have different acronyms in different languages (IOS in

English, OIN in French for Organisation internationale de normalisation). ISO is derived from the Greek isos, meaning equal."

Next ISO is the International Electrotechnical Commission (IEC). This is an organization that works together with ISO to create standards with the focus on the technical level. The Deutsches Institut für Normung e.v. (DIN) describes how the specializes system for the worldwide standardization are formed by the organizations ISO and the IEC. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees, they are established by the respective organizations to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in this work. The organization DIN also illustrates in the ISO/IEC JTC1/SC27 how the IT security Techniques should be implemented. They write that "in the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. The ISO/IEC JTC 1/SC 27 stands for it security techniques (SC) 27000 series and are related with the topic of this thesis. Draft International Standards adopted by the joint technical committees are circulated to the national bodies for voting. A publication as an International Standard requires an approval by at least 75% of the national bodies which are casting a vote.

The scope of SC 27 is the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas." We consider the cooperation between ISO and IEC as an important link to CSSC, because SC 27 focuses on de the development of standards for the protection of information and ICT. Although SC 27 is an important standard and is still focused on the suppliers and not on the product itself.

We will highlight one of the 27000 series the ISO/IEC FDIS 27036-1:2014 which can be found on www.ISO.org. This describes the Guidelines for information and communication technology for the supply chain security in part 3. "That an ICT product or service procured by the acquirer is not necessarily manufactured or operated solely by a single supplier. In supplier relationships, an ICT product or service procured by the acquirer is not necessarily manufactured or operated solely by the supplier.

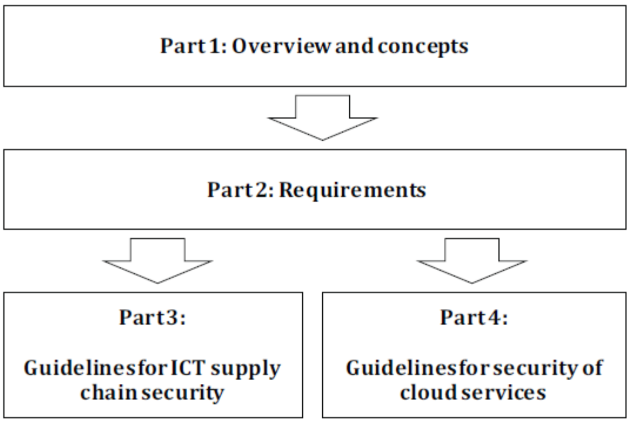

Part 1: Overview and concepts
Part 2: Requirements
Part3:
Guidelines for ICT supply chain security
Part4:
Guidelines for security of cloud services

Figure 4: ISO/IEC 27036 Architecture

For example, a product often contains parts that are made by other suppliers and is provided to the supplier by an indirect relationship with the acquirer. Or, an information processing service can be built on other information processing services as its underlying infrastructure. For instance, the supplier has an agreement with another supplier to maintain the ICT-hardware, to store backups on an external location or even have the entire backup process outsourced. Thus, ICT supply chains are formed by successive supplier relationships with inherent interdependencies. In a supply chain, information security management and controls implemented by the supplier in direct relationship with the acquirer are not always sufficient to manage information security risks of a product or service."

Part 2 of ISO/IEC FDIS 27036-1:2014 describes the ICT supply chain of ISO as a set of organizations with a linked set of resources and processes that form successive supplier relationships of ICT products and services. "An ICT product or service can be composed of components, resources and processes produced by a supplier which can have been produced, in whole or in part, by another supplier. As such, an ICT service in its entirety, may have been sourced by multiple suppliers.

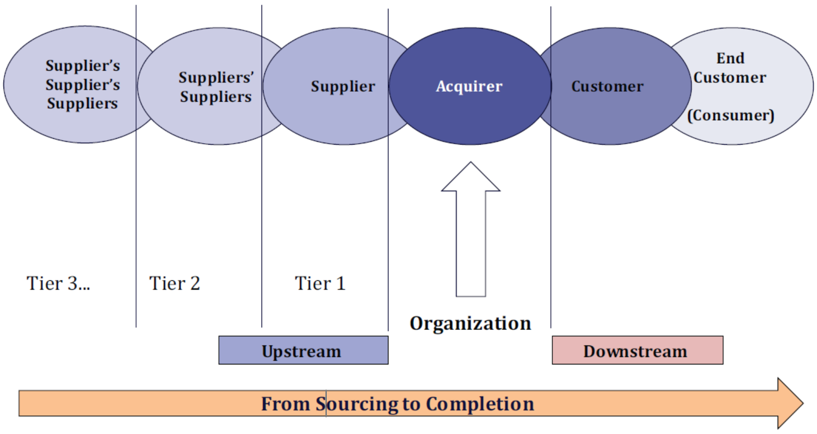


Figure 5: Supply chain relationships

Acquirers and suppliers throughout the ICT supply chain inherit information security risks associated with individual supplier relationships for products and services. However, it is challenging for acquirers to manage these information security risks through communicating, monitoring, and enforcing their information security throughout the complete ICT supply chain due to limited visibility for access to their suppliers' suppliers.

For example, an acquirer can require invasive audits of the supplier's systems that can result in the acquirer's access to the supplier's intellectual property. ISO/IEC 27036 Part 3 provides guidelines to acquirers and suppliers how to manage information security risks associated with the ICT products and services supply chain." Again we see that this standard is not focused on the product or the components of the product.

Here below we will show the ISO-standards that have a connection with CSSC. Next to the ISO/IEC JTC 1/SC 27 there are more ISO-standards related to Cyber Security in the Supply Chain.

These ISO-standards are:

- 28000 (Specification for security management systems for the supply chain).
- 28001 (Best practices for implementing supply chain security – Assessments and plans – Requirements and guidance).
- 28002 (Development of resilience in the supply chain).
- 28003 (Requirements for bodies providing audit and certification of supply chain security management systems).
- 28004 (Guidelines for the implementation of ISO 28000).
- 28005 (Electronic port clearance (EPC) part 1 and part 2).

These ISO-standards show us the complexity of the Cyber Security in the Supply Chain that we are dealing with. Next to the ISO-standards there are another important standard that we want to explain in relation with the CSSC.

ISA Standards

In this sub-section we want to highlight the ISA standards because of the relation to building 'trust'. These ISA-standards are closely related to the ISO-standards, they are also standing for the international Society of Automation (ISA). This society is founded in 1945. On the website of the ISA organization (www.isa.org) an explanation of ISA is given. "ISA is a global, nonprofit organization that is setting standards for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities. Based in Research Triangle Park, North Carolina, ISA develops standards, certifies industry professionals, provides education and training, publishes books and technical articles, and hosts conferences and exhibitions for automation professionals."

The ISA organization has founded the ISA99 committee which has as goal "to develop and establish standards, technical reports and related information that will define procedures for implementing electronically secure industrial automation, control systems, security practices and assessing electronic security performance. Guidance is directed towards those who are responsible for designing, implementing, or managing industrial automation and control systems as defined in the committee scope. This guidance also applies to users, system integrators, security practitioners, control systems manufacturers and vendors. ISA99's focus is to improve the confidentiality, integrity, and availability of components or systems used for industrial automation, control and provide criteria for procuring and implementing secure control systems. Compliance with ISA99's guidance is intended to improve system electronic security and help to identify and to address vulnerabilities, reducing the risk of compromising confidential information or causing degradation or failure of the equipment of process under control."

We see that the ISA organization has a strong collaborative relationship with IEC TC65 WG10, which is the primary responsibility for developing the documents of the ISA/IEC 62443 series (ISA99), except the IEC 62443-2-4. "The ISA99 describes that she is a committee that currently consists of more the 500 members which represent organizations and industry sectors from across the globe. ISA99 is an accredited standard developing organization in the United States, the ISA99 committee is open to participation at no fee from virtually all interested parties." The figure on the next page illustrates the status of the ISA/IEC 62443 series of IACS standards and the technical reports. Hopefully this standard will soon be finished.

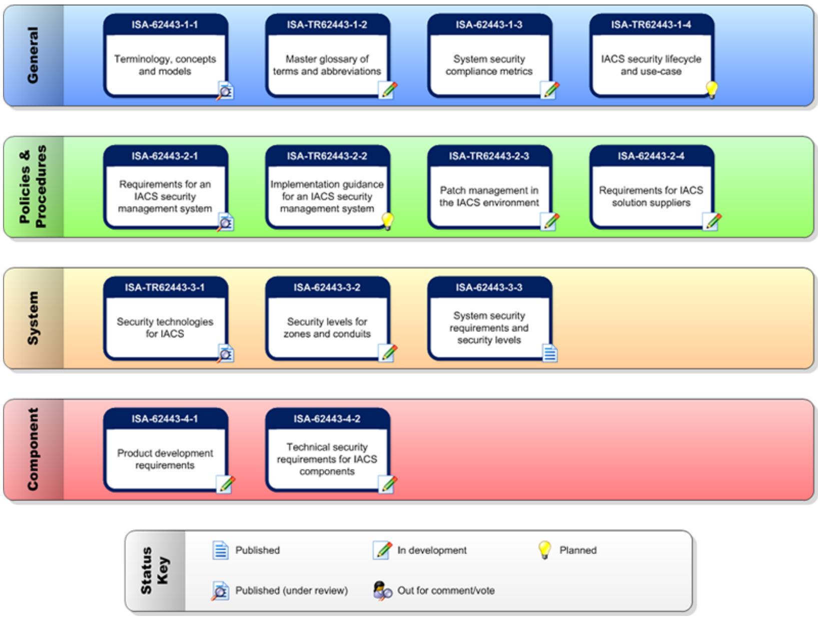

General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Policies & Procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Requirements for IACS solution suppliers
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components
Status Key
Published
In development
Planned
Published (under review)
Out for comment/vote

Figure 6

The ISA also explains that the ”institute ISA Security Compliance Institute (ISCI) has developed compliance test specifications for ISA99 and other control system security standards. The concept of manufacturing and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to ICT-hardware and software systems such as distributed control systems (DCS), programmable logic controllers (PLC), Supervisory Control And Data Acquisition (SCADA), safety instrumented systems (SIS) or associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Within this process physical security is an important component in the overall integrity of any control system environment, but it is not specifically addressed in this series of documents.” The ISA-standard is looking at components of large industries and not at components of products, therefore we will not use these standards. Although ISA is looking much deeper on technical level into systems and its components then ISO, for this thesis we will only focus on a product and its internal systems and the key-components within these critical systems. Countries are also working with certain standards to improve the ‘trust’ factor between them and the manufacturers in order to achieve CSSC. For state institutions the CSSC is different especially when military products are involved. These standards for countries often are a combination of multiple civil standards. In the next section we will explain how the United States has created their standards to create their ‘trust’ between them and their suppliers.

Countries

In this last part of the sub-section we will explain that there are also rules and standards made by countries. There are many countries which have a system to achieve some sort CSSC. These systems are similar with the ISO -and ISA-certificates. We will highlight in this thesis the United States. This is done because there are a lot of documents present on the internet to form a complete picture of how a CSSC is covered by them. The written documents about CSSC are provided to companies and manufacturers. They work together in order to prevent that there are creating systems which can be manipulated. Therefore the US according to the Whitehouse (2011) explains that “the US has made their own US-standards, these standards are created by the US National Institute of Standards and Technology (NIST) located on their website http://csrc.nist.gov. The NIST is the custodian of the NIST publications. The US Federal Information Processing Standard publications (FIPS)” have the responsibility for the computer security division, which also have publications and are named the Federal Information Processing Standards Publications (FIPS PUBS). These publications are issued by NIST after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002. All of these publications are mend to create some kind of 'trust'. This basis of trust is very important for Cyber Security in the Supply Chain for the future. This will be even more important since the disclosers of the surreptitious wistleblower Edward Snowden. I mention this informant because also a screening of personnel within companies working on high level systems of products are necessary to create a CSSC.

Woody (2013) writes in her article about a system that gives guidelines to a creation of technology products. It is, "the System Development Life Cycle (SDLC) and provides the structure within which technology products are created. This structure embeds organizational policies and practices and regulatory mandates in a repeatable framework that can be tuned to the uniqueness of each project. A growing recognition of the importance of security considerations throughout the life cycle has led to new initiatives to strengthen the ties for security within the SDLC. Woody explains different subjects that are relevant for this thesis. Like the National Defense Industrial Association (NDIA) that the System Assurance Committee has published on her website the "Engineering for System Assurance" guidebook. This document represents a collaboration of government and industry to establish the ways by which organizations can "assure effective functionality of our command, control, communications and related weapon systems with high confidence that the systems are not vulnerable to intrusion and cannot be compromised". This guidebook describes the process activities needed to achieve system assurance, a broad umbrella that includes security, safety, reliability, dependability and other quality attributes. With the help of an assurance case, an appropriate mechanism is introduced for assembling and evaluating the assurance attributes of a system.

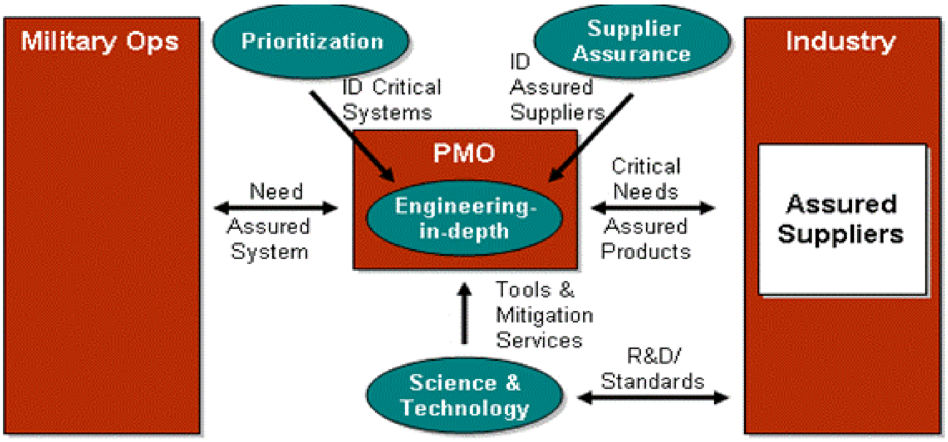


Figure 7: US Department of Defence concept of operations for software assurance

This guidebook is structured using the ISO/IEC 15288 for Systems Life Cycle Processes, but it can be adjusted for any standard SDLC structure. Assurance is recognized as a critical component in each level of processes:

- Agreement processes, which consist of acquisition and supply processes.
- Enterprise processes, which establish the capability to define and manage projects.
- Project processes, including project planning, project assessment, project control, decision making, risk management, configuration management, and information management.
- Technical processes, which cover stakeholder requirements definition, requirements analysis, architectural design, implementation, integration, verification, transition, validation, operation, maintenance, and disposal.

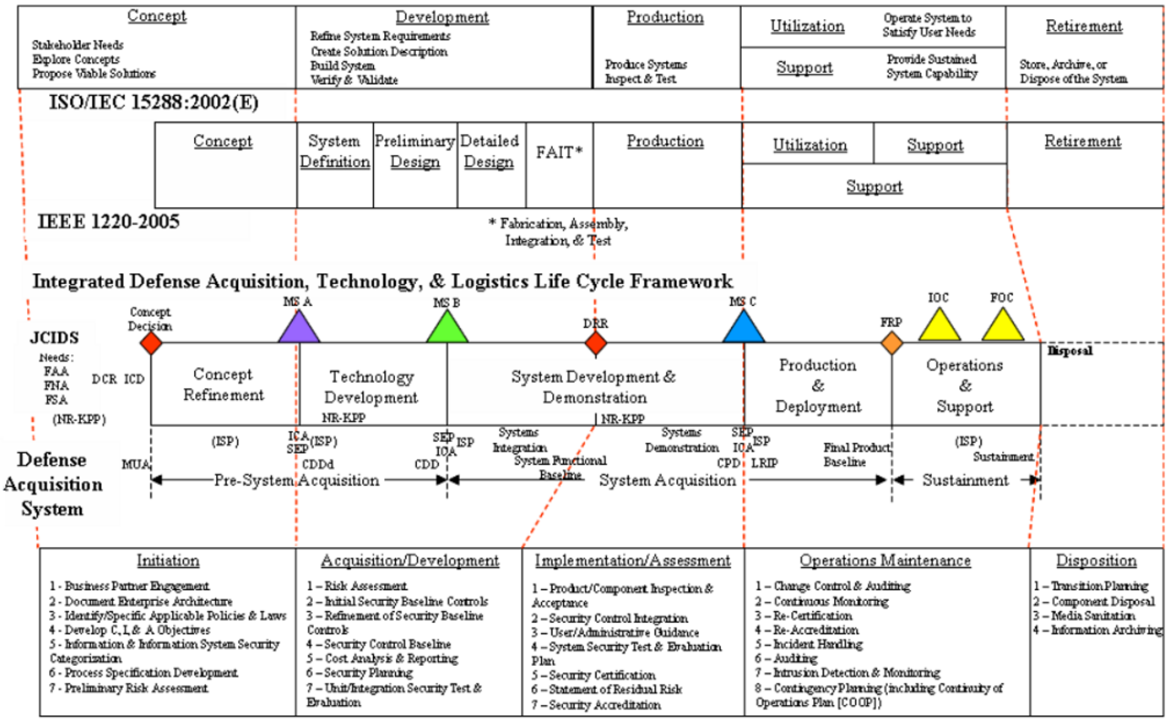
The activities that provide assurance of the outcome within each SDLC process must be considered and selected for every development effort. Project processes are of particular concern with respect to security. Projects must be planned to have appropriate funding for security, with mechanisms for managing the technical processes to ensure appropriate security. Risk management must consider and mitigate system assurance and security so that project stakeholders do not unknowingly accept risks that have severe financial, legal, and national security implications. A configuration management strategy must include control of configuration items critical to security, including change management for off-the-shelf components to effectively manage security patches and bug fixes. Information management must include protection and marking for proprietary, sensitive and confidential information.

Technical processes are also extremely critical to system assurance and security. Security requirements are to be tagged with a level of criticality that represents the allowed tolerance for compromise. Functionality must include considerations for both intrinsic (direct delivery of mission functions) and defensive (system security functions) elements. The architectural design must include considerations of least privilege, isolation/containment, monitoring and response for both legitimate and illegitimate actions, tolerance, identification and authentication mechanisms, cryptography, deception, use of interface standards and standard components, and anti-tampering techniques. The design must be evaluated for security weaknesses using appropriate techniques such as threat analysis, Failure Modes And Effects Analysis (FMEA), Failure Modes Effects And Criticality Analysis (FMECA), and Fault Tree Analysis (FTA). Implementation results must be evaluated to ensure, as much as reasonably possible, that known vulnerabilities have not been introduced."

The NDIA describes in the "Engineering for System Assurance" (2008) that the U.S. Department of Defense uses a Life Cycle Framework to give guidance to their used standards. Section 4 gives the guidance for system assurance in U.S. Department of Defense programs and explains that the document is "based on content to standards such as ISO/IEC 15288(The ISO/IEC 15288. This is a Systems Engineering standard which covers processes and life cycle stages.), relevant sections of U.S. Department of Defense Instruction 5000.2, relevant U.S. Department of Defense Information Assurance (IA) controls documented in U.S. Department of Defense Instruction 8500.2, and the Defense Acquisition Guide (DAG). The life cycle phases include:

- Concept Refinement;
- Technology Development;
- System Development and Demonstration;
- Production and Deployment;
- Operations and Support.

Figure 8 shows how the framework from the NDIA system assurance guidance in U.S. Department of Defense programs relates to industry systems engineering and information security standards."



Initiation	Acquisition/Development	Implementation/Assessment	Operations Maintenance	Disposition
1 - Business Partner Engagement 2 - Document Enterprise Architecture 3 - Identify/Specific Applicable Policies & Laws 4 - Develop C, I, & A Objectives 5 - Information & Information System Security Categorization 6 - Process Specification Development 7 - Preliminary Risk Assessment	1 – Risk Assessment 2 – Initial Security Baseline Controls 3 – Refinement of Security Baseline Controls 4 – Security Control Baseline 5 – Cost Analysis & Reporting 6 – Security Planning 7 – Unit/Integration Security Test & Evaluation	1 – Product/Component Inspection & Acceptance 2 – Security Control Integration 3 – User/Administrative Guidance 4 – System Security Test & Evaluation Plan 5 – Security Certification 6 – Statement of Residual Risk 7 – Security Accreditation	1 – Change Control & Auditing 2 – Continuous Monitoring 3 – Re-Certification 4 – Re-Accreditation 5 – Incident Handling 6 – Auditing 7 – Intrusion Detection & Monitoring 8 – Contingency Planning (including Continuity of Operations Plan [COOP])	1 – Transition Planning 2 – Component Disposal 3 – Media Sanitation 4 – Information Archiving

Figure8: U.S. Department of Defense Life Cycle Framework and National Institute of Standards and Technology Information Security and the System Development Life Cycle. Source: DAG

This picture above shows United States Department of Defense Life Cycle Framework and National Institute of Standards and Technology Information Security and the System Development Life Cycle. This gives a good view of the complexity of how a state institution is building their standards from the civil standards like ISO and ISA. Also these standards provide ‘trust’ between the companies and the State institutions. As we earlier described in this section the more suppliers a product has the more risks there are in which key-components can be compromised. Therefore we will elaborate on the subject of using a Government Off The Shelf (GOTS), Commercial Off The Shelf (COTS) and a Custom Element. Provide the CSSC it is important to know as the customer or acquirer how many and how deep the suppliers/sub-suppliers chain is.

In the “Engineering for System Assurance” (2008) from the NDIA there is stated that “there is a risk that lower-tier suppliers (down to the level of individual people) may insert, intentionally or unintentionally, vulnerabilities that impact the missions that the systems are to support. Thus, there is a need for management of this risk (including mitigation). Unfortunately, typical contracting approaches provide little insight into the supply chain, leading to great difficulty in decision making and risk management.

Therefore, there is a need to gain greater knowledge about the supply chain, to enable better decision making and risk management. Acquirers need more relevant and timely knowledge about their supply chain. Some suppliers are riskier than others. This does not mean that they cannot be used, but it does mean that additional countermeasures may be needed (e.g., greater transparency of the supplied element and/or its processes, limited privileges, blind buys, etc.).”

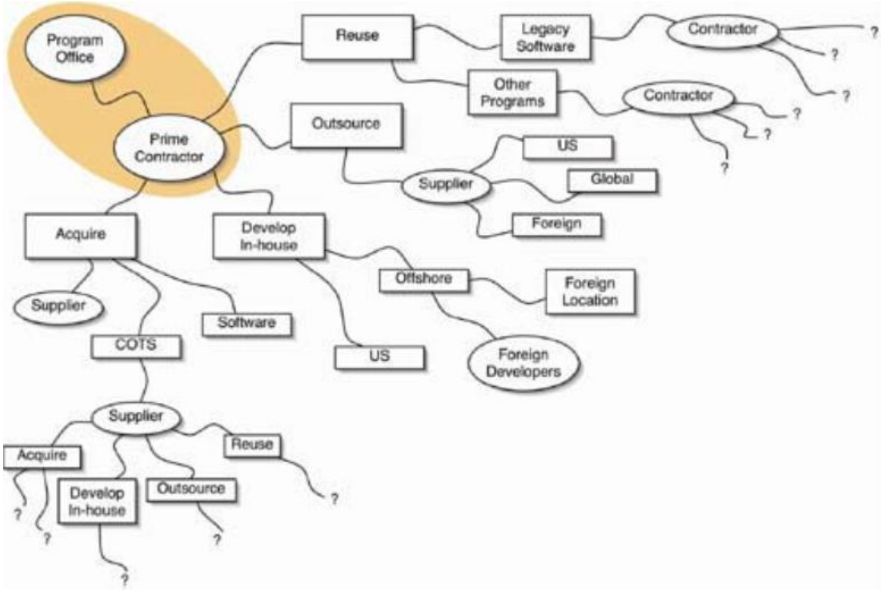


Figure 9: Source: Walker (2005)

At the apex of the supply chain is a system integrator, who selects Off-The-Shelf (OTS) elements (including Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS)) to be included in the component, develops/configures custom elements, or subcontracts to lower-tier system integrators who do the same. There are two major types of elements:

- OTS element, including COTS and GOTS. This often has the benefit of being used over time in many different applications and markets, providing a wealth of information about its risks through vetting by the marketplace. It may have been vetted through other mechanisms as well, like certifications and evaluations, etc. While vulnerabilities may be embedded in the OTS element, varying use of the OTS may expose them, and since the OTS supplier often does not know exactly how or where the element is used, targeted attacks are often more difficult to implement. OTS elements are often far less costly than custom development. Depending on the needs of the system, however, existing OTS options might not provide the properties required for the mission.

- Custom element, developed by a system integrator (at the top or lower tier). Such elements are typically not used in many different applications or markets. The developers of these elements typically have great insight into exactly how the element will be used, including its operational environment and its associated requirements. Vulnerabilities in custom elements present greater risks, because there is usually no marketplace vetting, and a malicious supplier could determine precisely how to cause the most damage to the system.

In some cases, an element may start as a custom element and then changes to become an OTS element. In other cases, an OTS element may require modification for use and that modified element becomes custom.

Any supplier could introduce a vulnerability into a system. However, the suppliers of custom elements should be examined especially carefully, because there is no vetting from the marketplace and it is easier for them to insert targeted attacks. Thankfully, it is also possible to impose additional requirements (e.g., on people, process, product/services, and tools) on custom elements to at least partly address this risk.” The information of the risks of an OTS/COTS/GOTS gives us a better picture of what key-component could be dangerous. Later we will describe how we will use this information to create a method.

In this section we have showed a few examples that cover standards like ISO and ISA and also standards within countries. Also the difference between OTS/COTS/GOTS and Custom elements are given. In the next section we like to address Software integrity, because with software integrity there are release and acceptance checks from supplier to supplier. There are already checks that to make sure that software does what it suppose to do. Like these tests, there should be a test on Cyber Security in the Supply Chain (CSSC) in the future.

4 Software Integrity

In section four we want to show that it is not a new concept/idea to check the inside of the product. With software it is not unusual to check the software on its functionalities. Software integrity has a link with Cyber Security in the Supply Chain (CSSC), because there is a method to make sure that the software is working like it should be. Simpson (2009) writes in the article "The Software Supply Chain Integrity Framework" and particularly at the Software Supply Chain. We can see that this gives a good overview of a product and the activity of different suppliers that participate in the creation of software. The article explains where Cyber Security in the Supply Chain directly can be achieved based on software. "Each IT solution is a collection of components. Each component or its parts can be a developed by its supplier or on behalf of that supplier by their sub-suppliers, which are licensed to the supplier by another supplier or obtained from Open Source repositories or acquired outright by the supplier.

However, this complexity of components within components can be organized. In the physical world many industries create complex products that contain components from multiple sources. Processes in the manufacturing of physical goods have two parallels that can be adopted in the cyber world. One is the use of a Bill of Materials (BOM) to organize the hierarchy of product components. The other is the use of supply chain management processes, which describe the business activities associated with satisfying a customer's demand spanning the range from the supplier's supplier to the customer's customer. By recognizing and adapting techniques pioneered for the physical world, IT suppliers can identify natural control points within Software Supply Chains. To identify these points, consider that each software supplier has three links of the supply chain. For these three links each IT supplier takes similar actions:

- Supplier Sourcing:
  Select the suppliers, establish the specification for the supplier's deliverables, and receive software/ ICT-hardware deliverables from the suppliers;
- Product Development and Testing:
  Build, assemble, integrate and test components and finalize for delivery;
- Product Delivery:
  Deliver and maintain their product components to their customer.

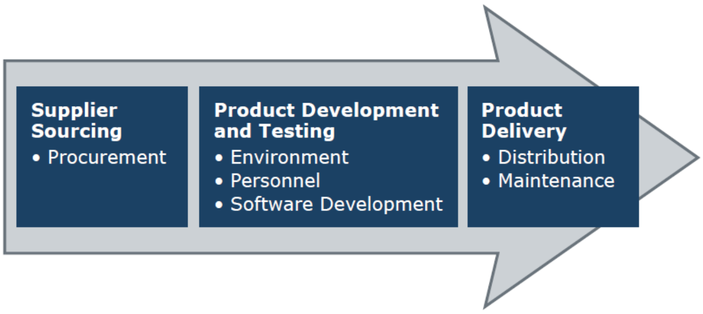


Figure 10: Each supplier in the software supply chain manages three sets of controls

Now consider that the delivered software is just one component of a larger IT solution and each software supplier is only one supplier in a complex chain of suppliers and systems integrators. Customer relationships extend even beyond the traditional system integrators since some "acquirers" implement systems as solutions for other end users. As such, the Software Supply Chain is only one part of a larger, more complex IT solution supply chain.

Figuratively, an IT solution supply chain resembles a collection of staircases. Each staircase aggregates smaller useful components from different suppliers into an increasing collection of components until ultimately sufficient IT components have been assembled to meet the customer's business requirements. Figure 11 illustrates the Software Supply Chain as one of these staircases, where each step holds a different supplier. Between each step is a step-up. The step-up represents the transmission of software components from a supplier to its customer. Components move along this "staircase" supply chain when they are handed over from one supplier to the next. At each step a supplier controls three links in the supply chain:

- goods received from suppliers.
- their products production.
- what is delivered to their customers.

Suppliers apply integrity controls at each link. For example, a supplier can conduct acceptance tests on components received from their suppliers, and release tests on the components they deliver to their customer. That means that each transition of custody along the chain of suppliers is an opportunity to preserve code integrity."

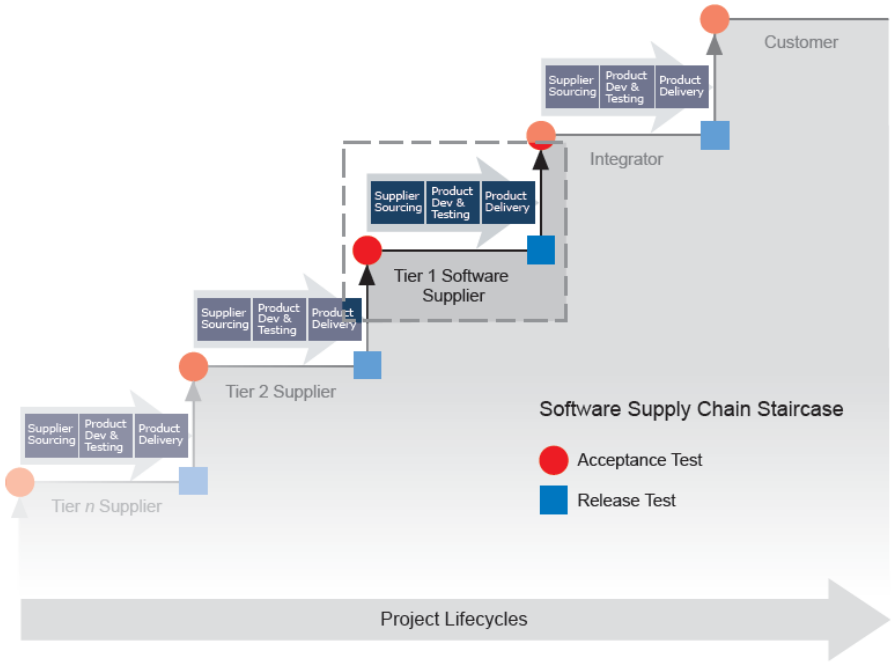


Figure 11: The Software Supply Chain resembles a staircase, where each step holds a different supplier. (SAFECODE)

This section explains how we should look at suppliers with a tier that is further then tier 1. In the context of software integrity it is normal that there are checks on high tiers, like Acceptance tests and Release tests. Nowadays a Cyber Security test can't be missed or forgotten. In the section "Six-step method" we explain how such a Cyber Security check can be performed to achieve CSSC.

5 State of Art

To answer the first question main question to answer the central question of the thesis is:

What is the State of Art in CSSC:

a. What is written in the literature about components and Cyber Security in the Supply Chain?
b. Is there currently a model or method for cyber security checks in the supply chain?

This question is answered in section 3 and 4. Overall we can say that all the current standards are focused on the on the suppliers and sub-suppliers infrastructures and processes that are being used to manufacture products. ISO and ISA standards are designed to a certain basic of trust between customers and producers of products. Building this trust factor between those parties is a very important part when deciding to choose for a certain supplier or manufacturer. Because the CSSC is based only at processes of building a product and for the customers it is not sure if the key-components of the product are not compromised. Although you could trust the last supplier it is not sure that you can trust the suppliers on tier 2, 3, 4 or even 5.

These standards are not only made by independent organizations, also many countries have created a standard. For example the US with NIST has created the Federal Information Processing Standards Publications (FIPS PUBS). These publications describes standards from countries are based on the public standards like ISO and ISA. This means that also countries are focused on the 'trust' and not check the key-components within the products to achieve CSSC.

We explained that Off The Shelf (OTS) plays an important role in CSSC. If we buy a product it is better to buy an OTS product then a custom element, because OTS is used in many different products it is likely that vulnerabilities will soon be revealed. With a custom element this is not likely. Buying of products with GOTS gives us the disadvantage of not knowing of how the product is build. Because governments don't like it when customers check their products and we therefore have to trust the governments of the GOTS. We can't predict that there are no back-doors in products with GOTS. This exactly describes what could happen when a product is manufactured. With GOTS, custom element there is no overview of what they exactly ad to the products. By only implementing the earlier described standards with requirements like custom elements (e.g., on people, process, product/services, and tools) to at least partly address this risk will not totally prevent the danger build in the 'back-doors'.

The Software Supply Chain described in the article from SAFE tells us that this is mainly focused on acceptance and release tests and still is not totally based on cyber security but on the functionality of the product, although it shows again the difficulty of CSSC. In CSSC we don't go further into detail about these acceptance and release tests. Nevertheless they are still needed to guarantee the functionalities of the product and its software. In the next section we will explain our Six-step method to achieve CSSC that is focused product and its components.

6 Six-step method

Now we will show the current state of how Cyber Security in the Supply Chain (CSSC) is organized. We will explain that it is important to have a complete picture of what key-components contain the relevant systems for the important functionalities of the products and how we can 'trust' these key-components. The first research question is answered, we could not find an existing model or method that can help us check the key-components of products. In this section we create our method that will check the certain key-components of the product to achieve Cyber Security in the Supply Chain.

We will explain how the CSSC Six-step method is build. As described in the previous section we will not go further into the 'trust' factor of the suppliers or sub-suppliers. We will only focus on the product itself with its key-components important for CSSC. If we take an average product it consists of many different components. The large major part of the components are irrelevant to the Cybersecurity of the product. John C. Ryan 1999 explains in the article "Spullen en hun geheimen" that a car consists of 10.000 different parts. It is impossible to check all 10.000 components and their mutual relationship, because this could take a very long time, which will not benefit the product as well as the acquirer. Therefore we will focus on the key-components of the product to achieve a certain percentage of CSSC. It is impossible to achieve a 100% of CSSC. These key-components are the key to CSSC.

We will walk through the following steps and are integrated into the Six-step method:

a. We will look at the product and where Confidentiality, Integrity and Availability (CIA) can be important to the product.
b. The functionalities of the product will be scaled based on CIA.
c. The systems that are responsible for these functionalities will be earmarked with the help of CIA.
d. We will go further into detail by locating the key-components within these systems.
e. The relation of key-components with other systems will be checked.
f. We will check which tier a key-component has.
g. A small amount of key-components of the product will be identified which provide the CSSC (In the future, with product updates of key-components, we only have to check these key-components for CSSC).

For the context it is important to explain what CIA-Triad is. Chad Perrin (2008) describes that the CIA-Triad is a widespread, well-known model for security policy development, used to identify problem areas and necessary solutions for information security. The CIA-triad helps people think about important aspects of IT security.

The article on www.echrepublic.com is used to explain the three pillars of the Confidentiality Integrity Availability (CIA) Triad. “Synonymous with privacy as a security concern is the Confidentiality of the CIA-Triad.

C. These are constraints of whom receives the information. With information exchange must be considered if a person “need to know” the information. Some of the most commonly used means of managing confidentiality on individual systems include traditional Unix file permissions, access control lists, and both file and volume encryption.

I. The “I” in CIA stands for Integrity to protect data from modification or deletion by unauthorized parties. It also makes sure, when people who are not authorized to change information, the actions/damage caused by the unauthorized people can be undone. Some data should not be inappropriately modified at all, like user account control for example, because even then a momentary change can lead to significant service interruptions and confidentiality breaches. Other data must be available for modification. Therefore sometimes it needs to be reversible as much as reasonably possible, in case of changes that may later be regretted (for example accidentally deleting the wrong files).

A. The last component is the Availability of data. Systems, access channels, and authentication mechanisms must work properly. The information they provide and protect need to be available whenever needed. High Availability (HA) systems are those computing resources whose architectures are specifically oriented towards improving availability. HA system might target power outages, upgrades, and ICT-hardware failures to improve availability, it might manage multiple network connections to route around network outages, or it might be designed to deal with potential availability problems such as Denial of Service attacks.”

The parts mentioned so far are used for information security Confidentiality, Integrity and Availability (CIA) are important, because later we will use these terms to find out if the product and functionalities of the product to Confidentiality, Integrity and/or Availability.

Now we will discuss the Six-step method step-by-step and give an explanation of what should be done to proceed to the next step. At every step a template must be filled in to make sure that after step 6 there can be given a prediction of a certain percentage of Cyber Security in the Supply Chain. By completing the steps and filling in the templates, they also give a scheduled picture of where the key-components the location in the product. The Six-step method as explained in this section is as method described in the appendix 1 attached to this thesis, which can be used to perform a CSSC-check.

Practical use of the Six-step method is important to state that a certain amount of CSSC can be successful. Therefore a use case will be used to test the Six-step method. We have developed a syllabus, which is attached to this master thesis. This syllabus contains all the templates and steps that need to be followed to achieve a certain percentage of CSSC. This syllabus will be handed over to the persons that will perform the test the product on CSSC. After these tests we will receive the completed templates, unfortunately due to the sensitivity of the outcome of the results, we can't add the results to the thesis. We will discuss the Six-step method with the persons that perform the checks of the product on CSSC, to find out if the Six-step method was helpful and provide all the resources that are necessary for an acceptable CSSC. Afterwards we will implement the feedback of the system engineer to improve the Six-step method.

The goal of the use case is to use a high-tech product. Next to this criteria, it has to be a product that will be even more reliable to ICT in the future. Looking at all this criteria we decided to use an 3D-navigation system. This product with its functionalities will be important a lot of people and in the future and will be more and more reliable to ICT.

In the media there are regular news items, like in the New York Times article by Markoff (2014) with the title *"Google's Next Phase in Driverless Cars: No Steering Wheel or Brake Pedals."* These companies like Google are performing tests with cars without a steering wheel or brake pedals. This visibly increased its relevance and impact of the results and the outcome of the research. For this thesis we will focus on a product that has not too much key-components to keep the use case simple and to show how the Six-step method can be adjusted where needed.

We will now start with the Six-step method at step 1.

Step 1: In this step we will check if the product is new or has one or more updated key-components. The product that we need to analyze for CSSC can be a new, not yet analyzed product or can be a product that has an update in one or more of its key-components. Both types of components, the new and update ones are important for the CSSC. We have two opportunities for this check of the product. In the picture below you can see where the two opportunities within the products lifetime are situated. Those two opportunities for analyzing the CSSC are:

1. During the manufacturing and assembling of the components into the final product.
2. During an update available for the key-components of Cyber security like the software, ICT-hardware and/or firmware.

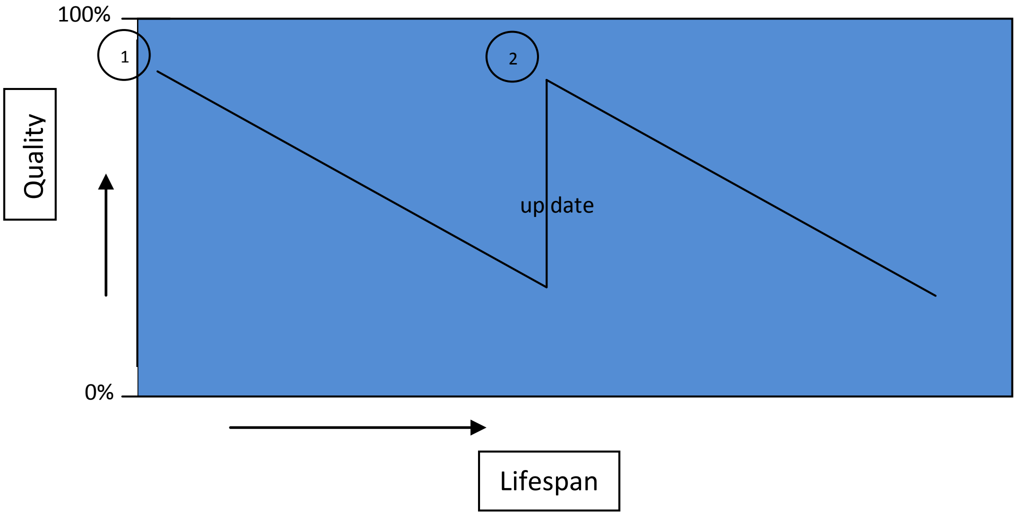


Figure 12: Product lifetime

When focusing on the first mentioned opportunity with a completely new product we will need an analysis of the product. When this first opportunity is completed we will get an overview of all essential systems with their key-components.

The second opportunity is an update of the product. This is mainly an update of one or more key-component inside a system that provides the functionality of the product. In this thesis we will focus on the first opportunity during the period of manufacturing and composition, because in this method it is not known if there has been a check on CSSC like the Six-step method. This check consists of locating the essential systems for every functionality. Also the key-components will be located within that the systems, that are important for the Confidentiality, Integrity and Availability of the functionalities.

We have used the CIA constructed to identify problem areas and necessary solutions for information security. When we use the CIA within the supply chain of a product, we are looking at the product itself. We are not looking at the information security, but we use CIA to categorize and rate the functionalities of the products. During this process the expertise of end-users it is important to make sure that no functionality will be missed.

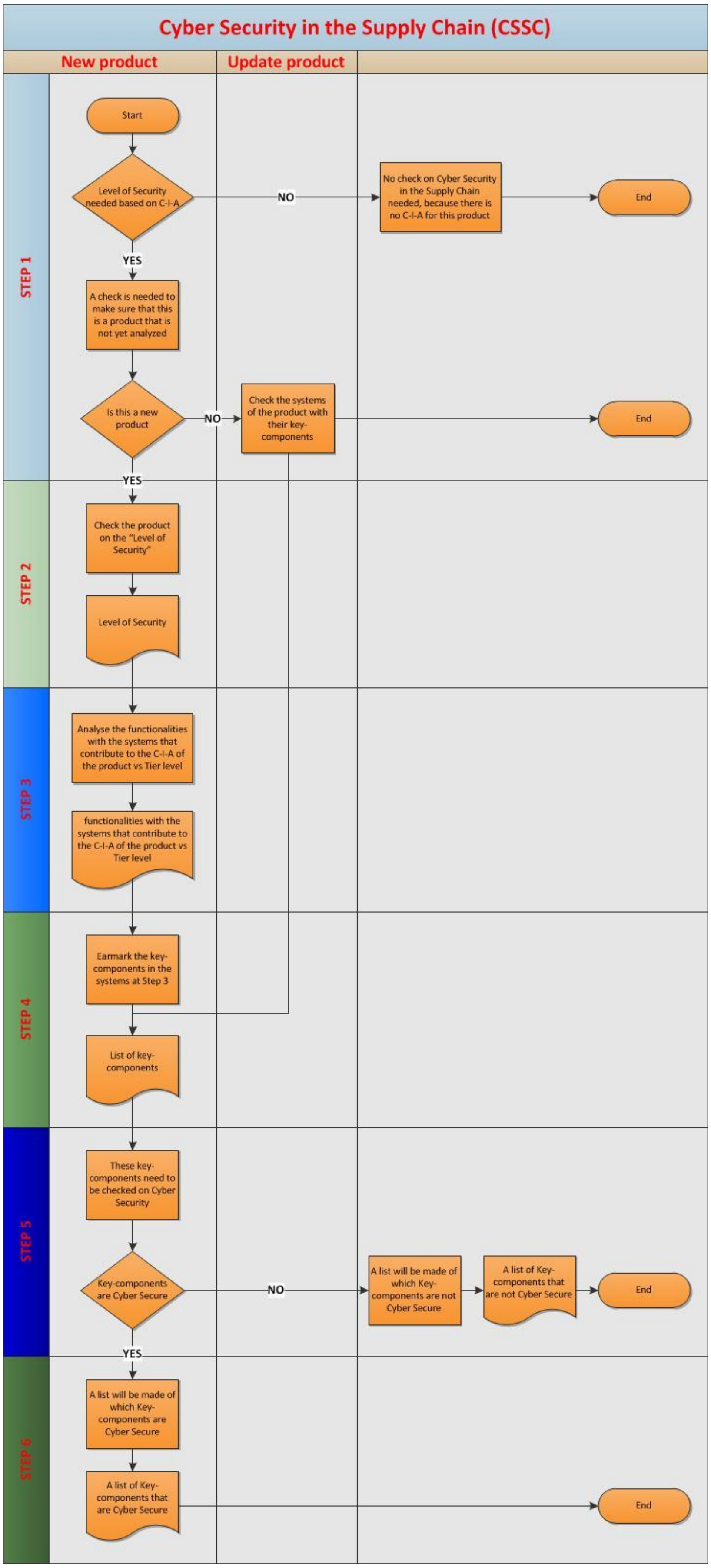

Cyber Security in the Supply Chain (CSSC)
New product
Update product
STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
Start
Level of Security needed based on C-I-A
NO
No check on Cyber Security in the Supply Chain needed, because there is no C-I-A for this product
End
YES
A check is needed to make sure that this is a product that is not yet analyzed
Is this a new product
NO
Check the systems of the product with their key-components
End
YES
Check the product on the "Level of Security"
Level of Security
Analyse the functionalities with the systems that contribute to the C-I-A of the product vs Tier level
functionalities with the systems that contribute to the C-I-A of the product vs Tier level
Earmark the key-components in the systems at Step 3
List of key-components
These key-components need to be checked on Cyber Security
Key-components are Cyber Secure
NO
A list will be made of which Key-components are not Cyber Secure
A list of Key-components that are not Cyber Secure
End
YES
A list will be made of which Key-components are Cyber Secure
A list of Key-components that are Cyber Secure
End

Figure 13: The Flow-chart that is showing the steps to be taken for analysis of the product to ensure CSSC.

Step 2: In this step the risk analysis of the concerning company or country which is leading. If there is no risk analysis available the following analysis could be applied.

For example we are the acquirer or consumer that accepts the product from the last supplier in the chain. In this step we have to answer the following three questions:

- Is the products confidentiality important or necessary for the purpose(s) for which the owner wishes to use the product for?
- Is the products integrity important or necessary for the purpose(s) for which the owner wishes to use the product for?
- Is the products availability important or necessary for the purpose(s) for which the owner wishes to use the product for?

These questions must not be answered with a yes or no, but need to be answered on a scale of 0 – 100 percentage. Without an answer in percentage of the three CIA questions, it is impossible to realize any level of CSSC. A product consists of many different components or parts. Not all the components are essential to achieve a cyber secure product. When we have answered these three questions with CIA we will get a conceivable graphical representation (see figure 14). You could envisage that although not all the answers will show a 100 percent, just one of the three CIA with a small percentage is acceptable for this functionality of the product. By identifying the systems that are important to the CIA of the product, further analysis is possible of related key-components in other systems, that interacts with the identified systems for CSSC.

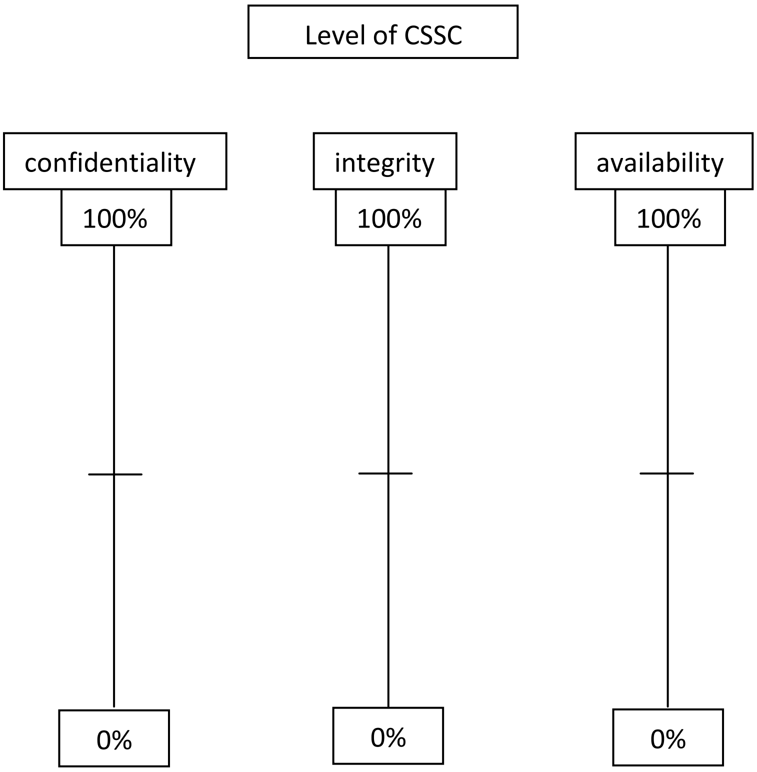


Figure 14: The level of CSSC

Now we can state that the Level of CSSC of the product conform CIA is determined. Although there has not been any analysis of components yet. This gives a clear picture in which tier the components of the system from the products needs to be analyzed. These percentages give an indication of the “Level of CSSC” in relation to the CIA of the product. Scaled from 0 to 100 percent with a free interpretation of choosing a percentage from 0 to 100 percent.

A level of CSSC of 100 percent stands for a complete attention expressed in percentage of whether a CIA for this product will be necessary. The level of CSSC of 0 percent stands for no attention expressed in this percentage whether a CIA for this product will be necessary.

Step 3: We have now identified how products can be scaled on CIA by the scale from 0 to 100 percent. In this step we will identify the systems within the product that are responsible in step 2 to achieve a Level of CSSC with CIA. In this step assistance from product experts is needed to make a complete identification possible of these systems. The product experts are important to prevent that essential systems will be over looked. When we fail to indentify systems during the Six-step method the CSSC-check will not be that effective and will result in a false sense of security.

Now we need a list of the essential systems that are important to achieve the percentage CIA in relation with the functionalities and their systems of the checked product. We have to perform a secure check to find relationships between systems via key-components with other functionalities from the product. You can imagine that a brake-system of a car has a relation to the engine system via the cruise control of the car. The functionalities and systems (CIA) are listed in this step.

To create an overview we have made a template that need to be filled in. You can find the table in figure 15. Start by completing the first column and write down all the functionalities of the analyzed system. In the second, third and fourth column you write which system is responsible for the products functionality.

Functionality and their responsible systems with CIA				
	FUNCTIONALITY	CONFIDENTIALITY	INTEGRITY	AVAILABLITY
1.				
2.				
3.				
4.				
5.				
6.				

Figure 15: Overview of functionalities in relationship with their responsible systems with CIA.

Step 4: In the previous step we defined all the systems of the identified functionalities on bases of CIA. Within these essential systems we can indentify many different components. Not all of the components are important for the cyber security of the product. For our Six-step method will only focus on the key-components within the systems. These key-components are the ICT-hardware, Firmware and Software of the systems. In the example of figure 16 the key-components are colored in red.

In this step we will decide which of these key-components will need to be analyzed to achieve the Cyber Security in the Supply Chain. When the key-components of the system are identified, a cross check with the tier must be made. When the key-components are a Commercial Off The Shelf (COTS), the Tier level is based on where in the systems the key-components will be used. The chance is null that a supplier from a key-component with a high tier and/or the chance that the suppliers will know that their key-components are used in the system (like a braking system of a car of a fuel system) of the product. These key-components are also used in other products and often with open source software. The chance that other users will find the ‘back door’ is relatively large. Therefore the key-components with a high tier do not need to be checked for CSSC.

When we look at Government Off The Shelf (GOTS) there are different values, because a lot of intelligence services nowadays are built in so called ´back doors´ to attack the system in a later stadium. These key-components will probably need a firm check to achieve CSSC. When the GOTS comes from a country that has a high ‘trust’ factor the team that performs the check can decide to accept the key-component which is based on ‘trust’. Although we would still advise to check the key-component, because ‘trust’ might not be enough.

Next to the COTS and the GOTS there is another important version of key-components. The third type of key-components are custom elements. These elements are specially made or written for particular systems. Because they are especially made for only one system and/or product, there is a big chance that these key-components can be compromised.

It is also important that we look at key-components which have a mutual relation with other systems and certain key-components within these systems. These key-components must also be checked, to make sure that there are no unidentified key-components that will influence the essential systems.

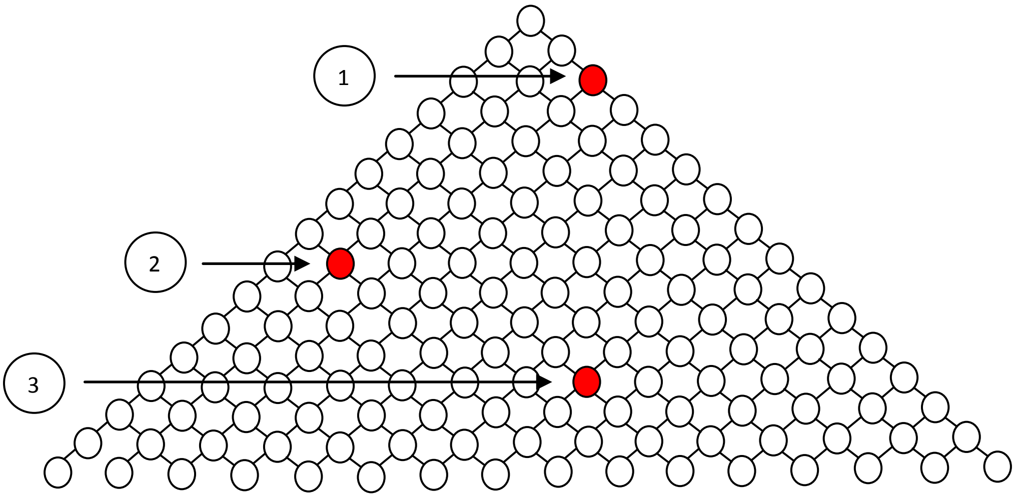


Figure 16: An essential system for the functionality of the product and in color the key-components.

In the figure 16 above you see the location of key-components in an essential system which is identified for the functionality of the product. We can see the key-components are marked in color. In this system there are three key-components. The arrows are pointing at the colored key-components. This system contains three key-components starting at tier 1 to tier 3. For instance the key-component with the level tier 3, they are used in many different products and systems. It is not likely that a supplier knows that this key-component is used in his system. Possible attacker will not know in which system or product the key-components will be used. For such an attacker the chance of detection of his initiated back-door is larger when it is used in many other systems. He will probably not compromise an OTS component that is widely used by many different products. He will always focus on the key-components that will end up in only one system or product in which he likes to compromise in a later stadium. This is the reason why the tier of the supplier is important. The key-components with a high level tier are not seen as a danger to CSSC, therefore we will not check these components with the Six-step method, although they are noted as key-components. The team that performs the Six-step method will decide until what tier-level the check is necessary. The more a key-component is in a specific element or this key-component controls multiple general components or functionalities, the more important it is to analyze this key-component.

Step 5: Until now we have identified all the key-components of the system, which tier they have and if the key-components are COTS, GOTS or custom elements. In step 4 we also made the system key-components visual. In this step we will start to analyze the relevant key-components for Cyber Security in the Supply Chain (CSSC). In the previous steps from 1 to 4 we analyzed the large amount of components, in which key-components are important and need to be checked on CSSC. We will only focus on the key-components described in step 4. Due to the complexity of key-components it is important that expertise is needed during the analysis of key-components used in a system. It is important that we perform this analysis, not only with an expert but also under supervision of the customer or acquirer of the product. This process is similar to the acceptance test or release test of software.

At the end of this step we will get a list of key-components that are not cyber secure and why they are not cyber secure. This list consists the analyzed key-components that are open for analysis and also the key-components that are GOTS and COTS which a government or commercial party has not given permission to analyze. The acquirer or customer, together with the team that performs the analysis will decide after finishing the analysis with the Six-step method, whether we can accept the CSSC-check of the product.

The table below contains the columns that need to be filled in. Column 1 contains the name of the key-component that is not cyber secure. The second column contains the country of the GOTS. The third column contains the company of the COTS. The fourth column contains the company of the custom element. And the fifth and last column contains some extra information. This additional information, includes why someone thinks that the key-component is not cyber secure. It is also possible that a country or company does not accept everyone to have a peek inside a key-component.

This table below contains all the key-components from the functionality described in step 3 and step 4 which reveals the key-components that are not cyber secure. The first column “key-components” contains the key-components that are not cyber secure. The columns 2, 3 and 4 show if the key-component is a GOTS, COTS or a custom element and who the manufacturer is. The last column is a column that gives the tester the ability to write his comments about the specific key-components. Note that the table is colored in red, because all the key-components in this table are not assessed as cyber secure.

	Key-components that are NOT cyber secure			
	GOTS	COTS	CUSTOM ELEMENT	REMARK
1.				
2.				
3.				
4.				
5.				
6.				

Figure 17: Table with the list of key-components that are NOT cyber secure.

Step 6: In the previous steps we have identified the CIA per functionality, as well we analyzed key-components that are selected for analysis of the systems. In this step we will make a list of all the key-components that are cyber secure after the CSSC check with the Six-step method. Below you can see a table that will be used to finalize step 6. The second column contains the name of the key-components and the country of the GOTS. The third column contains the name of the key-components and the company of the COTS. The fourth column contains the name of the key-components and the company of the Custom Elements. And the fifth and last column is for additional information about this key-component. This table contains all the key-components from the functionality described in step 3 and step 4, which finally will reveal the key-components that are cyber secure. Note the table is colored in green, because the key-components in this table are assessed as cyber secure.

Key-components that are cyber secure				
	GOTS	**COTS**	**CUSTOM ELEMENT**	**REMARK**
1.				
2.				
3.				
4.				
5.				
6.				

Figure 18: Table with the list of Key-components that are Cyber secure.

7 Evaluation of the Six-step method

We have developed the Six-step method to help us to achieve a certain percentage of Cyber Security in the Supply Chain. Together with the standards that are currently used, we have two ways which enhances the method of 'trust' and the Six-step method to achieve CSSC. We will take an use case to check the Six-step method. Therefore it is important that the use case is a high-tech product with multiple key-components. Because we only focus in the Master thesis on the Six-step method with its procedures, we will not perform an analysis of the key-components.

During the process of the Six-step method we will help and guide TNO that performs the CSSC check. We do this to make sure the all the Six steps described will be taken. After finishing the use case we will analyze the process of the CSSC check according to the Six-step method. And after the check we will modify the Six-step model, so we have a complete method which can be used for analysis on different kind of products.

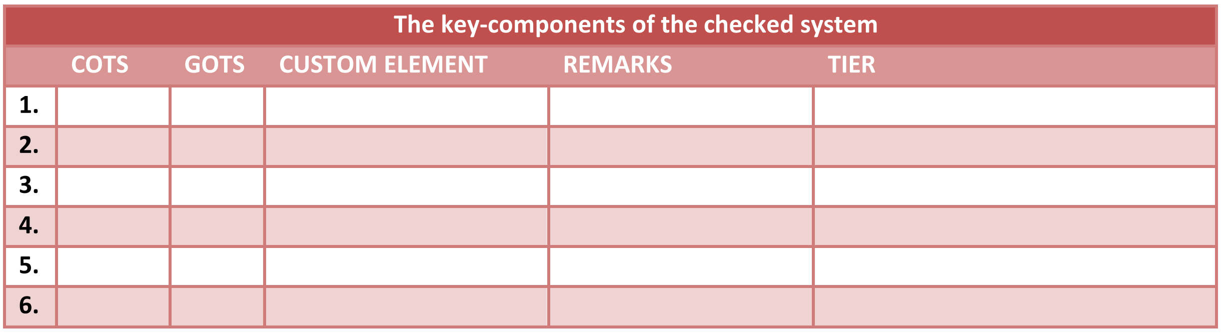
We have found the organization in Dutch Toegepast-Natuurwetenschappelijk Onderzoek (TNO) willing to present a product to perform a CSSC check by using the Six-step method and evaluate our method. For more information their website www.tno.nl can be visited. The product that we will check on CSSC for this thesis is a 3D-navigation system. This is a product that has an application, INS, GPS-system, barometer and a radar. With this product it is possible to navigate within buildings and at the different floors of buildings. This is a revolutionary product with a high intensity of ICT. There are multiple key-components used inside this product.

The focus of this thesis is to create a method on Cyber Security in the Supply Chain (CSSC) and therefore we will not check the software, firmware and ICT-hardware itself. These key-components will be divided in Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS), Custom Elements and also which tier they have. After analysis, on vulnerabilities of the key-components, we can give a list of secure and insecure key-components to achieve a certain amount of CSSC. The list of key-components that is addressed as not cyber secure and added in the table of step 5, needs further analysis by checking the key-component.

Because the focus is on the evaluating of the Six-method and the check on the product itself. We will focus at step 4 one system of the 3d-navigation system. This system is the Inertial Navigation System (INS) named driftless.

The analysis starts with step 1, this is where we checked if there has already been performed a check on CSSC according the Six-step method. In this case there has never been a check with the Six-step method. At step 2 we filled in the percentages on Confidentiality, Integrity and Availability (CIA). At step 3 the functionalities and their responsible systems of the product are scaled on the Confidentiality, Integrity and Availability (CIA) as formerly described. With this first three steps there have been no other issues found. The system engineer was able to perform this check easily.

At step 4 there must be filled in a scheme of the checked systems. The system engineer was not able to use this scheme, because he needed a table where he could write down extra information about the key-components and therefore we changed the scheme for this step 4 into a table which contains 7 columns. The first column consists of the record number of the key-components. The second, third and fourth column shows if the key-components are a COTS, GOTS or Custom Element. The sixed column contains remarks about every key-component for instance if the software is an open source or other relevant information. The last column tells us which tier the key-component has. This last column is not mandatory but could help us in our Six-step method. Below you can see the new table that is used in step 4.



The key-components of the checked system					
	COTS	GOTS	CUSTOM ELEMENT	REMARKS	TIER
1.					
2.					
3.					
4.					
5.					
6.					

Figure 19: Table used in step 4 of the improved Six-step model.

At step 5 the column only contains the key-component that needs extra checks and step 6 contains the key-components that do not need extra checks. In these two steps there were no issues found in relation to the evaluation of the Six-step method. In appendix 2 the new evaluated improved syllabus with the fully working and tested Six-step method has been added.

With filling in last table at step 6 of the Six-step method the check for achieving Cyber Security in the Supply Chain (CSSC) is finished. We have now an overview of what are the functionalities that are important for the use of the product and scaled on the Confidentiality, Integrity and Availability (CIA). All the systems that are responsible for this functionality with the key-components which are determined and used in the system. In this product we have only focused on the INS 'Driftless'. To have a complete overview of all the different systems, we must conduct the Six-step method.

These key-components can now be divided in Commercial Of The Shelf (COTS), Government Of The Shelf (GOTS), Custom Elements and the remarks and when applicable which tier they have. After the short analysis of the key-components we can tell if the list of secure and insecure key-components helped us to have a final judgment that we achieve a certain amount of CSSC.

With the final conclusions of the CSSC-check according to the Six-step method we can say that after checking the two key-components in step 5, the checked system is cyber secure for 80% percent on Confidentiality, 100% on Integrity and 30% on Availability.

8 Conclusions

We have explained that there are multiple standards and certifications of trust in the industry to ensure a global standard on CSSC. The research question is:

Can we achieve and guarantee a certain percentage of Cyber Security in the Supply Chain?

To answer the central question, we have divided the central question into three main research questions. Directly behind the question we will answer the questions. These questions are:

1. What is the State of Art in CSSC:
   a. What is written in the literature about components and Cyber Security in the Supply Chain?

      The state of the art of Cyber Security in the Supply Chain shows that there are at least two well known standards. These standards are the ISO and ISA standards. Which are performed for many years and helps the industry to produce and design components conform procedures that are stated in these standards. Next to standards for the industry there are also standards for the industry that delivers to the countries. In our example we show how the standards of the United States are set up. Both the standards for the industry as well as the standards for the countries are based on 'trust' towards the acquirers.

   b. Is there currently a model or method for cyber security checks in the supply chain?

      We have not found an existing method or model for checks on Cyber Security in the Supply Chain. Therefore we have developed a method our selves, which checks the key-components of the system which is responsible for the important functionalities of a product.

The first question is negative, that is why we have focused on the second question.

2. Can we develop a model or method for CSSC?

   We have succeeded to develop a method. The method we have developed is called the Six-step method and focuses on the final product that will go to the acquirer which is made to determine what the relevant key-components of the systems are which are responsible for the functionalities of the checked product. First the percentage of Confidentiality, Integrity and Availability (CIA) of the product will be determined. Then we will be analyzing what the functionalities are which will be responsible for using the product. Also per functionality the CIA will be given. In the next step per functionality the essential systems will be determined. The next step is where and if the key-components (ICT-hardware, firmware and software) are a Custom Off the Shelf (COTS), Government Off the Shelf (GOTS) or Custom element with the remarks and tier level per system. In the last steps these key-components will be devided in cyber secure key-components and key-components that are not cyber secure. Based on the last steps will be decided if a further check of a key-component is necessary. We now need to evaluate our Six-step method with the help of a use case.

3. Can we evaluate our developed model or method by checking a use case on security in the supply chain?

   The Six-step method described in section 5 is used to check a product at TNO. A syllabus with the Six-step method is made (appendix 1) which will be given to the appropriate person or team, who will perform the CSSC-check. By using the syllabus by TNO, we had to change step 4 of the method to the needs of the system engineer, which became clear during the CSSC-check according to the Six-step method.

   The system engineer was unable to use step 4, which visualizes the systems key-components into a scheme that are responsible for the products functionalities. He was missing a table where he could write down his findings and remarks of every key-component and which functionalities they were responsible for. These remarks are important for answering step 5 and step 6, because of the answers at step 5 and step 6 are based on the findings in step 4. In step 5 we have divided the Key-components in not cyber secure and key-components that are cyber secure in step 6.

   Except for step 4 all the other steps of the Six-step method were accepted and well used by the system engineer. The complete and improved Six-step method is attached in Appendix 2 to this thesis. TNO and the project team are positively surprised with the final outcome of the CSSC-check with the Six-step method. Because of the findings with the Six-step method, TNO will change certain key-components of systems to create a more CSSC product.

The Six-step method only gives a view of which key-components can be accepted and why. We advise to perform a deeper check on the key-components that are mentioned on step 5 (not cyber secure). Our method does not perform such a check. Other research should be conducted to find a way to perform these checks on the key-components.

The standards that are widely used by many organizations and countries are a perfect match together with our developed Six-step method to achieve Cyber Security in the Supply Chain.

References

Abhay Joshi, Top Layer Networks Inc. "How *to protect your company from 'zero-day' exploits*" www.computerworld.com. Mar 1, 2004 12:00 AM PT. (accessed on October 16, 2014).

Barnum S., Gegick M. (2005) *Defense in Depth*, https://buildsecurityin.us-cert.gov. (accessed on January 15 2013).

Chad Perrin, *"The CIA Triad,"* June 30, 2008, (Louisville, KY: TechRepublic), http://www.techrepublic.com/blog/security/the-cia-triad/488 (accessed october 17, 2014).

David Inserra and Steven P. Bucci, PhD. "*Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*" The Heritage Foundation. No. 2880 | 6 March 2014.

Dictionary for technical terms. http://www.techterms.com (accessed on October 21, 2014).

DIN Deutsches Institut für Normung e.V. "ISO/IEC JTC 1/SC 27 - IT SECURITY TECHNIQUES" http://www.jtc1sc27.din.de 2011-12-14 (accessed on October 26, 2014).

ISO/IEC (2014) "*ISO/IEC FDIS 27036-1:2014*" www.iso.org (accessed on October 21, 2014).

ISO (International Organization for Standardization) "*ISO is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standard*". www.iso.org. Founded in 1946. (accessed on October 21, 2014).

ISA Security Compliance Institute (ISCI) *"ISA sets the standard for automation by enabling automation professionals across the world to work together for the benefit of all."* www.isa.org. Founded in 1945. (accessed on October 24, 2014).

ISA99 "Developing the Vital ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security" *http://isa99.isa.org/ISA99%20Wiki/Home.aspx.* Founded in 1945 (accessed on October 25, 2014).

John C. Ryan, "Spullen en geheimen", 26 mei/juni 1999, http://theoptimist.nl/spullen-en-hun-geheimen/ (accessed october 18, 2014).

John Markoff *"Google's Next Phase in Driverless Cars: No Steering Wheel or Brake Pedals"* http://www.nytimes.com/ May 27, 2014 (accessed October 20, 2014).

Miller F. P., Vandome A. F., McBrewster J. (2010). *Defence in Depth; Defence in Depth (disambiguation), Military Strategy, Logistics, Pacification, Counterattack, Attrition Warfare, Strategy, Defense in Depth (computing).* USA: Alphascript.

National Coordinator for Security and Counterterrorism. "*Cyber Security Strategy 2.0*" National Cyber Security Centre, Ministery of Security and Justice. 2014.

National Defense Industrial Association (NDIA) System Assurance Committee. (2008) "*Engineering for System Assurance*". Arlington. (Accessed on November 03, 2014).

Ringler, J. "*How Cyber Attackers and Criminals Use Defense in Depth Against IT Professionals*", http://www.tech-wonders.com/2012/08/how-cyber-attackers-and-criminals-use.html. (Accessed on October 23, 2014).

Robert J. Bowman "*Why Cybersecurity Is a Supply-Chain Problem*", http://www.supplychainbrain.com, May 20, 2013 (Accessed on October 17, 2014).

Simpson, S (2009) "*The Software Supply Chain Integrity Framework"* Software Assurance Forum For Execllence in Code (SAFECODE).

Smith C.L. (oktober 2003). "*Understanding concepts in the defence in depth strategy"*. Conference: Security Technology, 2003. During the IEEE 37th Annual 2003 International Carnahan Conference op 14-16 oktober 2003, Taipei Taiwan.

"The Council of Supply Chain Management Professionals (CSCMP)" http://cscmp.org/. (accessed on November 04, 2014).

"The White House National Strategy For Trusted Identities In Cyberspace NSTIC-Strategy". *www.whitehouse.gov*, April 2011. (accessed on November 07, 2014).

US National Institute of Standards and Technology (NIST) *Information Technology Laboratory,* http://csrc.nist.gov/ (accessed on November 05, 2014).

Walker, Ellen. 2005. DACS analyst, software development security: A risk management perspective. *DoD Software Tech News* (July). https://www.softwaretechnews.com/stn_view.php?stn_id=2&article_id=31 (accessed on October 18, 2014).

Woody, C (2008) "*Strengthening Ties Between Process and Security*" Carnegie Mellon University 2005-2012. Published: August 01, 2008 | Last revised: July 31, 2013 (accessed on October 26,2014).

Appendix 1: Syllabus Six-step method

This appendix contains the version of the syllabus that is given to TNO for the use case analysis. It is used to check the product of TNO on Cyber Security in the Supply Chain (CSSC). Unfortunately we were not allowed to present the findings of the check, due to the sensitivity of the conclusions of the CSSC check.

Appendix 1

Syllabus

Six-step method

on

Cyber Security in the Supply Chain

This syllabus will help to achieve and guarantee a certain percentage of Cyber Security in the Supply Chain and refers to the Six-step method in the thesis “Cyber Security in the Supply Chain” developed by B.M.C.S Middendorf (2015). In the media it is showed that the statement “Cyber Security in the Supply Chain (CSSC) is not guaranteed” is well substantiated with several articles in the media. A product consists of many different components from different suppliers and sub-suppliers. Many developed and produced products are not made by one single supplier. In the process of making the product many sub-suppliers are involved in producing small parts which are used in many different products later on. This process with different components from different suppliers is the supply chain. Sometimes a product has components of suppliers that are three suppliers deep or even more. Because there are so many suppliers and suppliers from suppliers, it is impossible for us to check all these different suppliers and sub-suppliers of CSSC and to know if components are manipulated and.

There are already many initiatives to achieve some sort of CSSC. These initiatives are based on the factor of ‘trust’ and are created by implementing multiple procedures on different production processes of a manufacturer. These standards ISO, ISA and standards from countries are important, but there more and more products where ICT is implemented and therefore these standards on their own are not enough to achieve CSSC. Therefore a method is created that checks and focuses at the products itself.

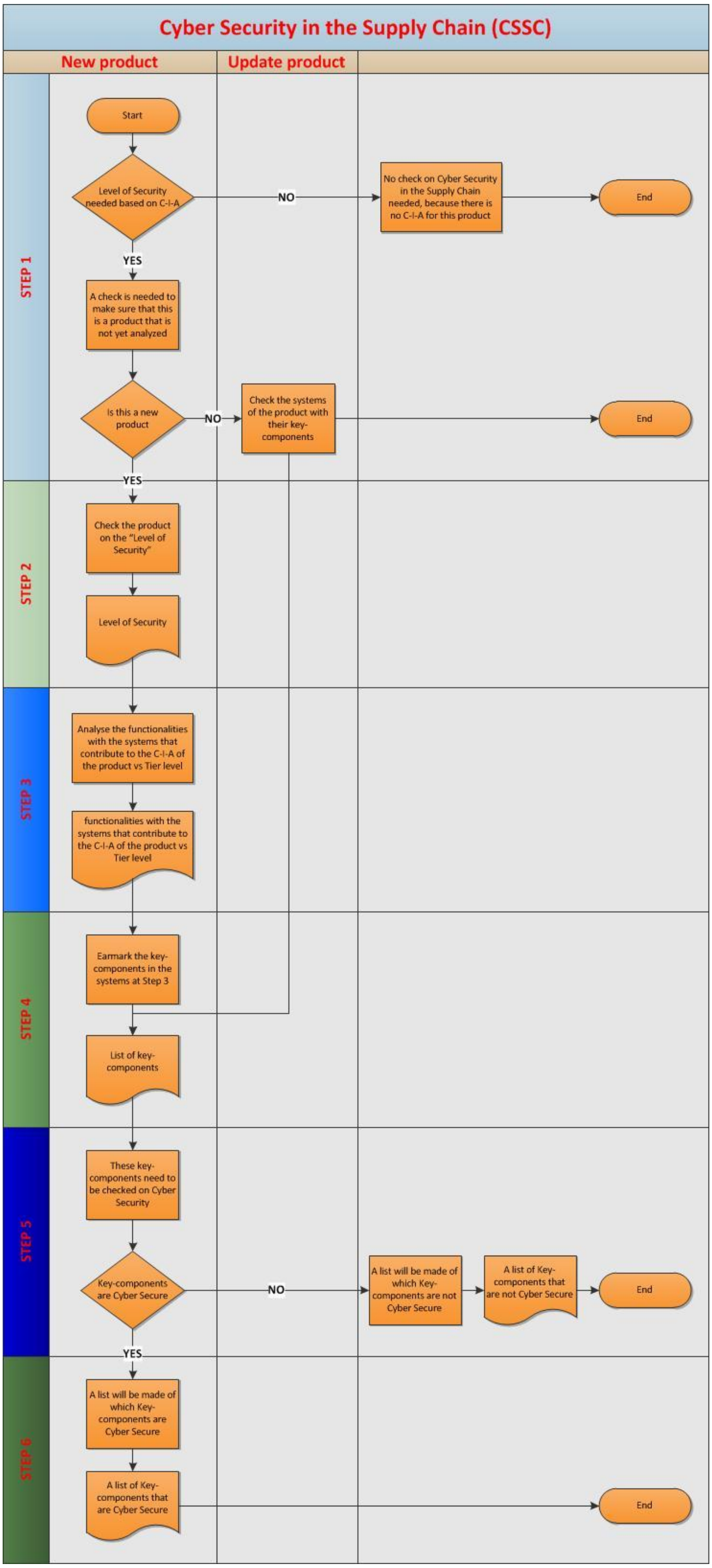
The Six-step method is build to give some sort of Cyber Security in the Supply Chain (CSSC). This syllabus contains all the steps with templates and the guidance for each step. To achieve a complete CSSC-check it is important that a product expert assists with going through all the steps of the Six-step method. When all the six steps are taken, a complete picture can be made of the key-Components (which consists of the hardware, firmware and software) which are cyber secure and which key-Components are not.

The first group of key-components at step 5 which are not cyber secure have to be checked on Cybersecurity after finishing all the steps of the presented Six-step method. At step 6 a list is created with all the key-components that are cyber secure conform the given percentage at step 1. When all the steps are taken a complete picture is available with the key-components of the systems that are important for the functionalities of the product. The following step 5 is to check the key-components whether they are cyber secure. This is a specialist job for programmers. In the perfect world when all the key-components are ok, the percentage found in step 2 on Confidentiality, Integrity and/or Availability should match the percentage given at step 2. In the future when there is a product update (step 1) of a key-component the completed templates can be used to see where the key-component matches the current position. When the product has already been checked conform the Six-step method, only then the updated key-component needs to be checked. In the flow chart of the Six-step method this step starts at step 4.

When you have finished all the six steps of the Six-step method you should check the software codes of the key-components that need an extra check (output step 5). In this method you will only go through the Six-step method.

On the next page the flowchart of our Six-step method is presented. Use the following flowchart to go from step to step to perform the check. After the flowchart you go in more detail through every step.

Appendix 1


Cyber Security in the Supply Chain (CSSC)
New product
Update product
STEP 1
Start
Level of Security needed based on C-I-A
NO
No check on Cyber Security in the Supply Chain needed, because there is no C-I-A for this product
End
YES
A check is needed to make sure that this is a product that is not yet analyzed
Is this a new product
NO
Check the systems of the product with their key-components
End
YES
STEP 2
Check the product on the "Level of Security"
Level of Security
STEP 3
Analyse the functionalities with the systems that contribute to the C-I-A of the product vs Tier level
functionalities with the systems that contribute to the C-I-A of the product vs Tier level
STEP 4
Earmark the key-components in the systems at Step 3
List of key-components
STEP 5
These key-components need to be checked on Cyber Security
Key-components are Cyber Secure
NO
A list will be made of which Key-components are not Cyber Secure
A list of Key-components that are not Cyber Secure
End
YES
STEP 6
A list will be made of which Key-components are Cyber Secure
A list of Key-components that are Cyber Secure
End

Six-step method.

Step 1: In this step you will check if the product is new or has one or more updated key-components. The product that you need to analyze for CSSC can be a new, not yet analyzed product or can be a product that contains one or more updated key-components. Both types of components, the new and updated ones are important for the CSSC. You have two opportunities for this check of the product. In the picture below you can see where the two opportunities within the products lifetime are displayed. Those two opportunities for analyzing the CSSC are:

1. During the manufacturing and assembling of the components into the final product.
2. During an update available for the key-components of Cyber security like the software, ICT-hardware and/or firmware.

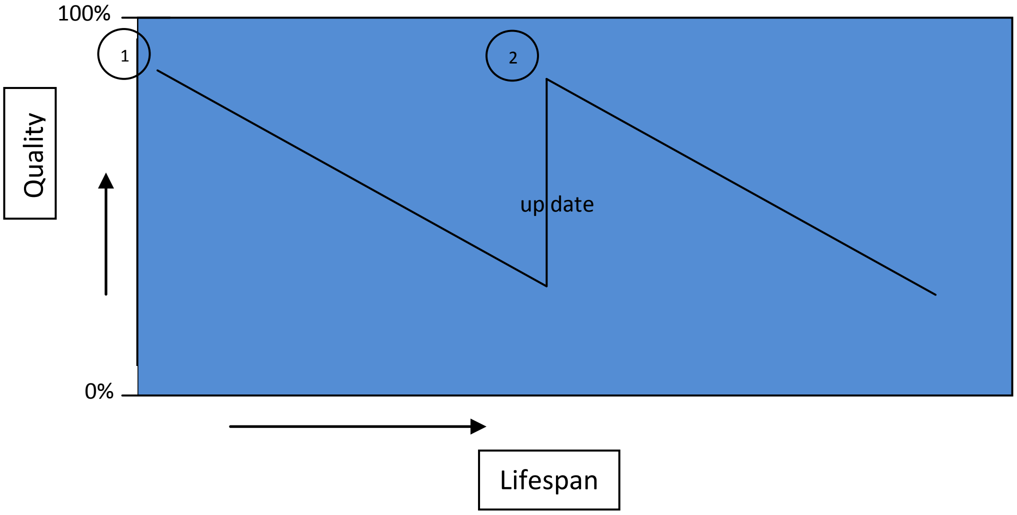


Figure1: Product lifetime

When focusing on the first mentioned opportunity with a completely new product you will need an analysis of the product. When this first opportunity is completed you will get an overview of all essential systems with their key-components.

The second opportunity is an update of the product. This is mainly an update of one or more key-component inside a system that provides the functionality of the product. You will focus on the first opportunity during the period of manufacturing and composition, because in this method it is not known if there has been a check on CSSC like the Six-step method. This check consists of locating the essential systems for every functionality. Also the key-components will be located within that systems that are important for the Confidentiality, Integrity and Availability of the functionalities.

You have used the CIA constructed to identify problem areas and necessary solutions for information security. When you use the CIA within the supply chain of a product, you are looking at the product itself. You are not looking at the information security, but you use CIA to categorize and rate the functionalities of the products. During this process the expertise of end-users is important to make sure that no functionality will be missed.

Step 2: In this step the risk analysis of the concerning company or country which is leading. When there is no risk analysis available the following analysis could be used.

For example you are the acquirer or consumer that accepts the product from the last supplier in the chain. In this step you have to answer the following three questions:

- Is the products confidentiality important or necessary for the purpose(s) for which the owner wishes to use the product for?
- Is the products integrity important or necessary for the purpose(s) for which the owner wishes to use the product for?
- Is the products availability important or necessary for the purpose(s) for which the owner wishes to use the product for?

These questions must not be answered with a yes or no, but need to be answered on a scale of 0 – 100 percentage. Without an answer in percentage of the three CIA questions, it is impossible to realize any level of CSSC. A product consists of many different components or parts. Not all the components are essential to achieve a cyber secure product. When you have answered these three questions with CIA you will get a conceivable graphical representation (see figure 2). You could envisage that although not all the answers will show a 100 percent, just one of the three CIA with a small percentage is acceptable for this functionality of the product. By identifying the systems that are important to the CIA of the product, further analysis is possible of related key-components in other systems, that interacts with the identified systems for CSSC.

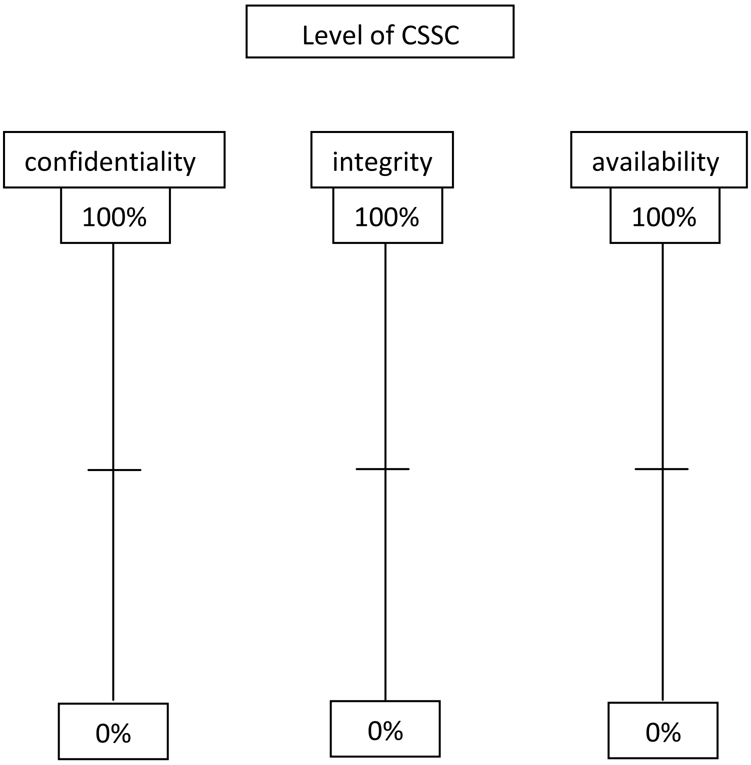


Figure 2: The Level of CSSC

Now you can state that the Level of CSSC of the product conform CIA is determined. Although there has not been any analysis of components yet. This gives a clear picture in which tier the components of the systems from the products needs to be analyzed. These percentages give an indication of the “Level of CSSC” in relation to the CIA of the product. Scaled from 0 to 100 percent with a free interpretation of choosing a percentage from 0 to 100 percent.

A level of CSSC of 100 percent stands for a complete attention expressed in percentage of whether a CIA for this product will be necessary. The level of CSSC of 0 percent stands for no attention expressed in this percentage whether a CIA for this product will be necessary.

Step 3: You have now identified how products can be scaled on CIA by the scale from 0 to 100 percent. In this step you will identify the systems within the product that are responsible in step 2 to achieve a Level of CSSC with CIA. In this step assistance from product experts is needed to make a complete identification of these systems. The product experts are important to prevent that essential systems will be over looked. When you fail to indentify systems during the Six-step method the CSSC-check will not be that effective and will result in a false sense of security.

Now you need a list of the essential systems that are important to achieve the percentage CIA in relation with the functionalities and their systems of the checked product. You have to perform a secure check to find relationships between systems via key-components with other functionalities from the product. You can imagine that a brake-system of a car has a relation to the engine system via the cruise control of the car. The functionalities and systems (CIA) are listed in this step.

To create an overview we made a template that need to be filled in. You can find the table in figure 15. Start by completing the first column and write down all the functionalities of the analyzed system. In the second, third and fourth column you write which system is responsible for the products functionality.

Appendix 1

Functionality and their responsible systems with CIA				
	FUNCTIONALITY	CONFIDENTIALITY	INTEGRITY	AVAILABLITY
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Step 4: In the previous step you defined all the systems of the identified functionalities on bases of CIA. Within these essential systems you can indentify many different components. Not all of the components are important for the Cybersecurity of the product. For our Six-step method will only focus on the key-components within the systems. These key-components are the ICT-hardware, Firmware and Software of the systems. In the example of figure3 the key-components are colored in red.

In this step you will decide which of these key-components will need to be analyzed to achieve the Cyber Security in the Supply Chain. When the key-components of the system are identified, a cross check with the tier must be made. When the key-components are a Commercial Off The Shelf (COTS), the tier level is based on where in the systems the key-components will be used. The chance is null that a supplier from a key-component with a high tier and/or the chance that the suppliers will know that their key-components are used in the system (like a braking system of a car of a fuel system) of the product. These key-components are also used in other products and often with open source software. The chance that other users will find the 'back door' is relatively large. Therefore the key-components with a high tier do not need to be checked for CSSC.

When you look at Government Off The Shelf (GOTS) there are different values, because a lot of intelligence services nowadays are built in so called ´back doors´ to attack the system in a later stadium. These key-components will probably need a firm check to achieve CSSC. When the GOTS comes from a country that has a high 'trust' factor the team that performs the check can decide to accept the key-component which is based on 'trust'. Although you would still advise to check the key-component, because 'trust' might not be enough.

Next to the COTS and the GOTS there is another important version of key-components. The third type of key-components are custom elements. These elements are specially made or written for particular systems. Because they are specially made for only one system and/or product, there is a big chance that these key-components can be compromised, because they are specifically made for this system or product.

It is also important that you look at key-components which have a mutual relation with other systems and certain key-components within these systems. These key-components must also be checked, to make sure that there are no unidentified key-components that will influence the essential systems.

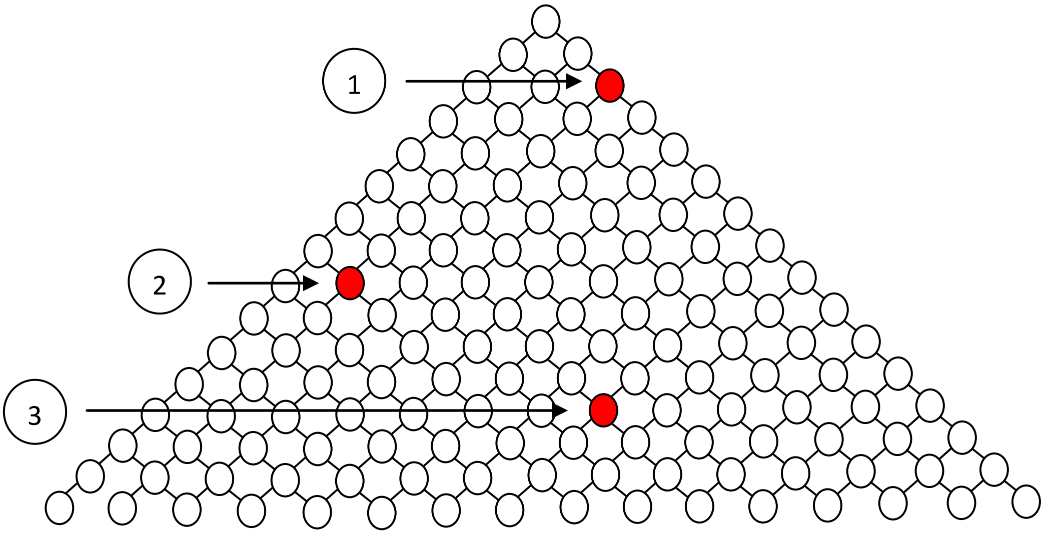


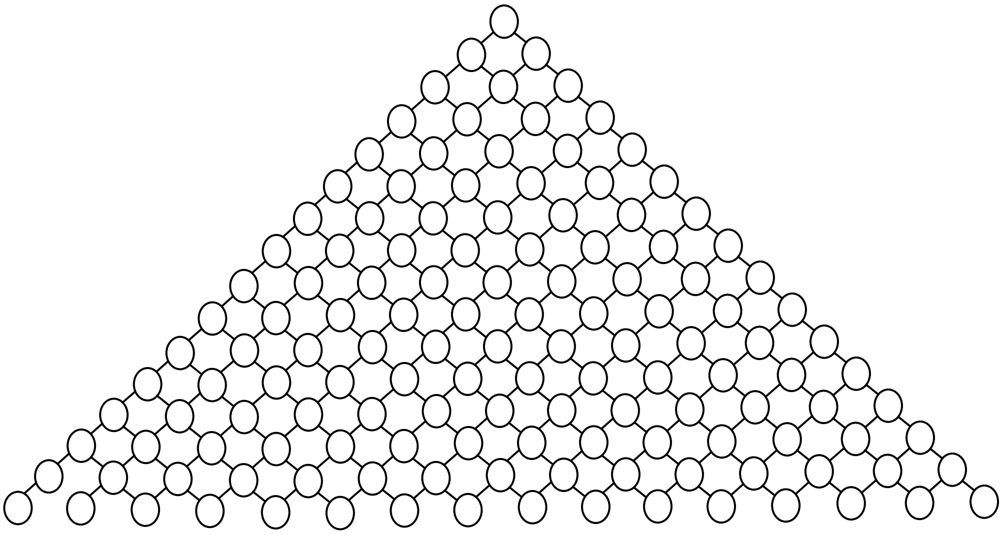
Figure 3: Template system with its components and key-components in red.

In the figure 16 above you see the location of key-components in an essential system which is identified for the functionality of the product. You can see the key-components are marked in color. In this system there are three key-components. The arrows are pointing at the colored key-components. This system contains three key-components starting at tier 1 to tier 3. For instance the key-component with the level tier 3, they are used in many different products and systems. It is not likely that a supplier knows that this key-component is used in his system. Possible attacker will not know in which system or product the key-components will be used. For such an attacker the chance of detection of his initiated back-door is larger when it is used in many other systems. He will probably not compromise an OTS component that is widely used by many different products. He will always focus on the key-components that will end up in only one system or product in which he likes to compromise in a later stadium. This is the reason why the tier of the supplier is important. The key-components with a high level tier are not seen as a danger to CSSC, therefore you will not check these components with the Six-step method, although they are noted as key-components. The team that performs the Six-step method will decide until what level the tier check is necessary. The more a key-component is in a specific element or this key-component controls multiple general components or functionalities, the more important it is to analyze this key-component.

The example shows in figure 3 the key-components of a particular system. Take the system that needs to be checked and fill in the scheme. Filling in this scheme will help visualizing on what level and with what tier the key-components within the systems are located.

Above in figure 3 you could say that inside this system there are three key-components. The arrows pointing at the red colored key-components. This system contains three key components from a tier 1 to tier 3. If the key-component with a tier 3 level, the component probably will be used in many different products and systems. Now you have to make a same scale of the systems by filling in all the key-components to you get a complete image of the whole system and its key-components.

Fill in:



Step 5: Until now you have identified all the key-components of the system, which tier they have and if the key-components are COTS, GOTS or custom elements. In step 4 you also made the system key-components visual. In this step you will start to analyze the relevant key-components for Cyber Security in the Supply Chain (CSSC). In the previous steps from 1 to 4 you analyzed the large amount of components, in which key-components are important and need to be checked on CSSC. You will only focus on the key-components described in step 4. Due to the complexity of key-components it is important that expertise is needed during the analysis of key-components used in a system. It is important that you perform this analyze, not only with an expert but also under supervision of the customer or acquirer of the product. This process is similar to the acceptance test or release test of software.

At the end of this step you will get a list of key-components that are not cyber secure and why they are not cyber secure. This list consists the analyzed key-components that are open for analysis and also the key-components that are GOTS and COTS which a government or commercial party has not given permission to analyze. The acquirer or customer, together with the team that performs the analysis will decide after finishing the analysis with the Six-step method, whether you can accept the CSSC-check of the product.

The table below contains the columns that need to be filled in. Column 1 contains the name of the key-component that is not cyber secure. The second column contains the country of the GOTS. The third column contains the company of the COTS. The fourth column contains the company of the Custom Element. And the fifth and last column contains some extra information. This additional information, includes why someone thinks that the key-component is not cyber secure. It is also possible that a country or company does not accept everyone to have a peek inside a key-component.

This table below contains all the key-components from the functionality described in step 3 and step 4 which reveals the key-components that are not cyber secure. The first column “key-components” contains the key-components that are not cyber secure. The columns 2, 3 and 4 show if the key-component is a GOTS, COTS or a custom element and who the manufacturer is. The last column is a column that gives the tester the ability to write his comments about the specific key-components. Note that the table is colored in red, because all the key-components in this table are not assessed as cyber secure.

Appendix 2

Key-components that are NOT cyber secure				
	GOTS	COTS	CUSTOM ELEMENT	REMARK
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				

Appendix 1

Step 6: In the previous steps we have identified the CIA per functionality, as well we analyzed key-components that are selected for analysis of the systems. In this step we will make a list of all the key-components that are cyber secure after the CSSC check with the Six-step method. Below you can see a table that will be used to finalize step 6. The second column contains the name of the key-components and the country of the GOTS. The third column contains the name of the key-components and the company of the COTS. The fourth column contains the name of the key-components and the company of the Custom Elements. And the fifth and last column is for additional information about this key-component. This table contains all the key-components from the functionality described in step 3 and step 4, which finally will reveal the key-components that are cyber secure. Note the table is colored in green, because the key-components in this table are assessed as cyber secure.

Key-components that are cyber secure				
	GOTS	**COTS**	**CUSTOM ELEMENT**	**REMARK**
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				

Six-step method

With filling this last table at step 6 the check on achieving Cyber Security in the Supply Chain (CSSC) is finished. You have now an overview of what are the functionalities that are important for the use of the product and scaled on the Confidentiality, Integrity and Availability (CIA). All the systems that are responsible for this functionality with the key-components which are used in the system(s) are determined. These key-components can now be divided in Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS) and Custom Elements, also which tier they have. After analysis of the key-components you can say if the lists of secure and insecure key-components achieve a certain amount of CSSC.

Appendix 2: Syllabus improved Six-step method

This appendix contains an improved version of the syllabus earlier mentioned in appendix 1. The only change is the improvement of step 4, where the schematics of a checked system with its key-components has been changed for a table. This table is able to clarify the key-components inside the systems needed to be checked.

Appendix 2

Syllabus

Six-step method

on

Cyber Security in the Supply Chain

Appendix 2

This syllabus will help to achieve and guarantee a certain percentage of Cyber Security in the Supply Chain and refers to the Six-step method in the thesis “Cyber Security in the Supply Chain” developed by B.M.C.S Middendorf (2015). In the media it is showed that the statement “Cyber Security in the Supply Chain (CSSC) is not guaranteed” is well substantiated with several articles in the media. A product consists of many different components from different suppliers and sub-suppliers. Many developed and produced products are not made by one single supplier. In the process of making the product many sub-suppliers are involved in producing small parts which are used later on in many different products. This process with different components from different suppliers is the supply chain. Sometimes a product has components of suppliers that are three suppliers deep or even more. Because there are so many suppliers and suppliers from suppliers, it is impossible for us to know if components are manipulated and to check all these different suppliers and sub-suppliers of CSSC.

There are already many initiatives to achieve some sort of CSSC. These initiatives are based on the factor of ‘trust’ and are created by implementing multiple procedures on different production processes of a manufacturer. These standards ISO, ISA and standards from countries are important, but there more and more products where ICT is implemented and therefore these standards on their own are not enough to achieve CSSC. Therefore a method is created that checks and focuses at the products itself.

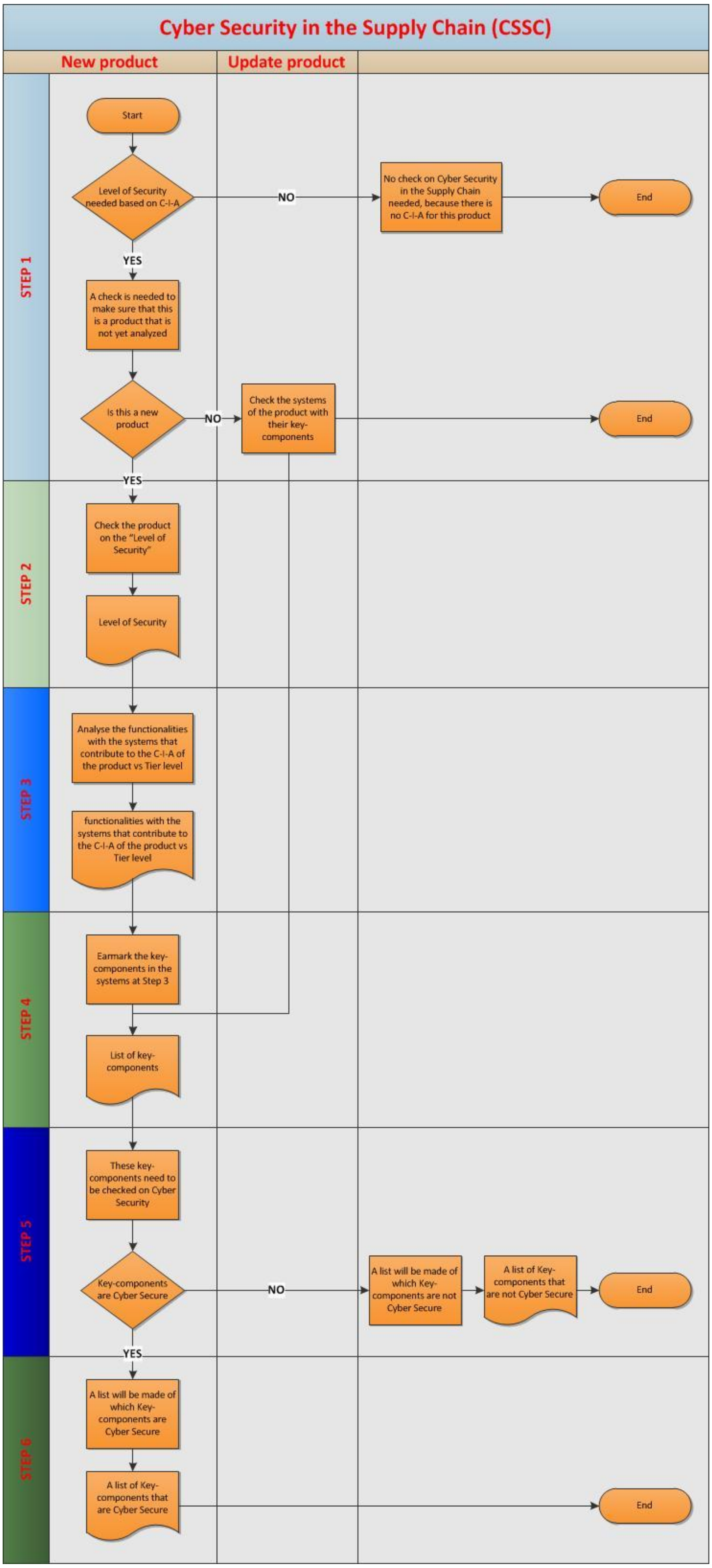
The Six-step method is build to give some sort of Cyber Security in the Supply Chain (CSSC). This syllabus contains all the steps with templates and the guidance per step. To achieve a complete CSSC-check it is important that a product expert will help going through all the steps of the Six-step method. When all the six steps are taken, a complete picture a complete picture can be made of the Key-Components (which consists of the hardware, firmware and software) which are cyber secure and which Key-Components are not.

The first group of key-components found at step 5 which are not cyber secure have to be checked on Cybersecurity after finishing all the steps of the presented Six-step method. At step 6 a list is created with all the key-components that are cyber secure conform the given percentage at step 1. When all the steps are taken a picture will be available with all the key-components that are important for the functionalities of the product, also for the key-components of the functionalities. The follow up of step 5 is to check the key-components if they are cyber secure. This is a specialist job for programmers. In the perfect world when all the key-components are ok, the percentage found in step 2 on Confidentiality, Integrity and/or Availability should match the percentage given at step 2. In the future when there is a product update (step 1) of a key-component the completed templates can be used to see where the key-component matches the current position. When the product has already been checked conform the Six-step method, then only the updated key-component have to be checked. In the flow chart of the Six-step method this step starts at step 4.

When you have finished all the six steps of the Six-step method you should check the software-codes of the key-components that need an extra check (output step 5). In this method you will only go through the Six-step method.

On the next page the flowchart of our Six-step method is presented. Use the following flowchart to go from step to step to perform the check. After the flowchart you go in more detail through every step.

Appendix 2


Cyber Security in the Supply Chain (CSSC)
New product
Update product
STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
Start
Level of Security needed based on C-I-A
NO
No check on Cyber Security in the Supply Chain needed, because there is no C-I-A for this product
End
YES
A check is needed to make sure that this is a product that is not yet analyzed
Is this a new product
NO
Check the systems of the product with their key-components
End
YES
Check the product on the "Level of Security"
Level of Security
Analyse the functionalities with the systems that contribute to the C-I-A of the product vs Tier level
functionalities with the systems that contribute to the C-I-A of the product vs Tier level
Earmark the key-components in the systems at Step 3
List of key-components
These key-components need to be checked on Cyber Security
Key-components are Cyber Secure
NO
A list will be made of which Key-components are not Cyber Secure
A list of Key-components that are not Cyber Secure
End
YES
A list will be made of which Key-components are Cyber Secure
A list of Key-components that are Cyber Secure
End

Six-step method.

Step 1: In this step you will check if the product is new or has one or more updated key-components. The product that you need to analyze for CSSC can be a new, not yet analyzed product or can be a product that contains one or more updated key-components. Both types of components, the new and updated ones are important for the CSSC. You have two opportunities for this check of the product. In the picture below you can see where the two opportunities within the products lifetime are displayed. Those two opportunities for analyzing the CSSC are:

1. During the manufacturing and assembling of the components into the final product.
2. During an update available for the key-components of Cyber security like the software, ICT-hardware and/or firmware.

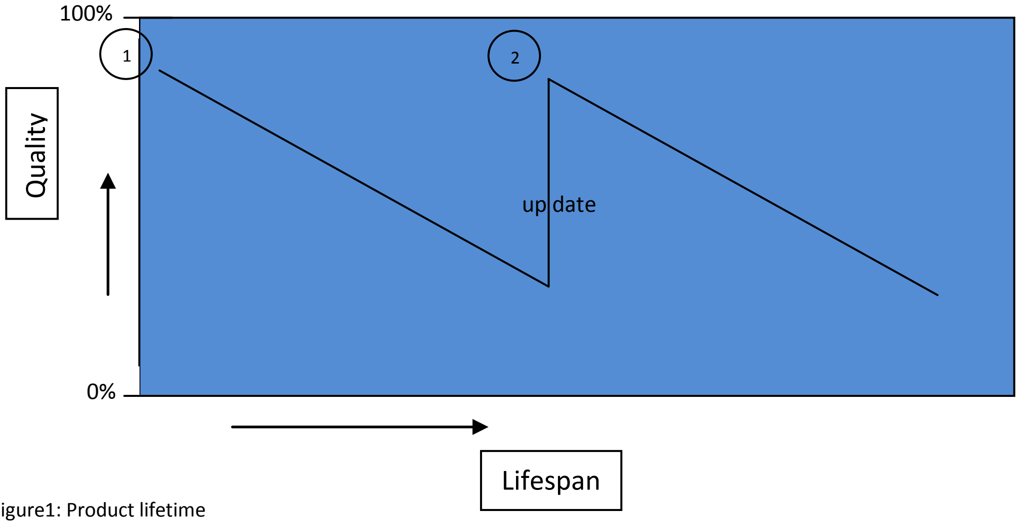


Figure1: Product lifetime

When focusing on the first mentioned opportunity with a completely new product you will need an analysis of the product. When this first opportunity is completed you will get an overview of all essential systems with their key-components.

The second opportunity is an update of the product. This is mainly an update of one or more key-component inside a system that provides the functionality of the product. You will focus on the first opportunity during the period of manufacturing and composition, because in this method it is not known if there has been a check on CSSC like the Six-step method. This check consists of locating the essential systems for every functionality. Also the key-components will be located within that systems that are important for the Confidentiality, Integrity and Availability of the functionalities.

You have used the CIA constructed to identify problem areas and necessary solutions for information security. When you use the CIA within the supply chain of a product, you are looking at the product itself. You are not looking at the information security, but you use CIA to categorize and rate the functionalities of the products. During this process the expertise of end-users is important to make sure that no functionality will be missed.

Step 2: In this step the risk analysis of the concerning company or country which is leading. When there is no risk analysis available the following analysis could be used.

For example you are the acquirer or consumer that accepts the product from the last supplier in the chain. In this step you have to answer the following three questions:

- Is the products confidentiality important or necessary for the purpose(s) for which the owner wishes to use the product for?
- Is the products integrity important or necessary for the purpose(s) for which the owner wishes to use the product for?
- Is the products availability important or necessary for the purpose(s) for which the owner wishes to use the product for?

These questions must not be answered with a yes or no, but need to be answered on a scale of 0 – 100 percentage. Without an answer in percentage of the three CIA questions, it is impossible to realize any level of CSSC. A product consists of many different components or parts. Not all the components are essential to achieve a cyber secure product. When you have answered these three questions with CIA you will get a conceivable graphical representation (see figure 2). You could envisage that although not all the answers will show a 100 percent, just one of the three CIA with a small percentage is acceptable for this functionality of the product. By identifying the systems that are important to the CIA of the product, further analysis is possible of related key-components in other systems, that interacts with the identified systems for CSSC.

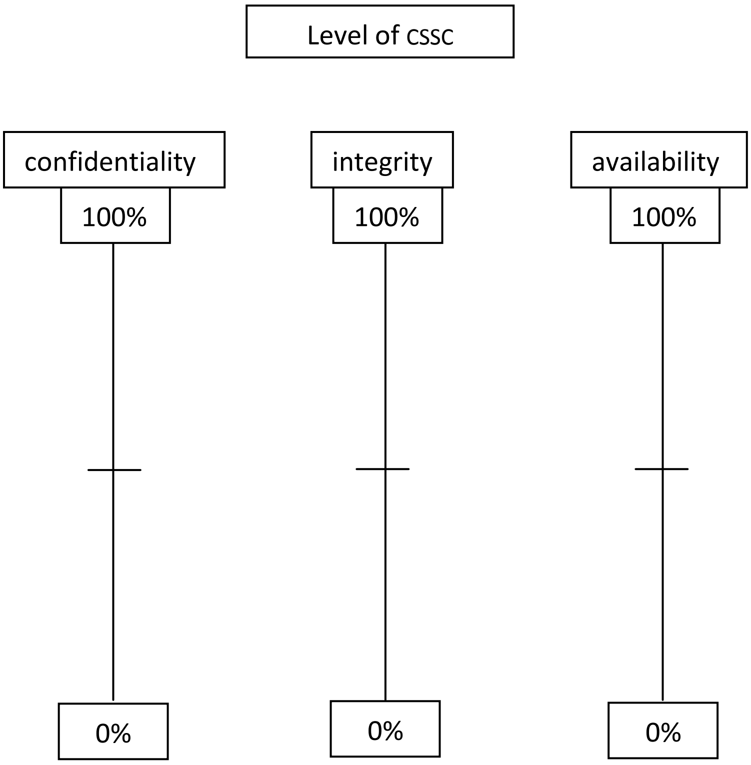


Figure 2: The level of CSSC

Now you can state that the Level of CSSC of the product conform CIA is determined. Although there has not been any analysis of components yet. This gives a clear picture in which tier the components of the systems from the products needs to be analyzed. These percentages give an indication of the “Level of CSSC” in relation to the CIA of the product. Scaled from 0 to 100 percent with a free interpretation of choosing a percentage from 0 to 100 percent.

A level of CSSC of 100 percent stands for a complete attention expressed in percentage of whether a CIA for this product will be necessary. The level of CSSC of 0 percent stands for no attention expressed in this percentage whether a CIA for this product will be necessary.

Step 3: You have now identified how products can be scaled on CIA by the scale from 0 to 100 percent. In this step you will identify the systems within the product that are responsible in step 2 to achieve a Level of CSSC with CIA. In this step assistance from product experts is needed to make a complete identification of these systems. The product experts are important to prevent that essential systems will be over looked. When you fail to indentify systems during the Six-step method the CSSC-check will not be that effective and will result in a false sense of security.

Now you need a list of the essential systems that are important to achieve the percentage CIA in relation with the functionalities and their systems of the checked product. You have to perform a secure check to find relationships between systems via key-components with other functionalities from the product. You can imagine that a brake-system of a car has a relation to the engine system via the cruise control of the car. The functionalities and systems (CIA) are listed in this step.

To create an overview we made a template that need to be filled in. You can find the table in figure 15. Start by completing the first column and write down all the functionalities of the analyzed system. In the second, third and fourth column you write which system is responsible for the products functionality.

.

Appendix 2

Functionality and their responsible systems with CIA				
	FUNCTIONALITY	CONFIDENTIALITY	INTEGRITY	AVAILABLITY
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Step 4: In the previous step you defined all the systems of the identified functionalities on bases of CIA. The essential system contains many different components. Not all of the components (only the key-components) within these systems are important for the Cybersecurity of the product. The Six-step method only focuses on the key-components within the essential systems. These key-components are the ICT-hardware, Firmware and Software of the systems.

In this step you will decide which of these key-components will need to be analyzed to achieve the Cyber Security in the Supply Chain. When the key-components of the system are identified, a cross check with the tier must be made.

When the key-components are a Commercial Off The Shelf (COTS), the tier level is based on where in the systems the key-components will be used. The chance that a supplier from a key-component with a high tier and/or the chance that the suppliers will know that their key-components are used in the system (like a braking system of a car of a fuel system) of the product is null. These key-components are also used in other products and often with open source software. The chance that other users will find the 'back door' is relatively large. Therefore the key-components with a high tier do not need to be checked for CSSC.

If you look at GOTS there are different values, because a lot of intelligence services nowadays have been built in so called 'back doors' to attack the system in a later stadium. These key-components will probably need a firm check to achieve CSSC. When the GOTS are coming from a country that has a high 'trust' factor, the team that performs the check can decide to accept the key-component based on 'trust'. Although you would advise to check the key-component, because 'trust' might not be enough.

Next to the COTS and the GOTS there is another important version of key-components. The third type of key-components are custom elements. These elements are specially made or written for particular systems. Because they are specially made for only one system and/or product, there is a large chance that these key-components can be compromised. If the Custom Element is made 'in house' the chance that the key-components are compromised is less. Therefore it is important to fill in the column remarks.

It is also important that you look at key-components which have a mutual relation with other systems and certain key-components within these systems. These key-components must also be checked, to make sure that there are no unidentified key-components that will influence the essential systems.

The key-components of the checked system					
	COTS	GOTS	CUSTOM ELEMENT	REMARKS	TIER
1.					
2.					
3.					
4.					
5.					
6.					

Figure 3: Table with all the relevant key-components of the checked system.

In the figure 3 above you see the location of key-components in an essential system which is identified for the functionality of the product. When key-components have a tier 3 level, it is likely used in many different products and systems. It is not likely that the supplier will likely not know that this key-component is used in this particular system. And a possible attacker will not know in which system or product the key-components will be used. For such an attacker the chance of detection of his initiated back-door is larger when it is used in many other systems. He will probably not compromise an OTS component that is widely used by many different products. He will always focus on the key-components that will end up in only one system or product which he likes to compromise in a later stadium. This is the reason that the tier of the supplier is important.

Despite the fact that the key-components with a high level tier are not seen as a danger to CSSC, you could decide that you will not check these components with the Six-step method, although you will note those components as key-components. The team that performs the Six-step method will decide until what tier-level the check is necessary. The more a key-component is in a specific element or this key-component controls multiple general components or functionalities, the more important it is to analyze this key-component.

If the key-component with a tier 3 level, the component probably will be used in many different products and systems. Now you have to make a same scale of the systems by filling in all the key-components to get a complete image of the whole system and its key-components.

Step 5: Until now you have identified all the key-components of the system, which tier they have and if the key-components are COTS, GOTS or custom elements. In step 4 you also made the system key-components visual. In this step you will start to analyze the relevant key-components for Cyber Security in the Supply Chain (CSSC). In the previous steps from 1 to 4 you analyzed the large amount of components, in which key-components are important and need to be checked on CSSC. You will only focus on the key-components described in step 4. Due to the complexity of key-components it is important that expertise is needed during the analysis of key-components used in a system. It is important that you perform this analyze, not only with an expert but also under supervision of the customer or acquirer of the product. This process is similar to the acceptance test or release test of software.

At the end of this step you will get a list of key-components that are not cyber secure and why they are not cyber secure. This list consists the analyzed key-components that are open for analysis and also the key-components that are GOTS and COTS which a government or commercial party has not given permission to analyze. The acquirer or customer, together with the team that performs the analysis will decide after finishing the analysis with the Six-step method, whether you can accept the CSSC-check of the product.

The table below contains the columns that need to be filled in. Column 1 contains the name of the key-component that is not cyber secure. The second column contains the country of the GOTS. The third column contains the company of the COTS. The fourth column contains the company of the Custom Element. And the fifth and last column contains some extra information. This additional information, includes why someone thinks that the key-component is not cyber secure. It is also possible that a country or company does not accept everyone to have a peek inside a key-component.

This table below contains all the key-components from the functionality described in step 3 and step 4 which reveals the key-components that are not cyber secure. The first column “key-components” contains the key-components that are not cyber secure. The columns 2, 3 and 4 show if the key-component is a GOTS, COTS or a custom element and who the manufacturer is. The last column is a column that gives the tester the ability to write his comments about the specific key-components. Note that the table is colored in red, because all the key-components in this table are not assessed as cyber secure.

Appendix 2

	Key-components that are NOT cyber secure			
	GOTS	COTS	CUSTOM ELEMENT	REMARK
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				

Appendix 2

Step 6: In the previous steps we have identified the CIA per functionality, as well we analyzed key-components that are selected for analysis of the systems. In this step we will make a list of all the key-components that are cyber secure after the CSSC check with the Six-step method. Below you can see a table that will be used to finalize step 6. The second column contains the name of the key-components and the country of the GOTS. The third column contains the name of the key-components and the company of the COTS. The fourth column contains the name of the key-components and the company of the Custom Elements. And the fifth and last column is for additional information about this key-component. This table contains all the key-components from the functionality described in step 3 and step 4, which finally will reveal the key-components that are cyber secure. Note the table is colored in green, because the key-components in this table are assessed as cyber secure.

Key-components that are cyber secure				
	GOTS	**COTS**	**CUSTOM ELEMENT**	**REMARK**
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				

Six-step method

With filling the table at step 6 the check on achieving Cyber Security in the Supply Chain (CSSC) is finished. You now have an overview of what are the important functionalities for using the product, scaled on the Confidentiality, Integrity and Availability (CIA). All the essential systems that are important and responsible for this functionalities and the key-components inside these systems are determined. These key-components can now be divided in Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS) and Custom Elements, also which remarks and tier they have. After a short analysis of the key-components you can say if the lists of secure and insecure key-components achieve a certain amount of CSSC.

With the final conclusions of the CSSC-check, according to the Six-step method, you can say that after checking the two key-components in step 5, the system for example is cyber secure for a certain percentage. For instance 80 percent on Confidentiality, 100 percent on Integrity and 100 percent on Availability.