Perspectives on Control System Security

Assessing security risks resulting from contradicting values between Operational and Information Technology

Master thesis

April 2013
Delft University of Technology
Faculty of Technology, Policy and Management
MSc. Systems Engineering, Policy Analysis and Management (SEPAM)

Personal

Author:	F.A. (Floris) Schoenmakers
Student number:	1311999
Telephone:	+31(0)-641 65 20 94
Email:	faschoenmakers@gmail.com

Committee

Chairman:	Prof. Dr. M.J.G. (Michel) van Eeten
First supervisor:	Dr. M.L.C. (Mark) de Bruijne
Second supervisor:	Dr. G.P.J. (Gerard) Dijkema
Company supervisor:	Drs. M.H.J. (Martijn) Knuiman - Manager Security & Privacy Deloitte
Company supervisor:	Ir. S. (Sergio) Hernando – Senior Manager Security & Privacy Deloitte

Keywords **IT/OT integration, Cyber security, Security Paradigm, Risk framework, Cultural values, Control systems**

Executive summary

Situation Industrial control systems in the electricity domain become increasingly connected. The change in the control systems industry has several drivers. Business drivers on the one hand; management is expecting more information and more steering possibilities. Market drivers on the other hand; better incorporation of decentralized generation, improvements of the existing services and maintaining or improving the existing high levels of system reliability. To facilitate the changing requirements, more intelligence and connectivity in control systems is necessary. In the past, control systems were connected with proprietary networks to the SCADA network. These systems and networks were often custom-made, isolated and had little processing power. The current trend is to implement and use control systems with off-the-shelf technology, with interconnectivity and with computing power. This trend is referred to as Internet Technology (IT) integration into Operational Technology (OT), in short: IT/OT integration. It brings a significant change in the status quo of the energy industry.

Complication The implementation of the increased connectivity and intelligence presents a two folded problem: technical related issues and people related issues. The technical issues originate from the difficult replaceability of control systems due to high investment costs and the necessity to keep the availability of the electricity supply as high as possible. The time a control system is in operation, referred to as the component lifetime, ranges from 15 to over 50 years. This implies that currently a significant amount of the equipment needs to be adapted in order to meet the connectivity and intelligence requirements. Besides the before mentioned technical issues, the human factor plays a vital role in the IT/OT integration. It seems that the IT experts and the OT experts have conflicting perspectives on security. In essence, the operational systems are brought out of isolation and consequently need to be secured. Securing the systems is even more important due to the fact that the SCADA and control systems are often part of a critical infrastructure. To accomplish secure control systems, the IT expert group - responsible for cyber security - and the OT expert group – responsible for the operations - are bound to work intensively together. However, it appeared from a preliminary analysis that the perspectives between the groups are not aligned. A difference in perspective might have a significant impact on how issues and solutions related to security are perceived. The differences in perspectives could impede advancement of the IT/OT integration in the electricity infrastructure and may increase cyber vulnerabilities resulting from conflicting values.

Approach There is little scientific research done on the existence of conflicting values between groups related to the IT/OT integration in the energy domain. To enable a relevant reflection on

the impact of different values on control system security, literature and empirical evidence was gathered. The following main research question was posed:

What are the differences in perspective on security between an IT expert and an OT expert in the control system domain of the electricity sector and how does this affect control system security?

As mentioned earlier, the difficulties are two-folded; both technical and human. A literature study on both subjects was conducted in part I of this research. The main subjects of this literature study were the technical details of the electricity sector and the paradigms of the IT and OT groups. The goal was to understand the current state of affairs of the control systems security in the electricity sector and to gather and discuss relevant research on the IT and OT perspectives. Part II of this study focused on comparing the literature with self-collected empirical data. The empirical data was gathered with a questionnaire and focused on finding significant differences in perspectives on security between the two groups of experts. In the first chapter of part III the empirical implications of the findings and the answer to the research question are discussed. In the second chapter of part III normative implications for control systems security is reflected, in particular the consequences of different perspectives and their relation to risk management.

Results In the literature, numerous technical difficulties can be pointed out which impede the IT/OT integration. Different ways to cope with availability, patch management, operating systems and component lifetime make it difficult for IT specialists to secure industrial control systems. Requirements for control systems like availability and reliability do not allow the standard IT security practices. The issues can range from too limited processing power for anti-virus software, to the inability to update and patch the systems due to uptime requirements. The IT/OT integration and accompanying technical difficulties require the people working on the IT security and on Operational systems to work closely together. With the IT/OT integration, the IT expert entered the terrain of the OT expert. According to the literature, the IT expert and the OT experts have a different set of values. OT experts are involved in the design and operation of systems that have a high physical interaction. Requirements as safety, reliability and availability (SRA) are values which are important to the OT experts. IT experts are involved in securing system and networks. In general, the IT expert has a different set of requirements than the OT expert. In the literature confidentiality, integrity and availability (CIA) are values which are associated with IT group. The intention of the gathered empirical data was to explore whether a difference in perspective on security could be found. The empirical data showed that there is a significant difference in perspectives on security between IT experts and OT experts in 21% of the statements. The IT and OT group significantly differed from opinion on aspects as security awareness, compliance, remote access and qualified personnel.

Implications & Outlook

Based on the literature as well as the questionnaire, we can argue that a difference in perspective can have an impact on control system security. The values that people have can determine - to a certain extend - the way security is interpreted and perceived. When there is a difference in perspectives, it might keep organizations aware, but when the differences are too comprehensive it will restrict the organization in properly dealing with threats. Whether shared values for the IT and OT group are likely to happen and desirable to have is an interesting question. When the IT and OT group maintain their current separate values, communication and interaction is important. Interaction and communication might improve understanding and commitment which can advocate control system security. To increase commitment, understanding and shared values, managers must play an active role in promoting shared values.

Risk management is to a large extent steered by people; the influence of their perspective on security is believed to be significant. Throughout every sections of our risk management framework the perspective on security was a reoccurring theme. Threat perception, vulnerability identification and risk response can all be influenced by the perspective on security. Again, a shared set of values on security can contribute in improving risk management. Some final thoughts – ideas and best practices - on control system security had been drafted in the last paragraph of this research. A short abstract of the recommendations: be selective in bringing control systems from isolation, use the wisdom of the crowd to find vulnerabilities, facilitate education and training for personnel, share practical knowledge and ideas with the industry, and make better use of online media monitoring (Twitter, Pastebin, forums) to actively search for threats.

Acknowledgements

I would like to thank my graduation committee, Prof. Dr. Michel van Eeten, Dr. Mark de Bruijne, Dr. Gerard Dijkema, Drs. Martijn Knuiman and Ir. Sergio Hernando, for their assistance and guidance during my Master thesis. Also I want to thank Deloitte NL Risk Services, in particular Marko van Zwam, facilitating and supporting the research.

Also, a special thanks for their assistance to: Erik Poll (Radboud University), Eric Luijjf (TNO), Eric van Aken (Liandon), Eric Byres (Tofino Security), Oscar Koeroo (Nikhef), Roelof Klein (Alliander), Samuel Linares (Intermark), Theo Fens (TU Delft), Charlotte de Roon (CRK).

Chapter 1. Introduction

Regardless of how quickly various utilities embrace smart grid concepts, technologies and systems, they all agree on the inevitability of this massive transformation (Farhangi H. , 2010). The possibilities of an intelligent grid - in theory - will have a positive contribution to the grid. Currently, the possibilities and difficulties are monitored in various smart grid pilots in the Netherlands and around the world. The possibilities and benefits are often highlighted, in particular increased reliability and decreased costs. Yet, the challenges and risks of the transition towards a smart grid are at least just as interesting.

1.1 A brief history on the electric grid

The first electrical network was created in 1887 on Pearl Street Station in New York City. This small system provided electricity for some 100 lamps (Edison, 1880). The design of both the electrical system as well as the lamps came from Thomas Edison (Bredhoff, 2001). Soon after his successful project, the electrical networks increased and early 1900's most of the big cities in the world had electricity for their households (Arnold, 2011). The industrial era changed significant parts of society but the layout of the grid stayed the same. Early signs of the possibilities of the smart grid were described in the 1985's research paper "The Design of an Integrated Distribution Control system" (Purucker, S.L; et al., 1985). It is interesting that these researchers identified much of the functionalities of the smart grid almost 30 years before it could become a reality. They wrote about electricity balancing, access to real time data, switching suppliers, demand response, monitor equipment failure and decentralized production. This is similar to many modern descriptions of an intelligent grid.

The principle of a smart grid is simple: every client, household and business, has a meter which can communicate with electricity companies. The electricity infrastructure is filled with sensors that monitor and remotely steer the real-time 'health' of the grid. The network operator and other authorized companies use the data and functionalities of the smart grid to make the grid more efficient. The control is facilitated by computerized systems – control systems as SCADA - that analyze and control data.

1.2 Reasons for a more intelligent grid

In October 2009 the Dutch Ministry of Economic Affairs constituted the *Taskforce Smart Grids*. The ministry only facilitated the taskforce and played no formal role. A nice example of the Dutch "poldermodel", where all relevant parties are being involved in the process.

Their vision on why smart grids should be implemented (Taskforce intelligente netten, 2010, p. 5):

> "Smart grids are innovations concerning energy networks, which have as their purpose to make the future energy supply more affordable, reliable and also make it more sustainable."

As for reliability, there are some concerns that the adaption of the electricity infrastructure to the new ICT infrastructure will cause issues (Vaessen P. , 2012). The connection between the old grid infrastructure and a new IT infrastructure appears to be a difficult process: the legacy control systems are not designed to have desired connectivity.
From a provider as well as the client perspective the smart grid offers new functionalities. The generic description of these functionalities is as follows: (European Commission, 2012); (Taskforce intelligente netten, 2010); (Electrical Power Research Institute, 2011); (ten Heuvelhof, 2012); (Collier, 2010)

1. Activate demand response at client side. Motivates and includes the consumer;
2. Better incorporation of decentralized generation and storage in the electric grid;
3. Stimulate the development of new products, services and markets;
4. Maintain and improve the existing services efficiently;
5. Limit or postpone investment in the infrastructure;
6. Maintain or even improve the existing high levels of system reliability, quality and security of supply; and,
7. Significantly reduce the environmental impact of the whole electricity supply system

1.3 Challenges & research objective

The design, build, test and implementation of critical infrastructure is a challenge. Grid operators, among others, have the responsibility of increasing the intelligence in the grid. Smart grids have the potential to contribute significantly to society, but risks are present. Recently, in September 2012, a major vendor of smart grid control systems reported its systems were successfully attacked by hackers. The hackers installed malicious software and obtained project files (Wired, 2012). This illustrates the relevance for ongoing research related to the grid security. Rod Beckstrom delineated during the World Economic Forum's Global Information Technology Report 2012 three laws regarding the hyper connectivity. Beckstrom called the law the 'connectivity of things', which consist of three laws: (World Economic Forum, 2012)

> Law 1: everything that is connected to the internet can be hacked;
> Law 2: everything is being connected to the internet, and

Law 3: everything else follows from the first two laws.

IT solutions being implemented into the grid also bring the disadvantage of 'everything is connected'. This means that security has to evolve in the same pace as the grid itself. What are the challenges?

Security is considered to be a critical factor of the infrastructure. Whereas the physical infrastructure has been an important subject in the past decades with the rising awareness of the vulnerabilities and dependency on electricity networks (ENISA, 2012), still almost no significant changes to the physical infrastructure have been done the past 50 years.

The focus today lies on the IT infrastructure, which developed rapidly since 1990's when the internet protocol became popular. This provides opportunities for hackers to compromise the security. When a hacker has access to the system, different scenarios are possible. Think of unauthorized control of appliances, insight in data or manipulation of data (Deloitte Consulting, 2012). It is often emphasized by security experts that security has to be built in from the start, also known as security by design (Cárdenas, Amin, & Sastry, 2008). Building the security into a system after it is completed is difficult, if not impossible (European Network and Information Security Agency, 2011). In 2008 researchers of the University of Berkley identified challenges for the security of control systems were facing. The following enumeration gives an overview of the origin of the security related problems in the grid (Cárdenas, Amin, & Sastry, 2008):

- *Process control systems are being turned into computers*. Controllers are more often equipped with microprocessors. Which gives more flexibility to, for example, configure the control via a webserver and remotely access and control the units.
- *The systems are networked*. Connection of control systems to corporate networks (the day-to-day business network) becomes more common which bring them out of prior isolation.
- *Commodity IT solutions are used*. Off-the-shelve IT solutions are used for control systems such as Windows operating systems and TCP/IP networking protocols.
- *Open design protocols are used*. Old control systems had their unique protocols. These protocols are now more accessible and open. In this way, attackers can gain knowledge about the protocols and undertake targeted attacks. Attacks on for example information and intellectual property.
- *Size and functionality increases*. New functionality, which is the intention of the smart grid, could lead to new vulnerabilities.

- *The IT global workforce becomes large and highly skilled*. The tools for attacks become easier to use and the crowd that could be able to use it grows rapidly.
- *Cybercrime increases*. With malicious actions criminal organizations and institutions can gain benefits.

Industrial control systems become more connected: control systems "have seen a significant increase in the use of computer networks and related Internet technologies to transfer information from the plant floor to supervisory and business computer systems" (Byres, Eng, & Lowe, 2004, p. 1). The grid, being a critical infrastructure for society, is expected to be highly reliable. Engineers designed and maintained the grid based on the safety, reliability and availability model (European Network and Information Security Agency, 2011). For decades this **paradigm** remained the focus of control system engineers. We pose that the focus should have changed when the information technology (IT) became an important aspect of the grid infrastructure. IT specialists designed their software from another perspective: the Confidentiality, Integrity and Availability (CIA) Triad. Here we find an interesting difference in perspective. Often, culture difference is alleged to play a considerable role in the discrepancy between an engineer and an IT specialist (Huston, 2012). It is for example possible, although not yet supported by a scientific study, that education and work experience lead to IT experts and engineers both having a tunnel vision on their topic. With a tunnel vision and without understanding of each other's profession, ensuring security for control systems in which engineering and IT are increasingly intertwined, becomes a daunting task.

Besides the different paradigms, there is a problem more inherent to the electricity sector. The equipment in the grid, from power stations to substations, are all designed and built to last for decades and were not designed to adapt new technologies (National Institute of Standards and Technology, 2011). Tendency in management, not only at grid companies, is the desire to have more data and more information. Unfortunately, the **legacy control systems** (elderly systems) are simply unsuitable for data analysis and communication. The solution was of course straightforward: make the legacy control systems suitable for communications. Information technology, and thus security, was built in afterwards: security after design instead of security by design. Security is never 100% impeccable, but the chance of a security breach when implementing security afterwards is believed to be a lot higher (ENISA, 2012). Secondly, what happened when IT security specialists secured the systems to IT standards? Several issues came to light, these issues were capable of causing malfunctions in the control systems. When for example a password in a legacy system was changed from default, the systems internal processes could not communicate because default passwords were expected (European Network and Information Security Agency,

2011). When it comes to IT implementation in legacy control systems and securing these systems, grid operators have limited choice because replacing the whole infrastructure is often not an option because of the high replacement costs. It is a challenge to optimize security with the increasing intelligence of (legacy) control systems.

The combination of ever present security risks, the legacy control systems and the difference in paradigm between the IT experts and the control system engineers present an interesting challenge. The accompanying **research objective** of this study is:

> *First, gain insight in the role that a difference in perspective on control systems security plays and provide insight of how this affects cyber security in the electricity domain. Second, give guidance on how to handle the integration of IT/OT systems with guidance of a risk management framework.*

1.4 Research questions

Based on the challenges and the research objectives, the main research question is defined as follows:

> *What are the differences in perspective on security between an IT expert and an engineer in the control system domain of the electricity sector and how does this affect control system security?*

To answer the main question, three sub questions are posed.

1. How do the control systems operate and what are the most important control systems and IT systems in the electrical grid?
2. What are the differences in perspective between IT and OT specialists?
3. What are the consequences of differences in perspectives on risk management for control systems in the electrical grid domain?

1.5 Research methods

To compare the perspective of control system experts and the perspective of IT specialists interviews and surveys will play a central role. We expect the two groups having different opinions on how security should be achieved. Firstly, the research aims to analyze literature on the technical part of the grid, in order to draft a comprehensive image of the grid with respect to control systems and IT. Consequently, with a literature study, the perspectives of both the control system experts and the IT experts were analyzed. How do they perceive security from their perspective? To confirm our hypothesis stated in paragraph 5.2, experts from both the control system industry as well as IT were asked to complete a survey. Their opinions were compared to each other and an analysis of the results is done. The three methods used in this research were:

- Desktop research: desktop research will be performed in order to search for the foundations of the differences.
- Interviews: during the research a dozen experts from both fields will be questioned on their opinions and expertise. In this way literature and experience could complement each other. Also expert validation is important to validate the results.
- Survey: the survey provides the opportunity to verify what is discussed in literature.

Information is composed of available literature and opinions of experts from, among others from the Technical University of Delft, Deloitte, Platform for Cyber Security, Dutch Network Operators and the National Cyber Security Centre.

1.6 Relevance & scope

Reliable risk identification and risk strategies contribute to the success of the smart grid. Identification of security risks and regulatory mechanisms help to gain insights in vulnerabilities and threats. Control system security is increasingly more important en relevant. This is confirmed by media coverage on control system security that intensified over the last year. To name a few examples:

- SCADA bugs make security a turkey shoot for hackers. November 2012. (V3, 2012)
- Maker of Smart-Grid Control Software Hacked. (Wired, 2012)
- DHS Warns of 'Hacktivist' Threat Against Industrial Control Systems. October 2012. (Krebs, 2012)
- Backdoor in computer controls opens critical infrastructure to hackers. October 2012 (Arstechnica, 2012)

Not only the news of attack on control systems increases. Also the availability of scan and attack tools for control systems increases. A few examples:

- PLC scanner: a port scanner designed to find and display properties of Siemens S7 and Modbus devices (PLC devices scanner, 2012);
- WinCC Harvester: exploit for Siemens SIMATIC WinCC. Can, according to the author, retrieve sensitive information (users, roles, PLCs) from the database. (WinCC harvester, 2012)
- ProFuzz: is capable of bombarding a SCADA system using the Profinet protocol (most used protocol in ICS) with various dataflows, which can lead to errors and/or system crashes. (ProFuzz, 2012)

The desired outcome of the research is to gain specific and practical results. Some demarcations are made to this research to enable in depth research.

Due to the fast evolution of computerized systems, it is difficult to focus research over a long time span. Also the research outdates easily because of the fast developments. Therefore our research focusses on a **time period** from approximately 2013 until 2020. At the beginning of this century smart grids became a popular topic. This created a vast amount of literature from that point onward. The European Union is a pioneer in gathering and bundling of the available information with research groups as the European Network and Information Security Agency (ENISA) and Smart Grid Coordination Group (SGCG). There is a lot to find on smart grids, but it outdates rapidly due to the fast changing IT environment. This applies also to this research: after a few years technology and policy have changed significantly, therefore it is very difficult to look far ahead in time. Although the implementation of the changes in the grid is taking longer much, this research focusses on current security problems. Therefore the scope ends at approximately 2020.

1.7 Research approach

The research has five steps: introduction, analysis, design & execution, data analysis and normative & empirical reflection. After the introduction chapter, a literature study is undertaken consisting of three parts. First, information on the current and future functions of the grid are discussed. Second, the control systems and IT systems which are relevant to the grid are described and analyzed. Understanding which components play a role in the grid infrastructure leads to a better understanding of the technical requirements and the consequent effect on the different perspectives. The literature study closes with an analysis of the existing engineering and IT paradigms found in literature. In this chapter we delineate the differences in perspective on security between the two groups. With the information gathered in the literature study, a questionnaire is composed. The questionnaire is based upon various literature on questionnaire design. After consulting the experts from both the IT as the engineering perspective, data analysis is done based upon the results. The results are analyzed upon significant differences in opinion between the IT specialists and the engineers. In chapter seven the empirical implications are discussed, where an answer is given on the main question. The research closes with a chapter on normative implications, where the impact of the results is discussed, the applicability towards other domains and some final thoughts on the control systems security future.

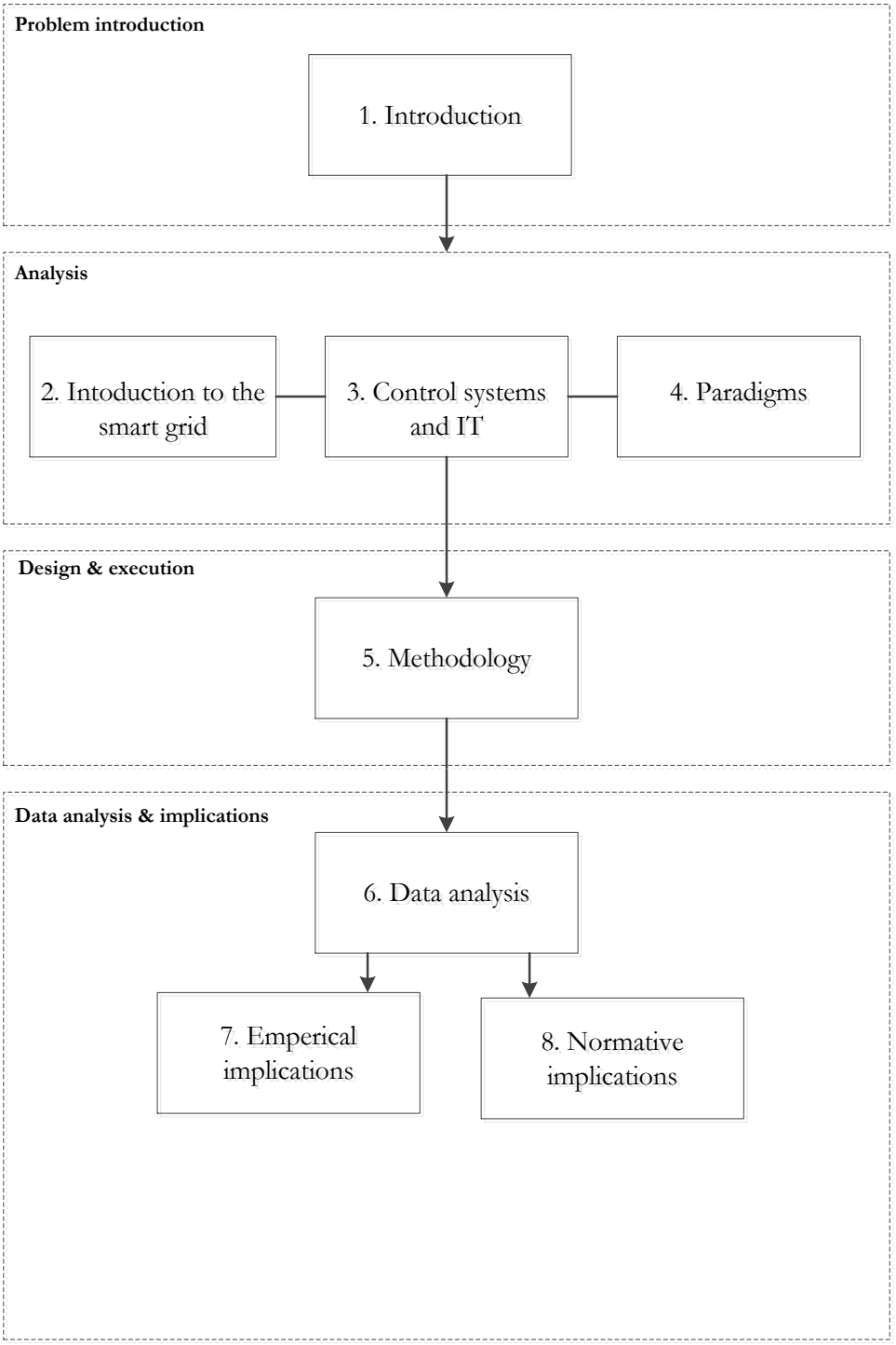


Figure 1: research setup

1.8 Definitions

This research deals with various definitions that need some additional explanation.

Security

Security in this paper is focused on critical infrastructure. The security comprises physical as well as cyber.

> *Physical security*
>
> Measures that are designed to deny access to unauthorized personnel - including attackers or accidental intruders - from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts (Conrath, 1999).
>
> *Cyber security*
>
> Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
>
> a) integrity, which means guarding against improper information modification or destruction;
> b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
> c) availability, which means ensuring timely and reliable access to and use of information. (U.S. Office of the Law Revision Counsel, 2012)

Risk

Wikipedia has formed an understandable and suiting explanation of what risk is:

> The potential that a chosen action or activity - including the choice of inaction - will lead to a loss (an undesirable outcome) (Wikipedia, 2012).

A more scientific definition is set by the International Organization for Standardization (ISO). We use two definitions of ISO 27005 (the risk management standard) and IS0 31000 (risk management):

> The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (ISO 27005, 2011), and
>
> The effect of uncertainty on objectives. (31000, 2009)

The latter three definitions give the reader enough understanding of what is meant by a risk and what the context is.

Legacy control systems

Legacy systems are systems which cannot be secured completely by regular measures and technologies and therefore pose a larger risk to the continuity, integrity and confidentiality of the controlled process(es). Examples of reasons to characterize systems as legacy systems are (CPNI, 2012):

- Missing (partial) support by supplier/vendor or lack of spare parts;
- Declining knowledge and expertise about systems on the market or in the own organization;
- Insufficient security against physical or logical threats from the environment.

The engineer

The engineer in this research is referred to as the person who works with operational technology (OT). Education can be focused on system design and development of (industrial control) systems. The operation technology in control systems, also referred to as industrial automation systems, are often mechanical/physical systems. These systems are guided by computers with either a custom operating system or an standard solution (i.e. Windows NT). While the engineers can also be engaged in developing software for the actual control system, this is stays closely dependent to the mechanical/physical interaction of the control system, which the IT specialist encounters significantly less. The overlap between the two professions mainly consists of the use of computers.

The IT specialist

In this research, we refer to IT specialists as the people who understand and practice computer, network and server security. The focus lies in this profession lies on non-physical aspects, such as software and programming.

Synonyms or equalities

Smart grid – Intelligent grid

Engineering specialist – Operational Technology (OT) specialist

IT specialist – IT expert

Industrial control systems – Control systems – Industrial IT system

Perspective – Paradigm - Culture

Part I

Grid basics, Control Systems and
IT networks in the electricity grid

Chapter 2. Introduction to the smart grid

Goal of this chapter Explain the basics of the transition in the electricity domain

The grid is a 'system of systems' across generation, transmission, distribution, control and consumption. It is the collective noun for everything that is affiliated with the electricity grid. The infrastructure could generally be viewed as two separate parts: cyber components (IT systems) and physical components (Operational systems). To be able to understand the grid infrastructure - how it is connected and what are the relevant devices – a preliminary analysis of the physical assets is undertaken.

Half a decade ago, 'smart grid' started to become a buzzword. In the period 2008 – 2009 the amount of Google searches on the term 'smart grid' increased by more than 800% (Google Trends, 2012). When reading articles about the smart grid, online as well as in newspapers, one can conclude that the term is often misused. It seems to be a common misunderstanding that the smart grid is already in place because a smart meter is installed. In this chapter the current state of the grid is described; the development of the intelligent grid has just begun. This chapter, the introduction to the smart grid, provides the basics for the understanding of the problems with the IT/OT integration of systems.

2.1 Grid functionality

What is the grid and what is the difference between a static grid and the intelligent grid? First, the change which enables almost every other change in the grid: the grid is making a transition from an electro-mechanical grid towards a digital-mechanical grid. In the electro-mechanical grid, information is not captured and stored. In smart grids the IT infrastructure plays a key role, as it assists two-way information exchange. This refers to the possibility of communication between every device in the network. Not only the information can be two directional, the intelligent grid also will enable more efficient decentralized production. The traditional grid was based on centralized production and distribution to the grid. Digitalization offers the opportunity to monitor virtually every location. Sensors in the network enable the operators to monitor input and output in the grid. An additional important feature is the ability to check the 'health' of the network. Detection of failing equipment, power losses and security breaches are properties of the intelligent grid. The self-monitoring aspect of the grid enables real time information on the current state and offers opportunities for a self-healing of the grid. When an incident occurs in the grid, sensor notices abnormal power flows and have the ability to isolate parts of the infrastructure. This

supervisory control functionality of the smart grid is called self-healing (National Energy Technology Laboratory, 2008). If the balance in energy supply and demand cannot be met, the supervisory control can also be used to switch off non-critical appliances. When indicated as not critical, this could be for example be the charging of an electric car. Finally, customers should benefit from the smart grid because of increased user functionality. Via the in-house display users potentially could control appliances, monitor usage and determine their energy plans.

Static grid	Intelligent grid
Electro-mechanical	Digital
One-way communication	Two-way communication
Centralized communication	Distributed communication
Few sensors	Sensors everywhere
Blind	Self-monitoring
Manual reports and repairs	Self-healing
Manual inspection	Remote testing
No remote control	Remote control
Limited customer control	Extensive customer control

Table 1: difference between static and intelligent grid. Based on (Farhangi H. , 2010)

What is the current state of the grid? The Dutch grid, as many other electric grids in the world, is in a transition. We are transitioning towards an intelligent grid and are currently in an arena where two way communication is piloted and analyzed. In other words: the smart grid is still in a very early stage of development.

2.2 Physical structure

The physical components of the grid are illustrated in Figure 2. The original grid is shown on the left. This illustration makes the layered model comprehensible: the power and information flows from the center to the outside as can be seen from the arrows. Starting at the power generation site, passing through transmission, distribution and is delivered at the homes and industrial sites. The right part of Figure 2 illustrates the modern, intelligent grid: an envisioned end result of the transition we are in right now. Power generation is party done by users themselves. When electricity is generated at the power station, it either flows to the users or it is stored. Most apparent aspect of the intelligent grid is the possibility to exchange information that allows decentralized generation. To be able to analyze and identify security issues related to the physical systems, the relevant aspects are discussed:

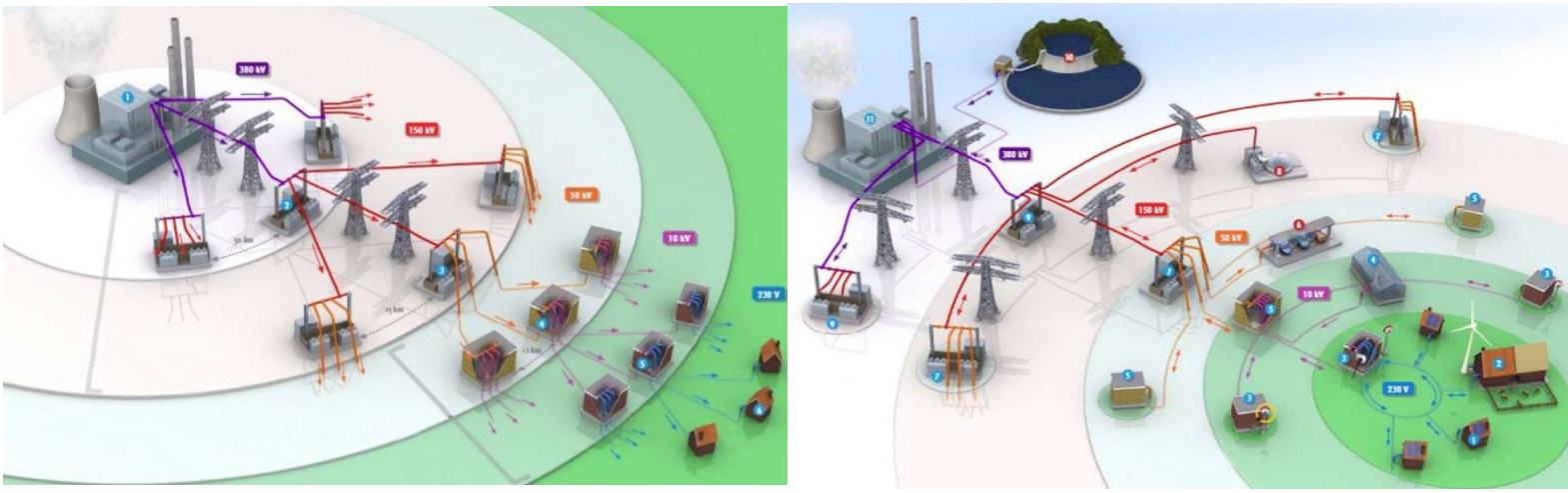


Figure 2: overview static (left) and intelligent grid (right). Obtained from (Xyngi, 2011)

power generation, transmission, distribution and consumption.

2.2.1 Power generation

Power plants come in different sizes and have various purposes; base load, intermediate and peak load. In the Netherlands approximately 70 power plants are currently in use, these were built between 1906 and 2011 (Figure 3 and Appendix I: Overview Dutch powerplants). The oldest power plant is owned by E.ON and resides in The Hague. This gas-fired power plant was built in 1906 and had a retrofit in 2007, where the old Rolls Royce turbines where replaced by new turbines (E-on, 2010). Almost half of the power plants are built before 1990 (44%), which means the systems were developed without modern IT knowledge. Engineers developed the systems from an engineering perspective. Because power plants are part of the critical infrastructure, it was common to design these plants with a focus on availability, safety and reliability (Stapelberg, 2008).

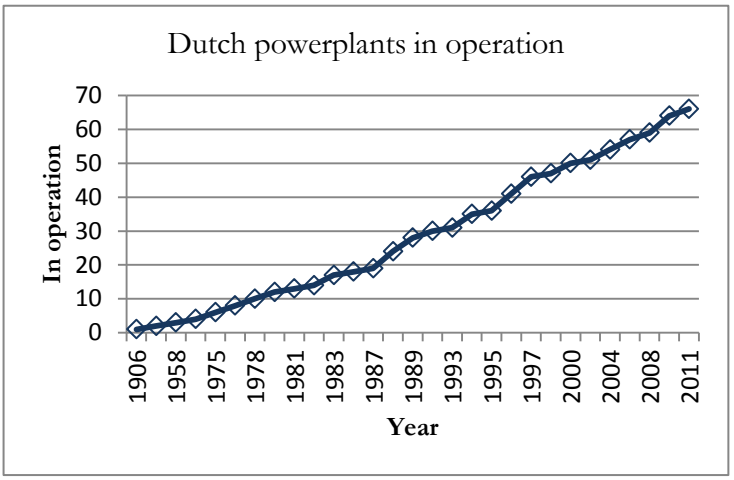


Figure 3: Dutch power plants in operation (based on Netbeheer NL and Wikipedia)

Power generation in an intelligent grid

Starting from the 1990's the TCP/IP protocols were introduced which implicated that power plants entered a new era. Systems which were normally isolated could now be connected with external networks, generating useful data and enabling new (remote) control functionalities. From a security perspective there is an issue: the control systems were not built with the requirement of communicating with other – external - networks. When connecting a control system to an external network, cyber security becomes vital. It is difficult to secure a system which was not designed to be secure; there is no security by design in the current control systems (ENISA, 2012).

2.2.2 Transmission and distribution

The Dutch transmission network transports electricity over long distances from the power plant to the distribution network. In total, the transmission network has a length of almost 10.000 km (Energie-Nederland; Netbeheer Nederland, 2011). It is composed of power lines and substations. Transmission substations are the first step in lowering the voltage. In these substations transformers, switchgear, measurement instruments and communications are housed (CEN/CENELEC/ETSI Joint Working Group, 2011). The transformers change the voltage levels. Switchgears are used to connect and disconnect parts of the infrastructure

(for example for safety or maintenance). Measurement collects data for monitoring and controlling. With the communication gear, the control center can operate the switches remotely.

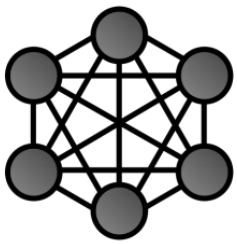


Figure 4: mesh network

The transmission network in the Netherlands is classified as a mesh network, depicted abstractly in Figure 4 (Tennet, 2010). A mesh network has redundancy built into it: there are more ways to reach a certain point. Due to this redundancy the system operator can provide electricity to places even when a power line or unit breaks down. The redundancy functionality also provides some difficulties. First, when power is fed into the grid, it flows along the path with the least resistance. The intelligent grid offers more insight in power flows because of the increased information flows. Second, it is possible that power differs in quality. Only a certain deviation is possible before equipment's failure is imminent. To prevent equipment from failing, clients expect to receive power with the correct voltage, current and frequency (Vaessen, 2012). Interestingly enough, according to DNV-KEMA the equipment used for the intelligent grid is highly sensitive to deviation in Power Quality. Peter Vaessen also argues the new equipment is likely to cause degrading power quality itself: "more and more (power) electronic equipment is connected to the grid with high frequency power switching characteristics that are likely to produce more distortion." (Vaessen P. , 2012, p. 1). The evolving grid with more intelligent systems could, by means of the previous example, also harm the reliability of the grid infrastructure. As a result of the varying power quality, mostly physical vulnerabilities are increasing. Physical vulnerabilities are mostly out of our scope, but it is relevant to keep in mind because the transition of the grid increases power quality distorting equipment.

2.2.3 Consumption

Consumers consist of four types: industrial, commercial and homes. The difference for these customers lies in the voltage (Bean & McGrory, 2010). 20kW for home connections, 20-200kW for commercial and more than 200kW for industrial customers.

The most important physical asset for the consumer is the power meter. It was common practice for electricity companies, as still is for a majority of home owners today, to manually obtain all metering data from the customers. In the intelligent grid a so called smart meter consists of a metering system and a gateway (National Institute of Standards and Technology, 2011). Where the meter registers the usage and the gateway is responsible for the communications. The gateway is the enabler of all kinds of possible applications (NIST, 2009), (Delloite, 2009) for example:

- *Remote smart load control*: Reduce consumption and increase network reliability during critical demand periods
- *Better monitoring and control:* this enables distributed generation and Electric Vehicle storage and charging;
- *In-home display*: customers will have more insight in their usage.
- *Integrating meters with building management systems*: this would allow consumers to switch on and off appliances via the in-home display or via internet;
- *Auditing or logging for security purposes*: because more sensors will be present, more data is gathered. The data can be used to track malicious behavior.

It is often discussed that end-user products are the most difficult to secure (Center for Strategic and International Studies, 2011). Partly because the amount of end-users is large, consequently many hours can be spend on exploring the device. Secondly, security awareness is lacking. While awareness of security threats increases over the last years, in general people underestimate their chance of exposure and believe they are dealing with the threats efficiently (Bauer & Van Eeten, 2009). In addition: it is not easy to convince the public of the advantages of the equipment, especially when the advantage for customers are mostly indirectly noticeable (i.e. easier administration, more transparency).

Vendors have to make the trade-off between usability and security. Where the security might affect usability directly. When consumers have too much difficulty using the appliance because it had to be secure, the vendor can expect bad sales. This is one reason why consumer awareness is becoming an increasingly more important aspect. When vendors make the trade-off and they deliberately opt for more usability and less security, the consumer should be informed and made aware.

2.3 Conclusion

In a relatively short time span from 1990 until now, new capabilities are implemented or due to be implemented. The capabilities are enabled by IT systems and implemented to increase overall capabilities, increase access and process data better and faster.

The legacy equipment in the grid has a long lifetime, which results in most systems having to be adapted to fit the new capabilities. This could regard adapting equipment rather than purchasing new equipment, which is most of time not economically viable. The problem with the industrial systems is their relative fragility, due to the real time supply and demand: reliability and availability are important factors in industrial infrastructure.

In short: the increased connectivity opens the industrial control world to the internet. Security issues that arise from this connectivity were unknown before and the systems were not designed for these capabilities. Where possible, the IT security specialist have to work in cooperation with the engineers to enable secure operations from a cyber-perspective, while ensuring availability and reliability.

Chapter 3. Control systems and IT systems

Goal of this chapter Discuss the various aspects of control systems and IT systems in the electrical grid

Relation to previous chapters More specific analysis based on the identified systems of the previous paragraph

Process engineers were able to save money and time by automating their processes. With computerized systems, the production and flexibility increased. However, control systems were originally not meant to share information with external networks and were not designed to be intelligent. Therefore, control systems did not have and did not need the processing power or bandwidth to be able to run anti-virus software or event logging (EPRI, 2011). In this chapter the integration of IT systems into control systems is described. The level of detail in this chapter is high because it enables finding conflicting requirements and values between information technology and operational technology.

3.1 History of Control Systems

Without diving too deep into historical aspects of control systems, a short introduction could improve understanding of how control systems currently operate. James Beniger wrote *The Control Revolution* in 1986. He describes how control systems evolved and came into place during the past millions of years, this is depicted in Figure 5.

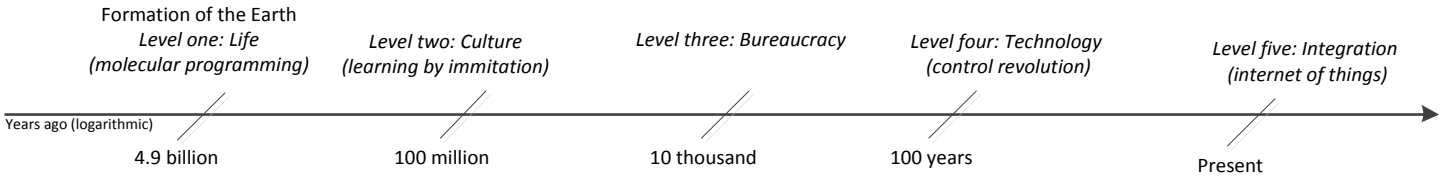


Figure 5: Control system timeline. Obtained from (Beniger, 1986) and adjusted.

He drew a timeline projecting the different stages prior to the control revolution. In phase two, ca. 1900 – 1970, the basis of control systems as we know them today was laid. During these decades, the infrastructures continued to expand and became increasingly in public hands with centralized management (Bruijne, 2006). The different levels of Beiniger indicate a certain maturity level. Transposing theory of the history of control systems to the control systems: if the technology and the people working on these systems can successfully managed, then the next phase of control systems can be reached: integration of things.

Practically, successfully managed means that the people working on the different systems work together on improving the system. This is exactly what we intend to identify in this research: what are the differences in perspective on security between IT experts and engineers?

3.2 Current Control Systems

The definition of a (industrial) control system according to the European Network and Information Security Agency is as follows:

> *"Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. These systems are responsible for monitoring and controlling a variety of processes and operations. ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the-shelf software. All this has led to cost reductions, ease of use and enabled the remote control and monitoring from various locations."* (ENISA, 2011, p. 1)

An industrial control system can be divided into three domains: the SCADA domain, the control domain and the instrumentation domain. A fourth domain consists of system modeling, where forecasting scheduling and load management is part of (Centre for Development of Advanced Computing, 2012). System modeling is not in the scope of the research because it does predominantly influence the control systems indirectly. We discuss the three domains in descending size: SCADA domain, control domain and instrumentation. In literature, these domain are often referred to as levels.

> Level 2: the SCADA domain - consists of: the workstations and panels located in the Main Control Room, the Remote Shutdown Station and the Man-Machine Interface (MMI).
>
> Level 1: the control domain - encompasses information and control systems to perform generator protection, generator control, surveillance and limitation functions, safety and process automation.
>
> Level 0: the instrumentation domain consists of sensors, switchgears which supply measured data for control, surveillance and protection instruments.

3.2.1. SCADA domain

Supervisory control and data acquisition (SCADA) systems are providing utility companies with knowledge, information and capabilities of the primary processes. These systems in the

grid are used for various purposes as monitoring power flow, monitoring power line voltage, circuit breaker status and controlling individual sections of the power grid. SCADA systems retrieve data from remote locations in order to assist operators in monitoring and controlling remote assets and processes in real time (Fernandez & Fernandez, 2005). Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions (National Institute of Standards and Technology, 2011).Presenting the data in an organized manner is one of the key features of the system. System operators base their decision on the data; therefore it is a critical component. The SCADA domain can be divided into three layers

1. SCADA client: this enables man-machine interaction. The Human Machine Interface, graphics editor and alarms & events display are components of the client side (Daneels & Salter, 1999)
2. SCADA server: the server processes the data of control activities. It comprises a real-time database, alarm & event database and reports database. Fault tolerance is also handled in the SCADA server. Fault tolerance entails for example backup servers (Giani, Karsai, Roosta, Shah, Sinopoli, & Wiley, 2008)
3. SCADA communications: the communications layer is used to connect the SCADA components together. The International Electrotechnical Commission composed a set of standards (IEC 60870-5) for communication in electrical engineering and power system automation applications. Examples of communications used are fiber optic, satellite, internet and GPRS. Internet protocols made it easier for applying standard presentation in web browsers for SCADA purposes. Legacy SCADA systems used proprietary protocols as profibus and modbus. To enable the capabilities discussed earlier, the legacy systems and protocols are converted to use TCP/IP protocol. (Giani, Karsai, Roosta, Shah, Sinopoli, & Wiley, 2008)

3.2.2 Control domain

The control domain covers the control components. It consists of several devices, depending on the situation. Three different devices can be found in this domain: the programmable logic controller (PLC), the remote terminal unit (RTU) and the intelligent electronic device (IED). We shortly describe these devices. Because the PLC, RTU and IED all fall in the control system family, their features are overall very similar. A PLC and RTU differs from one another on communication. A RTU is specially designed for

communication with other stations, were PLC are more suitable for local control (the plant floor, programmable applications). The RTUs are designed for wide area SCADA systems en remote sites (Semaphore, 2012). For example: a PLC is used in an assembly line in a factory and a RTU is used to monitor a remote valve of a lock.

Programmable Logic Controllers (PLC)

PLCs are used in SCADA systems as control components of an overall hierarchical system to provide local management of processes through feedback control (National Institute of Standards and Technology, 2011). Figure 6 depicts an abstract representation of how a SCADA and PLC system relate to each other. A PLC is a special form of microprocessor-based controller that uses programmable memory to store instructions. The term indicates that the programming is used for logic and switching operations: when A or B occurs, C is switched on (Bolton, 2009). A and B are the input devices, for example sensors, and C is an output device, for example a vale or a motor.

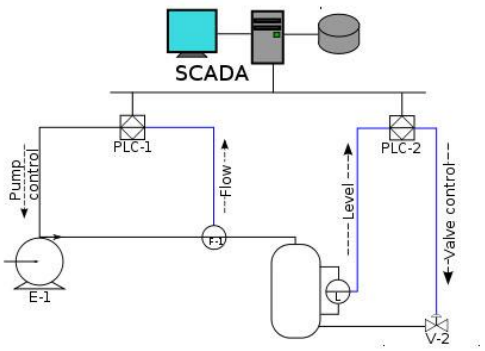


Figure 6: SCADA and PLC relation. Obtained from Wikipedia

Several functions and features have changed between the introduction of the PLC and what is expected of PLC today. A few changes:

- In the beginning of the 1990's, microprocessors started to be implemented in PLC's. The microprocessors added the intelligence to the PLC.
- The software changed from custom operating systems to standard operating systems as Windows or Linux.
- Old PLC systems, before microprocessors were installed, were inadequate to store data and produce a graphical representation. The renewed PLC's could gather, store and transfer data which could be used for decision making.

William Bolton (2009) argues in his book 'Programmable Logic Controllers' that the PLC's are designed to be easily operated by engineers, not needing much knowledge of computers or computing languages. In that sense it does not differ so much from a regular computer, except a computer is optimized for calculations and displaying where a PLC is optimized for control tasks and industrial environment (Bolton, 2009). It is notable that Bolton does not once speak about security in his 300-page book.

Remote Terminal Unit (RTU)

The remote terminal unit is a collection of remote station equipment of a SCADA system

(Smith & Wayne, 1993). This equipment comprises all control and associated telemetry equipment at the station. The remote terminal unit should provide an operator at a different location with enough information to determine the status ranging from individual equipment to an entire substation. The operator could consequently take actions without being physically present (Heng, 1996).

A RTU and PLC both being control systems, yet have different specifications. A comparison is depicted in Figure 7 between a high performance RTU, meaning an expensive high range RTU, with a PLC. When looking at memory and remote capabilities. This figure confirms for example the proposition that RTUs are more suitable for remote locations and PLCs more for local processes.

Feature	High Performance RTU	PLC
Temperature	-40° to +70° C	-20° to +60° C
CPU word size – clock rate	32 bit – 200 MHz	16/32 bit - 50-100 MHz
RAM/Total memory	4 MB/32 MB	32 KB/256 KB
On-board serial/Ethernet ports	2/2/other options	Typically 1 of each
Remote application upload	Yes	No
Remote software diagnostics	Yes	No
Remote firmware download	Yes	No
Encryption support	Yes	No
Integrated radio support	Yes	No
Store and forward standard feature	Yes	No
Report by exception mode	Yes	No
Integrated power supply options with battery charging	Yes	No

Figure 7: PLC/RTU comparison. Obtained from (Motorola, 2007)

Intelligent Electronic Device (IED)

The first Intelligent Electronic Devices (IEDs) with microcomputer technology were introduced in the early 1980s (Sezi, 1999). The IED falls in the same category of controllers as the RTUs and PLCs. While RTU focusses more on control in a large area, PLCs more on the local processes, the IEDs are focused on protection. Not cyber protection, but protection of physical systems. The most common found functions in an IED are enumerated below (Apostolov, 2002):

- *Protection*: device protection is a key task of IEDs: thermal overload, circuit breaker failure protection, broken conductor detection and so on;
- *Control*: circuit breaker control; programmable scheme;
- *Measurements*: Comprehensive measurement values;
- *Post Fault Analysis*: Fault location, event and fault records, disturbance records;
- *Monitoring*: Trip circuit supervision, breaker state monitoring, voltage transformer supervision;

The IEDS facilitate both operational and non-operational data. Operational data is data relevant for operational purposes: data such as voltages, circuit breakers status and switch positions (McDonald, 2012). Non-operational data regards related to reporting and logging of events. This is data which is not critical for SCADA operators when operating and monitoring the power system. The critical data, along with the real time monitoring, ensures

that operators can control and protect the grid. Cyber security regarding the measurements, monitoring and control for these devices is important because faults can directly lead to damage in the physical systems.

3.2.3 Instrumentation domain

The third domain is relatively straight forward; it comprises the instrumentation in the field. The most important instruments are: level sensors, circuit breakers, meters, flow sensors and temperature sensors. These are called the monitoring instruments, which monitor pressure, flow, temperature, density etcetera. The second group of instrumentation is called the controlling instruments. Equipment as valves and switches belong to the controlling instruments. The monitoring instrumentation provide operators real-time data on the health of the grid. The instrumentation domain is mostly out of the scope of our research.

3.3 IT networks

IT networks enable communication between systems, equipment and networks. For the electrical grid, IT systems manage and support the activities which are vital to the grid. The term 'information technology' first appeared in 1958. Levit and Wishler wrote an article in the Harvard Business Review about the storage, retrievement and communication of information. Saying: "the new technology does not yet have a single established name. We shall call it information technology" (Leavitt & Whisler, 1958, p. 15).

In a technical report on grid-penetration testing, Ernst and Young provided a visual overview of the IT networks in the grid. We explain the IT systems based on the overview in Figure 8.

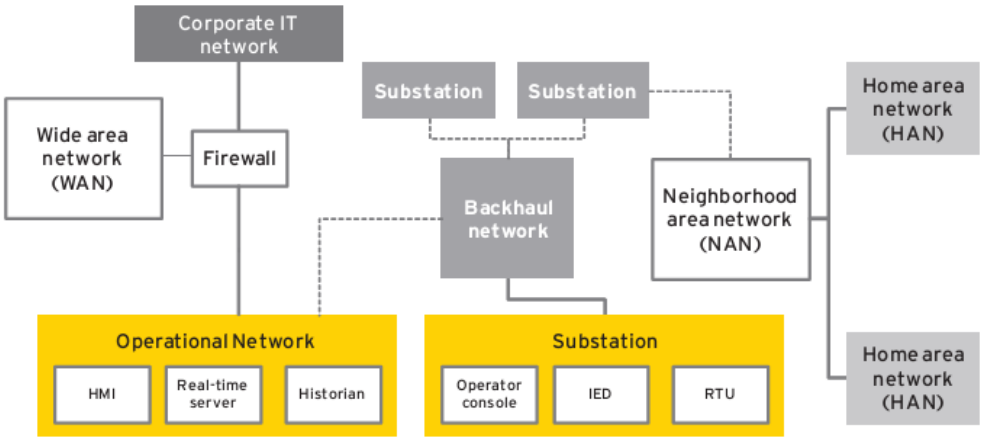


Figure 8: overview grid IT systems

The network can be divided into six parts. In yellow the operational and mechanical part of the network is indicated. Here, the equipment is located which was discussed in the previous paragraph (RTU, PLC, IED). The 'Wide Area Network', 'Neighborhood Area Network' and 'Home Area Network' lie outside the scope of this research, we only discuss it briefly to increase understanding of the whole infrastructure.

Backhaul network

As can be derived from Figure 8, the backhaul network provides two way communications between the substations and the operational network. Traditionally only proprietary SCADA protocols were used for communication between different substations. Currently this is evolving to TCP/IP protocols. The evolution in the systems led to SCADA systems being networked and accessed via the internet. Using the open/standard protocols has the advantage that the security possibilities are developed. This assumes that the latest patches and updates are installed. Unfortunately, patch management is a part where control systems have problems (National Institute of Standards and Technology, 2011).

Operational network

The operational network is where substation-operations are managed. Communication between the operational network and the field devices is required for, for instance, maintenance (Sorebo & Echols, 2011). The key function of the operational network is the centralized monitoring and controlling the field devices. Data originating from field devices is pushed to the network, via the backhaul network, to the central location. To a large extend, the field devices are self-regulating. When anomalies happen, the operators can make adjustments remotely based on the data which is fed in. Hereby preserving the health of the network. This part of the network is considered to be a high risk environment, a quote from the Ernst and Young reports delineates this projection:

> *"an attacker gaining the ability to issue unauthorized control instructions could have complete control of the environment. Obtaining this level of control requires an understanding of how instructions are issued and the ability to bypass any authentication or authorization controls in place. This can be done passively by analyzing control-based traffic for evidence of encryption, authentication sequences and authorization tokens. Active techniques would involve communicating with the device using specially crafted requests or other traffic to examine the device's response.* (Ernst & Young, 2011, p. 14)

Tsang, University of Berkley, argues that this part of the network is known to be vulnerable for Denial of Service (DoS) attacks (Tsang, 2009). During a Denial of Service attack a high amount of traffic is generated which lead to server overload and thus unavailability.

Corporate network

The corporate network is used by employees for everyday things like browsing the internet, emailing and running business software. The operational network and the corporate network can be interconnected. The Business IT systems, in many cases, constantly exchange data with the operational network relating production levels, sales and billing (Ernst & Young, 2011). Also, it is used the other way around: the operational network uses information from the corporate network (e.g. administrative information). Interesting quote from the EY report:

> *[..]ICS administrators/support engineers may create operational network access for themselves from the corporate network to create redundant access paths without fully considering the security implications.* (Ernst & Young, 2011, p. 12).

The finding implies that direct access to the operational network from the corporate network is possible. The corporate network is connected to the internet. Someone with connection to the internet and with the right knowledge can access the operational network via the corporate network. Some additional findings in the Ernst & Young rapport are indicating more vulnerabilities and difficulties:

- With few exceptions, IT network traffic is designated another TPC port for communication. Which leads to easily singling out the ICS communication;
- Corporate workstations often have remote access/remote desktop. The corporate network can be accessed from outside. Possibly connecting to the operational network;
- External market systems are connected with the corporate network and the operational network. Because of the shared databases, this is especially interesting from a integrity point of view.

From the latter, it becomes clear that the operational network is more connected with the corporate network. Besides the useful exchange of information, it also brings vulnerabilities.

Wide Area Network (WAN)

Within the electric grid, the power utilities are connecting the control system-

network-environment through wide area networks. It is used to obtain real-time data as well as historical data. Second the WAN's facilitate control with external utilities.

Neighborhood area networks (NAN)

The Neighborhood Area Networks are implemented to support the automated meter reading (AMR) and other services. After AMR, the next step in grid evolution is the Automated Metering Infrastructure (AMI), where the NAN also plays a big role. The AMI is a synonym for the intelligent grid and capable of two communications.

Home Area Network (HAN) or Home local Area Networks (LAN)

Home Area Network implicate the end-user products. This network is present in the home of a client (National Energy Technology Laboratory, 2008). Functions and capabilities of the HAN may include:

- In-home displays so the consumer always knows how much energy is being used and what it is costing;
- Responsiveness to price signals based on consumer-entered preferences
- Automated control of loads (necessary for decentralized electricity production).

Home Area Networks are directly connected to end-user; associated systems need to be completely fool-proof, and for this purpose security will play a key role. (ENISA, 2012)

In the chapter one several news articles concerning unauthorized access and breaches summed up. From this could be noted that the preferred and easy method to enter the operational network is via the cooperate network. The security breach late September 2012 at Telvent, a company which builds Industrial Control Systems for the smart grid, also was attacked via the cooperate network (Wired, 2012).

3.4 Comparison of IT and control systems

In the latter two paragraphs we discussed the control system and the IT system from a separate point of view. In reality the systems have different specifications but a high interconnectivity. The maturity of cyber security is very different between IT systems and control systems. A main reason for the differences in cyber security maturity is the difference in focus between IT and control systems. Control systems have focused on equipment safety, reliability and efficiency, while cyber security was not of importance. With

the increased connectivity this is no longer true. With the convergence of IT into control systems, expertise is required from both business IT and industrial control systems. Control systems running on top of typical business IT platforms are an integral part of the industrial infrastructure today (Honeywell, 2012). The industrial IT of control systems have different requirements than regular business IT systems. The difference between business IT and industrial IT pose a real challenge.

Integration of systems

Creating an intelligent grid comes down to making control systems intelligent. Due to the unique nature of the control systems, implementing IT into control systems should not be an off-the-shelve repetition. Performance degradation resulting in compromised availability and reliability is a real concern (Industrial Defender, 2012). The scenario that has been unfolding can be summarized as follows: control systems had little resemblance to IT systems, due to the fact control systems were isolated and running on proprietary control protocols with specialized hardware and software. Internet Protocol devices are now replacing and integrating the proprietary assets. This leads to a higher risk of cyber vulnerabilities and attacks. The evolution in control systems has as consequence that control systems are starting to resemble IT systems (National Institute of Standards and Technology, 2011). Remote access capabilities, data sharing and connectivity are achieved but at the same time, because of the reduced isolation, the need to secure control systems increases. The difficulty: security solutions focused on typical IT systems cannot be translated one-on-one for control system security. New security solutions have to be tailored to fit in the control system environment (National Institute of Standards and Technology, 2011).

Technical differences

The National Institute of Standards and Technology has written several papers on IT in control systems and securing these interconnected control systems. The *guide to Industrial Control Systems Security* is most valuable for this research. It describes a majority of the issues regarding integration. In addition to the guide, Macaulay and Singer have commented on the statements of the NIST, providing information from a practitioners perspective, which are also incorporated in the analysis.

Below, a comparison is made between the requirements of control systems and regular business IT systems. The most significant differences between control systems and IT are as follows:

Availability

Control systems have two inherent features when it comes to availability: a control

system cannot be rebooted easily without affecting the production (1) and unexpected maintenance of the control system is not acceptable(2). Therefor maintenance should be planned ahead in time. These two features form the basis of a significant difference in perspective on availability. Regular IT system are relatively easy to maintain. Control systems are, almost without exception, used in live production environments. A big contradiction with regular business IT systems.

Change/Patch Management

Change management is related to updating the software and hardware of the systems. Obviously, this can affect availability to a large extent. Due to the prudence that control system engineers have with updating, the software systems are often unpatched and remain unpatched (Ginter, 2011). This inherently leads to vulnerabilities from a security perspective. For regular IT systems, patches are regularly done (for example each week). This works different for control systems because of the reasons mentioned in the availability part: updates must be tested thoroughly by the vendor and control systems cannot be taken offline without good planning. Maybe one of the most interesting observations comes from Macaulay and Singer, who argue that "ICS older versions of operating systems are no longer supported by the vendor. Consequently, available patches may not be applicable" (Macaulay & Singer, 2011, p. 45). A process control manager at a US power plant put the problem in a few words: "SCADA systems don't play well with Microsoft patches" (Waller, 2012, p. 1). Implicating that updating the Windows Operating System which runs the SCADA system can cause downtime.

According to SCADA expert Eric Byres, "only about 10 to 20 percent of organizations today actually install patches that their SCADA vendors are releasing," (Dark Reading, 2013, p. 1). Dale Peterson, IT expert with SCADA experience, argues that major players in the ICS world patch on a quarterly basis, mainly on servers and workstations," (Dark Reading, 2013). Both these practical observations seem to indicate that there are difficulties with the patch management.

Component Lifetime

The difference in component lifetime is best illustrated by Moore's law. The law states that the amount of transistors on a computer chip doubles every 18 months (Moore, 1965). Moore's law, dating from the 1970's, has not yet been proven to be incorrect. Which of course does not mean it is guaranteed to be correct in the future, but it gives a good indication. Moore is arguing the computer technology is changing very rapidly. This is in contrast with control systems, where regular IT systems are relatively easy to replace, control systems are not. The underlying reason

has two aspects. First, the physical systems took years to develop and are quite expensive in comparison with IT systems (1). The component lifetime for control systems in the grid various from 15 to 50 years (2). This is in contrast with IT systems which have a component lifetime from somewhere between 3 to 5 years.

Managed Support

Regarding support of vendors, the NIST identified a significant difference between regular IT systems and control systems. NIST states that IT vendors usually will support a wider range of problems (e.g. when the IT system is interconnected with other systems, the IT vendor is typically also capable of handling the interconnectivity). While the control systems vendors are often limited in their support. As NIST puts it: "*which [the Vendor] may not have a diversified and interoperable support solution from another vendor.*" (National Institute of Standards and Technology, 2011). Control systems were historically only relying on their own software and hardware systems. This could explain the limited support of ICS vendors.

Risk Management

IT expert typically want to ensure data confidentiality and integrity. While control systems engineers find safety, fault tolerance and regulatory compliance important. We can assume that this will influence the way that risk management is handled. To what extend the different perspectives on risk management will lead to a challenge in securing the cooperation between IT systems and control system remains the question.

Security architecture & physical interaction

The security architectures between IT and control systems traditionally are different from each other. Because control systems have edge clients (PLC, operator station, RTU), physical security plays a significant role. Often, IT systems are labeled as 'not having a physical interaction' with their environment. Thereby being an opposite of control systems. However, IT systems can have very complex interactions that can 'manifest in physical events'. IT security usually stops at the firewalls of the corporate LAN, while a large part of operational technology security exists in the field. Grid operators discovered that the regular IT security is not directly applicable to the control systems because of the different requirements (Robinson, 2011).

Operating software & software tools

The operating software in control systems is currently often Windows based. Varying from the oldest to the newest Windows systems. In addition to the Windows operating system, a software tool is installed. These tools can be used to

analyze, visualize, control the systems. There are currently 58 different leading software tools for SCADA systems (SCADA products, 2010). Typical IT security solutions as virus scanners, password protection, encryption capability and error logging may not be possible on the computers of SCADA systems. First, the computer may not have the computing power or the administrator right to be able to install it. Second, when anti-virus software on a control systems makes a mistake and mis-diagnose legitimate traffic of software as malware, those anti-virus systems could shut down the very control systems they were supposed to protect. (Waterfall Security, 2012)

3.5 Conclusions

As an analogy for a successful integration of IT systems in operational technology, we can look at evolution of control systems drafted by James Beninger. In order to successfully proceed to the next step in the control systems domain - the integration of things - cooperation between the IT and OT domains is necessary.

In the scope of this research three layers in the control systems domain are analyzed: the SCADA, control and instrumentation layer. These three layers together represent the operational network. The SCADA system processes gathered data and sends operational commands to the local controllers in the control domain; the PLC's and RTU's. These control systems adjust or maintain processes by managing the instrumentation layer. In this layer the actual data gathering takes place with sensor equipment. Besides these monitoring instruments, also controlling instruments belong to this domain. This entitles mechanical instruments as valves and pumps.

New business and management requirements and technological advancements in the industry are driving factors behind the IT integration in control systems. Making the control systems more intelligent en more connected. In many cases, the operational network and the corporate network (used for email, internet and so on) are increasingly connected. Inherently to the connectivity that the corporate network has with the internet, vulnerabilities via the corporate network to the operational network are likely to increase. Boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems.

The differences between 'business IT' and 'industrial IT' are significant. Differences in availability, patch management, architecture, operating systems and component lifetime make it difficult for IT specialists to secure control systems. While the control systems are fitted with IT systems, securing these systems cannot be done with standard business IT security practices. Additional difficulties can be expected by the simultaneous implementation of the systems and the development of the security practices.

Goal of this chapter

Relation to previous chapters

Chapter 4. Paradigms

Identify the ruling paradigms and the research literature on conflicting values

Continue on the differences found, from a human perspective

The IT specialist and the control system engineer are bound to work together. Especially when it comes to security, cooperation is of importance. IT related issues can impact the operations. Vise versa, the way that control systems are designed can frustrate IT security. In other words: the dependency is high (Johnsson, 2012).

The European Union, via the European Network and Information Security Agency (ENISA), stated they perceive a large difference in perspective between ICS engineers and ICT specialists. This quote, obtained from a paper on recommendations for Member States on protecting ICS, gives the EU viewpoint:

> *"The ICS world is different from classic ICT systems and there are challenges that force them to adapt existing (or even create new) solutions and services. A fundamental difference is in the very basic guiding principles. The ruling security paradigm in classic ICT systems is based on the CIA model (Confidentiality, Integrity, Availability), but in the ICS environment what rules is the SRA model (Safety, Reliability, Availability)."* (ENISA, 2011, p. 15)

ENISA identifies a fundamental difference in guiding principles. Presumably referring to a difference in principles the both groups hold on to. Security is likely to be directly affected and possibly compromised due to the fact that the IT specialist and the Engineer have no shared perspective and/or have no shared perspective on security.

In this chapter an analysis is done on what is written about the statement of the ENISA. A literature research has been done on the values and perspectives of the IT specialist and the engineer. This is done by analyzing what perspective is used within the groups when designing, maintain and operate a system. The sub question in this chapter reads:

> *Is there a fundamental difference in design paradigm between an IT specialist and ICS engineers and how does this affect their perspectives on security and risks?*

The focus lays on what kind of role the paradigms plays in the transition from isolated control systems to connected networked control systems.

What is a paradigm?

We approach the term paradigm as a combination of the explanation of the Oxford dictionary (Oxford Dictionaries, 2012) and the Farlex Dictionary (Farlex Dictionary, 2012): a *set of assumptions, concepts, values, and practices – i.e. a pattern - that constitutes a way of viewing reality for the community that shares them.* It should be noted that a paradigm and especially the applicability of a paradigm is subjective. For example: when someone argues a certain paradigm is applicable, it is an opinion. Most of the times you can find people opposing this opinion. Therefore it must be delineated that we are analyzing if there is a ruling paradigm, or various paradigms, which can account for a majority of the professionals in question.

Time perspective

When a systems is created, software or mechanical, a design cycle will be used. Though there are many variations on the cycle, an average technical system undergoes a DBOM cycle: Design, Build, Operate and Maintain (Brady, Davies, & Gann, 2005). Roughly, two phases can be separated here. The first phase consists of design and build. The second phase, holds the operating and maintenance steps.

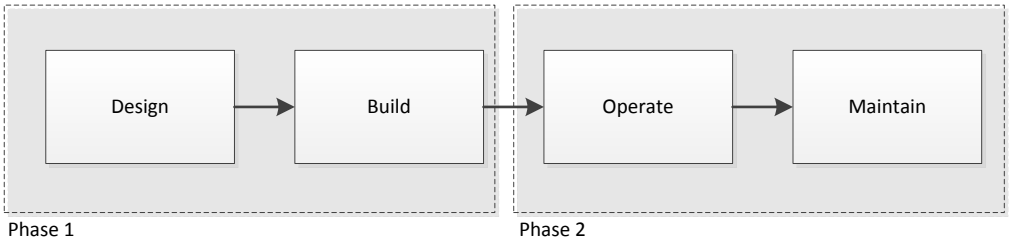


Figure 9: DBOM cycle

In this chapter, we analyze the two perspectives that were identified by ENISA: the IT and OT perspectives. From a security perspective, as we identified earlier in this paper, security-by-design is often better than security implemented when the system is already operational. With Figure 9, we want to delineate that it is important to understand that our analysis of the perspective spreads out over the design phase (phase 1) as well as the operational phase (phase2). For a comprehensible comparison between perspectives, an understanding of the design cycle could assist.

4.1 Paradigm of the Information Technology specialist

The IT specialist as we know the profession today is relatively new. The profession emerged somewhere between 1970 and 1980, when TPC/IP protocol was invented and networking became possible. An open door: networking comes with vulnerabilities. When you connect everyone to everything, the potential of unauthorized access grows (World Economic Forum, 2012). We can assume that IT specialist always have been devised on the possibility

of remote control and remote access. When designing a system this plays an important role; security by design is a well-known term in IT context. The IT specialist in the grid sector could be regarded as a 'consultant' of connected information systems. They are monitoring the information flow of the entire system and -from a security perspective - monitoring where vulnerabilities are.

Popular topic: cyber security

Nowadays, cyber security is a popular topic. For many people, hackers and cyber criminals only speak to their imagination. A large part of the working population had to adapt to computers very rapidly. Only 20 years ago, a computer of current standards was barely imaginable. Interesting element is that a significant part of the control systems engineers are raised and educated without computers, while the IT profession is relatively new: most IT specialists are raised and educated with computer systems. Does the composition of the workforce in IT and ICS contribute to hypothetical difference in paradigm? This question is embedded into the questionnaire.

The IT specialist is analyzed in two steps. First, based on literature, a paradigm is constructed. Is there in fact a ruling paradigm and how did this come about? Second, the work environment is discussed: how does the environment (compliance and regulation) potentially contribute and interacts with the paradigm.

Security by obscurity

An often used security strategy in IT back in the days, from 1970 till approximately 2000, was security by obscurity (SBO) (ENISA, 2011). This perspective on security says that a system can be secure when the code is secret. Security by obscurity involves taking a measure that does not stop unauthorized access but merely conceals it (Microsoft, 2008). It is common sense these days that solely SBO is not enough to stop attackers. The possibilities for mapping vulnerabilities are just too widely available. Take for example Nmap (port scanning), Nessus (vulnerability and configuration assessment) and Nikto (web server scanning). These tools are easy to download and ready for use. As Dafydd Stuttard (2005) points out, security by obscurity is often to easily rejected and but certainly "can significantly mitigate the security threats facing the organization" (Stuttard, 2005, p. 10). Small 'protective' measures, for example: using non-standard ports, use hidden folders and install applications to non-default directories could contribute in keeping out malicious activity. While it seems that the general perspective on IT security is no longer based on security by obscurity, it could (and perhaps should) play a role in the security strategy.

The IT ruling paradigm

The majority of papers, presentations and articles regarding an IT paradigm refer to

something called the CIA triad. CIA stands for Confidentiality, Integrity and Availability. CIA triad is also referred to as the PIA triad – Privacy, Integrity and Availability -, due to the fact the abbreviation CIA was already taken by the Central Intelligence Agency. Privacy in the PIA triad was supposed to mean Confidentiality (Greenwald, 1998). Briefly transposing this triad to the grid: for grid systems, confidentiality is vital (1). Confidentiality is attained when information is protected from unauthorized disclosure (Flick & Morehouse, 2011). Virtually no person is untouched by a connection to the grid. It is a key requirement that the information and systems are only accessible by authorized entities. Subsequently, intentional or unintentional disclosure of data may not occur. This is in close relation to integrity of the information: it should be authentic, correctly reflecting the source and be complete without modification or additions (2) (Cleveland, 2008). Integrity is attained when information is protected from unauthorized modification (Flick & Morehouse, 2011). Availability is the last aspect of the triad. Availability is attained when the service provided by the grid company is protected from unauthorized interruptions. In other words: the information (and their systems) should be accessible by authorized entities whenever they request information (3).

Perimeter defense; conventional IT security

There is some criticism on the CIA security paradigm. Anno 2012, it is mentioned that the CIA triad became obsolete. Dr. Wulf, president of the National Academy of Engineering, gathered reasons which, according to him, shows the CIA triad failed in respect to security (Bhargava, Lilien, & Zhong, 2005). He argues that computer security made little progress between the 1970's and mid 1990's due to thinking in conventional defenses. During those years, security was considered as an information fortress (Blakley, 1996). The information fortress (perimeter defense) is a synonym of how security was handled:

- A wall as the security perimeter: a firewall;
- A guard and gates: access control, passwords;
- Fortress content: computer systems and confidential data;
- Threats: attacks by spies, saboteurs and Trojan horses (e.g. viruses and worms)

Wulf argues that this perspective let to minor progress being made in security. He gives several reasons why he finds perimeter defense never worked. The most important reasons: that perimeter defense is not able to defend against legitimate insiders and to prevent Denial-of-Service attacks (Bhargava, Lilien, & Zhong, 2005). Prof. Jahanian - university of Michigan - adds to the statement of Wulf, that perimeter defense cannot address (Bhargava, Lilien, & Zhong, 2005):

- Zero-day threats
- Internal misuse;

- On-site consultant and contractors:
- Partner extranet:
- Exposed VPN clients and open wireless environments.

What has been said by Wulf and Jananian is also expressed by Andrew Ginter. Ginter published in a paper on control systems security, in which he delineates threats according to his experience. He states: "Conventional defenses do little to protect against low-volume, targeted attacks" and "targeted, low-and-slow attacks are the new and pose a big risk" (Waterfall Security, 2012).

Defense in depth

Professor Bharaga from the Center for Information Assurance and Security, proposed in 2005 a new approach to address security (Bhargava, Lilien, & Zhong, 2005). Security for IT should move more from *Perimeter Defense* to *Pervasive Security,* also referred to as defense in depth (Lilien, Al-Alawneh, & Othmane, 2010). Important aspects from pervasive security are the security should be inherent, not add-on, and adapt and evolved methodology of the systems. The strategy belonging to defense in depth is illustrated in Figure 10. The focus in this strategy lies on securing the privileged identities, thus working the security from the inside out. It is ironical that exactly these privileged accounts for control systems have some troubles. The usage is difficult to monitor, the passwords are not often changed (or not at all changed) and the same privileged identity is used by different employees and even third parties (ICS-CERT, 2012). When we examine the defense in depth further, it is clear that with the inside out the most important aspect is to protect the privileged identity. This means protecting (ICS-CERT, 2012):

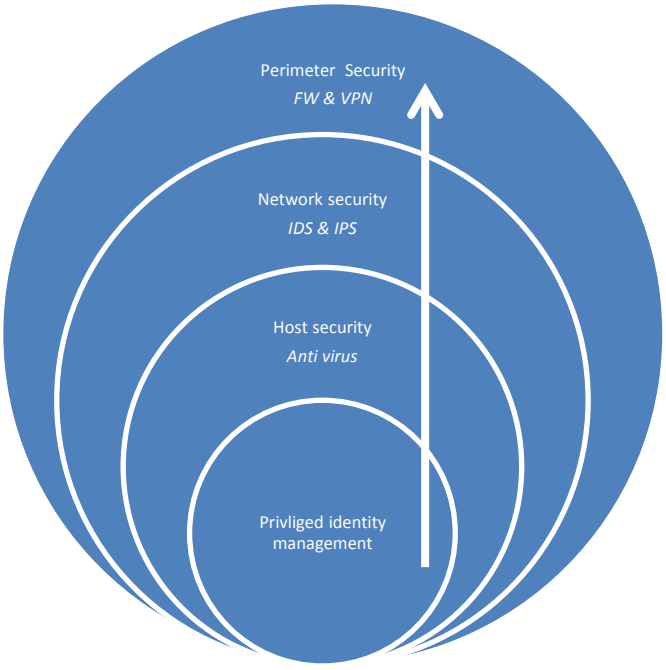


Figure 10: defense in depth, inside out approach

- Control Centre Applications;
- Operating systems (both servers and desktops)
- Control devices (RTUs, IEDs)
- Databases;
- Communication devices (e.g. routers and modems)
- Security devices (e.g. FWs, IDSs)

In essence, there are three protection layers. First, the host security, which uses anti-virus software to protect its systems. Second, the Network security, which uses an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS). An IDS and IPS are used for examining traffic, looking for attacks and detect malicious or unwanted traffic. The difference between an IDS and IPS is that an IPS is used for automatic enforcement of rules (preventive) and an IDS is used for security forensics (detective). The third layer, the perimeter security, is a protection via Firewalls and Virtual Private Lan.

Extension of the CIA triad

Defense in depth concerned a change in execution of defense, but still respecting the original CIA triad. Parker (Fighting Computer Crime: A New Framework for Protecting Information, 1998) argued, that the CIA triad should be extended because it had some limitations it was not addressing all aspects of cyber security. The triad is extended with three parts and consists of six parts in total. He extended his model with three elements: utility, authenticity and possession. Parker named his model the Parkerian Hexad. The six elements thus are (Parker, 1998):

1. Confidentiality: the limited observation and disclosure of knowledge;
2. Possession: the holding, control and ability to use information;
3. Integrity: the completeness, wholeness and readability of information and quality being unchanged from a previous state;
4. Authenticity: the validity, conformance and genuineness of information;
5. Availability: the usability of information for a purpose;
6. Utility: the usefulness of information for a purpose.

The extension of the triad seems to capture more aspects of information technology security. The article was published, but there is little proof that the Parkerian Hexad is actually used in the security literature.

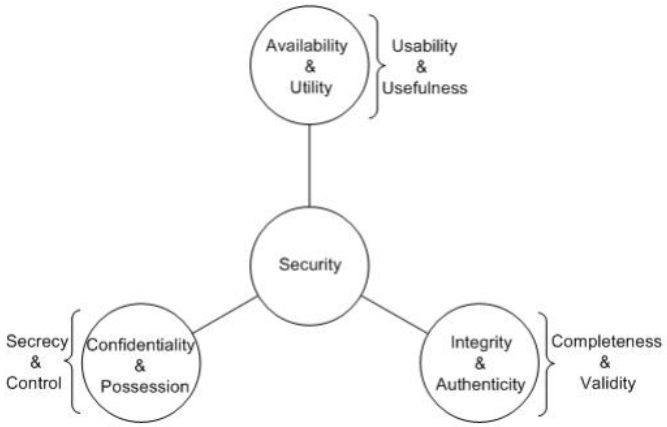


Figure 11: the Parkerian Hexad obtained from (Wu, 2009)

Concluding

While perimeter defense and defense in depth are different execution of the CIA triad, still the CIA values are the underlying factor. The Parkerian Hexad provided a more extensive

version of the Parkerian Hexad. Yet, in literature there is no reference to this model actually being used.

We can conclude that there has been some criticism on the CIA triad over the last decade. In this decade, a lot technical improvements on the IT equipment and IT infrastructure has been going one. Moore's law describes a significant growth in the amount of transistors on a computer chip, doubling every 18 months (see paragraph 3.3). The CIA triad was introduced in 1998, more than 15 years ago, which means the amount of transistors doubled approximately 10 times already. Still, it seems that CIA provides a solid foundation to review information security. This robust method remained valid although a lot of technical changes took place these last years.

4.2 Paradigm of the Control systems engineer

The purpose of control systems is to bring processes towards a desired state. The engineers working in this field often come from different beta related studies as electro-mechanical engineering, mechanical engineering and aerospace engineering. In the paragraph we analyze which requirements the engineers deem to find important during the design & build and the maintain & operate phases.

Control systems

Control system are computerized, therefore it can be argued why there would be a difference in perspective between the IT specialist and the Control engineer when they are both involved in designing computer systems. We can make a simple distinction between the IT specialist, who designs and views a system from an infrastructure and macro perspective, opposed to a control engineer who designs and views an isolated and dedicated part of the system. When designing only a fraction of the system, a possible consequence could be that less attention goes out to the securing the system (against outside threats). The idea that security is not a (primary) design objective for the engineer is strengthened by the fact that three other design objectives reoccur in the literature research: reliability, availability and safety. How these aspects fit in a potential paradigm is subject to discussion.

Safety, Reliability and Availability

The design paradigm of an engineer is subject to centuries of evolution. To illustrate: when old civilizations built their infrastructures, they probably had some idea of the desired end result. Perhaps a defined paradigm was not written down but only in the back of their minds safety and reliability played an important role. In the industrial area, from the 1750 - 1850 rapid changes in engineering took place: everything had to be bigger and better. How could this be achieved? By defining and optimizing objective parameters. According to William

Goble - author of Control systems safety evaluation and reliability – the parameters reliability, availability and safety have been developed most extensively over the last 60 years by the engineering community (Goble, 2010).

There seems to be an overall consensus of what the main targets and objectives are when designing a system. Still, it could be expected that the changing environment of control systems in the last two decades has some influence on the ruling paradigm. Take for example the expectation of connectivity and data analytics that clients and user have. For this purpose, the control systems have to be made intelligent. Then the systems are no longer isolated and engineers should keep cyber security in mind.

RAMS

In the search for the most important values for control engineers, the RAMS paradigm is frequently referred to as an important aspect. Reliability, Availability, Maintainability and Safety are the four aspect of the paradigm. Rudolph Stapelberg describes the meaning and implications of these terms in his book '*Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*' (2008). Some interesting connotations can be derived.

Reliability is separated into equipment reliability and system reliability. Where equipment reliability is considered to be less interesting due to the fact that "most equipment items have already been specified during the detail design" (Stapelberg, 2008, p. 16). System reliability is a concept with broader scope and reads: "the probability that a system will perform a specified function within prescribed limits, under given environmental conditions, for a specified time" (Stapelberg, 2008, p. 16). This is closely related to the second term, availability. Which indicates a time perspective. The definition reads: "the system's capability of being used over a period of time" (Stapelberg, 2008, p. 18). The definition is made practical by parameters such as mean time between failure, mean downtime and mean time to repair. Maintainability, the third aspect, is in close relation to the availability. By maintainability the probability that a failed system can be restored to an operational effective condition is meant. The last aspect of is safety. Safety reflects on the physical safety of the equipment. Exactly defined: "*Safety-critical systems are those that, on their own, achieve or maintain a safe state for equipment under their control.*" (Smith D. , 2011, p. 331)

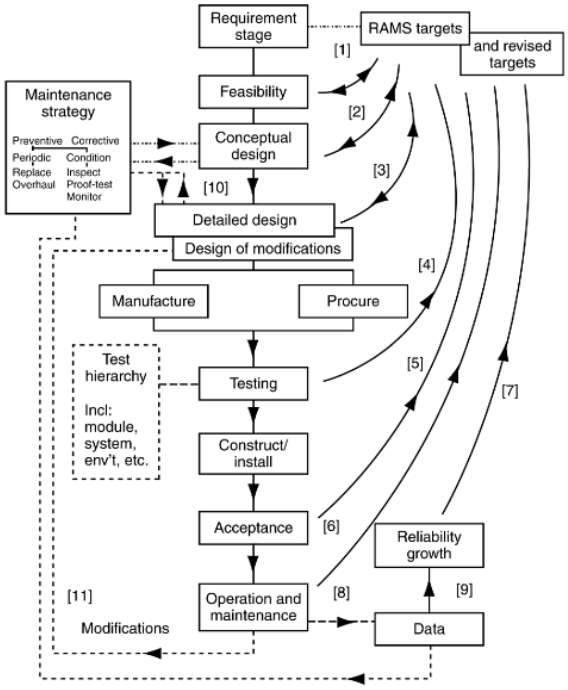


Figure 12: RAMS targets. Obtained from (Stapelberg, 2008)

Figure 12 shows how the RAMS aspects fall in the generic engineering design approach. We can make two observations which are directly related to security of the RAMS paradigm. First: security is not mentioned. Second: reliability aspects, and consequently also security aspects, are expected to be built in from the design.

Cyber security in engineering

Countless of companies are busy with securing control systems in the grid. Some key players in grid cyber security - as ABB, Industrial Defender and Waterfall security - have created and maintained successful companies which focus specifically on control system security. After several interview with employees at similar companies, it becomes clear that security is approached from an IT perspective. The respondents agreed that most of the employees have a background in engineering and later learned cyber security. Now they are aware of security, they seem to approach the security of control systems with more care. We must delineate that the people that understand how control systems operate and are aware of IT security issues are very valuable.

4.3 IT and OT comparison

Combining the knowledge gained from chapter two to chapter four, a comparison can be made between the IT and the OT perspective. The two perspectives are compared on the value found in the analysis of the different paradigms: Safety, Reliability, Availability, Confidentiality and Integrity. The values are disaggregated to several sub parameters based on information that is discussed, complemented with two other IT/OT comparison tables (Centre for Development of Advanced Computing, 2012), (Siemens, 2011).

Perspective from literature in regard with security		
Parameter	**IT Paradigm**	**OT paradigm**
1. Availability		
Remote access	Access anywhere from any remote location	Isolated assets without communication functionality
Communication	Large variety of communication protocols accepted.	Originally only SCADA communication between substations (often vendor specific).
Parameter	**IT Paradigm**	**OT paradigm**
2. Confidentiality		
Data storage	Data transfer over networks	Little data storage and often isolated
Parameter	**IT Paradigm**	**OT paradigm**

3. Integrity (IT)		
Authenticity	Use of passwords is common: often transmitted with encryption	Often no password protection (or standard passwords) to enable internal systems to communicate with each other
Change management	IT systems apply appropriate security policies and procedures. Often automated with server based tools.	Inability to immediately patch software, due to the need for thorough testing and scheduling, gives major security issues
Authorization	User based authorization	Location based authorization
Parameter	**IT Paradigm**	**OT paradigm**
4. Reliability (OT)		
Operating system (OS – secure by design	General and flexible OS. Security is done by design	OS were custom or of the shelf OS with little capabilities. Security not important.
Operating system - compatibility	OS compatible with the common security practices as virus scanners, error logging, encryption,	OS may not tolerate typical IT security practices. And/or could have no computing resources available for security
Lifetime	Typical IT components have a lifetime with a maximum of 5 years.	Due to high development and investment costs, primary OT has a lifetime of 15 to 50 years
Parameter	**IT Paradigm**	**OT paradigm**
5. Safety (OT)		
Human/physical safety	Little human safety issues due limited physical-cyber interaction	High interaction between physical and non-physical environment. Human safety is often high priority.
Parameter	**IT Paradigm**	**OT paradigm**
6. Maintainability (OT)		
Patches	With a regular system reboot updates can be installed or removed.	Patches can disturb the availability and reliability of the system, therefor must be thoroughly tested and screened.
Patches	Updates and patches for a system are obtained via an automatic procedure when connecting to the server	Updates and patches can often not easily be transferred to the system due to no their isolated nature. Updates possible via USB's.
Outrage	Rebooting is possible due to the nature of the system	Rebooting will affect the production process
Software	The operation system supports a variety of software from different vendors	Often only vendor specific software is accepted. Third party software is not always supported.
Hardware	Hardware can be changed with relative ease and is often standardized.	Hardware is expensive and often vendor specific.
Licenses	Third party solutions regarding security are supported	Third party solutions regarding security are not always allowed due to vendor license and service agreements (could lead to loss of service support by

		vendor)
Support	Support is widely available due to use of standards	Support via single vendor
Audits/penetration test	Use of modern methods and exploit kits possible	Testing has to be tuned to the system, modern methods inappropriate for testing ICS
Additional parameters	**IT Paradigm**	**OT paradigm**
7. Education	Information Technology study	Engineering study
8. System development	Security integral part of development	Usually security is not part of system development
9. Security awareness	Security awareness is high	Security awareness is increasing
10. Cultural values	Confidentiality, Integrity, Availability	Safety, Reliability, Availability

Tabel complemented with IT/OT comparison tables from (Centre for Development of Advanced Computing, 2012), (Siemens, 2011)

4.4 Conflicting perspectives

The latter paragraphs explained in detail where the possible conflicting interest between engineers and IT experts might be based on. The literature found to describe the two paradigms was unilateral, meaning it only described on specific point of view: engineering or information technology. In literature there are several relevant papers written regarding the conflicts between two or more subgroups. In this paragraph we discuss two papers in which similar conflicting perspectives are elaborated that are relevant for the research on the IT/OT differences.

4.4.1 Engineers versus operators

In 1999, Alexandera von Meier wrote an article about the role "that cognitive representation has on conflicting evaluations of new technology in the electric grid" (von Meier, 1999). She performed research on how operators and engineers evaluated certain advancements in technology from their own sub culture – perspective or paradigm if you will –. In her paper she argues that, instead of technological issues, cultural differences are often the reasons that there are difficulties implementing technological innovation.

As delineated in chapter three the next phase in control system technology requires the interaction of specialized knowledge workers, who work in separate parts of the organization but interact with each other to make the organization function and develop. To make this more tangible: the engineers who designed and built the control systems are now

challenged to retain availability and reliability, while undergoing changes in the functional requirements: no longer isolated but connected. This adds new vulnerabilities and threats to the control system domain. The IT specialists have to participate in securing the control systems: a close relation between the IT and OT employees is needed to enter the next phase of control systems.

The latter shows a discrepancy between what Von Meier found in her research and what the next step in control systems, and especially control system security, requires. When reflecting her research findings of the cultural difference between two subgroups, including the implications, to our findings regarding the IT/OT difference, perhaps some analogies can be found.

The analogies

Von Meier focusses on what she calls cultures, as decisive factor on conflicts in technological innovations. A group culture and group paradigm could be regarded as equivalent concepts. This is strengthened by the similarities in explanation of what a paradigm according to our explanation and the explanation of what a culture is in Von Meier's paper. Culture is defined:

> *"A cognitive phenomena - perceptions, experience, beliefs, and values - that are nurtured within occupational groups and guide behavior, judgment, and aesthetics. Culture thus characterizes ways of understanding how a technical system works, interpreting its purpose and goals, defining problems, generating solutions, and identifying general rules for action."* (von Meier, 1999, p. 102)

Suppose a technological innovation is available and ready for an organization to implement. It is believed that the two groups – in Von Meiers case: the operator and the engineer - have differences in interest. For example: the engineer finds the efficiency and reliability of the system of significant importance. While the operator predominately wants to ensure safety. These 'conflict of interest' were believed to be the root cause of failing to adopt new innovations. The most important conclusion of Von Meier was the following: "conflicting values and judgments can arise not only from conflicting interests, but from differences of interpretation" (von Meier, 1999, p. 101). This argument implicitly says that not only the criteria which an employee finds valuable cause disagreements between groups, but the way something is interpreted – which is inherent to a specific subgroup – is also an decisive factor. Further, two misunderstandings regarding the root cause of the disagreement between subgroups can be delineated:

1. *Evaluations of technology are determined only by facts.* If this statement is assumed to be true, there would be a relatively simple solution: educate both sub groups so the

'optimal' decisions can be made. Von Meier argues this is impossible due to the fact that important perceptual differences will always remain: "the root of the difference lies not in fact but in representation". This is inherent to their culture i.e. an engineer is adapted to analytical reasoning, while an operator uses mainly experience for their reasoning (von Meier, 1999, p. 109). Consequently, the two subgroups will have different opinions, even if they would agree on the facts.

2. *Cultural groups have inherently subjective or irrational biases.* Von Meier refutes this as a misunderstanding by an example: an opinion can be that operators are generally old-fashioned, afraid of the unknown, and prejudiced against computers. This would obstruct actual innovation to be implemented. She continues in her argument that cultural differences can also be understood in a constructive way that unifies the picture, while granting each perspective its own validity. Therefore implicating that they both are right in their own manner, this could be complementary and a good thing for the organization. (von Meier, 1999)

Implication on IT/OT subgroups

We see various similarities between our comparison and the comparison of Von Meier: the perspectives contradict between two groups, the type of conflicts are the similar and the possible root causes and the above misunderstandings could also be translated to IT/OT groups. One of the research objectives is to give guidance to the IT/OT integration, especially when it comes to the differences in perspectives between the group. When translating the conclusions of Von Meier to the IT/OT groups, not only the conflict of interest is an issue between the IT specialist and the engineer, but there are differences in interpretation inherently to their the subgroup. Implicating that, even when they would understand each other's profession to a great extent, they would still interpret issues differently. Von Meier proceeds in her paper on the fact that these differences in interpretation are important for an organization to take into account. First, a conflict needs to be addressed at one point in time otherwise it will obstruct improvement of the organization. Second, the conflicts between the subgroups can, sometimes, be considered an asset rather than a liability to an organization. Meaning; different interpretations can offer the decision makers more insight.

When the latter argument is identified and acknowledged by an organization, Von Meier suggest to make deliberate considerations which perspective (IT, OT or combining) is best applicable, every time a decision has to be made

4.4.2 Impact of IT on culture

The second reviewed article comprises of an extensive analysis of a paper regarding the impact of IT on culture and the impact of culture on IT. The paper is relevant because the IT integration described in the paper is similar to the IT integration in control systems. The research does not compare two different cultures, as in the last paragraph, but is reflects the impact of IT. Leidner and Kayworth assembled and analyzed 82 articles about the impact of IT and culture and vice versa (Leidner & Kayworth, 2006).

In the article the term culture is sometimes referred to as culture based on geographic location (i.e. the Western culture and the Arabic culture), but also subcultures in organizations are described (i.e. the IT culture and the engineering culture). In this review we reflect on the latter, called subcultural difference.

The authors argue that culture is often partially blamed when organizations experience failure. While IT is often seen as a possible resort to reduce errors or cut costs, yet the introduction of IT is often met with cultural resistance (Coombs, Knights, & Willmott, 1992). Leidner and Kayworth introduced several propositions, based on their research. Based on their expected impact on the organization, several propositions are relevant to reflect on the IT/OT integration.

Cultural distance and conflict

> *Proposition 1: The greater the cultural distance between the group responsible for championing the IT and the group adopting the IT, the greater the system conflict experienced by the group adopting the IT.* (Leidner & Kayworth, 2006, p. 375)

Simply put, this statement indicates that when an IT system is developed for one specific subgroup, the risk of conflicts increases when it is transferred to other subgroups. Leidner and Kayworth give an example of an IT system that is introduced at a subgroup of the organization, later management decides that the IT systems is a desirable solution for the rest of the organization. Even if the implementation of the global system was planned precisely, still a conflict might emerge because of the sheer constraints involved in adequately representing all group values.

We want to transfer proposition 1 to the IT integration in control systems. In the proposition the authors reflect the implementation of <u>one</u> particular IT system, for example an online monitoring system, to be implemented on several 'sites', for example

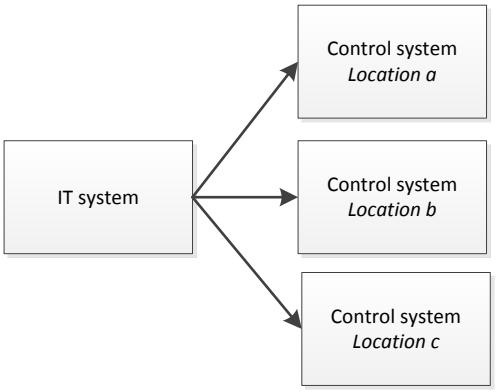


Figure 13: Relation of IT systems and location

several control systems on different locations (Illustrated in Figure 13). While it has to be delineated that the authors argue that conflicts arise when an IT system, developed for a specific (sub)group, is being implemented in different groups with different (sub)cultures (for example Banking and Retail). We assume here that the observation is also valid for different sites of control systems. Due to the fact that every organization and every department has its own culture, we assume that the cultures between 'location a' and 'location b' are different. Although our statement includes several assumptions, still the implication could be valuable to take into account. Concluding: when an IT solution for a control systems is developed for a specific location and a specific group, the cultural distance between this group and the group that consequently adopts the solution, might increase the severity to which a conflict is experienced.

Cultural conflict and adoption rate

The second proposition explains how an apparent cultural conflict indicates the likeliness of adoption.

> *Proposition 2: The greater the system conflict experienced by a group, the less likely the group is to be a forerunner in the adoption of the system.* (Leidner & Kayworth, 2006, p. 376)

Leidner and Kayworthht use the example of the adoption of the internet in Arab countries. While the cultural differences between the Western and Arabic countries is significant, the Arab's still adopted a Western system (the internet). Interestingly enough, even when the adopting culture seem to have completely other values than the culture were the system comes from, the adoption was deemed to be less likely but occurred most of the times (Kitchel 1995; Thatcher et al. 2003). The authors proceed by arguing that it is often not the case if a system is adopted, but when it is adopted. While culture often excludes early adoption of a new system, external factors eventually make adoption necessary. Thus, a particular system is adopted slower when the values of the adopting culture differ more from the values of the originating culture (Figure 14). The authors involve little additional variables that can explain lacking on the adoption of a system. This is a weak point in the analysis due to the fact that 'adoption rate' and 'cultural difference' are probably not 1 on 1 explanatory variables.

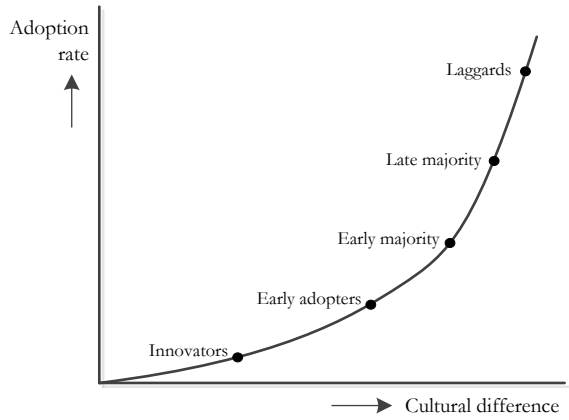


Figure 14: Adoption rate set out to cultural differences

When transferring proposition two on control systems. It could explain why some companies are further along with implementing IT systems and IT security systems in the operational systems. Having said that, it must be expressed that we expect that there is more than one variable responsible for the adoption rate. Thus, it is noted but in this research no further analysis is done on this aspect.

IT systems are adapted to strengthen existing values

The third proposition concerns the altering of an IT solution by responsible entities (managers or employees), in such a way that is suits the requirements and values of their company. The proposition is drafted as follows:

> *Proposition 3: The greater the system conflict experienced by a group, the greater the modification of use to support the group's values.* (Leidner & Kayworth, 2006, p. 376)

Leidner and Kayworth illustrate this with an example of a reorganization where IT is supposed to play an important role. Subgroups in the organization may not share common values, which could lead to conflicts (i.e. a certain security measure of the system is not wanted by department A, but required by department B). The proposition argues that the subgroup will modify a system to fit their values; to what is culturally acceptable. Implicating that groups will use an IT system in such a way as to reinforce, where possible, their existing values.

The transposition of proposition three to control systems can be illustrated by an example. When an IT security solution has been put forward by a vendor or third party, the opinions of this measure – and consequent conflicts - will differ between companies that will adopt the measure. Proposition three says that each organization will adopt the measure according to his own values. When we step one level down to the groups within the organization, we have to deal with the IT specialists and the operational teams. It is expected that, when having no shared values between the groups, the IT and OT groups are separately modifying measures to support their own group values. To overcome this, some organizations introduced special IT/OT integration team which has a set of shared values on, for example, security (see also paragraph 4.4.1). The IT/OT integration team should be capable of modifying the security measure to fit organizational value as a whole.

Managers can decrease conflict

The fourth proposition is a straight forward, but important finding of Leidner and Kayworth.

> *Proposition 4: Managers can reduce all forms of conflict by promoting shared IT values.* (Leidner & Kayworth, 2006, p. 380)

When there is a strong leader-driven vision, especially on how to use IT systems in a strategic manner, there will be more commitment. When managers succeed in developing a strong culture between the different departments and groups, there is an high change of commitment and embracing shared values.

4.4.3 Concluding on literature

The discussed literature tries to explain how cultural conflicts can arise and what the root causes could be. With the insights from the literature we can compose a more complete picture of the potential differences between IT and OT experts. The notion on the different perspectives and the propositions give a more extensive insight in the paradigms.

Von Meier delineates that different groups in an organization inherently have different values. When these values are not aligned, they may cause conflicts. Usually, organization handles the differences in values by promoting the exchange of knowledge. She argues that it is not possible to only focus on knowledge transfer, without realizing that there could be a difference between culture that influences the interpretation of what the problems and solutions actually are. The only way to overcome this is to address these cultural differences.

Leidner and Kayworth identified a number of propositions that illustrate how the gap between perspectives – which Von Meier researched - can be influenced. In the research of Leinder and Kayworth, 82 articles had been analyzed and the impact of technical solutions on culture and vise versa were reviewed. They concluded when a technical solution (often IT related) was created for a certain company or department, the technical solution was often not directly applicable to other companies or departments. It is argued, that the extent of cultural differences between groups (in companies or departments) influence the success and the adoption of a technical implementation. When the cultural differences are bigger between the group that supplied or mastered the solution and the group that has to adopt the solution, the experienced conflicts become bigger. Consequently, when a conflict is being perceived bigger, there will be more modifications to the technical solution to make it fit the culture in question. Finally, it is argued that every conflict can be reduced by promoting shared IT values.

4.5 Management of security

The literature study on the IT and engineering paradigms presents a mindset and perspectives which are ideal typical in nature and are in a sense obsolete. For one thing, seldom will the entire paradigm be identified in reality in a certain group of personnel.

Furthermore, security is not solely dependent on the IT and OT personnel. Management will in most cases have a decisive vote in security and the investments. How do organizations approach the overlapping IT and OT domains and how does management eventually decide upon what is adequate security?

4.5.1 IT/OT alignment

The integration of IT systems into the control systems is called 'IT/OT alignment', 'IT/OT integration' or 'IT/OT convergence'. IT/OT alignment is not confined to the grid; virtually every organization where SCADA systems operate, the presence of the alignment is known. Due to size and adoption rate of IT systems into the grid, we assume this sector lies on the forefront concerning innovative and creative ideas on the IT/OT integration.

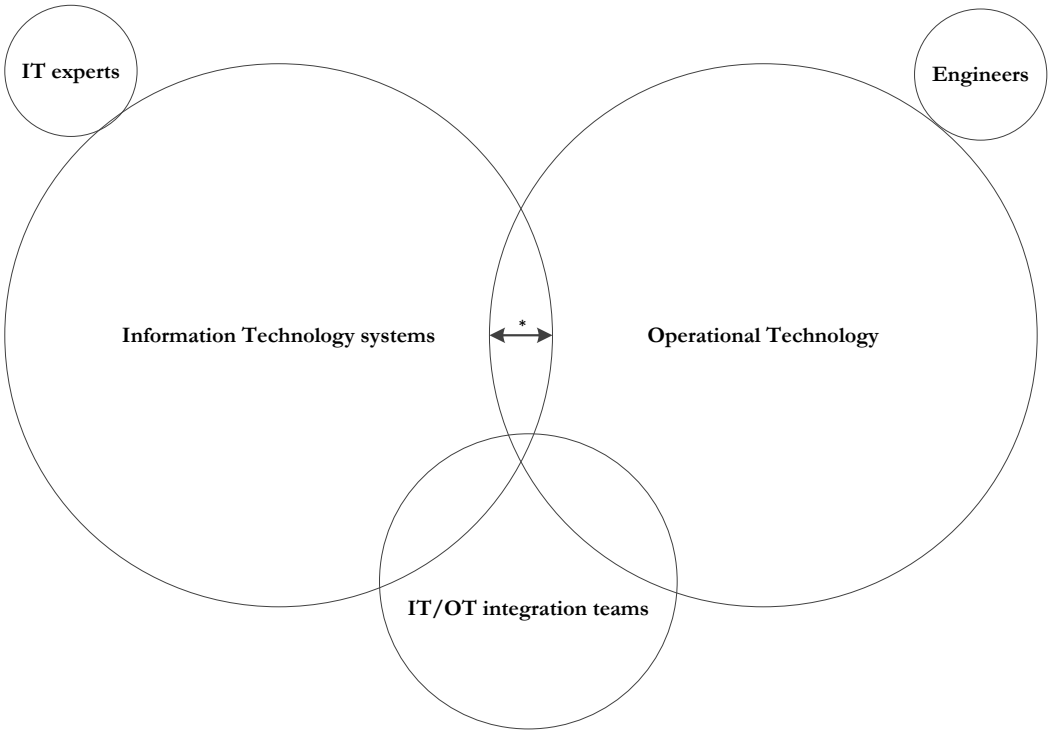


Figure 15: IT/OT integration. Based on an IT/OT composition of Sergio Hernando.

The core of the problem is that IT and OT are two groups with overlap. The engineers are the experts of the operational technology, while the IT experts are engaged on the information technology terrain. Based on chapter two and three we can assume that the area indicated with an asterisk (*) is increasing: information technology and operation technology are increasingly interconnected. A possible end state of this evolution could be a complete integration between IT and OT: the internet of things (discussed with the theory of Beniger). How do companies currently try to handle security issues associated with the integration?

4.5.2 Compliance based security

Companies and governmental institutions try to solve security issues resulting from the IT / OT integration partly through compliance. Institutes want to achieve security by creating and enforcing compliance rules. That this is currently happening can be substantiated by the fact that the European Union issues an increasing amount of research towards developing frameworks for grid security (ENISA, 2012). It is common for the governments in modern society to take responsibility for public goods, cyber security being one of them. However, there are doubts whether enforcing security from the top down, and not from the bottom up, is a robust solution. In the paper 'Control System Security: why expert disagree' a relevant statement is made why compliance based security has some risks:

> *"There is a real risk of falling into the "compliance vs. security" trap and putting lawyers in charge of our cyber security programs."* (Waterfall Security, 2012)

The author means that security frameworks are sometimes drafted by people that are not necessarily security specialist, but have a policy or law background. Consequently, when the drafted compliance rules are, for example, poorly applicable or too generic, it could be hindering security more than advocating security. Security of an organization should consist of more than only obliging to the compliance framework. Ideally it consists of (NIST, 2009):

- Compliance framework: Institutes as NIST and NERC setup rules to achieve security of systems;
- Best Practices: companies and institutions can share opinions and experience on security measures;
- Company specific rules: most companies will have (their own) additional rules and regulations which could enforce security.

Consequently these three aspects should be aligned with the business model. The compliance framework on its own is not able to ensure security of an organization. A framework is not created to align with individual companies, but it is a one-size-fits-all approach. Which often means a framework is too generic and can only provide guidance.

Besides being generic, compliance-based-security has two other downfalls: the lifecycle is long and compliance can be understood as obligatory. The long lifecycle refers to the fact that it is difficult to keep a framework updated. It could take months (or even years) before certain regulations are made obligatory. Possibly being outdated before they are included in frameworks. The second downfall of compliance based security, also show with the above quote of Ginter, is the obligation that companies have to satisfy the compliance standards. Generally, it would be a good thing when companies have commitment to oblige to rules. A

precondition for this to work is that the compliance rules have to be suitable (specific enough, relevant en up-to-date).

4.5.3 Risk based security

Risk based security are quantitative or qualitative methods to assess risks and take decisions regarding security based on the identified risks. Compliance based security and risk based security will mostly be done simultaneously. Some companies will focus more on a compliance based approach, and some a more risk based approach, the one does not exclude the other.

There is an extensive range of risk frameworks which can be adapted for our purpose. To be able to attach the results from the literature analysis and the questionnaire as good as possible to a risk framework, two existing frameworks are adapted to fit the purpose. The World Economic Forum 'Cyber Security Risk Framework' and the ISA contextual model "information security assurance and threat-risk assessment" are combined. The result is the control system risk framework in Figure 16.

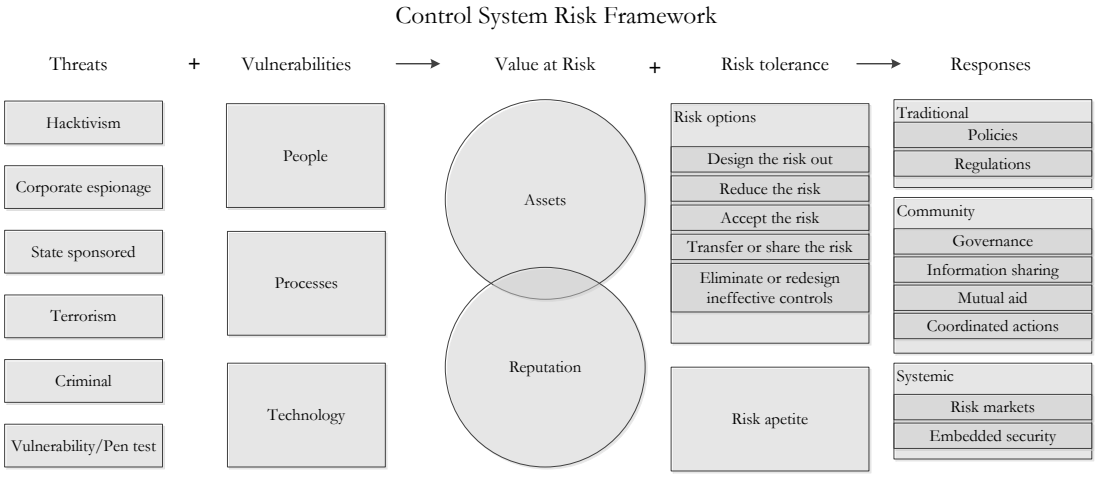


Figure 16: control system risk framework. Based on (ANSI/ISA, 2007), (World Economic Forum, 2012)

The framework consists of five layers: threats, vulnerabilities, Value at Risks, Risk tolerance and responses.

Threats

Cyber threats vary in complexity but through the whole range of the organization they are present in abundance. Identifying the source of the threats is done to increase understanding and insight, so the most effective and efficient ways are found of dealing with the risks. ICS-CERT identified that most attacks between 2009 and 2011 in industrial control were originating from "Sophisticated threat actors" (ICS-CERT, 2012). Because only data was

extracted and no intrusion was identified on the control system network, ICS-CERT believes these actors were only interested in intellectual property. Sophisticated threat actors are believed are more capable because of their financial means and apparent goal (ICS-CERT, 2012). Stuxnet, is believed to be created by state sponsored entities and was used to directly target equipment (Bronk & Tikk-Ringas, 2013). Another known piece of malware, Flame, focused on gathering and deleting information. The underground market provides the possibility to sell the stolen information for significant amounts. Due to limited physical effort and large potential damage, terrorist organizations focusing on targeting the control systems of critical infrastructure are possible. Eventually, threats differ on three different aspects: on the amount of (financial) means, on their skill level and on their intentions or goals. These three aspects identify how serious a certain threat actor could be.

Vulnerabilities

The weaknesses of systems can be found in three different aspects; technology, process or human. People are believed to be a high risk factor when it comes to securing industrial control systems. According to ICS-CERT (2012) people are a liability to control system security, primarily because of a combination of three things:

1. Lack of understanding of the overall security risk to control systems;
2. Technical and security impacts of inadequate security policies or implementation is not considered;
3. Lack of cyber security skills to ensure protection against cyber-attacks.

Understanding of control system security has to extend from the operational activities, all the way to the management. It has been pressed many times; when awareness is not present, necessary investments are not made. Additionally, the difficulties in aligning the business requirements with the security strategy has been proven to be difficult. Process vulnerabilities reflect the insufficient processes in place that facilitate, for example, incident response, security strategies and security standards. When processes are lacking that should facilitate these activities, process vulnerabilities can be expected.

ICS CERT also provides information on what they believe to cause vulnerabilities in technology. These vulnerabilities can be summarized by:

- Lack of control systems risk assessment. The potential impact on the operations is not or not sufficiently analyzed.
- Lack of security management framework. From this, deficiency problems as not segmenting the operational network from the corporate network.

- Lack of updating equipment. Generally, the control systems are not often patched, updated or adapted.

From a technical point of view, there are various things that cause issues: security was not a design criterion, use of legacy systems, long system deployments, component lifetime, patch management, technical requirements and so on.

Risk mitigation

While the vulnerability identification also delineated that people are contributing to security issues, people are also a leading factor in the risk tolerance domain. The risk tolerance domain consists of two parts: risk mitigation options – or strategies if you will - and the organization's risk appetite.

There are five common strategies for risk mitigation: design the risk out, reduce the risk, accept the risk, transfer or share the risk and eliminate or redesign ineffective controls (ANSI/ISA, 2007). Depending on the threats that are identified, the vulnerabilities that are found and the value at risk, an organization can determine the amount of risk it is willing to take (the risk appetite). We must delineate that these kinds of strategies are only valuable when a solid risk assessment is carried out. Without a good understanding of the vulnerabilities, threats and possible responses, it is only guessing.

Value at Risk

Value at Risk (VaR) is one of the methods to come to an assessment of which objects are subject to risks. VaR being a quantitative analyses, gives a monetary representation of the risks. The disadvantage is that this requires an extensive analysis, based upon a significant amount of data. The other analysis method focusses on qualitative analysis, this could be a percentage or a scale (low impact, medium impact, high impact). A large amount of the risk assessments are carried out this way, certainly because it is difficult to assigns a monetary value to everything. While it is not a very precise and reliable method, it could serve as a good initial assessment or as a support tool for the quantitative analysis.

In a VaR analysis each asset is associated with a monetary loss that could occur. In the quantitative valuation an asset is assigned a precise monetary loss with it. This could be in terms of cost of replacement, cost of lost sales, or other monetary measures. Assets is defined as being: data (also intellectual property), networks, devices and infrastructure. Both direct as indirect costs will be assigned in a VaR analysis. Especially the indirect cost are very difficult the assign. The amount of assumptions and variables needed for these relational models is high. Indirect costs can be for example the decrease in business continuity or operational costs because of equipment failure and shutdown. Interpretations of the people that perform these risk assessments influence outcomes. If a risk assessments can be

executed in an objective manner, and to what extent, is a question that deserves further attention.

Reputation is the second aspect of a Value at Risk analysis. The reputation reflects the trust of customers, partners, owners and employees in the organization. Any kind of damage in the assets could lead to reputational damage. In this case, where there is dealt with critical infrastructures, also political damage and decrease in citizen-confidence is a reputational risk. Again, it is very difficult to objectively determine what the damage means for the organization. Differences in interpretations only make it more difficult.

4.5.2 Cost of security

Discussing costs of security is a bit of a sidestep in this research. Yet, cost might influence the perspective on security. Security requires investment and organizations will have different perspectives on how to invest. Because investment in security is also part of the questionnaire, we will discuss cost of security briefly.

Based on rational market decisions, cost is likely to be one of the trade-offs in an organization when making decisions. Besides the identified values - Confidentiality, Integrity, Availability, Reliability, Maintainability and Safety –, investment is an always present criteria. Investment will somehow influence the values of the IT and OT perspectives. We therefore will reflect in a nutshell what the relation between cost and control system security is with two questions:

1. How is the tradeoff investment & security correlated?
2. Is there a market for secure control systems?

These questions in itself comprise quite some writing. We answer the questions concise with available literature.

1. The correlation of the tradeoff: investment & security

Is it likely that the more you invest the more secure a system is? Two aspects are important when analyzing investments in security: differences between individual products and the total quantity investment in security.

Differences between products

There are different readings on this account. One reading can be illustrated by a Dutch saying "goedkoop; duurkoop" (when you buy something cheap, it ends up being expensive because additional or replacement costs). It cannot be proven that quality comes with a higher price. However, when the market for security would follow the classical economic

theories, products which are more expensive should carry an advantage over the cheaper equivalent products. This doesn't mean that better security in the more expensive products is guaranteed.

Efficiency of the investment

When analyzing investments, information technology is argued to follow the law of diminishing returns (Case & Fair, 1998). This law, described by Case and Fair, says that: "adding more of one factor of production, while holding all others constant, will at some point yield lower per-unit returns." Converted to tradeoff between investments and cyber security, this implies that at some point almost no change in security level can be achieved by additional investments. See Figure 17 for a graphical representation. Every additional investment in security will bring such a small difference in security, that it will not be worth the spending. A similar effect can be seen when we look at the efficiency of fighting cybercrime. Attacks against information systems, which is part of cybercrime, is an aspect what control systems could encounter. Unfortunately, it seems to be the case that fighting these types of cybercrime is done very inefficient. An examples the authors of 'Measuring the cost of cybercrime' give, reflects this on the investments in spam prevention. The total cost of spam prevention exceeded more than one billion USD, while the income for the largest spam-sender was estimated around 2.7 million USD (Anderson, et al., 2012). The framework to identify the cost of cybercrime, can be transposed to systems in the grid. The total cost of cybercrime in the electricity grid can be divided in three parts: defense costs, indirect losses and direct losses. When the adding up the three aspects, the sum will be the total cost for society: the losses that society bear. Pike Research estimates the total investment in cyber security for the electricity grid will be around 14 billion USD – Worldwide from 2014 to 2018 – (Pike Research, 2011). What is interesting in relation to compliance based security, a researcher from Pike Research wrote: "*Cyber security remains a check-the-box exercise for many utilities, with spending limited to whatever is needed to survive compliance audits*" (Pike Research, 2012, p. 1). Management would argue 'why invest more than necessary in cyber security of control system'.

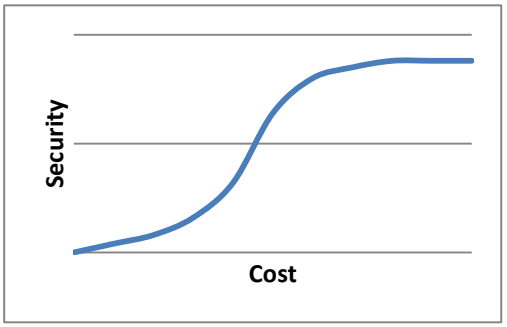


Figure 17: Law of diminishing results (adapted from Case&Fair)

2. The market for secure control systems

We assume that the supply and demand for control systems is market driven. Indicating that product development of control systems will follow the demand of buyers. In the last decade, especially in the last 5 years, the focus on security of industrial control systems

increased significantly. According to Pike Research, Smart grid technology vendors are now proactively seeking out security vendors for assistance in building cyber security into their new products. As result, Pike Research estimates that 63% of smart grid cyber security investment through 2018 will be focused on utility control system segments. (Pike Research, 2012) Currently the market starts to ask for more secure products. A relevant question is: is there a market for secure control systems? This can be approached from a demand and from the supply perspective. Is the demand large enough to make it attractive for vendors to produce the secure products? And are there enough other incentives (i.e. compliance) to produce secure products?

Vendors

The most known vendors of control systems in the electricity sector are Schneider Electric, Siemens and General Electric. For a preliminary analysis of the market we focus on the products of Siemens. A connotation has to be given: Siemens is believed to be one of the more progressive vendors on security. Basically, the industrial automation branch of Siemens consists of five parts. Process control Systems of Siemens (SIMATIC) being the branch that supplies control system to the grid sector. Within SIMANTIC there is a high variety of products. For now, the products that enable (remote) access – thus enabling connectivity outside the isolated network to the control systems – are relevant. Siemens indicate the growing increasing remote connectivity themselves:

> *Industrial Remote Communication offers efficient remote access to machines and plants with SIMATIC.* ***Global remote access to far-flung plants, remote machines and mobile applications is gaining in significance*** *– both in industry and in industry-related areas.* (Siemens, 2013)

After analyzing several dozens of Siemens' product catalogues, white papers and webpages pages, the most important conclusions are:

1. Almost every - currently sold - control system has a standard RJ45 Industrial Ethernet connection;
2. Almost every – currently sold – control systems has built-in security capabilities;
3. There is a Siemens division focused on Industrial Security;
4. Several whitepapers on security are available. Extensive recommendation on security to the buyers of these systems is given;

The conclusion of the Siemens review is that the vendor-support and awareness for secure process control systems is high. With the papers on security recommendations and frequent released software updates, Siemens seems acknowledge the importance of cyber security. The newer generation of process control systems has built-in security: security is not an add-

on. However, the legacy control systems do not have the built in security. While Siemens has several possibilities to upgrade or buy add-ons to increase security, these systems remain to be the biggest issue. Relating the latter review to the cost for security, we can argue that when new control systems are acquired, the security aspects are in place. Products without any security are currently not sold, so Siemens does not have price differentiation on security. Securing legacy systems requires additional investments of the legacy control system owner, but the possibilities to secure these systems are available.

4.6 Conclusion

In literature we found significant differences regarding technical requirements and aspects when comparing the 'business IT' to the 'industrial IT'. In theory, the people working on these different systems also have separate shared values, depending on the subgroup they belong to. In this research we distinguished between the Operation Technology (OT) experts, who work on the operational technology, and the IT specialists, who aim to implement and secure IT systems.

In literature the engineers are involved in the design and operation of systems that have a high physical interaction: the systems can significantly impact the real world. Requirements as safety, reliability and availability (SRA) are valued as the most important design criteria. A particular system must be available, with for example an uptime of 99,9%. Also, due to the high physical interaction safety is important and must be guaranteed. This mostly refers to the (physical) safety of the people involved and in contact with this system. The third criteria is the availability, which entitles whether a systems performs within the specified limits.

The IT specialist - or (cyber) security specialist – in general has a different set of requirements than the OT specialist. In literature confidentiality, integrity and availability (CIA) are the criteria that are valued the most. In the literature, these criteria are reoccurring and seem to be dominant in securing the systems and networks. While the cyber environment is changing fast, also the security methods and security measures changed, yet the CIA-criteria remained the same.

In the third paragraph the criteria – SRA and CIA – are set out against the two perspectives: IT specialist and the OT specialists. When reflecting both perspectives on each of the criteria more insight is gained in the practical implication of the differences between the IT and OT. Several aspects as remote access, authentication, updates, lifetime give a clear contrast between IT and OT.

To gain more insight in what the possible consequences of contradicting and opposite values between groups can provoke, we have discussed literature on conflicting cultures.

The literature of Von Meier explained how certain values are inherent to specific subgroups. Consequently, problem perception, problem definition and possible solutions are difficult to decouple from the specific subgroup, because in respect to their own values their arguments make sense. Contradicting values between groups could cause and/or contribute a great deal the difficulties in securing control systems. The issues with the difference in perspective occur are at the bottom of the organization, where people influence the organization with practical actions and decisions. Management can decide to invest heavily in security, but in the end the people who work with the consequences have to **understand, agree and accept** it. Not only understanding is necessary, but also shared values on security, because this can minimize the conflicts caused by problem perception and solution.

In an effort to understand how the integration of IT into operational systems – the IT/OT integration – is managed, we analyzed how security could be handled. Managing security has two major streams which are intertwined to a large extent: security based compliance and security based on risk management. With risk framework, the threats, vulnerabilities, assets at risk and possible responses can be mapped and informed decisions can be made.

Part II

Design & execution of the questionnaire

Chapter 5. Methodology

Goal of this chapter Explain research method

Relation to previous chapters Based on previous findings the hypothesis and the questionnaire is drafted

5.1 Introduction

The literature shows a discrepancy between operational technology and information technology. With data gathered with the questionnaire, a better understanding of the possible differences between the perspectives can be gained. To maximize the utility of the expert consultation, it is helpful to look at literature regarding surveys. There are various books which are renowned to give good guidance, the four selected books for this research:

1. Asking Questions: The Definitive Guide to Questionnaire Design (Bradburn, Sudman, & Wansink, 2004)
2. Questionnaire design, interviewing and attitude measurement (Oppenheim, 1992)
3. The psychology of survey response (Tourangeau, Rips, & Rasinski, 2000)
4. Improving survey questions by F.J. Fowler (Fowler, 1995)

Best practices, recommendations and remarks from these books were used in this chapter.

5.2 Research approach and methodology

When combining the literature on questionnaire design, a recurring pattern in the approach can be identified. The most relevant steps are (Oppenheim, 1992):

1. Decide the aim of the study. Turn this into operational aims, which lead to a statement of variables to be measured;
2. Decide on the design of the study in regard to feasibility;
3. Decide on which hypothesis will be investigated;
4. Design the research instruments and techniques (e.g. questionnaire, interview schedules, attitude scales);
5. Test the research instruments and make adjustments when necessary;
6. Do the 'field-work': data collection;
7. Process the data, do analysis, test the hypotheses and analyses the outcomes.

5.2.1 Aim of the research

From the literature study significant differences in perspective between IT specialists and the engineers are identified. With the questionnaire we aim to validate the differences on an individual statement (practical) level between the two groups. Can the difference in paradigms between an engineer and an IT specialist found in the literature, be confirmed or refuted based on the outcome of the questionnaire?

A second aspect of this study lies in the explorative nature of this research. To observe differences in perspectives is the main goal. At the same time, with some questions, projections for the future of control system security is a secondary aim. The different groups are asked about their opinions on threats and vulnerabilities. When analyzing the two opinions, we can provide insight in the differences and similarities.

5.2.2 Hypothesis

Where the aim defines the desired end result, the hypothesis is an operational expectation of the aim. The hypothesis for the expert consultation is posed as follows:

> *When looking at cyber security for control systems, there is a difference in perspective on security between the IT and OT specialists.*

As mentioned, the hypothesis reflects the main question of this research.

5.2.3 Feasibility

To be able to say something relevant about the groups, the amount of respondent usually has a minimum. To be able to do a useful SPSS analysis the minimum group size needs to be above 10 persons per group, depending on the kind of analysis (Bradburn, Sudman, & Wansink, 2004). For academic research - taking into account the margin of error, level of confidence, the population and the spread – the calculated sample size per group needs to be around 60 persons. From a feasibility perspective, time and respondents, this amount is not realistic. Therefore, we choose to design a survey which according to literature is not statistically representative for the whole population. The explorative nature of this research allows to focus on the theoretical concept of differences in perspectives. The emphasis is not on statistically assessing and proving the theoretical concepts, which could be the next step. From the IT and the engineers group we ask 40 professionals to participate. The research instruments are also being confined to satisfy time and respondent criteria (physical meetings are difficult). A questionnaire is therefore the chosen instrument.

5.2.4 Data gathering

Data was gathered via an online questionnaire – facilitated by Deloitte – with a timespan of approximately 10 minutes. A part of the respondents were selected from the Deloitte staff, the Technical University Delft staff and both their networks. Besides the direct approach via networks, we also choose to approach possible respondents via Linkedin, where the respondents qualified themselves for example as 'control system engineer' or 'control system security specialist'. The advantage of this approach is that the respondent group is controlled and credentials can be monitored. A disadvantage is that an unknown amount of the people working in the control systems domain is not on Linkedin. While this could possibly affect the outcomes, we cannot influence the risk and have to accept it.

An additional issue was a confidentiality issue. Some respondent working in the security industry, have to sign confidentiality contracts. This means some (potential) respondents could not fill in the questionnaire due to their contracts. It is difficult to say whether the confidentiality issue affects the outcomes. We encountered the confidentiality issue in 5% to 10% of all the respondents.

5.2.5 Data analysis

The data analysis is done with the statistical program SPSS. This program enables us to analyze whether there is a significant difference between the answers of two subgroups. Besides the analysis, SPSS can present the output in visual-friendly graphs.

The analysis is focused on comparing the two perspectives to each other. Due to the diversity of the questionnaire, we expect some interesting relations and/or findings between other variables.

5.3 Questionnaire design

To create a logical path of questions in the questionnaire, some guidance is necessary. The questionnaire needs to be organized so that the respondent can follow a logical line of reasoning (1) and the structure has to be fit for analysis (2). From this, two things follow: the categorization of questions and the content & type of questions have to be determined.

5.3.1 Categorization

In paragraph 4.5 a risk framework is introduced. This risk framework gives a good insight in the different categories of control system security. The range from cause to consequence and the possible remediation is covered in this framework. Threats and vulnerabilities are important categories where insight on a difference in perspective on security can be gained.

Besides these two indicators also response is meaningful aspect. Response indicates how organizations and people currently handle security (according to the perspective of the respondent). The below structure is used in the questionnaire. Where the 'paragraph name' indicates the theme of the section, the 'content' explains what is asked from the respondent and the 'respondent input' explains what kind of input is asked from the respondent.

1. *Paragraph name:* organization and system processes.
    a. *Content*: the respondents view on the current processes and organizational matters are asked. This comprises questions about reporting, risk assessments, investments, compliance and management
    b. *Respondent input*: 14 questions are posed with a Likert scale[1] from 1 to 5. Where 1 means 'totally disagree' and 5 means 'totally agree'.

2. *Paragraph name:* Threat identification – system.
    a. *Content*: in this paragraph the statements on functionality of control system are posed. Each statement beholds an apparent threat for the continuity of the organization. The respondent is asked how he values this threat. This regards for example remote access, security, updates and component lifetime.
    b. *Respondent input*: the respondent is asked how he values the threat on a Likert scale ranging from 'non-threat', 'low threat', 'average threat', 'high threat' to 'extreme threat'.

3. *Paragraph name:* Threat identification – external.
    a. *Content*: the external threats actors are presented in these statements. The respondent is asked how he values the threat that these actors pose for the continuity their organization.
    b. *Respondent input*: the respondent is asked how he values the threat on a Likert scale ranging from 'non-threat', 'low threat', 'average threat', 'high threat' to 'extreme threat'.

4. *Paragraph name:* Threat identification – people.
    a. *Content*: this section focusses on people. The respondent is asked to value threats on awareness, training and qualifications of the personnel.
    b. *Respondent input*: the respondent is asked how he values the threat on a Likert scale ranging from 'non-threat', 'low threat', 'average threat', 'high threat' to 'extreme threat'.

[1] Likert scaling is a bipolar scaling method, measuring either positive or negative response to a statement.

5. *Paragraph name:* Audits, breaches and future.
    a. *Content*: the respondent is presented with twelve statements reflecting possible findings when an audit is done on the control systems. The content regards various topics from documentation, compliance, access to segregation of duties. Additionally some questions are posed on third parties and the level of innovation in control systems
    b. *Respondent input*: the respondent is asked to choose three statements out of the twelve, of which he thinks, are the most probable findings in an audit.

6. *Paragraph name:* Personal
    a. *Content*: the last section is about personal aspects of the respondent, i.e. age, education and occupation.
    b. *Respondent input*: every question is divided into several options, the respondent is asked to check the box which is most suitable. When none of the options is suitable, the respondent can also choose for 'other', and then fill in an answer.

While not all categories of the risk framework are directly used in the questionnaire, several question on every subject are posed, intertwined throughout the categories of the questionnaire.

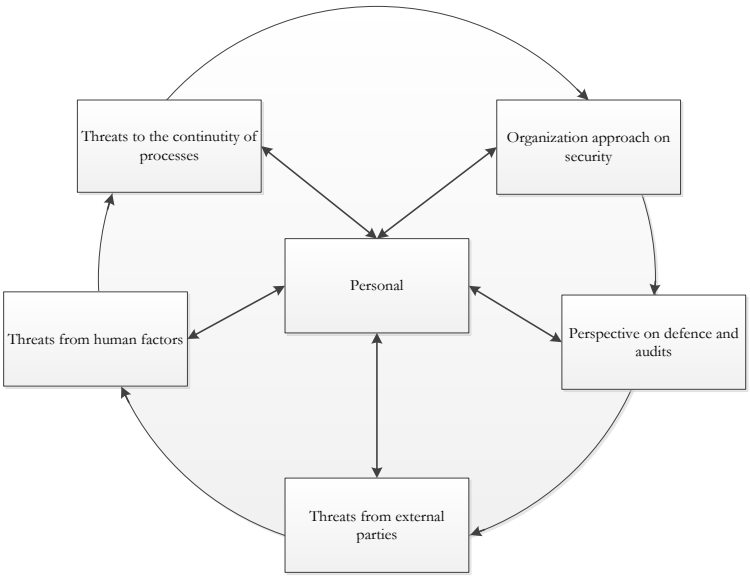


Figure 18: domains in the questionnaire

Figure 18 summarizes the relations that are incorporated into the questionnaire. Each block in the figure illustrates a paragraph of different questions related to that subject. In theory, the aspects discussed in the questionnaire are influenced by each other. The block in the middle of the circle indicates the personal domain. With the questions from this domain we can determine to which group a respondent belongs.

5.3.2 Questionnaire design validation

The questionnaire has been reviewed by different IT experts, Control system experts, researchers, as well as two statistical experts. In several meetings with employees of Deloitte's Security & Privacy team, the questionnaire was reviewed and adjusted. Via phone interviews the questionnaire was discussed with three people, working in de control systems domain. From a statistical point of view (not content focused), the questionnaire was reviewed by a statistical expert from the Technical University of Delft and an expert from the University of Leiden. The combined feedback received in these interviews, meetings and discussing led to several adjustments on content and setup of the questionnaire.

Part III

Analysis and conclusions

Chapter 6. Data analysis

Goal of this chapter Analyses of the gathered data from the questionnaire

Relation to previous chapters Based on developed methodology and questionnaire, the data is gathered

With the collected data from the questionnaire, a statistical analysis has been done to find out more about the respondents perspective on security. In this chapter we describe the results found in the analysis. This is done by graphically presenting the outcomes of the questionnaire. The discussion on every outcome is limited to observation. In the next chapter the empirical analysis based on the outcomes is done.

6.1 Statistical analysis

The data is collected via the Deloitte online survey tool "Invision". This tool allows easy extraction and presentation of the results. The data is extracted to a Microsoft Excel (XLS) file. To be able to do statistical analysis, this dataset had to be transferred to a SPSS file, meaning two things:

1. The dataset had to be transformed into variables and cases;
2. Cases that had the option 'other', have been analyzed separately. These answers are included in the empirical analysis of chapter seven.

6.2 Results

We discuss the results of the analysis per domain. These domains are: organization and system processes (1), threat identification – system (2), threat identification – external (3), threat identification – people (4), Audits, breaches and future (5) and personal (6).

The analysis has been done by comparing the answers of the respondents and analyzing whether there is a significant difference between the groups, distinguished by current occupation. As explained in chapter 5, the questions were posed on a Likert scale from 1 to 5. Two sections in the questionnaire use a Likert scale, the first runs from totally disagree (1) to totally agree (5). The second runs from non-threat(1)

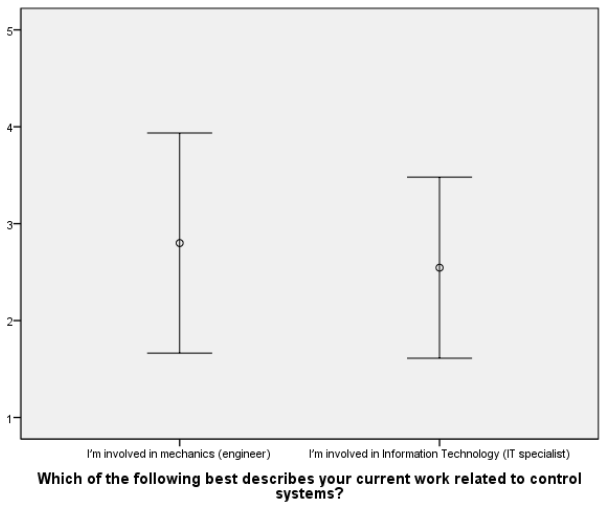


Figure 19: the means between groups and standard deviation

to extreme threat (5). Which scale is used, is indicated at the different sections.

Figure 19 is an example of the graphical representation of the differences in means and standard deviations. The circle represents the mean, the line thought the circle is the standard deviations. The longer the line, the larger the deviation. This implies that the people of the same group differ from opinion. On the y-axis the range of the Likert scale is shown.

The second graphical representations illustrates the difference of opinion inside the group (Figure 20). The bar chart shows the two groups, on the left the Engineering (OT) respondents group, on the right the IT respondents group. The 'count' on the vertical axis represents the number total number of respondents that chose the answer.

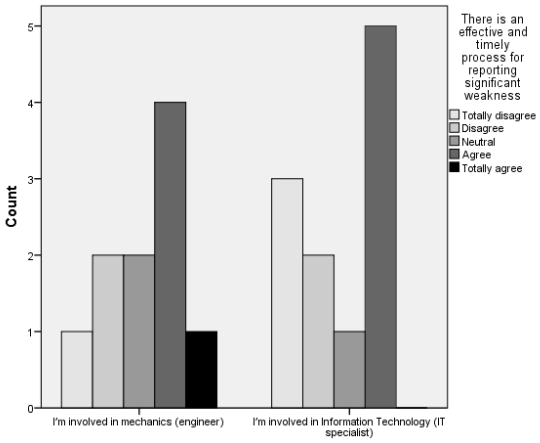


Figure 20: Barchart of differences between groups

In the analysis two things are important: the difference between two groups and the difference within one group. The difference between the groups is used to assess whether the groups share the same opinion. The differences within a group are reviewed in order to asses if opinions differ within a group (based on the standard deviation).

The difference between the groups were analyzed by the reviewing the P-value. There are three possibilities (Mackey & Gass, 2009):

- Significant relations: the relations where the P-value is below 0,05. Which means there is a significant difference between the groups;
- Near-significant: a demonstrated relation which is not significant, but still indicates meaningful statistical relations. This so called "approaching-significance" has a P-value between 0,051 and 0,1;
- Other (insignificant) relations: every P-value above 0,1 and up to 1.

The values are expressed at every question with a formula that is similar to the following: [F(1,19) = 1.39, **p = 0.252**]. We use the official statistical notation, so replication of the results is possible. Here the first two numbers mean the Degrees of Freedom[2], the third number represents the F-Value, the fourth value means indicates the significance.

The function 'One-Way-Anove'(One Way Analysis of Variance) is suitable for the analysis because the means of two or more groups can be compared. In this research the means and deviations of the IT and OT group were compared on the statements. The overview of the

[2] the number of values in the final calculation of a statistic that are free to vary.

One-Way-ANOVA results on significance, standard deviation and mean can be found for review in Appendix III. For every question, these variables are drawn from the Appendix table and a short explanation on the result is given. The implications of the results are discussed in chapter 7; empirical implications.

At the end of every section of questions, there is a short conclusion on the outcomes of that domain.

6.2.1 People

In this paragraph an exposition is given on the properties of the respondents. Age, education and professional characteristics are discussed.

The respondents are asked via Linkedin to participate. It is expected that this leads to a representative snapshot of the population regarding age, experience and occupation. In total 35 experts in either Control System Engineering or Control System Security participated in the research. Some facts on the respondents. 14% of the respondents did not provide their age. From the respondents that did provide their age, 11% was 30 years or younger, 36% was between 31 and 40, 39% is older than 41 years.

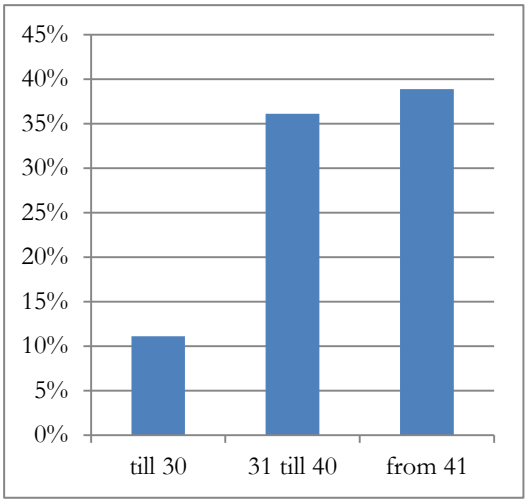


Figure 24: age distribution

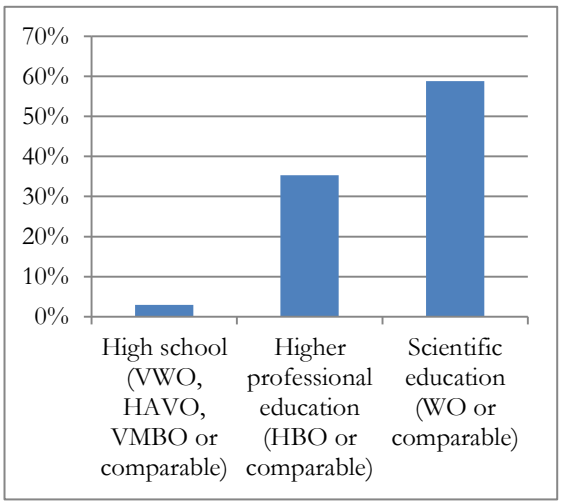


Figure 24: education distribution

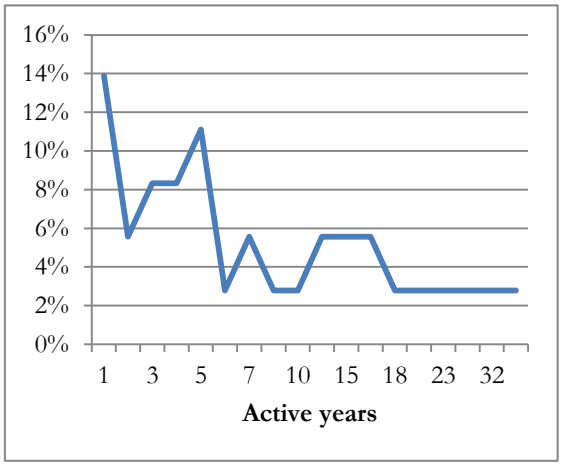


Figure 24: years active in profession

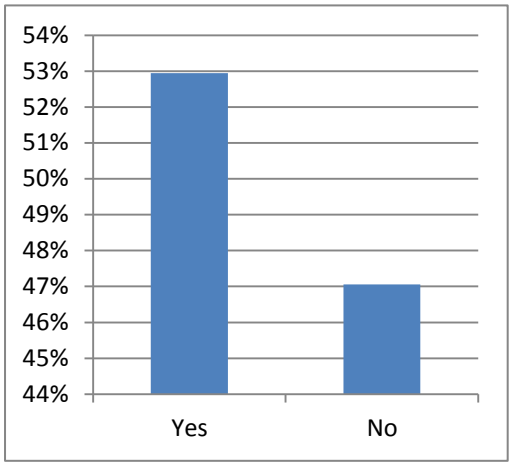


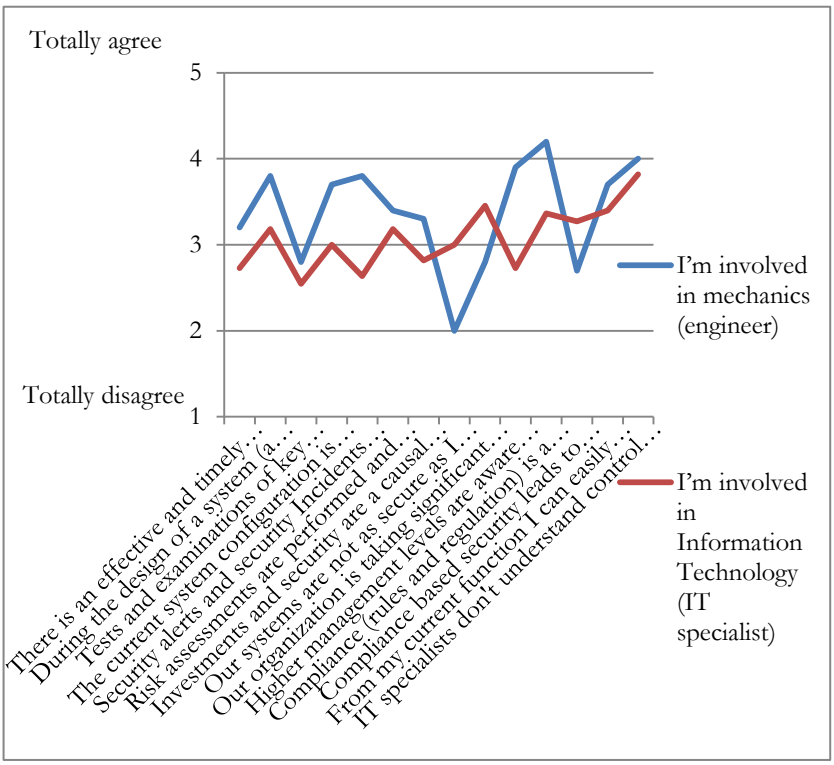
Figure 24: always worked in the control systems industry

Figure 24 shows the educational distribution. More than 90% of the respondents attended at least higher professional education. To find out more about the respondent professional background, we asked how many years the respondent worked in the current occupation and if the respondent always worked in this domain. 36% of the people working in the control systems domain are active at least 10 years. 53% of the group have always worked in the control systems industry.

The difference in 'active years' between the IT group and Engineering group is not significant. However, it is noteworthy that the mean of 'active years' of the IT specialist is 7.34 years and for the Engineer it is 11.3. 54.5% of the IT group works 5 years or less in security of control systems.

6.2.2 Organization and system processes

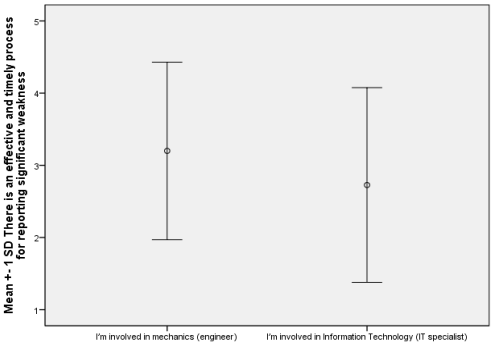
The first domain of the questionnaire reflected organizational and system processes. Mainly reporting, risk assessments, investments and compliance are discussed. The below figure shows an overview of how respondents, disaggregated to subgroups, score on the questions.



There is an effective and timely process for reporting significant weakness
During the design of a system (a device or service), the security requirements are identified
Tests and examinations of key controls are routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?
The current system configuration is documented, including links to other systems
Security alerts and security Incidents are analysed and remedial actions are taken
Risk assessments are performed and documented on a regular basis or whenever the system, facilities, or other conditions change
Investments and security are a causal relation: the more you invest, the more secure your system is
Our systems are not as secure as I want them to be, because it is too expensive
Our organization is taking significant risks by not investing or postponing investments in security
Higher management levels are aware of security risks in everyday processes
Compliance (rules and regulation) is a good way of ensuring security and safety for control systems
Compliance based security leads to regulations that not necessarily contribute to security
From my current function I can easily reach higher management when I identify a risk
IT specialists don't understand control systems (from an engineering perspective)

Figure 25: organization and system processes

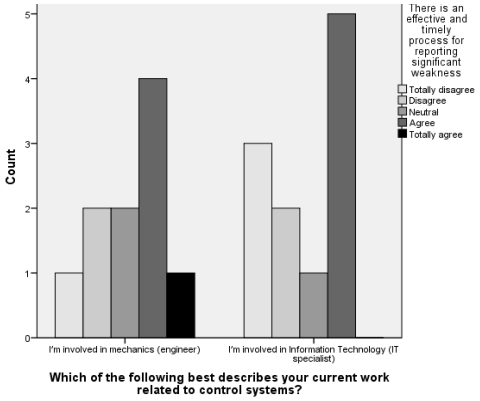
From the graph, several similarities and differences in perception can be seen. The lines deviate quite a bit from each other on three questions. This is where the significant differences between IT and engineers are found, also discussed further in this paragraph.

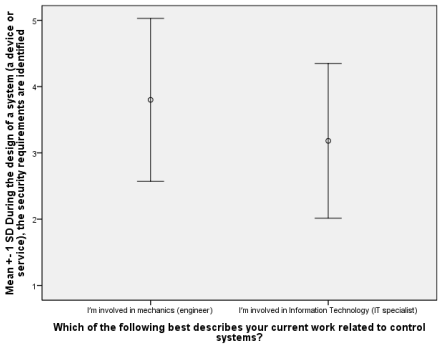


Question 1: There is an effective and timely process for reporting significant weakness.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.7, **p = 0.413**]

Remarks: the mean of the engineers was on average higher than the IT specialists, but the difference is not significant. This statement does not support a difference in perspective. Also the spread (standard deviation) in the groups is high; the respondents had divergent answers. When combining the answers of the groups, the average is 2.95 which equals 'neither agree or disagree' on this statement. From the bar chart is it notable that "agree" counts the most answers in both groups.

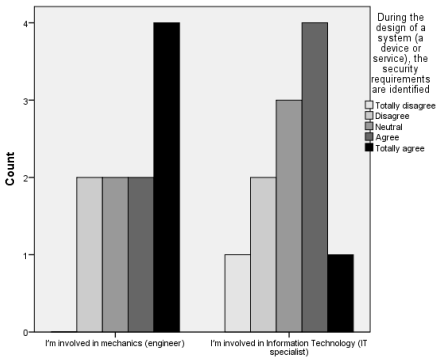


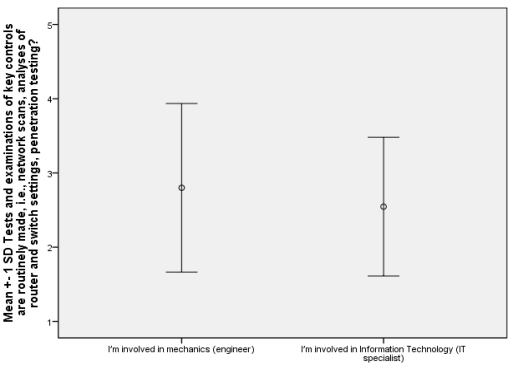


Question 2: During the design of a system (a device or service), the security requirements are identified.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.39, **p = 0.252**].

Remarks: the mean of the engineers was on average higher than the IT specialists, but the difference is not significant. This statement does not support a difference in perspective. From the bar chart is it notable that "totally agree" and "agree" were the most chosen answers. .

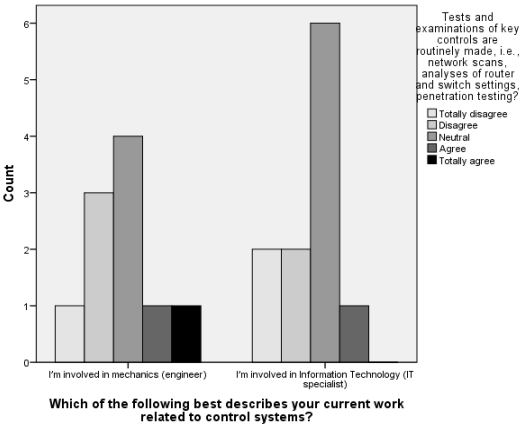


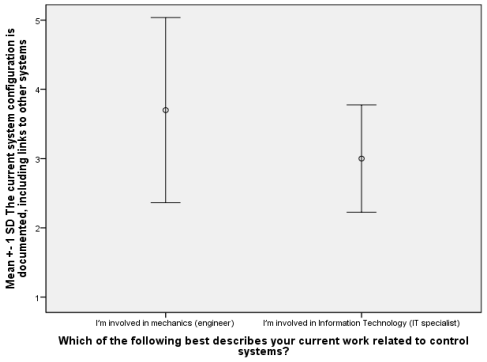


Question 3: Tests and examinations of key controls are routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.317, **p = 0.580**]

Remarks: the outcome of this statement does not support a difference in perspective between the groups. When combining the answers of all respondents the average is 2.6; between 'disagree' and 'neither agree or disagree'. In both groups the most chosen answer was 'neither agree or disagree'.

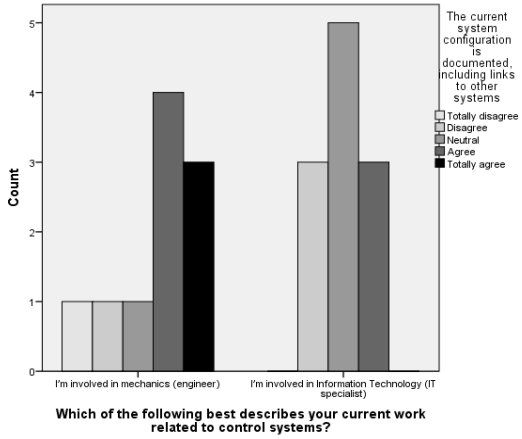


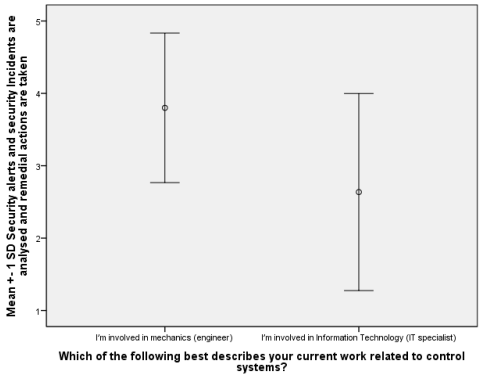


Question 4: **The current system configuration is documented, including links to other systems**

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 2.207, **p = 0.154**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The standard deviation in the Engineers group is almost two times as big as in the IT specialist group, respectively 1.337 and 0.775. This implies that the opinion between engineers differs, which can also be seen in the bar chart. More than 50% of the engineers 'agrees' or 'totally agrees' with the statement.

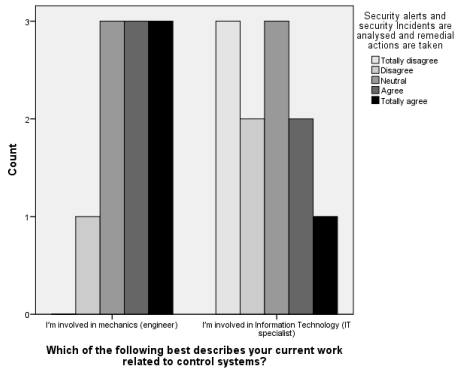


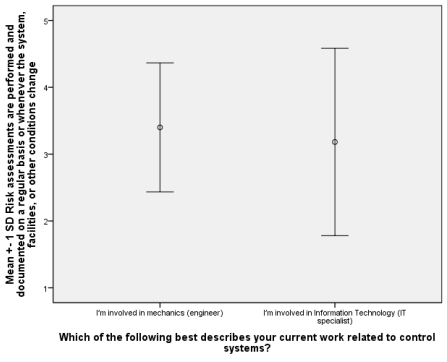


Question 5: Security alerts and security incidents are analyzed and remedial actions are taken.

Significance: There is a significant difference between the two groups on the above statement [F(1,19) = 4.778, **p = 0.041**].

Remarks: The means of the engineers is 3.8 (close to 'agree') and the means of the IT specialists is 2.64 (between 'disagree' and 'neither agree or disagree'). It is notable that the standard deviation in the IT group is 30% bigger than in the engineering group. Respectively 1.362 for IT, against 1.033 for engineers.

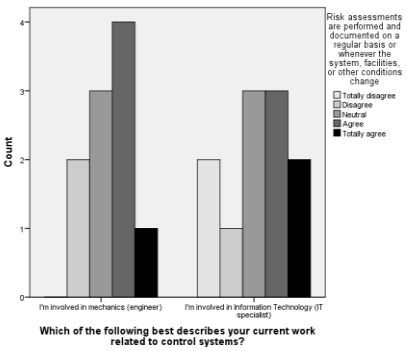


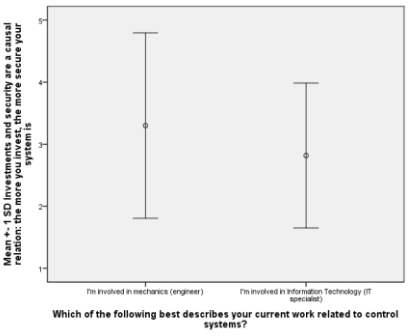


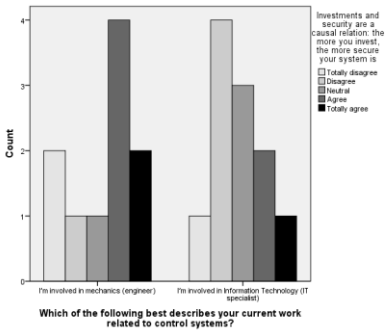
Question 6 : **Risk assessments are performed and documented on a regular basis or whenever the system, facilities, or other conditions change.**

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.169, **p = 0.686**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. On average the engineers scored higher than the IT specialists (3.4 against 3.18). Yet the standard deviation in the IT group was 50% larger than the standard deviation of the Engineering group.

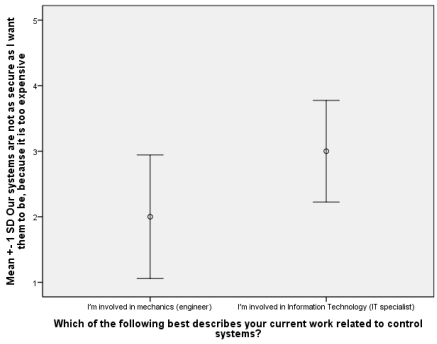


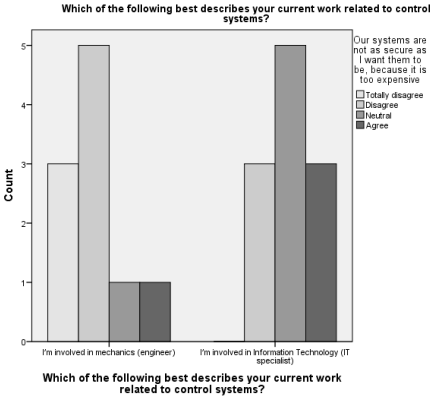




Question 7: **Investments and security are a causal relation: the more you invest, the more secure your system is.**

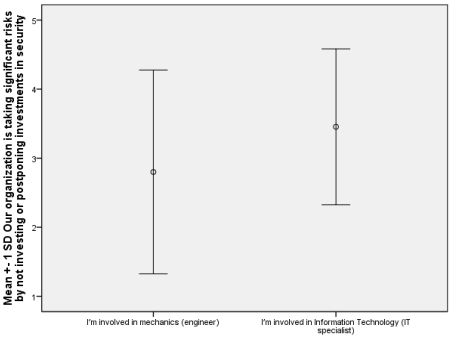
Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.685, **p = 0.418**]. *Remarks:* the outcome of this statement does not support a difference in perspective between the groups. It is notable that both groups show a large standard deviation. 1.494 for the Engineers and 1.168 for the IT specialists. This implies that the respondents did not agree with each other, which is also visible in the bar chart. Yet, it is remarkable that most respondents in the engineering group chose to 'agree' with the statement, while most respondents in the IT group chose to 'disagree' with the statement.

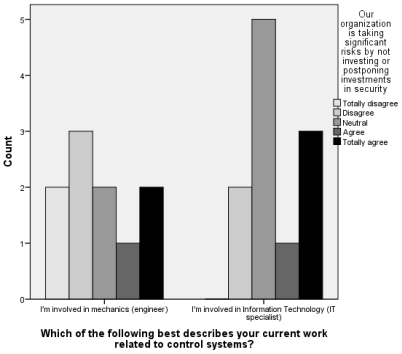




Question 8: **Our systems are not as secure as I want them to be, because it is too expensive.**

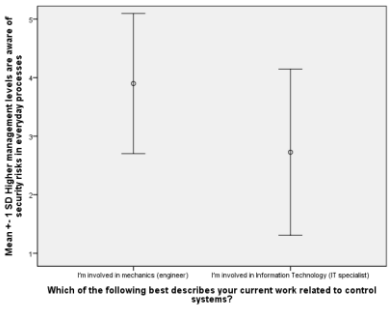
Significance: There is a significant difference between the two groups on the above statement [F(1,19) = 7.109, **p = 0.015**]. *Remarks:* this statement does support a difference in perspective between the groups. The engineers disagree with the statement and differ one point with IT specialists. Both means and standard deviations are relatively low: 'disagree' with a standard deviation of 0.943 for the engineers and 'neither disagree or agree' with a standard deviation of 0.775 for the IT specialists.





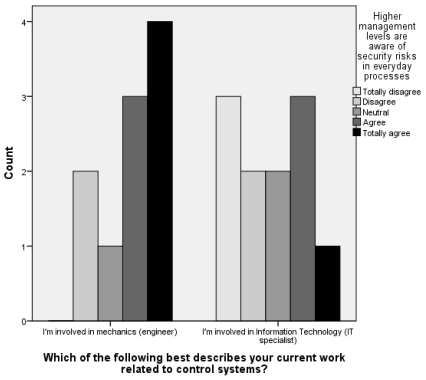
Question 9: **Our organization is taking significant risks by not investing or postponing investments in security**

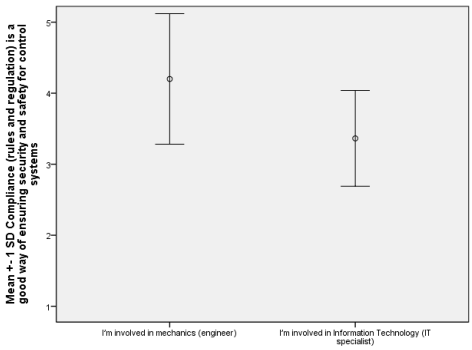
Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.319, **p = 0.265**]. *Remarks:* the outcome of this statement does not support a difference in perspective between the groups. The standard deviation in both groups is high. 1.476 for the IT group and 1.128 for the Engineering group. This implies that the respondents did not agree on the answers, as is also visible in the bar chart. The means of the groups differs, due to the high standard deviation the difference between the groups is not significant. For Engineering group the means was 2.8, for the IT specialists the means was 3.45.



Question 10: **Higher management levels are aware of security risks in everyday processes.**

Significance: There is a near-significant difference between the two groups on the above statement [F(1,19) = 4.137, **p = 0.056**]. *Remarks:* while the standard deviation is relatively high inside the groups, 1.197 for Engineers and 1.421 for IT, the difference between the groups is found to be significant. The means of the Engineering group is 3.9, the means for the IT group is 2.73.

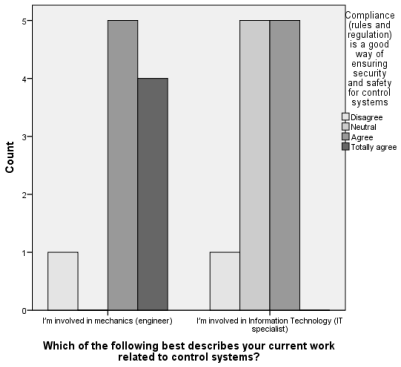


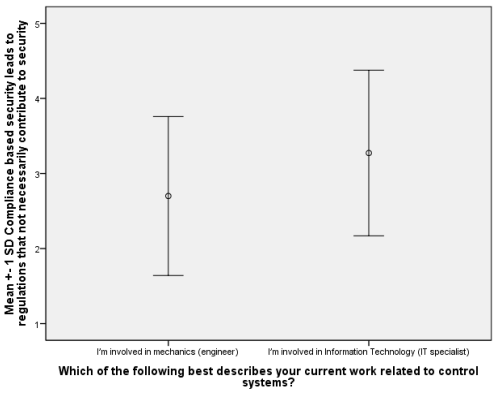


***Question 11*: Compliance (rules and regulation) is a good way of ensuring security and safety for control systems.**

Significance: There is a significant difference between the two groups on the above statement [F(1,19) = 4.137, **p = 0.027**].

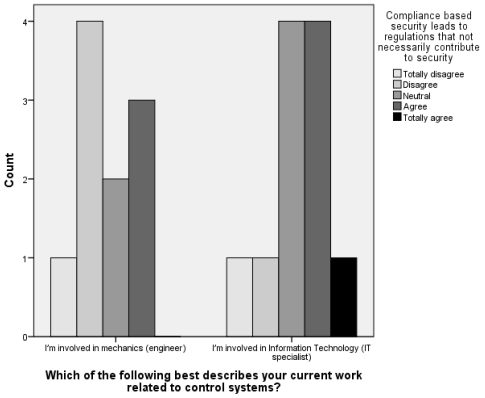
Remarks: this statement does support a difference in perspective between the groups. The engineers agree with the statement and differ almost one point with IT specialists (4.2 against 3.3). Both the standard deviations are relatively low: 0.919 for the Engineers and 0.674 for the IT specialists. While both groups are leaning towards agreeing on the statement. The engineers agree significantly more to this statement.

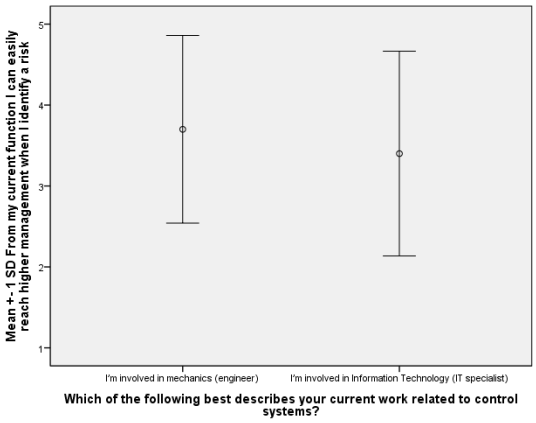




Question 12: **Compliance based security leads to regulations that not necessarily contribute to security.**

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.465, **p = 0.241**]. *Remarks:* the mean and standard deviations of the groups are as follows: 2.7 with a std.dev. of 1.059 for Engineers and 3.27 with a std.dev. of 1.104 for IT. From this result, little implications can be drawn because the standard deviation is relatively high and the means of the groups are close to each other.

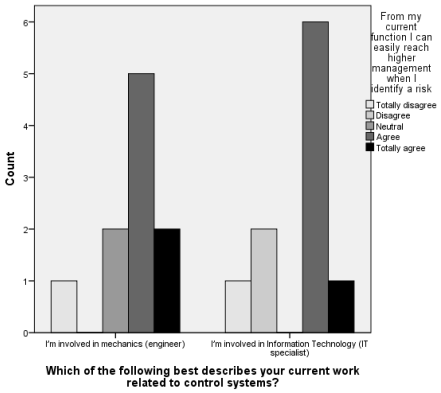


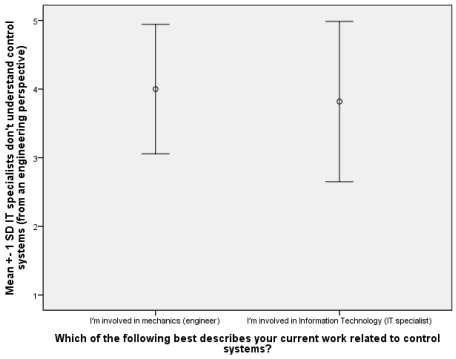


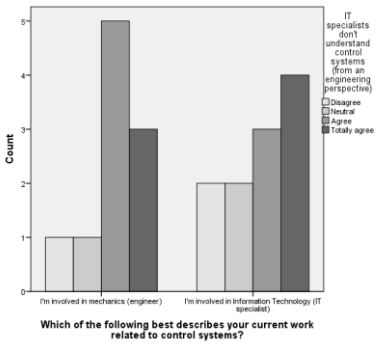
Question 13: **From my current function I can easily reach higher management when I identify a risk**

Significance: There is not a significant difference between the two groups on the above statement [F(1,18) = 0.306, **p = 0.587**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. From the bar chart it can be visually concluded that the respondent in both groups preferred the answer 'agree'. This also reflects in the relative high means of the groups; 3.7 for the engineering group and 3.4 for the IT group.







Question 14: **IT specialists don't understand control systems (from an engineering perspective).**

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.152, **p = 0.701**].

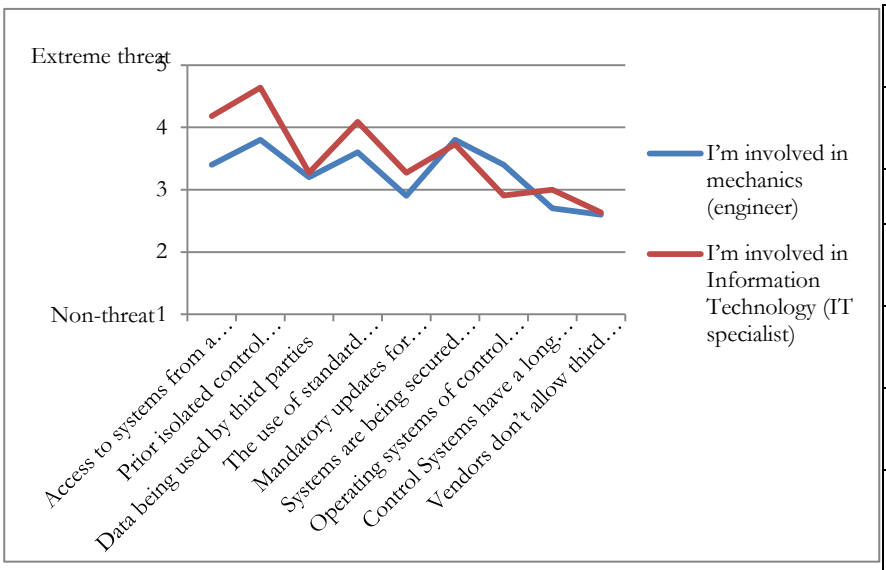
Remarks: the outcome of this statement does not support a difference in perspective between the groups. Both groups agree on the above statement. Also the means are relatively high; 4.0 for the Engineering group and 3.82 for the IT group. The preference is also visible in the bar chart.

Summary on 'Organization and systems processes'

We found a significant difference between the Engineering group and the IT group in four out of the fourteen questions. In general, we can categorize the results of the statistical analysis in two categories. First, in several questions it was notable that there were no significant differences between the groups while this could be expected from the literature. Question two - *during the design of a system (a device or service) , the security requirements are identified* – is a good example of such a question. In the engineering literature, no references are made to security-by-design. Second, the four questions where significant differences between the groups were found are interesting for empirical reflection.

6.2.3 Threat identification – system

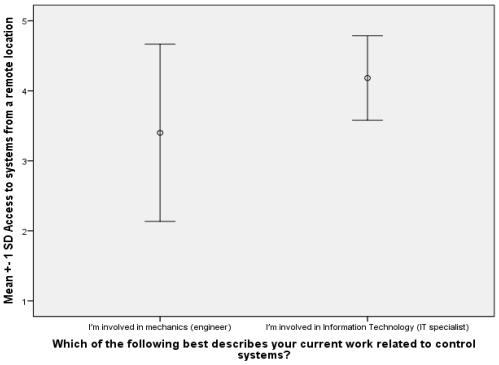
The second domain regards threat identification. Respondent were asked to classify the statement from their perspective. They could choose from 'non-threat', 'low threat', 'medium threat', 'high threat' and 'extreme threat'.



Access to systems from a remote location
Prior isolated control systems being integrated with internet
Data being used by third parties
The use of standard passwords for legacy control systems
Mandatory updates for software systems
Systems are being secured after there are built (not security by design)
Operating systems of control systems may have little computing resources available for common security practices
Control Systems have a long lifespan and have to be ready for 30 to 40 years of technical development
Vendors don't allow third party solutions for security

From the graph we can pose that most of the statements on average are valued 'medium threat' or higher. This implies that the two subgroups mostly agree upon the statements posed here. The statements regard for example: 'Access to systems from a remote location', 'The use of standard passwords for legacy control systems' or 'Systems are being secured after there are built'. While the lines are quite similar, still there were some significant difference between the engineer and the IT specialist.

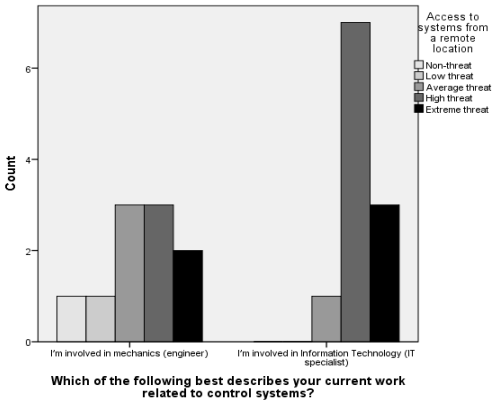
The last question in this domain regarded the third party solutions for security. We expected, based on paragraph 4.3, that third party solutions pose a threat for the availability of the control system and thus be viewed as a significant threat by the engineers. However, the respondents (in agreement) did not value it as a threat. Also additional information about third party solutions was provided by one respondent. This is discussed in chapter seven.

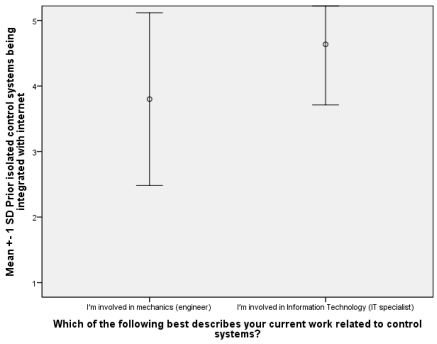


Question 15: Access to systems from a remote location

Significance: There is a near-significant difference between the two groups on the above statement [F(1,19) = 3.373, **p = 0.082**].

Remarks: this statement does support a difference in perspective between the groups. The standard deviation in the Engineering group is twice as large as the standard deviation in the IT group (1.265 against 0.603). This implies that the diversity of answers was larger in this group, as can be seen in the bar chart. The means of the groups are fairly high. 4.18 for the IT specialists, which implies a high threat, and 3.4 for the Engineers, which is between 'average threat' and 'high threat'.

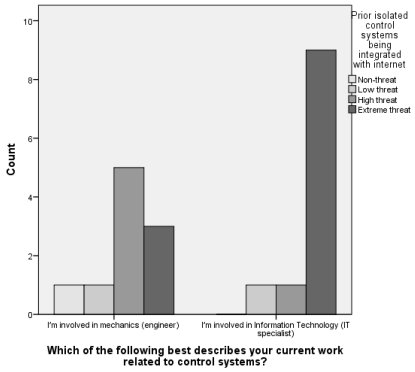


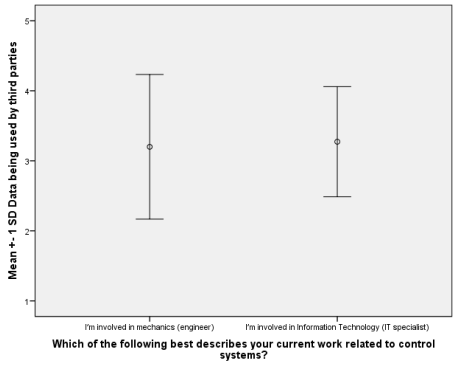


Question 16: Prior isolated control systems being integrated with internet.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 2.883, **p = 0.106**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the groups are the highest means in this subject of the questionnaire. A mean of 3.8 for the engineers (with a std.dev. of 0.924) and a mean of 4.64 for the IT specialists (with a std.dev. of 1.317). Similar to the previous question, the standard deviation of the engineers is fairly high). From the bar chart can be concluded that a significant amount of the IT specialists agreed on the classification of 'high threat' on this statement

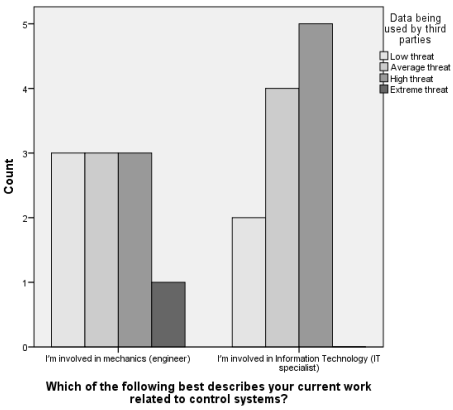


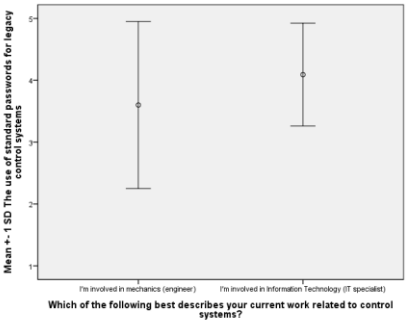


Question 17: Data being used by third parties.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.033, **p = 0.857**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the IT specialist and the engineer are almost equal (respectively 3.27 and 3.20). The respondents seem to differ from opinion on this question, judging from the bar chart.

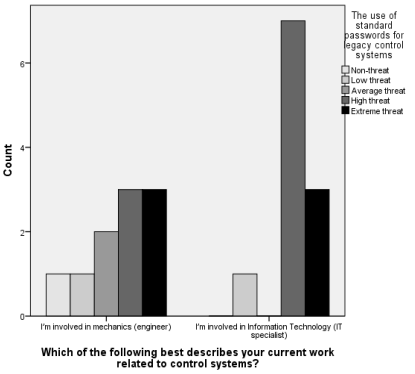


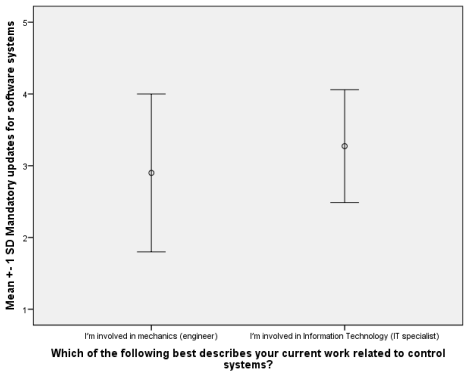


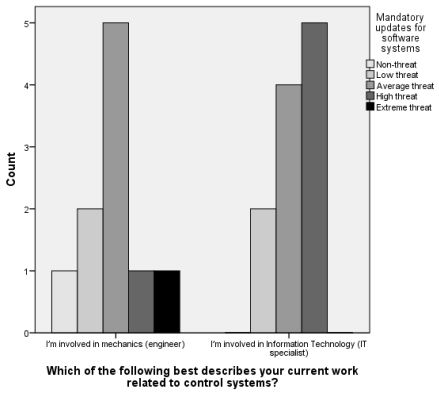
Question 18: The use of standard passwords for legacy control systems.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.029, **p = 0.323**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the Engineers is 3.6 (between 'average threat' and 'high threat'), the means of the IT specialists is 4.09 ('high threat'). Judging on the bar chart, it can be concluded that the respondents in the engineering group had different opinions on this statement. The standard deviation of the Engineers is 1.350 and the standard deviation of the IT specialists is 0.831.



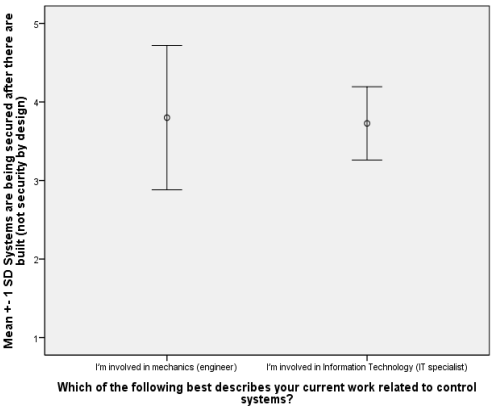




Question 19: Mandatory updates for software systems.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.809, **p = 0.380**].

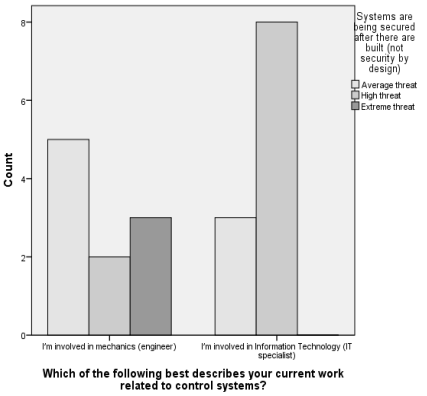
Remarks: the outcome of this statement does not support a difference in perspective between the groups. Both the means of the IT specialist and the Engineer lie around 'average threat' (respectively 3.2 and 2.9). From the bar chart and the standard deviation (respectively 0.789 and 1.10), it can be argued that the respondents overall agreed on this statement.

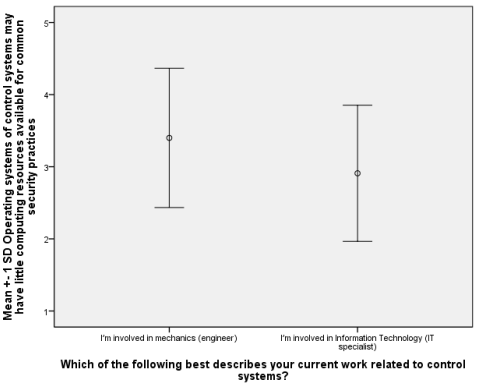


Question 20: Systems are being secured after there are built (not security by design)

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.054, **p = 0.819**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. Both the IT group and the Engineering group have similar means, respectively 3.8 and 3.72. Which implies near-'high threat'. Several of the engineers also indicated this statement as an 'extreme threat'.

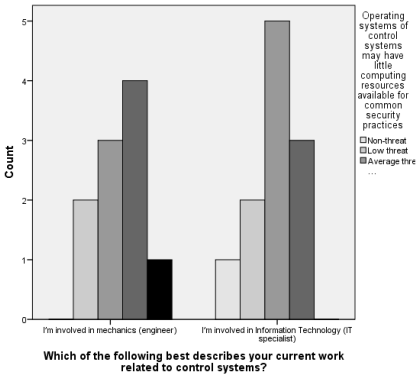


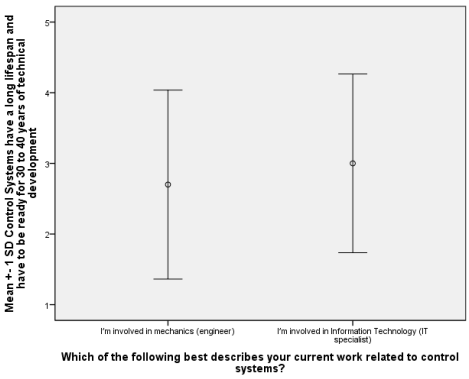


Question 21: Operating systems of control systems may have little computing resources available for common security practices

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.386, **p = 0.254**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the IT group and the Engineering group differ a little from each other (respectively 2.91 and 3.4). Due to both groups having a standard deviation of around 1, the difference between the group is not significant. The equalities are also visible in the bar chart.

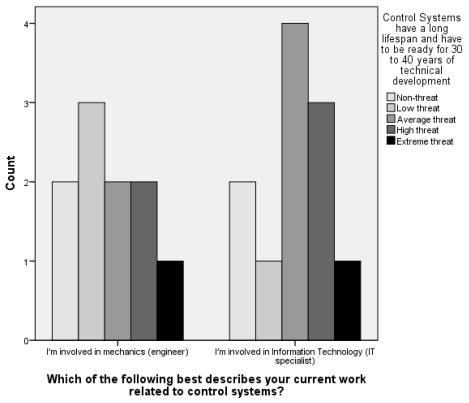


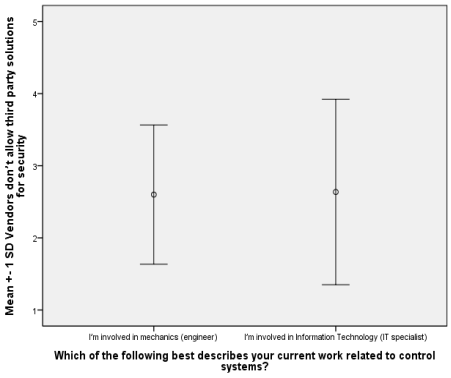


Question 22: Control Systems have a long lifespan and have to be ready for 30 to 40 years of technical development

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.279, **p = 0.603**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. Again, the means of the group are close to each other (2.7 for the Engineers and 3.0 for the IT specialists). Partly because of the high standard deviation, respectively 1.337 and 1.265, the groups do not significantly differ from each other.

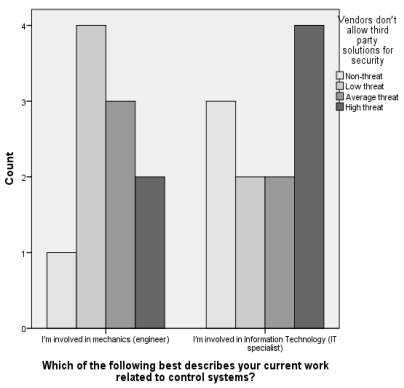




Question 23: Vendors don't allow third party solutions for security

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.05, **p = 0.943**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the groups are practically the same: 2.6 for the Engineers and 2.64 for the IT specialists

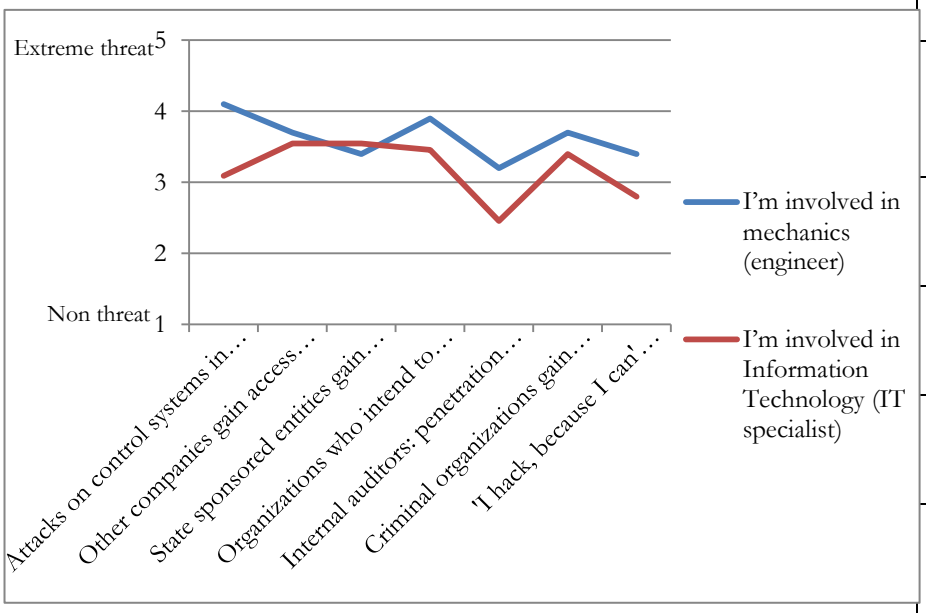


Summary on 'Threat identification - systems'

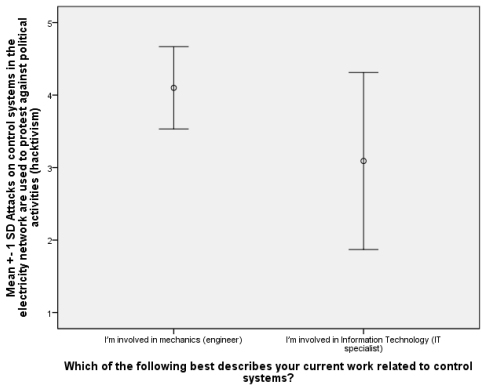
This section, regarding threat identification of systems, the statements on functionality of control system were posed. Each statement holds an apparent threat for the continuity of the organization. In only one out of nine statements a significant difference between the two groups could be statistically substantiated. Thus, in over 90% of the statements the groups did not significantly differ from each other. This projection is interesting, due to the fact that conflicts found in literature, set out in paragraph 4.3, might expected to be reflected more clearly in differences in threat perception.

6.2.4 Threat identification – external

This part the questionnaire aims to identify how the respondents value threats from different actors. We classified seven groups that possibly could pose a threat for control systems security. All threats, except for internal auditors, where assed to be 'average threat' or higher.



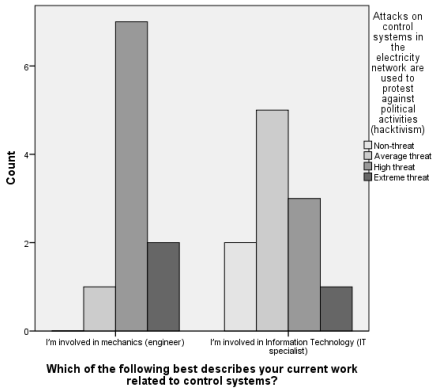
Attacks on control systems in the electricity network are used to protest against political activities (hacktivism)
Other companies gain access to files and information in order to gain economical advantage (competitive intelligence
State sponsored entities gain access in order to gain intelligence about critical process and infrastructures
Organizations who intend to cause damage, physical and/or economical (terrorism)
Internal auditors: penetration testers or vulnerability assesments which are done on control systems
Criminal organizations gain access to information and files and intend to sell the information or blackmail the relevant actors
'I hack, because I can' individuals who breach a system

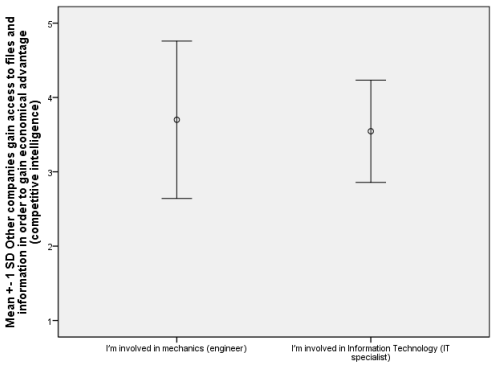


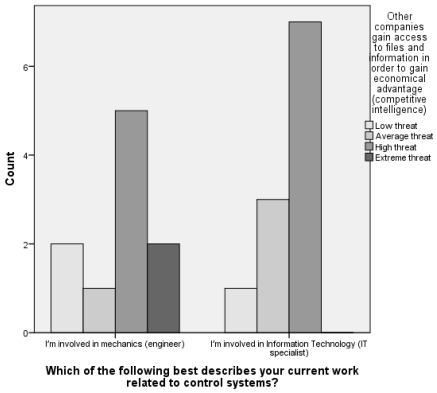
Question 24: Attacks on control systems in the electricity network are used to protest against political activities (hacktivism)

Significance: There is a significant difference between the two groups on the above statement [F(1,19) = 5.690, **p = 0.028**]

Discussion: this statement does support a difference in perspective between the groups. The opinion of the IT specialist differs significantly from the engineer on hacktivism. While the engineer values on average hacktivism as a 'high threat', the IT specialist values it as 'neutral'. The standard deviation of the IT group is twice as large as the Engineering group (respectively 1.221 against 0.568).



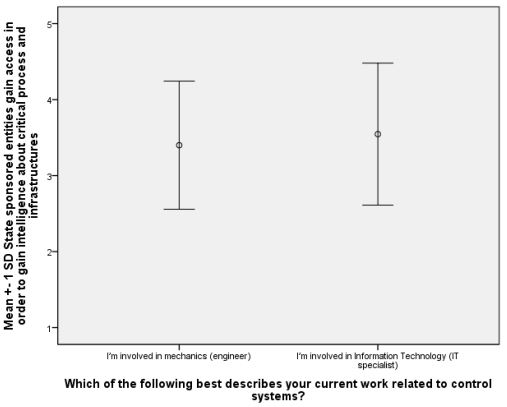




Question 25: Other companies gain access to files and information in order to gain economical advantage (competitive intelligence)

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.160, **p = 0.693**].

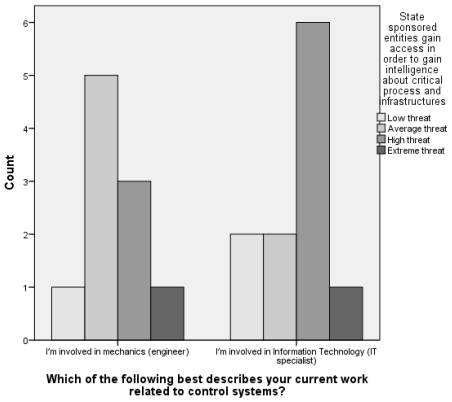
Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the two groups are almost equal (3.70 and 3.55). From the bar chart it can be derived that the most chosen classification of both groups was 'high threat'.

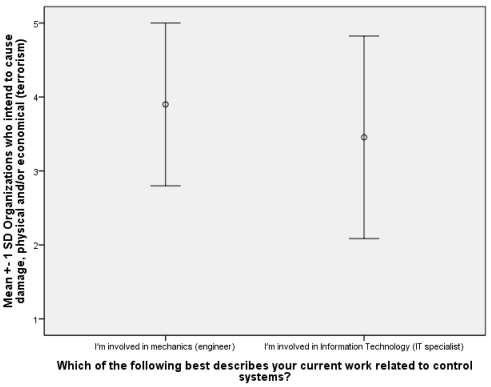


Question 26: State sponsored entities gain access in order to gain intelligence about critical process and infrastructures

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.139, **p = 0.713**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the groups are again quite similar (respectively 3.4 and 3.55).

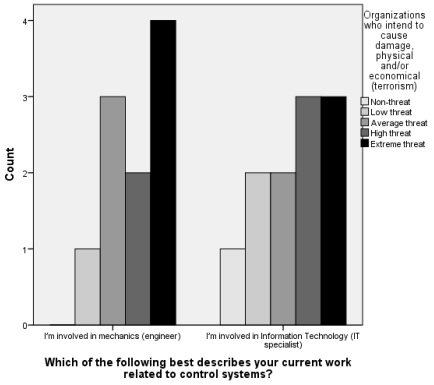


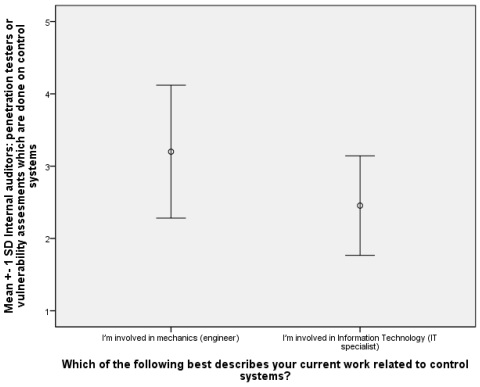


Question 27: Organizations who intend to cause damage, physical and/or economical (terrorism)

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.667, **p = 0.424**].

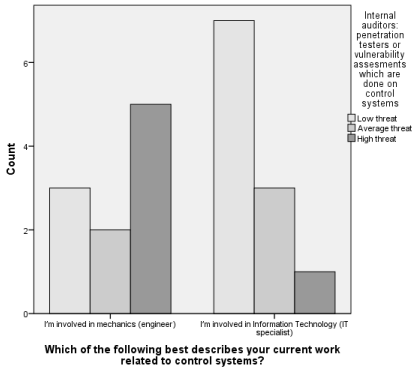
Remarks: the outcome of this statement does not support a difference in perspective between the groups. The average classification is reasonably high. The mean of the IT group is 3.45 (with a std.dev. of 1.368) and the mean of the Engineering group is 3.9 (with a std.dev. of 1.101). In the bar chart it is visible that the categorization leans toward the 'extreme threat'.

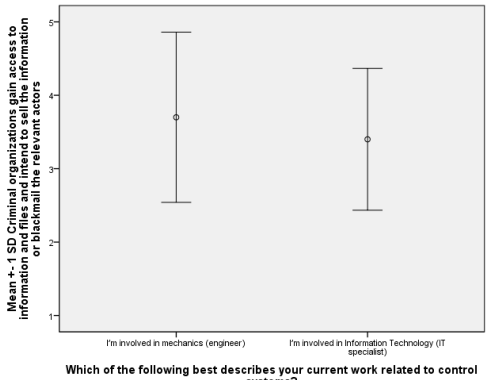




Question 28: **Internal auditors: penetration testers or vulnerability assessments which are done on control systems.** *Significance:* There is a significant difference between the two groups on the above statement [F(1,19) = 4.486, **p = 0.048**]

Discussion: the outcome of this statement does support a difference in perspective between the groups. The IT specialists value the threat to control systems of penetration testers between 'low threat' and 'average threats' (with an means of 2.45 and a standard deviation of 0.688). While engineers value the threats between 'average threat' and 'high threat' (with a means of 3.2 and a standard deviation of 0.919).

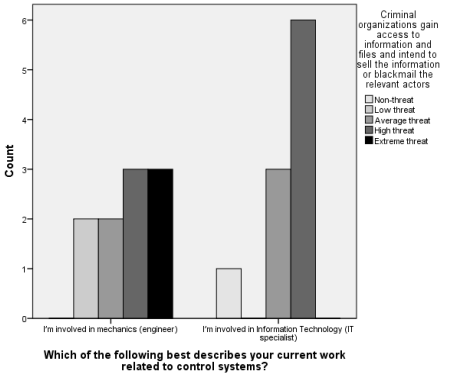




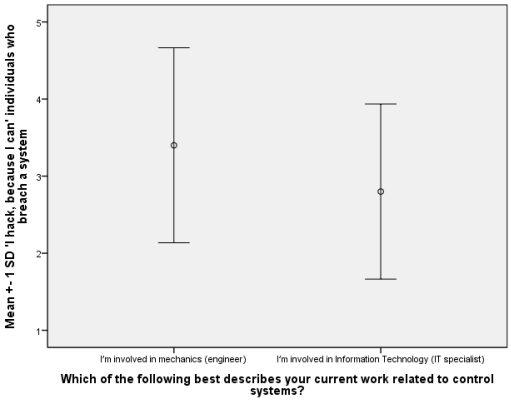
Question 29: Criminal organizations gain access to information and files and intend to sell the information or blackmail the relevant actors

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 3.95, **p = 0.538**].

Remarks: the outcome of this statement does not support a

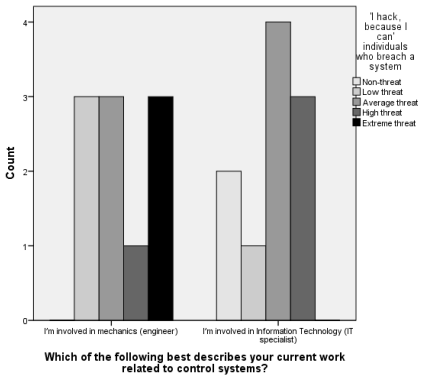


difference in perspective between the groups. Both groups assess the statement between 'average threat' and 'high threat'.



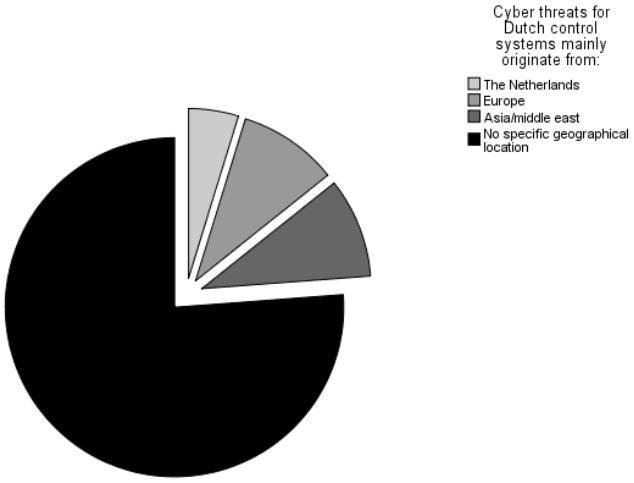
Question 30: 'I hack, because I can' individuals who breach a system.

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.246, **p = 0.279**]. *Remarks:* the outcome of this statement does not support a difference in perspective between the groups. The IT specialist categorize the threat lower than the Engineers (respectively 2.8 and 3.4). Due to the large standard deviation (respectively 1.265 and 1.135), the difference is not significant.



Question 31: Cyber threats for Dutch control systems mainly originate from.

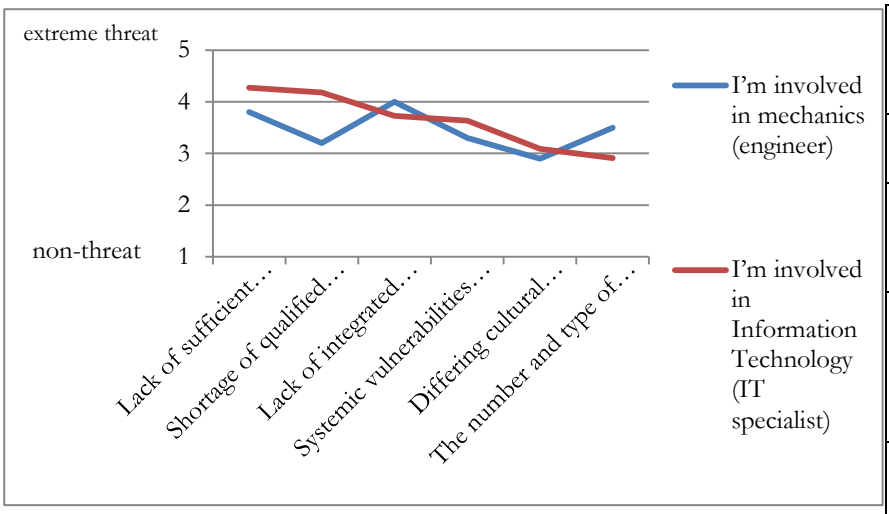
The respondents were asked to give their opinion on where cyber threats for control systems originate from. 85% of the respondents answered that cyber threats have no specific geographical origin. 9% says the threats mainly originate from Asia/middle east, 3% says Europe and 3% says the Netherlands.



Summary on 'Threat identification - external'

From the seven statements, two statements showed significant differences between the IT group and the OT group. The Engineers perceived hacktivism as a significantly larger threat, in contrast with the IT respondents group. Most threats were classified relatively high by both groups. Competitive Intelligence, State Sponsored Entities and Terrorism were all approaching 'high threat'. The two groups also significantly differed of opinion on the Internal Auditor. The IT group perceived these actors as a low threat, while the OT group classified it as an average threat.

6.2.5 Threat identification – people



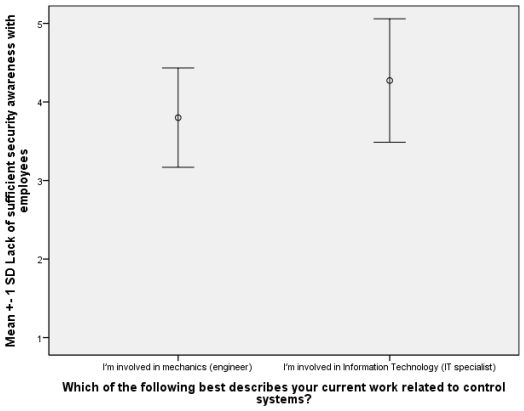
Lack of sufficient security awareness with employees
Shortage of qualified security personnel
Lack of integrated incident response training and testing
Systemic vulnerabilities (e.g. vulnerabilities inherent to the system of organizations and way-of-working)
Differing cultural perspectives on information security
The number and type of third parties that the organization interacts and does business with (e.g. suppliers, partners, or contractors)

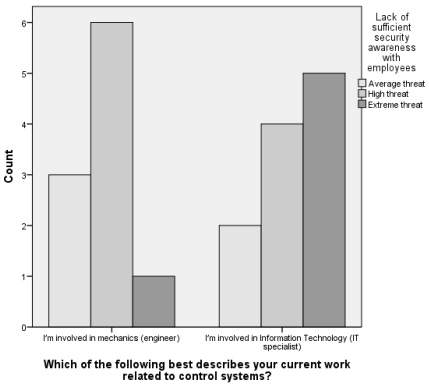
The fourth section of the questionnaire regarded the assessment of threats concerning people. Only the second statement has a significant difference between the subgroups. Generally the IT specialist and engineers agree on the threats regarding people.

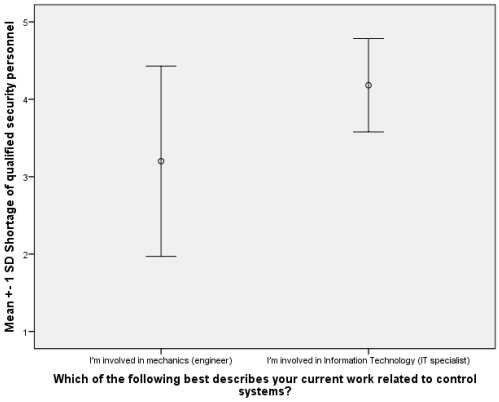
Question 32: Lack of sufficient security awareness with employees

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 2.274, **p = 0.148**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of both the IT group and the Engineering group are high, respectively 4.27 and 3.8. The standard deviation is limited, respectively 0.78 and 0.63. The results imply a mutual agreement between the groups on the gravity of the threat.



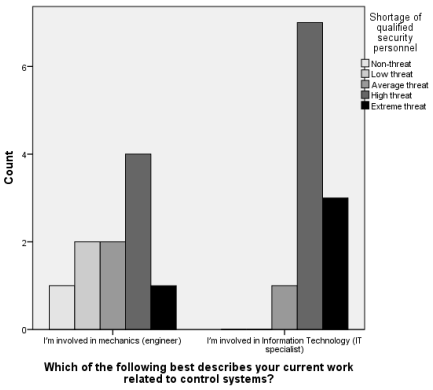


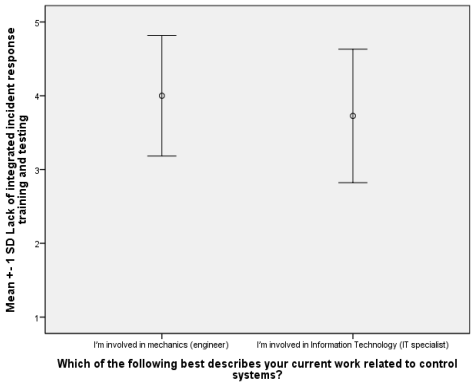


Question 33: Shortage of qualified security personnel

Significance: There is a significant difference between the two groups on the above statement [F(1,19) = 5.566, **p = 0.029**].

Remarks: the outcome of this statement does support a difference in perspective between the groups. The mean of the engineers is very close to 'average threat' on this statement. A difference with the IT specialists, where the mean of the respondents is classified as 'high threat'. The standard deviation is twice as large in the Engineering group (1.229 against 0.603). When considering the bar graph, 'the shortage of qualified security personal' is in both groups most often classified as 'high threat'.

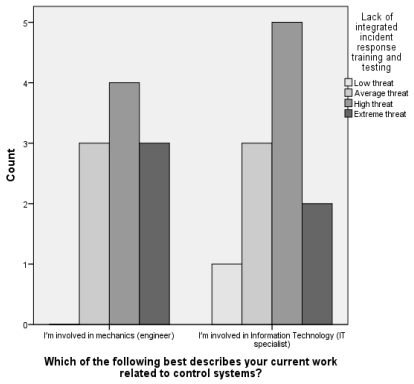


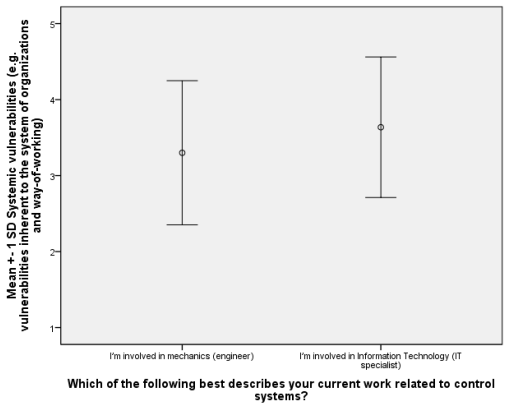


Question 34: Lack of integrated incident response training and testing

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.552, **p = 0.479**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. Similar to question 32, the means of the two groups are fairly high. 4.0 for the Engineering group and 3.73 for the IT group. When reviewing the bar chart, the most chosen classification in both groups is 'High threat' on this statement

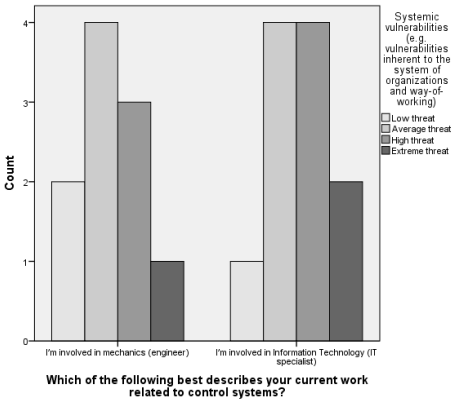


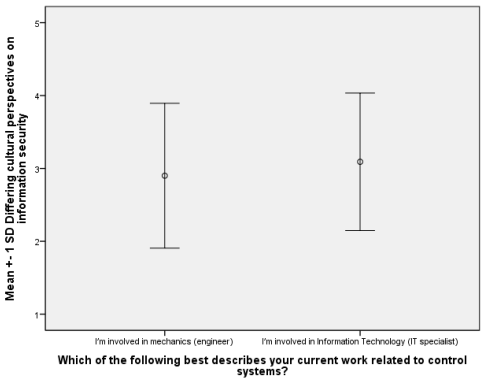


Question 35: Systemic vulnerabilities (e.g. vulnerabilities inherent to the system of organizations and way-of-working)

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.676, **p = 0.421**].

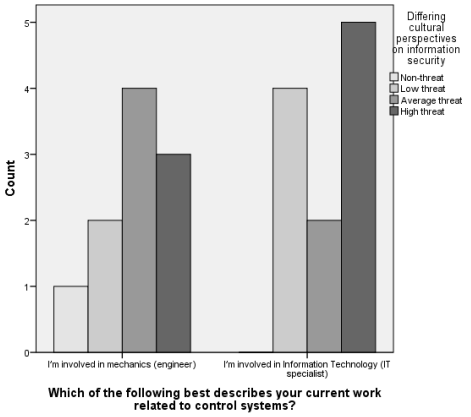
Remarks: the outcome of this statement does not support a difference in perspective between the groups. Both groups classify the statement between 'average threat' and 'high threat'. The bar chart also shows the correlation between the two groups; the groups have similar results.

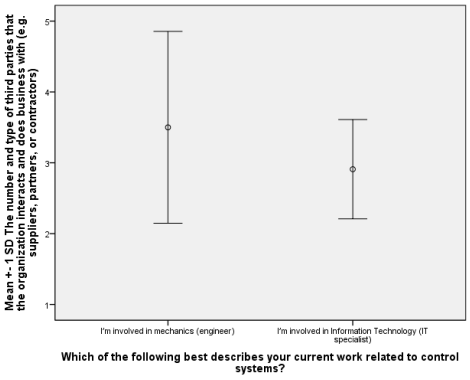


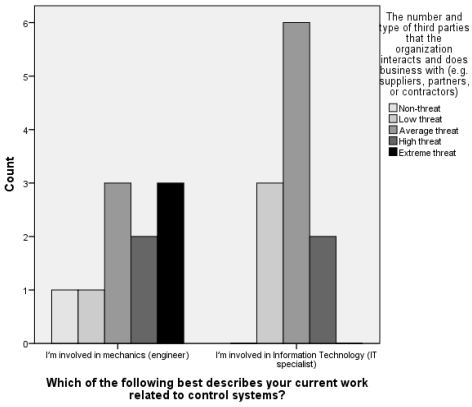


Question 36: Differing cultural perspectives on information security

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 0.204, **p = 0.657**]. *Remarks:* the outcome of this statement does not support a difference in perspective between the groups. The means of the groups are again almost equal. It is noticeable that the classification is quite low (2.90 and 3.09) which implies that the statement is not classified as an apparent threat.







Question 37: The number and type of third parties that the organization interacts and does business with (e.g. suppliers, partners, or contractors)

Significance: There is not a significant difference between the two groups on the above statement [F(1,19) = 1.623, **p = 0.218**].

Remarks: the outcome of this statement does not support a difference in perspective between the groups. The means of the groups differ from each other (2.91 and 3.50) but the standard deviation of the Engineering group is high (1.353) which impedes a significant difference between the groups.

Summary on 'Threat identification – people'

In this section, one out of six questions showed a significant difference between the groups. The IT and engineering group disagreed upon 'the shortage of qualified security personal'. The Engineering group classified the corresponding threat significantly lower than the IT specialist group.

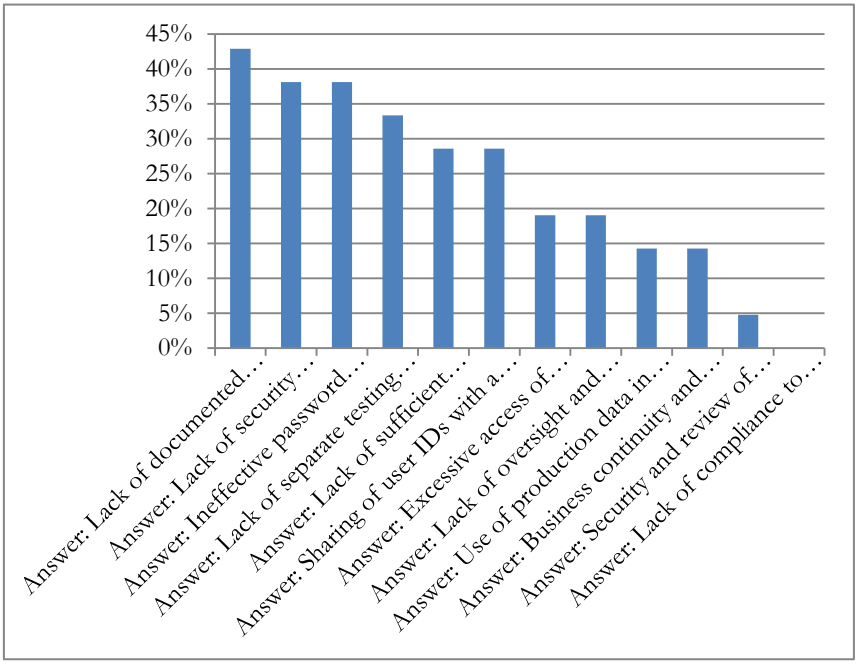
Some notable conclusions from this section:

1. Both groups have a high score on "lack of security awareness";
2. Both groups have a high score on "lack of incident response";

3. Both groups score low on the questions regarding the influence of cultural perspectives on security.

6.2.6 Audits, breaches and future

The respondents were asked which findings they would expect when an audit on their organization would take place. The figure below shows how big the percentage of the total respondents is that voted for a certain answer. The figure is categorized from large too small.



Lack of documented security policies and procedures
Lack of security awareness programs
Ineffective password management
Lack of separate testing environment
Lack of sufficient segregation of duties
Sharing of user IDs with a commonly known password
Excessive access of certain employees
Lack of oversight and compliance to security control requirements
Use of production data in testing
Business continuity and disaster recovery (lack of or non-current documentation, lack of testing)
Security and review of third party connections
Lack of compliance to privacy regulations

The respondents were able to choose 3 answers and could – if preferred – add an extra custom answer. We can compose a top 4 of findings where at least 30% of the respondents assigned their vote to:

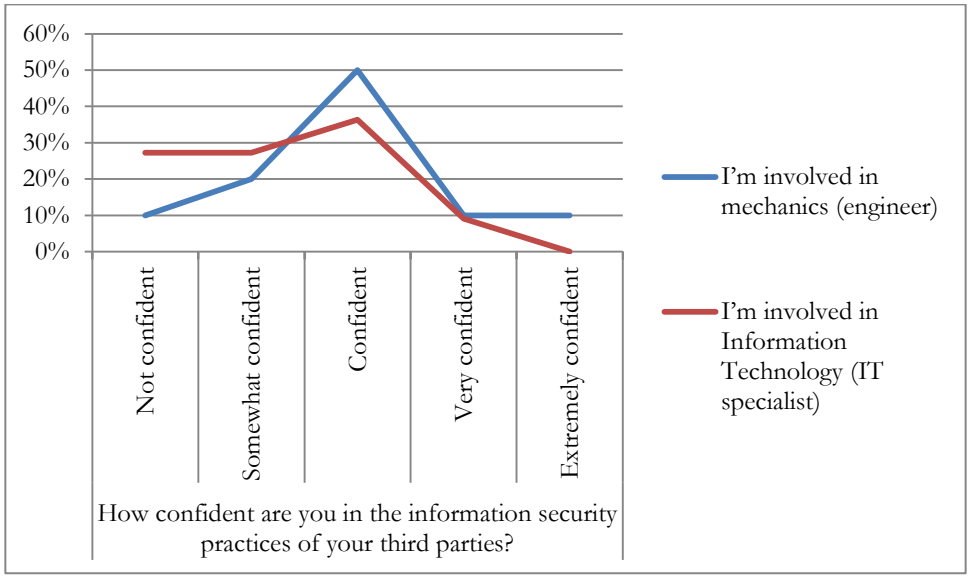
1. Lack of documented security policies and procedures;
2. Lack of security awareness programs;
3. Ineffective password management;
4. Lack of separate testing environment

The first three statements are self-explanatory, the fourth need some further explanation. Control systems in critical infrastructure are, with few exceptions, physical and live systems. The availability - from a time perspective - of these systems need to approach 100%.

Because control systems are physical and thus have no backup or copy (except for redundancy means), organizations who own these systems have no testing environment were patches and updates can be tried. Vendors of the control systems will thoroughly test the patches on factory machines, but this cannot guarantee the operators that these patches also will work without problems on their operational systems. In addition: even if the patches work, the control systems needs to be taken offline, which means downtime, which is not desirable.

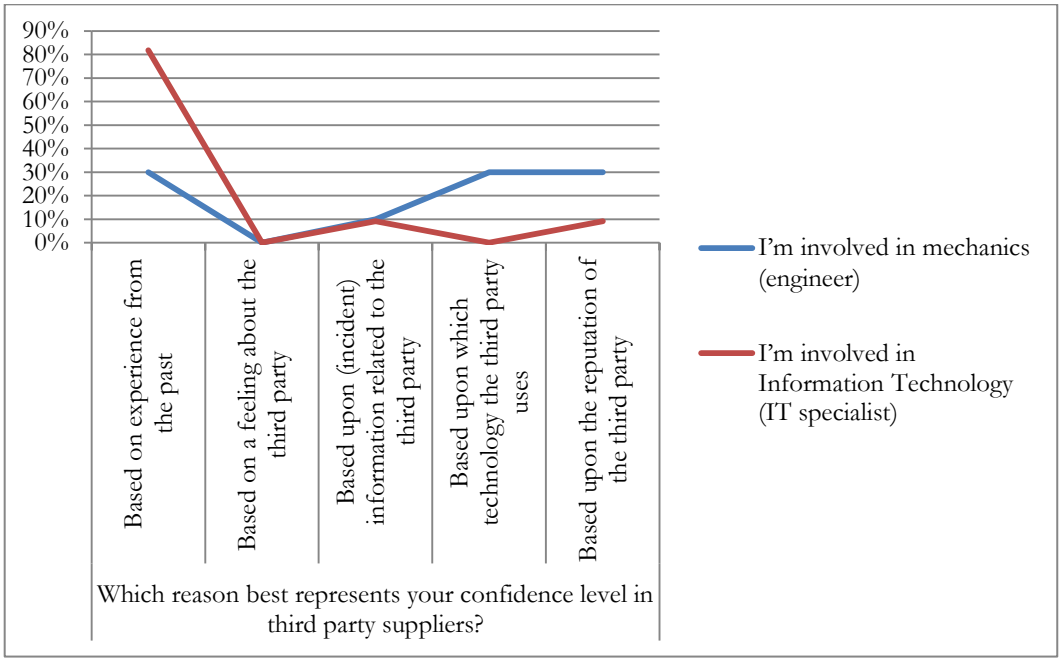
Confidence in third party practices

To analyze whether the respondents have confidence in their third party suppliers, the question in the figure below was presented to them. When comparing the means of the groups, there was no significant difference found between the opinion of IT specialist and engineers.



We posed a second question regarding the confidence of the security practice of third parties; asking where the respondents base their confidence on. The difference between the two groups was significant (P = 0,015). Predominately because 80% of the IT specialists indicated that they base their confidence on past experience, while 30% of the engineers have this opinion. On average, the engineers tend to look at the specific technology used by the third party and/or the reputation of the third party.

Both groups granted little value, regarding confidence to incident information of third parties. Implying that when a third party has had an incident in the past, this would not significantly damage the confidence of the respondents.



The difference in perspective

Difference in perspective?	Table N %
Yes	96,7%
No	3,3%

Question 46 of the questionnaire posed the following:

Do you think there is a difference in perspective on security between the engineer (mechanical) and the IT specialists (cyber)?

The response on this question was almost collective; 96,7% of the respondents answered that there is a difference in perspective on security between the two groups. Based on this result, we can argue that the people of both groups working on control systems recognize and acknowledge that there is a difference in perspective. The amount of people that said yes to this question is surprisingly high. The respondents do say that there is a difference, but when asked if they see a threat in the cultural difference (question 36) it scores lowest on the ranks (the groups agree). The apparent contradiction between question 36 and 46 is very important. The results from question 36 and question 46 seem to contradict each other. There could be logical explanations. First, the respondents agree upon the difference but expect no threat to arise. Second, the respondent interpreted the questions different. For example, cultural perspective are not interpreted as difference between IT and OT, but difference between geographical culture (Western and Asian)

6.3 Demarcations

The questionnaire has some known limitations. We discuss interpretation differences, issues with confidentiality, respondent group size and completeness of the questionnaire.

6.3.1 Interpretation

Three respondents sent remarks on interpretational issues of the questionnaire. Although there were only three respondents that sent remarks, we can expect that the issues could also be applicable for more respondents.

The first debated interpretation, regarded the term 'the engineer'. The questionnaire focusses on separating the viewpoint of engineers and IT specialist. For this to succeed, the respondent had to answer how he was educated and what his current occupation was. Thus, making it possible to differentiate between IT specialists and engineers in the analysis. The issue lies in explaining what is meant with 'an engineer' in the questionnaire. The engineer in the questionnaire was described as: "being involved in mechanics of control systems". On further consideration, this could better be indicated as "being involved in the operational or mechanical aspects of control systems". Mechanical as a term was not incorrect, but did not encompass the whole group of relevant engineers. Implications of the misunderstanding led some respondents to fill in their exact occupation at the 'other' field. To make the questionnaire more accurate, all entries where manually inspected.

The second issue regarded the term "system", which was used several times throughout the questionnaire. As also described in the questionnaire, system referred to "control systems or IT systems which are related to your everyday activities". Despite of the explanation, 'system' remains an abstract concept. Adding an example could have contributed to more understanding of what was meant by the concept. We believe that this issue had little influence on the outcomes of the analysis.

6.3.2 Confidentiality

Confidentiality, unexpectedly, played an important role in the questionnaire. While keeping security policies hidden from the public is an understandable thing to do, there was no compromising information asked from the respondent (only opinions and perspectives). Not able to participate due to the fact that security policies have to stay confidential is therefore not a valid reason. Due to the fact that employers had obliged several of the intended respondents with confidentiality contracts, they could not participate in the survey. It is possibly better for the organization to assess whether or not to participate in research, on a case-to-case bases. Rather than excluding research on security in general. This is not positive for the validity of our (and other) research as well as not sharing information is not

improving security practices and security understanding of the organization involved.

6.3.3 Generalization

As discussed earlier, the questionnaire allows us to compare results on different levels. First, on a generic level, where the results of all the respondents as one group are analyzed. Second, on the level of a specific category, where the results of two groups are compared with each other. Due to the relatively small group of respondents, the subgroups – engineer and IT specialists- are even smaller. This leads to the fact that the outcomes cannot be generalized to the population from a statistical point of view. This research intended to identify relations between several variables and see whether they showed clear differences. While not statistical generalizable for the whole population, the demonstrated differences are still interesting to base further research and ideas on.

6.4 Conclusions & reflection

The hypothesis, posed in paragraph 5.2.2, comprised the following:

> *When looking at cyber security for control systems, there is a difference in perspective on security between IT specialists and the engineers.*

The expectations in this research are partly met. The perspectives on security between IT specialists and engineers differ on 8 of the 37 statements (21%). In the following statements, significant differences between the groups were found:

- Question 5: Security alerts and security incidents are analyzed and remedial actions are taken.
  - Engineers scored higher
- Question 8: Our systems are not as secure as I want them to be, because it is too expensive.
  - IT specialists scored higher
- Question 10: Higher management levels are aware of security risks in everyday processes.
  - Engineers scored higher on agreement
- Question 11: Compliance (rules and regulation) is a good way of ensuring security and safety for control systems.
  - Engineers scored higher on agreement
- Question 15: Access to systems from a remote location
  - IT specialists found this a bigger threat
- Question 24: Attacks on control systems in the electricity network are used to protest against political activities (hacktivism)
  - Engineers found this a bigger threat
- Question 28: Internal auditors: penetration testers or vulnerability assessments which are done on control systems.

    - Engineers found this a bigger threat
- Question 33: Shortage of qualified security personnel
    - IT specialists found this a bigger threat

From our dataset it is not possible to subtract an underlying variable to explain why there is a difference in precisely these questions. In the next chapter, we review whether, according to the values drawn from literature, the particular outcome of the respondents group is a logical result..

Besides the questions where the IT and OT group had significant results, there were several questions with notable results.

- Question 14: IT specialists don't understand control systems (from an engineering perspective).
    - Both groups highly agreed on this statement
- Question 36: Differing cultural perspectives on information security
    - Both groups identified this as the lowest threat in that section of questions
- Question 46: do you think there is a difference in perspective on security between the engineer (mechanical) and the IT specialists (cyber)?
    - 96,7% of the respondents answered "yes"

As discussed in paragraph 6.2.6, the apparent contradiction between the answers of questions 36 and 46 was not expected. It is difficult to substantiate whether this results from interpretation issues or the fact that no threat is perceived on differing cultural perspectives.

IT and OT were asked to fill in which reason best represent the confidence level in third party suppliers (question 40). In the IT group, 80% of the respondents based their confidence on experience from the past. In the OT group, no clear answer came out. The respondent predominantly chose for experience from the past, the technology that is used by the third party and the reputation of the third party.

The respondent was asked to fill in what would be probable findings in an audit. No significant differences were found in the answers. The respondent could chose three statements. For the top three answers, at least 30% of the respondents chose the following three: First, lack of documented security policies and procedures. Second, lack of security awareness programs. Third, ineffective password management.

Chapter 7. Empirical implications

Goal of this chapter Discuss the empirical implications of the data

Relation to previous chapters Bring together knowledge from the literature study and data from the questionnaire

In this chapter the results from the questionnaire and the findings in literature are brought together, assisting in answering the main question:

> 'What are the differences in perspective on security between an IT expert and an engineer in the control system domain and how does this affect control system security?'

The main question is partly empirical and partly normative. In order to discuss and answer the questions, the empirical and normative parts are divided into two chapters. We answer sub questions related to empirical findings and reflect the empirical findings on the answers in this chapter. In chapter eight the main focus lies on the second – normative - part of the main question: "[…] how does this affect control system security".

7.1 Control systems and IT systems

The aim of discussing the sub questions is to complement and/or adjust findings of the literature study with findings in the empirical data. The first sub question reads:

> *How do the control systems operate and what are the most important control systems and IT systems in the electrical grid?*

Operations

Control systems in the grid domain have three relevant layers: the SCADA layer, the control layer and the instrumentation layer. These three layers together represent the operational network. The SCADA system gathers data and sends operational commands to the local controllers in the control domain; the PLC's and RTU's. These control systems adjust or maintain processes by managing the instrumentation layer. In this layer the actual data gathering takes place with sensor equipment. Besides these monitoring instruments, also controlling instruments belong to this domain. This entitles mechanical instruments like valves and pumps.

IT networks enable communication between systems, equipment and networks. For the electrical grid, IT systems manage and support the activities which are vital to the grid. In the electricity domain, two IT infrastructures can described: the Business IT Network and the Operational IT network. While the Operational network is used to enable the control system communication, the Business IT network enables the administrative and support activities.

Most important systems

When answering the sub questions, we are looking for the "most important" control system or IT system. This is subjective and difficult to answer question. We can however, assess the question from a security perspective: where do the vulnerabilities arise? Based on the literature, we can conclude which aspects are classified as 'vulnerable' or 'critical'. In literature we found critical issues on:

1. Integration of systems and networks;
2. Technical and physical limitations, and
3. Differences in perspectives.

With the integration of systems and networks, the operational network is exposed to connections from outside the 'secure' perimeter. When combining this new exposure to risk with the technical deficiencies related to security of the equipment, it is understandable that the number of vulnerability issues increase rapidly. In the questionnaire, the respondents classified the access from remote locations as one of the highest ranking threats of the questionnaire. Almost equal with the question of making prior isolated control systems available to the internet.

The questionnaire was focused on researching a difference in perspectives. The first and second issue that were found did not relate to a differences in perspective, therefore the reflection on these the issues is not extensive. Issue three 'differences in perspective' is discussed in the next paragraph.

7.2 Perspectives in literature & questionnaire

A significant part of this research focusses on analyzing the differences in perspectives between two groups. The accompanying sub question is as follows:

What are the differences in perspective between IT and OT specialists?

Differences in perspectives refer to the values were the two groups differ in their opinions. In the literature the analysis of the differences in perspectives is done on a fairly high level;

indicating the values of a whole group. In the questionnaire, the difference in perspectives are analyzed on a very low, individual-statement level. This provides one big advantage and one big disadvantage. On the one hand, the comparison of groups on low level statements offers a good insight in the operational/practical implications of a shared value in a group. On the other hand, the statements – which are often low level/practical statements – are difficult to relate to the high level values that are found in the literature (the SRA and CIA values).

Perspectives in literature

In the literature significant differences in perspectives between the OT specialist and the IT specialist can be found. Where the OT specialists are involved in the design and operation of systems that have a high physical interaction: the systems can significantly impact the real world. Requirements as safety, reliability and availability (SRA) are valued as the most important design criteria. The IT specialist - or (cyber) security specialist – in general has a different set of requirements than the OT specialist. The criteria that are valued by the engineering community are: Confidentiality, Integrity and Availability (CIA). In the literature, these criteria are reoccurring and seem to be dominant in securing the systems and networks (paragraph 4.2).

As became apparent from the literature review of Von Meier (1999) and Leidner & Kayworth (2006), perspectives are formed and maintained by the values of a group. The shared values of a group can originate from their environment, occupation, cultural background and so on. Consequently, these shared values influence the perspective on problems, ideas and solutions. Implicating that people with different perspectives will consequently have different perspectives on problems, idea's and solutions. The goal of the questionnaire was to verify whether different occupation result in differences in outcomes on the statements.

Values in questionnaire

In the questionnaire, the respondents were asked to assess 36 statements on a Likert scale. In 8 questions a significant difference in outcome was found. We analyzed whether a relations could be found between the questions that had significant difference between the groups. For example: when six of the eight questions had 'security' as common subject, there would be a clear common variable. After reviewing the values from the literature study (SRA and CIA) on these questions it seems difficult to argue, without making assumptions, that these questions have an underlying reason which explains why a difference in opinion between groups is found on precisely these questions. Based on the questionnaire, we cannot substantiate an exact answer to the sub question "*What are the differences in perspective*

between IT and OT specialists?" The questionnaire only demonstrates that there is a differences in perspectives between the groups in 21,7% of the statements.

7.3 Threat perception

When it comes to the identification of external threats, the only significant difference between the IT and OT group regard the threat of hacktivism and the threat of internal auditors. IT specialists value both of these threats significantly less. This could be explained by different theorems:

1. There is an information asymmetry (understanding) between the IT and OT specialists on these threats, which results in differently perceiving threats;
2. The threats affect different values and are therefore more important for the group whose values are affected. For example: both the threats can inflict direct damage to the operations, for which the OT specialist is responsible. Therefore the OT specialists perceive the threat higher;

When taking the mean all the respondents in the external threat section, a top three threats can be composed. Terrorism is referred to as the highest threat. Surprising, because there is no actual (declassified) information which points to any incidents in the control system domain as terrorist acts. It is conceivable that media coverage on terrorism plays a role in this opinion. There is a large body of literature on the effects of media coverage of terrorism on people (Shoshani & Slone, 2008) (Weimann, 2003). One of these effects is the influence of the media on the threat perception. The threat perceptions have an influence on the behavior. For example, persons who perceive a greater general risk of attack are less like to use public transport (Goodwin, Willson, & Stanley Jr, 2005). It is possible that threat perception for control system security is also influenced by press and opinion makers. The gap between perceived threats and real threats is important for risk management, implications are elaborated in paragraph 8.1.

Second highest threat according to the respondents was hacktivism. In 2012, the control systems industry was targeted numerous times and some of the hacks could be related back to activism (Krebs, 2012). According to the National Cyber Security Centre (NCSC), hacktivism is most of the times not deemed serious. Often only defacements – changing visual appearance – or denial of service attacks are carried out by these entities (Bronk & Tikk-Ringas, 2013). According to the NCSC, one of the most pressing threats from a general cyber-security perspective is corporate espionage (PVIB conference, 2012). The NCSC does not specifically reflect this threat to the energy domain, whether this is also the most pressing issue for the energy industry remain the question. In the questionnaire,

corporate espionage was valued the third highest threat. Corporate espionage is focused on retrieving (confidential) information and is not focused on interfering with the control systems. In theory (although the systems are compromised) there should be no intention of the hacker to interfere with the operational environment.

7.4 Vulnerabilities

Overall, the respondent agreed upon the fact that there is a lack of sufficient security awareness with employees. The IT experts found the lack of qualified personal, an average, a more pressing issue. But the difference between the two groups was not significant. Surprisingly, the respondents groups did not agree with each other that there is a lack of qualified security personal. On average, the IT respondents identified the lack of qualified personal as a big threat for the continuity of their organization. While the Engineers scored, on average, a whole step down and qualified it as a mediocre threat. A recent study of ICS2 confirms the threat of having too little qualified IT security personal. The shortage of skills is projected to be a direct perpetrator of incidents and breaches (Dark Reading, 2013).

7.5 Responses to risks

While the vulnerability identification also delineated that people are contributing to security issues, people are also a leading factor in the risk tolerance domain. The risk tolerance domain consists of two parts: risk mitigation options – or strategies if you will - and the organization's risk appetite.

There are five common strategies for risk mitigation: design the risk out, reduce the risk, accept the risk, transfer or share the risk and eliminate or redesign ineffective controls. Depending on the threats that are identified, the vulnerabilities that are found and the value at risk, an organization can determine the amount of risk it is willing to take (the risk appetite). We must delineate that these kinds of strategies are only valuable when a solid risk assessment is carried out. Without a good understanding of the vulnerabilities, threats and possible responses, it is only guessing.

The questionnaire did not contain direct questions on organizational risk appetite. Yet, it could be possible to subtract from the questionnaire how much risk the respondents (employees) are willing to take.

In the questionnaire we asked the respondents two questions related to risks. These risk regarded the awareness and the accessibility of the management.

> Question 10: Higher management levels are aware of security risks in everyday processes;
> Question 13: From my current function I can easily reach higher management when I identify a risk;

The engineer and the IT specialist did differ on the first matter. The average of the engineers was around 'Agree', while the average of the IT specialist was between disagree and neutral. Both groups did agree on the statement that higher management is easily reachable when risk are found. In the questionnaire, we reflected two questions on compliance:

> Question 12:Compliance based security leads to regulations that not necessarily contribute to security;
> Question 11: Compliance (rules and regulation) is a good way of ensuring security and safety for control systems.

There was no significant difference found between the groups on these questions. The mean of question 12 approached 'disagree'. Question 11 had 'agreed' as mean. Based on this, we can argue that the respondents find that compliance-based-security supports their security practice.

In the questionnaire, there were no questions about community aid to ensure control systems security. During the search for respondents we had several responses regarding difficulties sharing information about security policies. We can argue that security is (and probably will) remain under some sort of veil. It is a valid reason for organizations not to share all their knowledge, settings, practices and equipment with the outside world because this will enable bad guys from exploiting this knowledge.

7.6 Remarks & completeness of the questionnaire

Several remarks about the content were made by respondents. Mostly regarding minor improvements of statements. Yet, one respondent seemed to not agree with the questionnaire as a whole and posed the following:

> "I did have a look at your questions and I can tell there is no difference in paradigm between IT and engineers, there is simply a lack of knowledge what cyber security really means." (Quote made anonymous)

While the respondent theoretically could be right – that there is in fact no difference in perspective between the IT specialist and engineers and they perceive threats, vulnerabilities and risks in the same manner -, still the respondent argument is incorrect. He argues that the issues in securing control systems do not originate from the differences in profession, but

the differences of what the people understand about security. We would argue that the respondent skipped the step of professional education and occupation and did not account for the fact that professionals learn to think from their own values, often related to the subgroup that they belong to (as explained in paragraph 4.4.2: Conflicting cultures). Giving all groups have an understanding of what cyber security is, still they could interpret the vulnerabilities, threats and risk differently because they interpret it from their own values.

Concerning the correctness, one remark was posed by a respondent. The respondent argued that question 1.23 needed amendment. This statement regarded 3th party security solutions: "Vendors don't allow third party solutions for security". The respondent posed:

> "Vendors do use 3rd party security for example; Honeywell, Invensys and others use Tofino Firewalls in fact they "badge" engineer their own versions." (Quote made anonymous)

While this is true for many organization involved in control systems, yet different control systems vendors are known to suspend the warranty & support when alterations to the equipment are made. In this specific question the respondents are asked to evaluate the threat of the statement. While it is likely that users of Honeywell and Invensys, do not perceive this threat, non-users may see a threat due to the fact that support for the systems is suspended.

One of the limitations of a questionnaire is that it cannot be too time consuming for the respondents. The most relevant topics for this research were integrated into the questionnaire. Of course security of control systems is not limited to the questions in the questionnaire.

Additional answers

Two respondents added an extra answer. Discussing these additions gives some insight in their thoughts. One of the respondents added "Lack of proper patch management process". This is a valid answer, and should – with hindsight – have been included in the questionnaire. Patch management was a bit underexposed in the questionnaire, while it is an important aspect of control system security and was/is expected to raise conflicting values between the groups.

The second additional answer that was added by a respondent was not specifically applicable to this question, but is still valuable: "Priority: production is secure or not secure. Every security wall you build is a delay and disturbance for smooth production." This being argued from an operational perspective, every additional measure could indeed delay production. Under the current conditions (and even more in the future), security measures are necessary:

what if there was no security and the system would be terminated by unauthorized entities. This would delay and disturb the production even more than regular or additional security measures. Derived from the respondents comment, he strives to minimize security (and still be secure) so that the influence of security on production is minimized. It is difficult to determine when a production process is secure enough or not. With the risk framework, discussed in chapter eight, a risk based analyses can be made to determine whether a control systems are at risk.

7.7 Concluding on data & literature

We can conclude that there are technical issues on one hand and conflicting perspectives between the expert groups on the other hand. The technical issues originate from the difficult replaceability of control systems: amongst others other factors, high investment cost and the necessity to keep the availability as high as possible play an important role. The time a control system is in operation, referred to as the component lifetime, ranges from 15 to over 50 years. This implies that a significant amount of the equipment needs to be adapted (often not replaced) in order to meet the connectivity and intelligence requirements. Besides the before mentioned technical issues, the human factor plays a vital role in the IT/OT integration. In essence, the operational systems are brought out of isolation and consequently need to be secured. Securing the systems is even more important due to the fact that the SCADA and control systems are often part of critical components. To accomplish secure control systems, the IT expert group and the OT expert group are bound to work intensively together. Based on the literature as well as the questionnaire, we can argue that the differences have an impact control system security. A difference in perspectives could have a significant impact on the advancement of the grid infrastructure and, in particular, could have an impact on cyber vulnerabilities resulting from conflicting values. The values that people have, determine to a certain extend the way things are interpreted. Ideas and opinions on the effect of the difference in interpretation is discussed in the next chapter.

Chapter 8. Normative implications

Goal of this chapter Discuss normative implications and reflect opportunities & ideas
Relation to previous chapters The implications and reflection is based upon the knowledge of previous chapters

In this research a two folded analysis has been done: first, an analysis on the state of affairs in the control system domain and second, an analysis of the influence of different perspectives on control systems security. While combining the literature and questionnaire has been done in the previous chapter, this chapter reflects the findings to implications various kinds. The sub question relevant for this chapter reads:

> What are the consequences of differences in perspectives on risk management for control systems in the electrical grid domain?

This chapter focusses on three things:

1. Reflect the implications of a difference in perspective on a risk framework. The knowledge collected and gained in this research is reflected on a risk framework. The influence of people is key in this reflection.
2. Reflect the differences in perspective on other domains outside the electricity domain.
3. Reflect on the 'new' content. In the research period, ranging from September 2012 until April 2013, control system security gained increasing attention of media, hackers and organizations. The attention resulted in many new trends, ideas and readings by people inside and outside the domain which can be relevant for control systems security.

8.1 Risk and the influence of people

The framework is a combination of The World Economic Forum 'Cyber Security Risk Framework' and the ISA contextual model "information security assurance and threat-risk assessment". The risk control framework is introduced in paragraph 4.5 and holds the five segments: threats, vulnerabilities, value at risk, risk tolerance and responses. Every segment of the risk framework is discussed based on what we know, what we expect and how this

influences the risk framework. Hereby, keeping the influence of the differences in perspectives in mind.

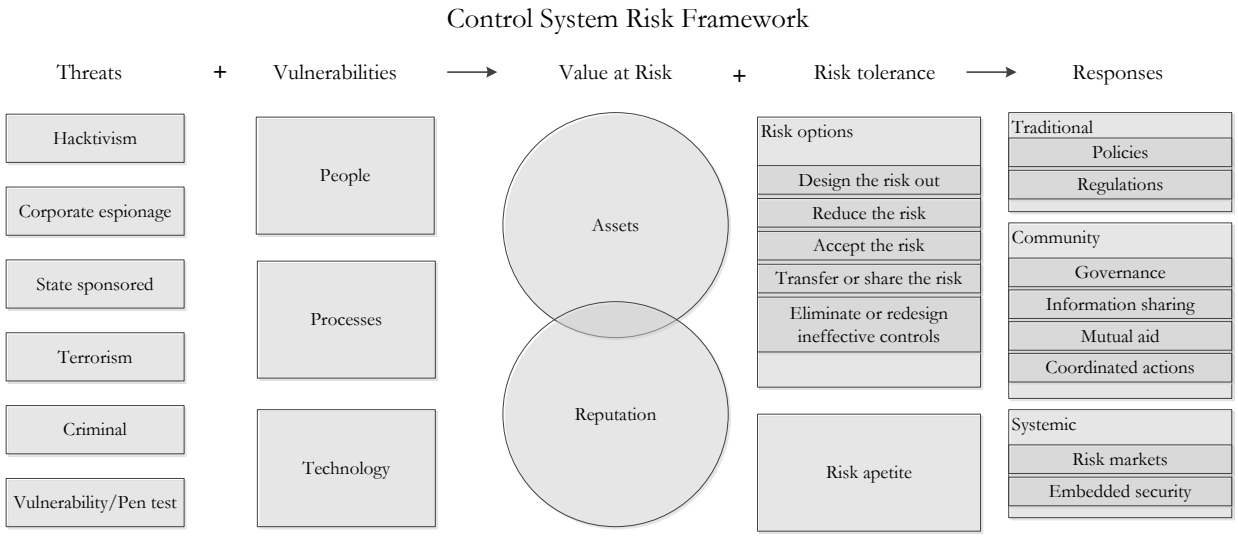


Figure 26: control system risk framework. Based on (ANSI/ISA, 2007), (World Economic Forum, 2012)

8.1.1 Threats

The people working in the cyber security domain are aware of the threat actors, the classification of threat actors and what their intentions are (paragraph 4.5.3). These threat actors vary to a great extend from each other in (financial) means, skills and goals. How the threats actors consequently are perceived is interesting. This is not always based on empirical evidence on (financial) means, skills and goals. Also media can influence to a large extent on how a threats are perceived (paragraph 7.3.1).

The 'Perceived Threat' - what does an organization or any individual perceive - and the 'Real Threat' - what is the actual threat - are difficult concepts. For an effective approach in dealing with threats, the perceived threat and the real threat have to be aligned with each other. The alignment is difficult, if not impossible, because it requires objectively assessing threats. When threats are not accurately estimated, the expenditures and the actual benefits from the attempts to minimize the threats are not cost-effective (paragraph 4.5.4). It is therefore in the organizations best interest to actively try to minimize the gap between perceived threat and real threat.

Occupation can be seen as a gathering of experience and knowledge on a specific topic, which leads to a set of shared values, which implies a group perspective or paradigm. Precisely because it is so important to minimize the gap between perceived threat and real threat, it is of importance that the different groups – IT and OT in this case – have shared

values up to a certain extend. When having shared values, this would imply that there is understanding, agreement and acceptance on how threats are perceived (paragraph 4.6). Yet, to a certain extent a different perspectives on threats can be beneficial. Discussion related to differences in perspective on threats can ensure a better balanced solution (paragraph 4.4). Differences in perspectives keep organizations aware, but when the differences are too big it will restrict the organization in properly dealing with threats. .

8.1.2 Vulnerability identification

The vulnerabilities in control systems in the electricity domain arise from technical deficiencies and people related issues. People are believed to be a high risk factor when it comes to securing the automation industry. According to ICS CERT people are a liability to control system security, primarily because of a combination of three things (ICS-CERT, 2012):

1. Lack of understanding of the overall security risk to control systems;
2. Technical and security impacts of inadequate security policies or implementation is not considered;
3. Lack of cyber security skills to ensure protection against cyber-attacks.

The understanding of control system security has to extend from the operational activities, all the way to the management. It has been pressed many times; lacking security awareness can cause problems. For example: issues can be overlooked on an operational level and necessary investments in security are not made from the strategic level. Currently, organizations try to increase security awareness by training, compliance and integration teams. These integration teams are an increasing technique to overcome, amongst others, awareness issues. The IT/OT integration teams contain people with both the operational and IT perspective, and have as objective to support, educate and advocate shared values in an organization (paragraph 4.5). The influence of conflicting values between SRA and CIA should be a more integral part of the awareness programs. Only factual knowledge to ensure awareness is not enough to cover the people side of cyber security.

From a technical point of view, there are various aspects that cause issues: security was not a design criterion, use of legacy systems, long system deployments, component lifetime, patch management, technical requirements and so on (paragraph 4.3). Although 100% security does not exist, everything attached to the internet can be hacked (World Economic Forum, 2012). Still, with the current technological solutions to improve control system security a lot can be done. Solutions as firewalls, unidirectional gateways, restricted access and isolation are possibilities to secure systems from a technical point of view. However, people play an

important role. People decide which security products are bought (management) and people have to implement, operate and maintain security measures (IT specialists). The people who are active on the operational level have a significant influence on security. A recent article on network segmentation illustrates the required commitment from employees on the operational level. In the research among firewall administrators, more than half argued that firewall-rule-change-management is putting the organization at risk to be breached. The administrator of an enterprise needs to manage "hundreds of thousands to even millions of firewall rules settings on a daily basis" (ISSC, 2013). These firewall settings need to be created, monitored and adapted by people. Besides the required commitment from people, the example is also illustrative for the differences in values between two groups. For the IT specialist, firewalls are an essential contributor to security. Operational experts can be weary in the use of firewalls because it can obstruct operational traffic and cause downtime. The contradiction here is: isolation offers security; for isolation strict firewall rules are necessary; firewall rules can cause downtime because they block operational traffic.

8.1.3 Value at Risk & Risk tolerance

Value at risk is an essential step in the risk assessment. Depending on which type of risk assessment is chosen (quantitative, qualitative or hybrid), a certain arbitrariness is involved: people have a decisive role. The arbitrary factor is lowest in a Quantitative Risk Assessment, where monetary values are calculated for every asset. Yet, after a monetary value is assigned the importance of the asset has to be assigned. Value at Risk is not extensively discussed in this research because these assessments are mostly strategic decisions. The differences in perspectives between IT and OT are of less importance in these assessments.

Similar to the 'Value at Risk', also the risk tolerance is for a significant part determined by management. What are acceptable levels of risk and how much risk is management willing to take (risk appetite). Risk appetite is very low at organizations involved in critical infrastructures due to the availability, safety and reliability requirements. The employee's personal perspective is one of the variables that influence the way organization handles risks. In the top as well as at the bottom of an organization different perspectives play a part in risk tolerance. Two issues arise from the influence of perspectives. First, differences in perspectives could steer strategic decisions in different directions. Second, when the people at the bottom of the organization (operational) have different values as the top level, they might interpret issues from their own values (principal-agent problem). It can therefore be beneficial when the strategic decisions are in line with the values of operational experts and IT specialists.

8.1.4 Responses

Response to risks can be categorized into three aspects: traditional, community and systemic response. In this paragraph individual response to risks is discussed as well as higher level strategic response.

Traditional

The European Union announced a Cyber security strategy and proposal for a Directive early February 2013 (European Commission, 2013). Before the end of 2013 the EU is planning to propose legislation to assist Member States in their cyber security defenses. The EU is of the opinion that cyber security needs to be handled from European level and be transposed to Member states. Because cyber related issues cross borders easily, this approach seems to be logical. Realistically, there is a danger of falling into "compliance versus security", where organizations only focus on being compliant and not necessarily on being secure (see paragraph 4.4.1). European legislation contributes to this threat as it increases the amount of legislation. When taking into account the fact that compliance is a generic understanding: the same compliance rule and regulations are not blindly applicable for every organization.

We come to the conclusion that the European Union is lacking behind on the United States when it comes to control system security. Mainly because the amount of detailed literature which the National Institute of Standards and Technology (NIST) and the Department of Homeland Defence publishes. It seems that ENISA (EU) and NCSC (NL) are currently more focused on the strategic level than on a practical – knowledge sharing- level. Possibly, the USA anticipates better on the control systems domain due to easier implementation of legislation. In the European Union, it seems that the time from problem identification to actual output is taken significantly longer, but this is only a theorem.

Community

The community response is about information sharing, mutual aid, coordinated actions. In this paragraph some examples of community response to improve control systems security is discussed.

The American nonprofit consortium EnergySec was one of the first organizations that work with energy companies to improve security. Their mission is to "Strengthen the cyber security posture of critical energy infrastructures", which they pursue by sharing security related information (EnergySec, 2013, p. 1). Another example of innovative knowledge sharing is real-time knowledge sharing. According to the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), real-time information sharing "among academia today is saving many millions of dollars and actively stopping

attacks in progress" (Blask, 2013). According to the industrial control systems department of REN-ISAC, real-time information sharing can significantly improve control systems security. By forming a network that connects actors and identifies new active threats a "distributed immune system" is created (Blask, 2013, p. 1). When an attack is active somewhere in the network, all other parties are informed and can act accordingly.

In the community based approach, wisdom of the crowd has a significant role; a large group of professionals know more than a smaller, more exclusive group of professionals. The focus lies on sharing information and supporting other professionals to improve. There is some criticism on the community based approach, especially from the traditional approach. The criticism entails the difficulties on two aspects:

1. How can be ensured that the information available to the professionals is shared? The professional can chose the listen, but is not obliged to share his own information. This could be for various reasons (i.e. economic or personal);
2. Making information public can lead to additional issues in securing control systems. This reflects onto two things that are discussed earlier in this paper. The idea that hackers have unlimited time to spent on attacking the systems, while the company security professional are constrained by time. Second, security by obscurity is not an option when making vulnerabilities and vital information known to the public.

In the community approach, a separation between sharing best practices and sharing vulnerabilities has to be made. Regarding sharing vulnerabilities, a discussing is currently going on about Responsible Disclosure that is relevant to the criticism on the community approach. The central question posed in this discussion revolves around what would be the right manner to address vulnerabilities before mischievous people use the vulnerabilities. The current standpoint of the Dutch leading institute on this point, the National Cyber Security Centrum (NCSC), states that "*the amount of links between the person that discovers the vulnerability and the organization that has to resolve the vulnerability*" (NCSC, 2013, p. 1). Sharing vulnerabilities directly with the public is a no-go for the NCSC, which can lead to prosecution. The community approach is therefore more focused on sharing best practices. The World Economic Forum states the following on sharing knowledge: *"mutual aid or coordinated action so that every stakeholder can mitigate cyber risk and contribute to a safer cyber environment"* (World Economic Forum, 2012, p. 14).

Systemic

The systemic response has two aspects: risk markets and embedded security. Risk Markets is indicated by ENISA as a 'prevention-focused cyber insurance market' (ENISA, 2012). It concerns achieving to put true cost on cyber incidents, hereby consequently showing the

benefits of implementing good security practices. For now, risk markets are hypothetical. Eventually, it should work similar to the car insurance, house insurance or health insurance: when costs of incidents can be mapped and quantified, more can be done on prevention and reduction of the impact. The cyber insurance market is currently non existing because there is not enough robust data, it still uncertain what risk is being insured are and the difficulties predicting future losses from past events (ENISA, 2012).

The second aspect van the systemic response is embedded security. Embedded security refers to security-by-design of control systems. In this research several aspects of embedded security are discussed: the non-existing embedded security of legacy control systems, the new technologies of securing legacy control systems and the embedded security in the control systems currently sold. The first aspect is primarily focused on identification of issues, the second and third are reflecting solutions. We identified that the market for secure control systems is developed. One of the market leaders provides only control systems with built in security possibilities. The configuration and deployment of the systems, when it comes to the security, is still dependent on people. Awareness and education plays an important role here.

The last aspect of systemic response to ensure control systems security is understanding and working towards a shared perspective on security. The risk framework should give some guidance in estimating the threats, vulnerabilities, value at risk and the responses. What is important to keep in mind: every idea, problem, decision and solution can be tainted by interpretation. Depending on the perspective of a person or a group of persons, the perception of an idea, problem, decision and solution can differ. Therefor a shared perspective on security between, in this research, the IT specialist and the engineers is important.

8.2 Applicability to other domains

The electricity sector is a domain where society is directly and often seriously affected by a distortion in the supply. Because of the relevance for society, this research focused on control systems in the electricity domain. Yet, the IT/OT integration - bringing control systems out of isolation - is not confined to the electricity sector. When looking at the reasons for such a change, we can look back at paragraph 1.2 where the reasons for change in the electricity infrastructure were summed up:

1. Activate demand response at client side. Motivates and includes the consumer;
2. Better incorporation of decentralized generation and storage in the electric grid;
3. Stimulate the development of new products, services and markets;

4. Maintain and improve the existing services efficiently;
5. Limit or postpone investment in the infrastructure;
6. Maintain or even improve the existing high levels of system reliability, quality and security of supply; and,
7. Significantly reduce the environmental impact of the whole electricity supply system

The reason to make control systems smarter are not limited to these reasons, but if gives a comprehensive image. 'Maintain and improve the existing services efficiently', could also be applicable for to other sectors. Take for example the gas, water and (heavy) industry. We can pose the following questions: why is the electricity sector one of the leading sectors in the transition, what can be expected and learned for the other domain regarding a transition and could the other sectors encounter similar issues regarding differences in perspective between IT and OT?

It is speculation as to why the electricity sector leads in this area, but literature gives some idea as to why:

1. Consumer contact is very high in the electricity domain (paragraph 2.2.3). Consumers expect more transparency, information and interaction. In this manner accelerating innovation;
2. With information gathering and active steering (a more intelligent grid) efficiency improvements can be made which can decrease costs. (paragraph 2.1)

These two reasons indicate important drivers behind the IT integration in control systems. When transposing these drivers to other sectors, the consumer interaction is will be mostly less intensive because consumers are actively interacting with the electricity infrastructure. For in (heavy) industry is seems likely that consumers will be less important drivers for innovation. Yet efficiency and costs considerations are more applicable. The trend in the electricity domain of increasing transparency and information supply towards consumers leads to believe that gas and water cannot stay behind. In the coming years it is likely that the operators of these infrastructures also increase their expenditures on intelligence in their infrastructure.

The third question - could the other domains encounter similar issues regarding differences in perspective between IT and OT – refers to the conflicting values between groups. For the electricity domain it was fairly clear that securing the control systems (the IT group) could impede the operational availability (the OT group). For gas and water domain, the timing requirements and the availability requirements are less critical. Mainly due to the fact that gas and water can both be stored easily, which gives some benefits.

In (heavy) industry and production facilities, downtime of production is very costly. In theory this is a similar situation as in the electricity domain. Also business network and corporate network are increasingly more often connected (data is flowing from operations to business and the other way around). When bringing these industries and facilities more and more out of isolation (connect them via the operational network and the business network to the internet), the need for securing the enterprise increases, the pressure on IT specialist not to interfere with production increases and conflicting values between IT and OT will increase.

8.3 Final thoughts and further research

In the closing paragraph of this research, some thoughts on control system security and ideas for further research are elaborated.

Insecure systems, yet reliable systems

Why has the critical infrastructure in the electricity domain such a high reliability? Judging from the literature, there are several technical and human issues which could cause unreliability or disturbances. Yet, the control systems in the electricity grid seem cope all right the increasing intelligence and connectivity specifications. Further research on this topic, similar to the research on reliability of Mark de Bruijne (2006), would be complementary to the existing literature.

Future scenarios of shared values

We assume that companies are rational and want to decrease apparent vulnerabilities that can endanger the continuity of the organization. A relatively easy way to decrease conflicts between groups is education and communication. When decreasing conflicts, it is likely these means are deployed first. Communication is reckoned to be of vital importance when it concerns overcoming the issues related to contradicting values. The IT/OT integration in control systems and the subsequent security issues can develop into three different future scenarios:

1. *Separate values and minimal communication.* Decision makers from the IT and OT domains do not see the need or ignore the need for intensive communications between experts. Logically, minimal communications ensure that shared values are not likely to arise;

2. *Separate values and intensive communications.* There is a general consensus that communications and increased understanding of each other's values is of

importance. Intensive communications comprise (awareness)training and education;

3. *Shared values.* When both groups understand, agree and adopt the same set of values, the organization has a shared perspective.

When recognizing the possible future scenarios, the ability to steer towards a desired end state becomes an option. For this, one vital question has to be answered: when does the tension between contradicting values become dysfunctional? Based on the previous sections, it can be argued that a shared perspective is – to a certain extent - desirable. When values significantly differ, the security of control systems is expected to suffer. Somewhere on the spectrum from 'contradicting values' to 'shared values', there is an area that utilizes the tradeoff for a company between investment and risks.

The desirability of a shared perspective

As described in this research, different perspectives on issues and solutions could also contribute to the security of control systems. So how desirable are 100% shared values? We would argue that separate values and intense communication between groups would be preferred scenario. The first scenario - *Separate values and minimal communication* - is bound to cause conflicts, in the third scenario - s*hared values* – the critical opinion would be lost. During the World Economic Forum of 2010 Prof. Goshal gave a speech which is very applicable to the conflicting values issue. To quote Prof. Goshal:

> "Agree or disagree, but commit. Yes, people debate, people argue, but in the end a decision is taken and - agreed or disagreed – the people will commit." (World Economic Forum, 2005)

Commitment is above all desirable. When the shared values are not present, but there is commitment, the chance that agreed solutions are altered by groups is less likely. How to reach commitment is different question. As the discussed literature of Leidner & Kayworth, endorsed by Prof. Goshal, managers can influence commitment.

Short term outlook

Cyber security is a constant battle with time and money. The select group of hired Security Officers against the enormous group of hackers with virtually unlimited time. Some ideas and recommendations:

1. *Be selective in bringing control systems from isolation.* Until control systems are designed so they can be safely and easily updated, compartmentalization is a best practice.

2. *Use the wisdom of the crowd.* The Pw2Own and Pwnium conferences are examples were the wisdom of hackers is used to find vulnerabilities. The hacker earns credits and money when he succeeds, the organizations will be thoroughly tested for vulnerabilities. For the control system industry, Siemens is considering to offer a bug bounty program. (Dark Reading, 2013)
3. *Facilitate education and training for personnel.* A better understanding of personal values and perspectives would lead to more commitment. Managers and management play a big role in facilitating the process.
4. *Share practical knowledge with the industry*. Several examples of non-profit organizations that share knowledge, can be found in the United States (i.e. EnergySec)
5. *Monitoring media as Twitter, Pastebin and forums turns out to be valuable*. Not only organizations spread best practices, knowledge and insights via this medium, hackers are also very active. The Twitter platform allows hackers to publicly earn credits for their exploits and (to a certain extend) allows anonymity. Vulnerabilities, exploits and breaches are therefor often announced or spread via online media as Twitter, pastebin and underground forums.

Cost and security

In chapter four, it has been argued that security and investment are difficult tradeoffs. How secure a system or network is, is often subjective. The ability to assess more precisely if an investment in security is proportionate and effective would be very valuable. Currently, assessing cyber security risks has been proven to be difficult because of the difficulties in allocating monetary values to cyber risks. It is recommended that more research is done towards improvement and understanding risk assessments related to cyber security.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., et al. (2012). *Measuring the Cost of Cybercrime.*

ANSI/ISA. (2007). *Security for Industrial Automation and Control Systems.* Alexander Drive: ANSI/ISAISA.

Apostolov, A. (2002). Integration of legacy intelligent electronic devices in UCA based digital control systems . *Power Engineering Society Winter Meeting,*, (pp. 648 - 653). Los Angeles.

Arnold, G. W. (2011). Challenges and Opportunities in Smart Grid: A Position Article. *Proceedings of the IEEE. Vol. 99, No. 6*, p. 922. IEEE.

Arstechnica. (2012, October 25). *Backdoor in computer controls opens critical infrastructure to hackers.* Retrieved November 7, 2012, from Arstechnica: http://arstechnica.com/security/2012/10/backdoor-in-computer-controls-opens-critical-infrastructure-to-hackers/

Bauer, J., & Van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, pp. 706-719.

Bean, T., & McGrory, J. (2010). *The Integration of Smart Meters Into Electrical Grids to Ensure Maximum Benefit for Consumers, Generators and Network Operators.* Dublin: School of Electrical Engineering Systems.

Beniger, J. (1986). *The Control Revolution: technological and economic origins of the information society.* Cambridge: Harvard University Press.

Bhargava, B., Lilien, L., & Zhong, Y. (2005). Security Paradigms and Pervasive Trust Paradigm. West Lafayette, Perdue University , USA.

Bhargava, P. B. (2012, April). Presentation: Security Paradigms and Pervasive Trust Paradigm. Perdue.

Blakley, B. (1996). The Emperor's old armor. *New Security Paradigms Workshop*, (pp. 2-16). Banff.

Blask, C. (2013, 1 14). *Lessons learned in smart grid cybersecurity*. Retrieved 1 23, 2013, from Energy Central: http://gridinsights.energycentral.com/detail.cfm

Bolton, W. (2009). *Programmable Logic Controllers.* Oxford: Elsevier Ltd.

Bradburn, N., Sudman, S., & Wansink, B. (2004). *Asking Questions: The Definitive Guide to Questionnaire* . San Fransisco: John Wiley & Sons.

Bredhoff, S. (2001). *American originals*. Washington, D.C: National Archives and Records Administration.

Bronk, C., & Tikk-Ringas, E. (2013). *Hack or attack: Shamoon and the evolution of cyber conlfict*. Houston: Rice Univercity.

Bruijne, M. d. (2006). *Networked reliability: institutional fragmentation and the reliability of service provision in critical infrastructures*. Enschede.

Byres, E., Eng, P., & Lowe, J. (2004). *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*.

Cárdenas, A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. *3rd USENIX Workshop on Hot Topics in Security*. San Jose.

Case, K., & Fair, R. (1998). *Principles of Economics*. London: Prentice Hall.

CEN/CENELEC/ETSI Joint Working Group. (2011). *Standards for Smart Grids*. Brussels: The European Commission.

Center for Strategic and International Studies. (2011). *Twenty Critical Security Controls for Effective Cyber Defense*. SANS.

Centre for Development of Advanced Computing. (2012, 2 10). *SCADA Security Awareness*. Retrieved 12 10, 2012, from Forum of load despatchers: http://www.forumofld.in/Data/Meeting/6th%20fold%20meeting/Awareness%20-%2010Feb2012-Ver2.0.pdf

Cleveland, F. (2008). Cyber Security Issues for Advanced Metering Infrastructure. *IEEE PES Power System Communications Committee*.

Collier, S. (2010). Ten Steps to a Smarter Grid. *Industry Applications Magazine, IEEE*, 62 - 68.

Conrath, E. (1999). *Structural Design for Physical Security*. ASCE Publications.

Coombs, R., Knights, D., & Willmott, H. C. (1992). Culture, Control and Competition: Towards a Conceptual Framework for the Study of Information Technology in Organizations. *Organization Science*, 51-72.

CPNI. (2012). *Security of legacy control systems*. The Hague: CPNI.

Daneels, A., & Salter, W. (1999). What is SCADA. *International Conference on Accelerator and Large Experimental Physics Control Systems*, (pp. 339 - 343). Trieste.

Dark Reading. (2013, 2 25). *Businesses Feel Impact Of IT Security Skill Shortage, Study Finds*. Retrieved 2 27, 2013, from Dark Reading: http://www.darkreading.com/security/security-management/240149286/businesses-feel-impact-of-it-security-skill-shortage-study-finds.html/

Dark Reading. (2013, 1 24). *SCADA security 2.0*. Retrieved 1 24, 2013, from Dark Reading: http://www.darkreading.com/vulnerability-management/167901026/security/vulnerabilities/240146913/scada-security-2-0.html

Dark Reading. (2013, 1 15). *The SCADA Patch Problem*. Retrieved 2 10, 2013, from Dark Reading: http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240146355/the-scada-patch-problem.html.html?itc=edit_in_body_cross

Delloite. (2009). Presentation: Smart Grid; Managing Risks Through Prudent, Staged investments. USA.

Deloitte. (2011). *Advanced metering infrastructure cost benefit analysis*. Palo Alto: Electical Power Research Institute.

Deloitte Consulting. (2012). Smart Grid Service Offering - Risk and Security Management for AMI and Smart Grid Implementations.

Edison, T. (1880). *Patent No. 223,898*. United States.

Electrical Power Research Institute. (2011). *Estimating the Costs and Benefits of the Smart Grid*. Palo Alto: Electric Power Research Institute.

Energie-Nederland; Netbeheer Nederland. (2011). *Energy in the Netherlands*. Zwolle.

EnergySec. (2013, 1). *About EnergySec*. Retrieved 2 24, 2013, from EnergySec: http://www.energysec.org/about-energysec/

ENISA. (2011). *Protecting Industrial Control Systems*. Heraklion: European Network and Information Security Agency.

ENISA. (2012). *Cyber Incident Reporting in the EU: An overview of security articles in EU legislation*. Heraklion: European Network and Information Security Agency.

ENISA. (2012, 6 29). *ENISA report calls for kick-start in cyber insurance market*. Retrieved 1 15, 2013, from ENISA: http://www.enisa.europa.eu/media/press-releases/enisa-report-calls-for-kick-start-for-kick-start-in-cyber-insurance-market

ENISA. (2012). *Incentives and barriers of the cyber insurance market in Europe*. Brussels: 6.

E-on. (2010, 1 1). *Productiepark*. Retrieved 11 18, 2012, from E-on: http://www.eon.nl/corporate/organisatie/productiepark

Ernst & Young. (2011). *Attacking the smart grid*. London: Ernst & Young.

European Commission. (2012). *Cyber Security of the smart grids - Expert Group on the security and resilience of communication networks and information systems for Smart Grids*. Brussels: European Commission.

European Commission. (2013, 2 7). *EU Cybersecurity plan to protect open internet and online freedom and opportunity*. Retrieved 2 8, 2013, from Digital Agenda for Europe.

European Network and Information Security Agency. (2011). *Protecting Industrial Control Systems: Recommendations for Europe and Member States.* Heraklion.

European Network and Information Security Agency. (2012). *Smart Grid Security.* Brussels: ENISA.

Farhangi, H. (2010, Januari). The path of the smart grid. *IEEE power & energy magazine*, 20.

Farhangi, H. (2010, january/february). The Path of the smart grid. *IEEE power & energy magazine*, pp. 18-28.

Farlex Dictionary. (2012, 12 23). *Farlex Dictionary*. Retrieved 12 23, 2012, from Farlex Dictionary: http://www.thefreedictionary.com/paradigm

Fernandez, J., & Fernandez, A. (2005). SCADA systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, 160-168.

Flick, T., & Morehouse, J. (2011). *Securing the smart grid: next generation power grid security.* Burlington: Elsevier Inc.

Fowler, F. (1995). *Improving Survey Questions: Design and Evaluation*. California: Sage Publications.

G. Deconinck, D. B. (2007). *Studie communicatiemiddelen voor slimme meters.* Leuven: K.U. Leuven.

Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B., & Wiley, J. (2008). A Testbed for Secure and Robust SCADA Systems. *Proceedings of 14th IEEE Real-time and Embedded Technology and Applications Symposium.*

Ginter, A. (2011, 3 26). *Vulnerabilities Not News to Experts*. Retrieved 10 8, 2012, from Industrial Control System Security: http://controlsystemsecurity.blogspot.nl/2011/03/vulnerabilities-not-news-to-experts.html

Goble, W. (2010). *Control Systems Safety Evaluation and Reliability.* Alexander drive: International Society of Automation.

Goodwin, R., Willson, M., & Stanley Jr, G. (2005). Terror threat perception and its consequences in contemporary Britain. *British Journal of Psychology*, 389- 406.

Google Trends. (2012, 12 17). *Google Trends*. Retrieved 12 17, 2012, from Smart grid: http://www.google.com/trends/explore?hl=nl#q=smart%20grid

Greenwald, S. (1998). New Security Paradigms Workshop., (p. Workshop: What is the old security paradigm). Charlottesville, USA.

Heng, G. (1996, October). Microcomputer-based remote terminal unit for a SCADA system. *Microprocessors and Microsystems*, pp. 39-45.

Honeywell. (2012). *Industrial IT*. Houston: Honeywell Process Solutions.

Huston, B. (2012, 09 12). *InfoSec*. Retrieved 10 1, 2012, from Ask The Experts: Important SCADA Security Tips: http://www.infosecisland.com/blogview/22355-Ask-The-Experts-Important-SCADA-Security-Tips.html

ICS-CERT. (2012). *ICSJWG Quarterly newsletter - December*. ICS-CERT.

ICS-CERT. (2012). *Incident Response Summary Report*. Washington: Department of Homeland Security.

Industrial Defender. (2012, 10 24). *Industrial Defender*. Retrieved 10 24, 2012, from ICS Challenges: http://www.industrialdefender.com/asm_solutions/security.php

ISO 27005. (2011). ISO/IEC 27005. *Information security risk management*. ISO.

ISSC. (2013, 2 28). *Network Segmentation Brings Security Woes*. Retrieved 3 4, 2013, from Industrial Safety and Security source: http://www.isssource.com/network-segmentation-brings-security-woes/

Johnsson, E. (2012, April). Depandability and Security - Department of Computer Engineering Chalmer University of Technology. Chalmers. Retrieved October 19, 2012, from http://www.cse.chalmers.se/edu/course/EDA263/oh12/L10%20depsec%20modelling.pdf

Keemink, S., & Roos, B. (2008). *Security analysis of Dutch smart metering systems*. Amsterdam: University of Amsterdam.

Krebs, B. (2012, October 26). *DHS Warns of 'Hacktivist' Threat Against Industrial Control Systems*. Retrieved November 3, 2012, from Krebsonsecurity.com: http://krebsonsecurity.com/2012/10/dhs-warns-of-hacktivist-threat-against-industrial-control-systems/

Leavitt, H. J., & Whisler, T. L. (1958). Management in the 1980s. *Harvard Business Review*.

Leidner, E., & Kayworth, T. (2006). A review of culture in information systems. *MIS Quarterly Vol. 30 No. 2*, 357-399.

Leonardo Energy. (2008). *European Power Quality Survey*. Siemens.

Lilien, L., Al-Alawneh, A., & Othmane, L. (2010). The Pervasive Trust Foundation for Security in Next Generation Networks . *NSPW'10* (pp. 129 - 141). Concord: ACM.

Macaulay, T., & Singer, B. (2011). *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. Portland: Auerbach Publications.

Mackey, A., & Gass, S. (2009). *Second Language Research: Methodology And Design.* New Yersey: Lawrence Erlbaum Associates.

McDonald, J. (2012, 9 12). *Electric online.* Retrieved 12 19, 2012, from Substation Automation Basics - The Next Generation: http://www.electricenergyonline.com/?page=show_article&mag=43&article=321

Microsoft. (2008, 6). *The Great Debate: Security by Obscurity*. Retrieved 10 12, 2012, from TechNet Magazine: http://technet.microsoft.com/nl-nl/magazine/2008.06.obscurity(en-us).aspx

Moore, G. (1965). Cramming more components onto integrated circuits. *Electronics, Volume 38, Number 8*.

Motorola. (2007). *SCADA Systems.* Schaumburg: Motorola.

National Energy Technology Laboratory. (2008). *Advanced Metering Infrastructure.* U.S. Department of Energy.

National Institute of Standards and Technology. (2011). *Guide to Industrial Control Systems (ICS) Security.* Gaithersburg: NIST.

NCSC. (2013, 1 3). *Leidraad responsible disclosure*. Retrieved 1 5, 2013, from Nationaal Cyber Security Centrum: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html

Netbeheer Nederland. (2012). *The road to a sustainable and efficient energy supply: Smart Grid Roadmap.* Netbeheer Nederland.

NIST. (2009, 9). *National Institute of Standards and Technology Smart Grid Conceptual Model.* Retrieved 10 5, 2012, from Smart Grid Information Clearinghouse: http://www.sgiclearinghouse.org/ConceptualModel

Oppenheim, A. (1992). *Questionnaire Design, Interviewing and Attitude Measurement.* New York: Continuum.

Oxford Dictionaries. (2012, 11 25). *Oxford Dictionaries*. Retrieved 11 25, 2012, from Oxford Dictionaries: http://oxforddictionaries.com/definition/english/paradigm

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information.* New York: Wiley Computer Publishing, John Wiley & Sons, Inc.

Pike Research. (2011, 9). *Smart Grid Cyber Security*. Retrieved 12 9, 2012, from Navigant Research: http://www.navigantresearch.com/research/smart-grid-cyber-security

Pike Research. (2012, 3). *Investments in Smart Grid Cyber Security to Total $14 Billion Through 2018*. Retrieved 12 10, 2012, from Navigant Research:

http://www.navigantresearch.com/newsroom/investments-in-smart-grid-cyber-security-to-total-14-billion-through-2018

Proctor, K. S. (2011). *Optimizing and Assessing Information Technology: Improving Business Project Execution*. John Wiley & Sons.

Purucker, S. e. (1985, March). The design of an integrated distribution control system. *IEEE Transactions on Power Apparatus and Systems, Vol. PAS-104, No. 3,*.

Rijksoverheid. (2012). *Energie en consumenten*. Retrieved September 21, 2012, from Wanneer komt de slimme meter?: http://www.rijksoverheid.nl/onderwerpen/energie-en-consumenten/vraag-en-antwoord/wanneer-komt-de-slimme-meter.html

Robinson, D. (2011, 10 5). *The integrated network operations center: an IT-OT enabler*. Retrieved 9 15, 2012, from Smart Grid Technology: http://www.smartgridnews.com/artman/publish/Business_Strategy/The-integrated-network-operations-center-an-IT-OT-enabler-4053.html

Semaphore. (2012). *Remote Automation and Monitoring: PLC or RTU?* Lake Mary: Semaphore.

Sezi, T. (1999). New intelligent electronic devices change the structure of power distribution systems. *Industry Applications Conference*, (pp. 944 - 952). Phoenix.

Shannon, S. (1997, May). RTUs vs PLCs. *Tetragenics Company Newsletter*, pp. 1-5.

Shoshani, A., & Slone, M. (2008). The Drama of Media Coverage of Terrorism: Emotional and Attitudinal Impact on the Audience. *Studies in Conflict & Terrorism*, 627-240.

Siemens. (2010, 7 19). *Malware Affecting Siemens WinCC and PCS7 Products*. Retrieved 11 8, 2012, from Siemens Forum: https://www.automation.siemens.com/WW/forum/guests/PostShow.aspx?PageIndex=1&PostID=225811&Language=en

Siemens. (2011). *Securing the smart grid*. Retrieved 10 4, 2012, from International Conference on Sensor Technologies and Applications: http://www.iaria.org/conferences2011/filesENERGY11/keynote_energy2011_sfries.pdf

Siemens. (2013, 1). *Industrial Remote Communication*. Retrieved 1 18, 2013, from Siemens Automation: https://eb.automation.siemens.com/mall/en/nl/Catalog/Products/10034139?tree=CatalogTree

Smart Metering Projects Map. (2012, October). *Smart Metering Projects Map*. Retrieved September 10, 2012, from Smart Metering Projects Map: http://goo.gl/maps/ff6lm

Smith, D. (2011). *Reliability, maintainability and risk: practical safety-related systems*. Oxford: Elsevier Ltd.

Smith, H., & Wayne, R. (1993, January). RTUs Slave for Supervisory Systems. *IEEE Computer Applications in Power*, pp. 27-32.

Sorebo, G., & Echols, M. (2011). *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid*. Florida: Taylor & Francis Group.

Stapelberg, R. (2008). *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*. Springer.

Stuttard. (2005). Security & obscurity. *Network Security*, 10-12.

SCADA products. (2010, 1 1). Retrieved 12 4, 2012, from SCADA world: http://scadaworld.org/index-sel-products.htm

PLC devices scanner. (2012, November 15). Retrieved November 18, 2012, from Code.google.com: http://code.google.com/p/plcscan/

ProFuzz. (2012, December 7). Retrieved December 7, 2012, from Github.com: https://github.com/HSASec/ProFuzz

Taskforce intelligente netten. (2010). *Op weg naar intelligente netten in Nederland*. Den Haag: Ministerie van Economische Zaken.

ten Heuvelhof, P. d. (2012, September 13). Actor and their incentives in Dutch Smart Grid. (F. Schoenmakers, Interviewer)

Tennet. (2010). *Visie 2030*. Arhnem: Tennet.

Tourangeau, R., Rips, L., & Rasinski, K. (2000). *The Psychology of Survey Response*. Cambridge: Caimbridge University Press.

Tsang, R. (2009). Attacks on SCADA Networks. *Goldman School of Public Polic*, 4-6.

U.S. Office of the Law Revision Counsel. (2012, January). Code of Laws of the United States of America. *44 USC § 3542 - Definitions*. Washington: US Government Printing Office.

V3. (2012, November 27). *Scada bugs make security a turkey shoot for hackers*. Retrieved November 29, 2012, from V3.co.uk: http://www.v3.co.uk/v3-uk/news/2227489/researchers-slam-weak-security-in-scada-appliances

Vaessen. (2012, 9 18). *Can power quality be managed and controlled by Smart Grids?* Retrieved 9 27, 2012, from Smart Grid Sherpa: http://smartgridsherpa.com/blog/can-power-quality-be-managed-and-controlled-by-smart-grids

Vaessen, P. (2012, September 12). *Can power quality be managed and controlled by Smart Grids?* Retrieved September 18, 2012, from Smart Grid Sherpa: http://smartgridsherpa.com/blog/can-power-quality-be-managed-and-controlled-by-smart-grids

Verbong, G., Beemsterboer, S., & Sengers, F. (2012). *Smart grids or smart users?* Eindhoven: Energy Policy.

von Meier, A. (1999). Occupational Cultures as a Challenge to Technological Innovation. *IEEE Transaction on engineering management*, 101 - 112.

Waller, T. (2012, 5 9). Security of industrial control systems questioned at DHS conference. (Messmer, Interviewer)

Waterfall Security. (2012). *Control System Security: why expert disagree.* New York: Waterfall Security Solutions.

Weimann, G. (2003). The Theater of Terror: effects of press coverage. *Journal of Communication*, 38 - 45.

Weiss, J. (2010, December). Cyber security for industrial control systems. Den Haag.

Wikipedia. (2012, Oktober 1). *Wikipedia.* Retrieved Oktober 1, 2012, from Risk: http://en.wikipedia.org/wiki/Risk

Wired. (2012, September 17). *Maker of Smart-Grid Control Software Hacked.* Retrieved September 17, 2012, from Wired: http://www.wired.com/threatlevel/2012/09/scada-vendor-telvent-hacked/

World Economic Forum. (2005). The smell of the Place by Prof Sumantra Ghoshal.

World Economic Forum. (2012). *Risk and responsibility in a hyperconnected word: pathways to golbab cyber resilience.* Geneva: World Economic Forum.

Wu, X. (2009). *Security Architecture for Sensitive Information Systems.* Monash: Faculty of Information Technology Monash University.

Xyngi, I. (2011). *An intelligent algorithm for smart grid protection applications.* Delft: TU Delft.

WinCC harvester. (2012, November 7). Retrieved November 7, 2012, from Github.com: https://github.com/nxnrt/wincc_harvester

Appendix I: Overview Dutch powerplants

Construction year	Cumulative number
1906	1
1956	2
1958	3
1974	4
1975	6
1976	8
1978	10
1979	12
1981	13
1982	14
1983	17
1985	18
1987	19
1988	24
1989	28
1990	30
1993	31
1994	35
1995	36
1996	41
1997	46
1998	47
2000	50
2002	51
2004	54
2007	57
2008	59
2010	64
2011	66

Questionnaire Control System Security

Time
This questionnaire takes a maximum of 15 minutes to fill in.

Privacy
Your data is processed anonymously.

Perspective
All questions have to be answered from the respondents perspective.

Questions
The questions are related to control systems and IT systems in the grid sector.

Goal
This questionnaire is created to gain insight in the respondents perspective on security.

Background
The research is conducted as part of a student internship (a cooperation between the TU Delft and Deloitte)

If you wish to recieve the results, you can fill in your emailadress in the questionnaire. You will recieve a digital copy of the resulting paper on Control System Security late februari 2013

Thank you in advance for your time.

Questionnaire

Organization and system processes

Below you find 14 statements concerning security, risk assessment and awareness.
Rate each statement from your own perspective.
Where 1 means 'totally disagree' and 5 means 'totally agree'.

In this question the term "System" is used. This refers to control systems or IT systems which are related to your everyday activities.

		1	2	3	4	5
1.1	There is an effective and timely process for reporting significant weakness					
1.2	During the design of a system (a device or service) , the security requirements are identified					
1.3	Tests and examinations of key controls are routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?					
1.4	The current system configuration is documented, including links to other					

	systems	
1.5	Security alerts and security Incidents are analysed and remedial actions are taken	1 2 3 4 5
1.6	Risk assessments are performed and documented on a regular basis or whenever the system, facilities, or other conditions change	1 2 3 4 5
1.7	Investments and security are a causal relation: the more you invest, the more secure your system is	1 2 3 4 5
1.8	Our systems are not as secure as I want them to be, because it is too expensive	1 2 3 4 5
1.9	Our organization is taking significant risks by not investing or postponing investments in security	1 2 3 4 5
1.10	Higher management levels are aware of security risks in everyday processes	1 2 3 4 5
1.11	Compliance (rules and regulation) is a good way of ensuring security and safety for control systems	1 2 3 4 5
1.12	Compliance based security leads to regulations that not necessarily contribute to security	1 2 3 4 5
1.13	From my current function I can easily reach higher management when I identify a risk	1 2 3 4 5
1.14	IT specialists don't understand control systems (from an engineering perspective)	1 2 3 4 5

Threat identification - system

Below you find 9 aspects/functions of control systems.
Each aspect can be seen as a threat for the **continuity** of your organization.
Rate each statement from your own perspective.

1.15	Access to systems from a remote location	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.16	Prior isolated control systems being integrated with internet	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.17	Data being used by third parties	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.18	The use of standard passwords for legacy control systems	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.19	Mandatory updates for software systems	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.20	Systems are being secured after there are built (not security by design)	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.21	Operating systems of control systems may have little computing resources available for common security practices	Non-threat	Low threat	Average threat	High threat	Extreme threat

1.22 Control Systems have a long lifespan and have to be ready for 30 to 40 years of technical development	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.23 Vendors don't allow third party solutions for security	Non-threat	Low threat	Average threat	High threat	Extreme threat

Threat identification - external

Below you find 7 threats from different external actors.
The behaviour of these actor can be seen as a threat for the **continuity** of your organization.
Rate the threats from your own perspective.

1.24 Attacks on control systems in the electricity network are used to protest against political activities (hacktivism)	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.25 Other companies gain access to files and information in order to gain economical advantage (competitive intelligence)	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.26 State sponsored entities gain access in order to gain intelligence about critical process and infrastructures	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.27 Organizations who intend to cause damage, physical and/or economical (terrorism)	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.28 Internal auditors: penetration testers or vulnerability assesments which are done on control systems	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.29 Criminal organizations gain access to information and files and intend to sell the information or blackmail the relevant actors	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.30 'I hack, because I can' individuals who breach a system	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.31 Cyber threats for Dutch control systems mainly originate from:	The Netherlands Europe Asia/middle east No specific geographical location				

Threat identification - people

Below you find 6 statements which can be a threat for your organization
Rate the threats from your own perspective.

1.32 Lack of sufficient security awareness with employees	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.33 Shortage of qualified security personnel	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.34 Lack of integrated incident response training and testing	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.35 Systemic vulnerabilities (e.g. vulnerabilities inherent to the system of organizations and way-of-working)	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.36 Differing cultural perspectives on information security	Non-threat	Low threat	Average threat	High threat	Extreme threat
1.37 The number and type of third parties that the organization interacts and does business with (e.g. suppliers, partners, or contractors)	Non-threat	Low threat	Average threat	High threat	Extreme threat

Statements audit, breach and future

1.38 Which findings are most probable when an audit is done on systems of your organization (**choose a maximum of three**)

- ☐ Lack of documented security policies and procedures
- ☐ Lack of oversight and compliance to security control requirements
- ☐ Lack of security awareness programs
- ☐ Lack of sufficient segregation of duties
- ☐ Excessive access of certain employees
- ☐ Ineffective password management (e.g., use of weak passwords, default passwords, etc.)
- ☐ Sharing of user IDs with a commonly known password
- ☐ Security and review of third party connections
- ☐ Lack of separate testing environment
- ☐ Lack of compliance to privacy regulations
- ☐ Use of production data in testing
- ☐ Business continuity and disaster recovery (e.g., lack of or non-current documentation, lack of testing, etc.)
- ☐ Other

1.39 How confident are you in the information security practices of your third parties?	Not confident

	○ Somewhat confident ○ Confident ○ Very confident ○ Extremely confident
1.40 Which reason best represents your confidence level in third party suppliers?	○ Based on experiance from the past ○ Based on a feeling about the third party ○ Based upon (incident) information related to the third party ○ Based upon which technology the third party uses ○ Based upon the reputation of the third party
1.41 Which of the following categories best describes your organization's adoption of security measures?	○ Innovators ○ Early adopters ○ Early majority ○ Late majority ○ Laggards
1.42 Do you think there is a difference in perspective on security between the engineer (mechanical) and the IT specialists (cyber)?	○ Yes ○ No

Personal

Age, education and work

1.43 Gender	○ Male ○ Female
1.44 Age	
1.45 What is your highest level of education?	○ High school (VWO, HAVO, VMBO or comparable) ○ Higher professional education (HBO or comparable) ○ Scientific education (WO or comparable) ○ Other

1.46 In which discipline were you educated?	○ Computer science (study related to IT or software programming) ○ Mechanical science (study related to design/build of technical systems, mechanisms) ○ Policy / Law (study related to policy management or law) ○ Social science (related to human behaviour) ○ Other 
1.47 How long have you been working at your current job? (years)	
1.48 Have you always been working in the domain you currently work in?	○ Yes ○ No
1.49 Which of the following best describes your current work related to control systems?	○ I'm involved in mechanics (engineer) ○ I'm involved in Information Technology (IT specialist) ○ I'm involved in policy/strategic decisions ○ Other 
1.50 Your email (*only If you want to recieve the resulting paper on Control Systems Security*)	

Appendix III: Statistical analysis: one way Anova

Part I: organization and system processes

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
There is an effective and timely process for reporting significant weakness	Between Groups	1,171	1	1,171	,700	,413
	Within Groups	31,782	19	1,673		
	Total	32,952	20			
During the design of a system (a device or service), the security requirements are identified	Between Groups	2,002	1	2,002	1,396	,252
	Within Groups	27,236	19	1,433		
	Total	29,238	20			
Tests and examinations of key controls are routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?	Between Groups	,339	1	,339	,317	,580
	Within Groups	20,327	19	1,070		
	Total	20,667	20			
The current system configuration is documented, including links to other systems	Between Groups	2,567	1	2,567	2,207	,154
	Within Groups	22,100	19	1,163		
	Total	24,667	20			
Security alerts and security Incidents are analysed and remedial actions are taken	Between Groups	7,093	1	7,093	4,788	,041
	Within Groups	28,145	19	1,481		
	Total	35,238	20			
Risk assessments are performed and documented on a regular basis or whenever the system, facilities, or other conditions change	Between Groups	,249	1	,249	,169	,686
	Within Groups	28,036	19	1,476		
	Total	28,286	20			
Investments and security are a causal relation: the more you invest, the more secure your system is	Between Groups	1,216	1	1,216	,685	,418
	Within Groups	33,736	19	1,776		
	Total	34,952	20			
Our systems are not as secure as I want them to be, because it is too expensive	Between Groups	5,238	1	5,238	7,109	,015
	Within Groups	14,000	19	,737		
	Total	19,238	20			
Our organization is taking significant risks by not investing or postponing investments in security	Between Groups	2,244	1	2,244	1,319	,265
	Within Groups	32,327	19	1,701		
	Total	34,571	20			
Higher management levels are aware of security risks in everyday processes	Between Groups	7,204	1	7,204	4,137	,056
	Within Groups	33,082	19	1,741		
	Total	40,286	20			
Compliance (rules and regulation) is a good way of ensuring security and safety for control systems	Between Groups	3,664	1	3,664	5,732	,027
	Within Groups	12,145	19	,639		
	Total	15,810	20			
Compliance based security leads to regulations that not necessarily contribute to security	Between Groups	1,718	1	1,718	1,465	,241
	Within Groups	22,282	19	1,173		
	Total	24,000	20			
From my current function I can easily reach higher management when I identify a risk	Between Groups	,450	1	,450	,306	,587
	Within Groups	26,500	18	1,472		
	Total	26,950	19			
IT specialists don't understand control systems (from an engineering perspective)	Between Groups	,173	1	,173	,152	,701
	Within Groups	21,636	19	1,139		
	Total	21,810	20			

Part II: Threat identification – systems

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Access to systems from a remote location	Between Groups	3,202	1	3,202	3,373	,082
	Within Groups	18,036	19	,949		
	Total	21,238	20			
Prior isolated control systems being integrated with internet	Between Groups	3,664	1	3,664	2,883	,106
	Within Groups	24,145	19	1,271		
	Total	27,810	20			
Data being used by third parties	Between Groups	,028	1	,028	,033	,857
	Within Groups	15,782	19	,831		
	Total	15,810	20			
The use of standard passwords for legacy control systems	Between Groups	1,262	1	1,262	1,029	,323
	Within Groups	23,309	19	1,227		
	Total	24,571	20			
Mandatory updates for software systems	Between Groups	,728	1	,728	,809	,380
	Within Groups	17,082	19	,899		
	Total	17,810	20			
Systems are being secured after there are built (not security by design)	Between Groups	,028	1	,028	,054	,819
	Within Groups	9,782	19	,515		
	Total	9,810	20			
Operating systems of control systems may have little computing resources available for common security practices	Between Groups	1,262	1	1,262	1,386	,254
	Within Groups	17,309	19	,911		
	Total	18,571	20			
Control Systems have a long lifespan and have to be ready for 30 to 40 years of technical development	Between Groups	,471	1	,471	,279	,603
	Within Groups	32,100	19	1,689		
	Total	32,571	20			
Vendors don't allow third party solutions for security	Between Groups	,007	1	,007	,005	,943
	Within Groups	24,945	19	1,313		
	Total	24,952	20			

Part III: Threat identification – external

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Attacks on control systems in the electricity network are used to protest against political activities (hacktivism)	Between Groups	5,334	1	5,334	5,690	,028
	Within Groups	17,809	19	,937		
	Total	23,143	20			
Other companies gain access to files and information in order to gain economical advantage (competitive intelligence)	Between Groups	,125	1	,125	,160	,693
	Within Groups	14,827	19	,780		
	Total	14,952	20			
State sponsored entities gain access in order to gain intelligence about critical process and infrastructures	Between Groups	,111	1	,111	,139	,713
	Within Groups	15,127	19	,796		
	Total	15,238	20			
Organizations who intend to cause damage, physical and/or economical (terrorism)	Between Groups	1,039	1	1,039	,667	,424
	Within Groups	29,627	19	1,559		
	Total	30,667	20			
Internal auditors: penetration testers or vulnerability assesments which are done on control systems	Between Groups	2,911	1	2,911	4,486	,048
	Within Groups	12,327	19	,649		
	Total	15,238	20			
Criminal organizations gain access to information and files and intend to sell the information or blackmail the relevant actors	Between Groups	,450	1	,450	,395	,538
	Within Groups	20,500	18	1,139		
	Total	20,950	19			
'I hack, because I can' individuals who breach a system	Between Groups	1,800	1	1,800	1,246	,279
	Within Groups	26,000	18	1,444		
	Total	27,800	19			

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Lack of sufficient security awareness with employees	Between Groups	1,171	1	1,171	2,274	,148
	Within Groups	9,782	19	,515		
	Total	10,952	20			
Shortage of qualified security personnel	Between Groups	5,049	1	5,049	5,566	,029
	Within Groups	17,236	19	,907		
	Total	22,286	20			
Lack of integrated incident response training and testing	Between Groups	,390	1	,390	,522	,479
	Within Groups	14,182	19	,746		
	Total	14,571	20			
Systemic vulnerabilities (e.g. vulnerabilities inherent to the system of organizations and way-of-working)	Between Groups	,593	1	,593	,676	,421
	Within Groups	16,645	19	,876		
	Total	17,238	20			
Differing cultural perspectives on information security	Between Groups	,191	1	,191	,204	,657
	Within Groups	17,809	19	,937		
	Total	18,000	20			
The number and type of third parties that the organization interacts and does business with (e.g. suppliers, partners, or contractors)	Between Groups	1,829	1	1,829	1,623	,218
	Within Groups	21,409	19	1,127		
	Total	23,238	20			

Appendix IV: Statistical analysis – Means and standard deviation

Part I: organization and system processes

Report

Which of the following best describes your current work related to control systems?		There is an effective and timely process for reporting significant weakness	During the design of a system (a device or service), the security requirements are identified	Tests and examinations of key controls are routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?	The current system configuration is documented, including links to other systems	Security alerts and security Incidents are analysed and remedial actions are taken	Risk assessments are performed and documented on a regular basis or whenever the system, facilities, or other conditions change	Investments and security are a causal relation: the more you invest, the more secure your system is	Our systems are not as secure as I want them to be, because it is too expensive	Our organization is taking significant risks by not investing or postponing investments in security	Higher management levels are aware of security risks in everyday processes	Compliance (rules and regulation) is a good way of ensuring security and safety for control systems	Compliance based security leads to regulations that not necessarily contribute to security	From my current function I can easily reach higher management when I identify a risk	IT specialists don't understand control systems (from an engineering perspective)
I'm involved in mechanics (engineer)	Mean	3,20	3,80	2,80	3,70	3,80	3,40	3,30	2,00	2,80	3,90	4,20	2,70	3,70	4,00
	N	10	10	10	10	10	10	10	10	10	10	10	10	10	10
	Std. Deviation	1,229	1,229	1,135	1,337	1,033	,966	1,494	,943	1,476	1,197	,919	1,059	1,160	,943
I'm involved in Information Technology (IT specialist)	Mean	2,73	3,18	2,55	3,00	2,64	3,18	2,82	3,00	3,45	2,73	3,36	3,27	3,40	3,82
	N	11	11	11	11	11	11	11	11	11	11	11	11	10	11
	Std. Deviation	1,348	1,168	,934	,775	1,362	1,401	1,168	,775	1,128	1,421	,674	1,104	1,265	1,168
Total	Mean	2,95	3,48	2,67	3,33	3,19	3,29	3,05	2,52	3,14	3,29	3,76	3,00	3,55	3,90
	N	21	21	21	21	21	21	21	21	21	21	21	21	20	21
	Std. Deviation	1,284	1,209	1,017	1,111	1,327	1,189	1,322	,981	1,315	1,419	,889	1,095	1,191	1,044

Part II: Threat identification - systems

Report

Which of the following best describes your current work related to control systems?		Access to systems from a remote location	Prior isolated control systems being integrated with internet	Data being used by third parties	The use of standard passwords for legacy control systems	Mandatory updates for software systems	Systems are being secured after there are built (not security by design)	Operating systems of control systems may have little computing resources available for common security practices	Control Systems have a long lifespan and have to be ready for 30 to 40 years of technical development	Vendors don't allow third party solutions for security
I'm involved in mechanics (engineer)	Mean	3,40	3,80	3,20	3,60	2,90	3,80	3,40	2,70	2,60
	N	10	10	10	10	10	10	10	10	10
	Std. Deviation	1,265	1,317	1,033	1,350	1,101	,919	,966	1,337	,966
I'm involved in Information Technology (IT specialist)	Mean	4,18	4,64	3,27	4,09	3,27	3,73	2,91	3,00	2,64
	N	11	11	11	11	11	11	11	11	11
	Std. Deviation	,603	,924	,786	,831	,786	,467	,944	1,265	1,286
Total	Mean	3,81	4,24	3,24	3,86	3,10	3,76	3,14	2,86	2,62
	N	21	21	21	21	21	21	21	21	21
	Std. Deviation	1,030	1,179	,889	1,108	,944	,700	,964	1,276	1,117

Part III: Threat identification - external

Report

Which of the following best describes your current work related to control systems?		Attacks on control systems in the electricity network are used to protest against political activities (hacktivism)	Other companies gain access to files and information in order to gain economical advantage (competitive intelligence)	State sponsored entities gain access in order to gain intelligence about critical process and infrastructures	Organizations who intend to cause damage, physical and/or economical (terrorism)	Internal auditors: penetration testers or vulnerability assesments which are done on control systems	Criminal organizations gain access to information and files and intend to sell the information or blackmail the relevant actors	'I hack, because I can' individuals who breach a system
I'm involved in mechanics (engineer)	Mean	4,10	3,70	3,40	3,90	3,20	3,70	3,40
	N	10	10	10	10	10	10	10
	Std. Deviation	,568	1,059	,843	1,101	,919	1,160	1,265
I'm involved in Information Technology (IT specialist)	Mean	3,09	3,55	3,55	3,45	2,45	3,40	2,80
	N	11	11	11	11	11	10	10
	Std. Deviation	1,221	,688	,934	1,368	,688	,966	1,135
Total	Mean	3,57	3,62	3,48	3,67	2,81	3,55	3,10
	N	21	21	21	21	21	20	20
	Std. Deviation	1,076	,865	,873	1,238	,873	1,050	1,210

Part IV: Threat identification – people

Report

Which of the following best describes your current work related to control systems?		Lack of sufficient security awareness with employees	Shortage of qualified security personnel	Lack of integrated incident response training and testing	Systemic vulnerabilities (e.g. vulnerabilities inherent to the system of organizations and way-of-working)	Differing cultural perspectives on information security	The number and type of third parties that the organization interacts and does business with (e.g. suppliers, partners, or contractors)
I'm involved in mechanics (engineer)	Mean	3,80	3,20	4,00	3,30	2,90	3,50
	N	10	10	10	10	10	10
	Std. Deviation	,632	1,229	,816	,949	,994	1,354
I'm involved in Information Technology (IT specialist)	Mean	4,27	4,18	3,73	3,64	3,09	2,91
	N	11	11	11	11	11	11
	Std. Deviation	,786	,603	,905	,924	,944	,701
Total	Mean	4,05	3,71	3,86	3,48	3,00	3,19
	N	21	21	21	21	21	21
	Std. Deviation	,740	1,056	,854	,928	,949	1,078