August 2014

Universiteit Leiden
Opleiding Informatica

Risk assessment

for the cyber threats

to networked critical infrastructure

Michail Douramanis
Student No: 1249681

1st supervisor: Prof. Dr. Stephan Wolfgang Pickl
2nd supervisor: Prof. Dr. Hans Le Fever

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Acknowledgments

I would like to thank Prof. Dr. Hans Le Fever for his trust in me and support throughout my studies. I would like to thank my supervisor Prof. Dr. Stephan Pickl for his support and for making this thesis possible, Armin Leopold and Jan Stutzki for their support and valuable ideas and input during the conduct of the research.

Last but not least, I would like to thank my parents for their continuous support, patience and trust in myself regarding all my personal decisions and efforts. They are greatly responsible for the person I am.

Contents

List of Tables

List of Figures

Abstract

Technology has changed considerably the way we do business, we behave as people, we interact with our environment and also the way certain basic operations are performed and delivered. More specifically public and private infrastructure designed and built to provide us with some fundamental goods and services like electricity, gas, transportation, finance etc. is relying heavily on Information and Communication Technology (ICT) like Supervisory Control and Data Acquisition (SCADA) control centres, to operate, deliver theirs goods and services and also communicate with other types of infrastructure. Their reliance on ICT has created new opportunities for their operations, but also new risks with new types of threats, ranging from cyber criminal activities to cyberwarfare and new ways to execute them through the internet.

Some of these infrastructures can be considered as critical to the normal operation of a society and the ICT supporting them referred to as critical information infrastructure. Therefore, they need to be constantly protected against such risks. The purpose of this thesis is to perform a risk assessment for such critical infrastructure and its critical information infrastructure, namely a power plant in Germany and then identify the cyber threats that exist, by creating three virtual networks with virtual machines to mimic the operation of the SCADA control centre of the power plant.

1 Introduction

Since man first started forming social groups, the way of life has always been dependent on the provision of specific goods and services specified by the division of labour among the members of the groups. Such goods would be for example the provision of food to eat or leather for clothes and the services would be the cooking of food and the sewing of leather producing additional basic goods for a group. As societies evolve and propagate the services and goods needed become more complex and affect a greater number of people. These are today for example the provision of electricity, natural gas, fresh water or services like financial transactions, education, transportation etc. as we will discuss later.

These goods and services are produced in what is usually a set of complex installations like in the case of a thermopower plant, silos for storage of fuel and water, boilers to produce steam from water and turbines that are powered from the steam and turn the kinetic force of the steam to electricity. At the end point usually exists a distribution network or storage equipment, e.g. a set of high capacity batteries, to distribute or store the electricity. These installations for their operation rely on some electromechanical controllers, also called actuators, that perform specific functions for the operation and cooperation among the various installations. These can be valves to control the flow of water or fuel to the boilers, pipes and flow meters to adjust the flow of steam to the turbines etc.

1.1 The research problem

The electromechanical components described earlier are often referred to as Supervisory Control and Data Acquisition (SCADA) (Stamp, Dillinger, Young, & DePoy, 2003). In the past such SCADA components were manually controlled usually on the spot in various parts of the infrastructure. Advancements in technology in general and specifically in information and communication technology (ICT) have allowed the remote control of these through a computer centre located inside the infrastructure via a private network isolated from other networks and the internet. However, the need of the infrastructure owners to modernise their facilities to reduce operational costs and to be more efficient have lead them to have more centralised control and additional remote capabilities of the SCADA systems. Usually this means that the SCADA control centres are now connected to the corporate network of the infrastructure owner and most probably to the internet (Igure, Laughter, & Williams, 2006; Amanullah, Kalam, & Zayegh, 2005; Johnson, 2010; Nicholson, Webber, Dyer, Patel, & Janicke, 2012; Sridhar & Manimaran, 2010).

The internet has served since its creation as a means to facilitate communication among individuals and institutions through personal computers that are connected to it (Leiner et al., 2009). However, it has also become a new playground for criminals to carry out their illegitimate activities or has provided ground for new forms of criminal activities (Wall, 2010). One obvious question arising, having in mind the connectivity capabilities of the infrastructures, is how secure are they against cyber threats that target specifically to reduce their capabilities through an unscheduled downtime for an indefinite time or a total shut down.

1.2 The research question

Thus, based on this context, our research questions is formulated as: ***"What cyber threats can a SCADA network control centre attract?"***

1.3 Structure of the thesis

The remainder of the document is structured as following, in Section 2 a literature review shall be conducted in order to gather some of the definitions that exist in the academic literature for some major terms of the research. Then specific working definitions of these terms will be selected for the purpose of the thesis. These terms are risk, risk assessment, cybercrime, critical infrastructure, critical information infrastructure and cyberwarfare. In Section 3 a risk assessment of an imaginary power plant located in Germany will be performed, where the components of the infrastructure are controlled by a SCADA centre with internet connectivity. In Section 4 the design of the experiment will be presented and analysed followed by the presentation of the results in Section 5. In Section 6 we discuses and interpret the results and try to assess whether our research question has been answered or not. Lastly in Section 7 the concluding remarks of our research will be presented.

2 Definition of Risk and Risk assessment, "Cybercrime", "cyberwarfare", critical infrastructure and critical information infrastructure

In this section we will provide the definitions needed of major terms of this thesis, in order for the reader to understand the context under which the research for this thesis will be conducted. Various definitions of the terms will be presented, analysed and one working definition for each term will be selected.

2.1 Definition of Risk

Risk is prevalent in most aspects of our lives since the very beginning of our human history (Renn, 1998). Mankind had been trying to act in ways that would prevent or reduce the effect of unwanted outcomes of events usually out of its own control. When people realised that certain adverse events could be avoided based on an individuals or a groups actions, the perception of risk and its avoidance were born. Thus, traditionally risk has mostly been associated with the negative effects or consequences of our actions or the effect that unknown situations and actions will have on our present situation. These effects are quite often stated, in literature around risk definition, as undesired or unwanted outcomes (DHS Risk Steering Committee, 2010; Luko, 2013; Renn, 2005), to our course of action or objectives. However, the characterisation of an outcome as unwanted is quite subjective and depends usually on the context of the discipline that tries to define risk (Renn, 1998). For example sciences like health, finance, economics, business operations etc. have a different concept of risk compared to other sciences like sociology, politics, law etc. Even among the same field of study there may be differences within the definition of risk since people tend to have different perspective on what can be an undesired effect based on their values and preferences (Dietz, E., Scott Frey, R., and Rosa, E., 1996; Rosa, 1998).

The focus of the research over the past years has been to try to quantify risk using mathematical tools, mainly statistics and probability theory, and an effort to reach a definition of risk that can help interested parties on the purpose of quantifying it and its consequences. According to Renn (Renn, 1998), research around risk has been around for nearly four decades, although the tools used to quantify the effect and probability of it preceded risk research for over one hundred years.

By conducting a literature review to find the available definitions of risk in academic research, one can find an abundance of definitions born out of necessity of different disciplines, most based on the different views and inputs of these disciplines. Among the varying definitions certain similarities can be observed. What is common in some is the consideration of the human life either directly or indirectly in the definition of risk by many public organisations and intuitions, i.e. Rosa, Society of Risk Analysis (SRA), European Environment Agency (EEA) and United Nations (UN). This observation is not surprising given the nature and the mission of such public organisations, which exist to serve the interests of the broader population or the citizens of a specific country. With regard to cybersecurity of networked critical infrastructures, the life of humans may be as well jeopardised in a security breach event, but this will be discussed later on in this thesis.

Another similarity in many of the definitions is the consideration of the unknown besides the effort to predict future adverse situations i.e. UKs Cabinet Office, Rosa, Aven, American National Standards Institute (ANSI), International Standards Organisation (ISO), German Advisory Council on Global Change (GACGC). Most definitions refer to certain events that can have an unwanted outcome on the present situation of future objectives. However, it is impossible to think of every possible future event and be able to accurately quantify its probability of occurring besides some well educated guesses or based on the frequency of similar past events. It is important to consider also the unknown when trying to assess the potential risk that can affect a certain plan or course of actions.

Important is also to mention that some definitions do not consider only the negative consequences of a string of actions or events to our current or future situation, but also the positive ones i.e. UKs Cabinet Office, Rosa, Aven, US Homeland Security, ANSI, ISO, Australian and New Zealand Standard, World Health Organisation (WHO) and US Nuclear Regulatory Commission (US NCR). Thus, it is in general the deviation from a set of planned or wishful future status that should be taken into account when considering risk. In a business context imagine a situation where a company introduces a new product and plans production capacity for a specific number of items. There is the risk that demand may be less or more than expected and of course being according to the actual plan (being equal should not be considered as risk). Only one situation is negative, but the consequences vary and have different implications for the company (i.e. stock surplus from overproduction or evading revenue from missed sales).

Lastly, while some of the definitions consider risk as only the chance of an occurrence of an unwanted event, most of them adopt the conceptualisation of risk as a function of the probability of a certain event and the impact that it will have in a given situation i.e. UKs Cabinet Office, Aven, US Homeland Security, ANSI, ISO, Australian and New Zealand Standard, GACGC, SRA and US NCR. The impact is quite important to be able to quantify the significance of risk and the consequences that some events will have on our situation or goals. For example, having the previous context in mind, the probability for a stock surplus due to under performing sales may be low because a really thorough market scan preceded the launch of the product. However, the impact of such a risk occurring could be huge with the company being forced to scrap the unsold merchandise and write it off. This scenario indicates the need for a good market scan before the launch of a new product and can even justify the cost for such an action. Thus, when an organisation needs to implement specific measures to counter unpredicted events, these measures usually cost resources either it is people, cash or capacity (i.e. manufacturing capacity), the organisation then needs to justify the cost of these based on the chance of risk occurrence and the magnitude that the risk will have should it occur.

To summarise we can distinguish certain characteristics among the various definitions of risk available in the academic literature and those used by public institutions. These are:

- the consideration of human life
- the consideration of the unknown

- the deviation from plan/objectives and
- it is a function of probability and impact.

On Table 1 are listed some of the available definitions in the academic literature with relation to these characteristics:

Table 1: Definitions of Risk

Definition	Consideration of human life	Consideration of the unknown	Deviation from plan objectives	Function of probability and impact
Risk refers to uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance. This definition acknowledges the uncertainty that underlies much of the work of government. (UK Cabinet Office, 2002)		✓	✓	✓
Risk is a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain. (Rosa, 1998)	✓	✓	✓	
Risk is defined as the combination of possible consequences and associated uncertainties (uncertainties of what will be the consequences), whereas vulnerability is defined as the combination of possible consequences and associated uncertainties given a source. Hence risk is the combination of sources (Aven, 2007)		✓	✓	✓

Table 1 – continued from previous page

Definition	Consideration of human life	Consideration of the unknown	Deviation from plan objectives	Function of probability and impact
Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences (DHS Risk Steering Committee, 2010)			✓	✓
Effect of uncertainty on objectives. NOTE 1: An effect is a deviation from the expected positive and=or negative. NOTE 2: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). NOTE 3: Risk is often characterised by reference to potential events and consequences, or a combination of these. NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. NOTE 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. (ANSI=ASSE Z690.1–2011, 2011)		✓	✓	✓

Table 1 – continued from previous page

Definition	Consideration of human life	Consideration of the unknown	Deviation from plan objectives	Function of probability and impact
Risk is the effect of uncertainty on objectives. An effect is a deviation from the expected (positive and/or negative). Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence. Likelihood is defined as the chance of something happening, whether defined, measured or determined objectively or subjectively, quantitatively or qualitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). Probability is defined as a measure of the chance of occurrence expressed as a number between 0 and 1. Uncertainty is considered the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequences or likelihood. (ISO, 2009)		✓	✓	✓
The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood (Australian/New Zealand Standard). (Renn, 2005)			✓	✓

Table 1 – continued from previous page				
Definition	Consideration of human life	Consideration of the unknown	Deviation from plan objectives	Function of probability and impact
In a technical perspective, risk refers to two variables the probability of occurrence of a specific instance of damage and the extent of that damage. The social science perspective focuses on aspects of societal and psychological risk experience and risk perception, while socio-economic approaches focus on risks to livelihood, security and the satisfaction of basic needs (German Advisory Council on Global Change, GACGC). (Renn, 2005)		✓		✓
The potential for realisation of unwanted, adverse consequences to human life, health, property, or the environment; estimation of risk is usually based on the expected value of the conditional probability of the event occurring times the consequence of the event given that it has occurred (Society for Risk Analysis, SRA). (Renn, 2005)	✓			✓
The probability of harmful consequences, or expected losses (death, injuries, property, livelihoods, economic activity disrupted or environment damaged) resulting from the interactions between natural or human-induced hazards and vulnerable conditions (UN Living with Risk Report). (Renn, 2005)	✓			

Table 1 – continued from previous page				
Definition	Consideration of human life	Consideration of the unknown	Deviation from plan objectives	Function of probability and impact
A probability of an adverse outcome, or a factor that raises this probability (WHO World Health Report 2002)?. (Renn, 2005)			✓	
The combined answers to (1) What can go wrong? (2) How likely is it? and (3) What are the consequences? (US Nuclear Regulatory Commission). (Renn, 2005)			✓	✓
Knowledge based (subjective Risk): Risk=(A,C,U), where U is the uncertainty about A and C (will A occur and what will the consequences C be?), including uncertainty about underlying factors influencing A and C. (Aven, 2010)		✓		✓
Expected losses (of lives, persons injured, property damaged and economic activity disrupted) due to a particular hazard for a given area and reference period. Based on mathematical calculations, risk is the product of hazard and vulnerability. (European Environment Agency) (Renn, 2005)	✓			✓

2.2 Risk Management and Risk Assessment

After one has been accustomed with the definition of what actions could be considered as a risk to an organisation, the next logical action would be to try to imagine what these risks could be, what would be the impact to the organisation, what would the organisation do to protect itself and what would the reaction be if the protective measures failed. This process is known as risk management and is an integral part of most business operations. The goal of a generic Risk management process is to protect an organisation from future risks and ensure the business continuity (Business Continuity Planning, BCP).

A lot of different approaches and frameworks exist among risk management practitioners

themselves and the academic community as well. Most of them have emerged from public intuitions or government bodies since risk can have many aspects involving a lot of different elements of public interest. These tend to be quite extensive with a significant amount of supporting documentation. Among these, risk assessment and risk management are treated quite differently. For example in some, risk assessment is part of risk management while in others they are set apart as different processes in the risk protection effort of an organisation. In most of the approaches and frameworks risk assessment and management mean also different things. A practitioner or researcher can find different items in their set tasks and description for each phase or process.

For more information on the various available methodologies and tools, the European Union's Agency for Network and Information Security (ENISA) has compiled a list comparing available methodologies including their respective tools for risk assessment and risk management (ENISA, 2014). Since the purpose of this thesis is not to conduct a comparison and evaluation of the available methodologies, only a few examples and some in relation to ICT security will be presented to showcase the differences between them. Some like the ISO and CRAMM are not available for free so the information provided here is somewhat limited from external references to them.

2.2.1 The IRGC Risk Governance Framework

For example, the International Risk Governance Council (IRGC) provides with a Risk Governance framework, shown in Figure 1, where risk management is one of the four procedures in the framework while risk assessment is only one aspect in the risk appraisal procedure (Renn, 2005). The risk effort starts with a Pre-assessment phase, which aims to identify certain issues of stakeholders and environmental indicators that could help practitioners to characterise what can be considered as risk. This phase is followed by Risk Appraisal, with the target of making decisions on how to reduce, contain and establish the knowledge base on whether to accept or not the occurrence of risk and its possible consequences. The Risk assessment process included here is set to identify the source of a possible risk, quantify the probability of its occurrence and its possible impact. Main tasks in risk assessment are the hazard identification and estimation, the exposure and vulnerability assessment and risk estimation.

Tolerability and Acceptability Judgement phase follows where risk and its consequences are actually characterised as acceptable and/or tolerable or not, then argumentation on the need of risk prevention and mitigation measures is provided to decision makers. The last phase in the framework is risk management. This phase involves the generation, evaluation and selection of the appropriate measures based on the knowledge base established on Risk Appraisal. This phase ends with the actual implementation of these measures and the monitoring of the performance of these against real life situations.

2.2.2 The ISO 31000:2009 Risk Management Framework

The latest ISO standard for risk management, the ISO 31000:2009, has its basis on the Australian/New Zealand standard, AS/NZS 4360:2004 (Purdy, 2010). For ISO risk as-

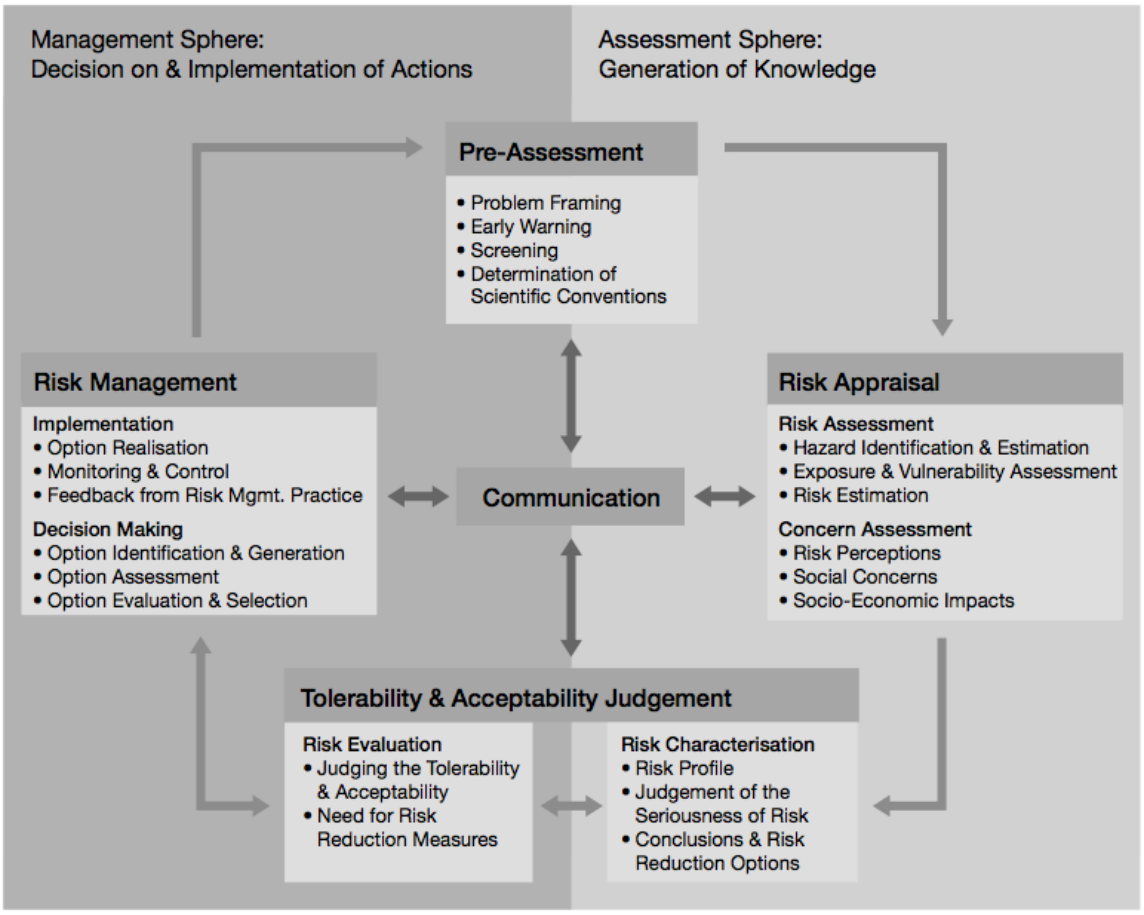


Figure 1: The Risk Governance Framework from IRGC

sessment is a core part of the risk management process. Risk management is a stepwise process and starts with establishing the environment where risk needs to be set. Then risk assessment occurs which involves risk identification, analysis and evaluation to be followed by Risk Evaluation. Risk Evaluation involves the evaluation of a possible risk against certain predefined criteria to assess the significance of it. Furthermore in risk identification one must conduct tasks like hazard identification, exposure assessment and consequence of impact. After risk assessment, Risk treatment follows with implementing countermeasures to risk All the steps are supplemented by continuous communication, monitoring and review of what has be done in each step.

2.2.3 The CRAMM Framework

NATO is using the CRAMM methodology, shown in Figure 2, which is based on a computer software for risk assessment and management (NATO Science and Technology Organization, 2008, ch. 3,p. 1). It is mostly focused on security risk management of personnel, physical infrastructure and information. It consists of three main stages; stage one is the assessment of the value of information and the assets that support business processes, stage two is aimed at identifying the threats to these assets and how vulnerable are they to these threats reaching to a conclusion about risks, stage three is focused on the countermeasures that need to be established for these risks including improvement to existing

ones. Based on CRAMM, risk management is a different process from assessment, while the latter includes tasks as risk identification, analysis and evaluation.

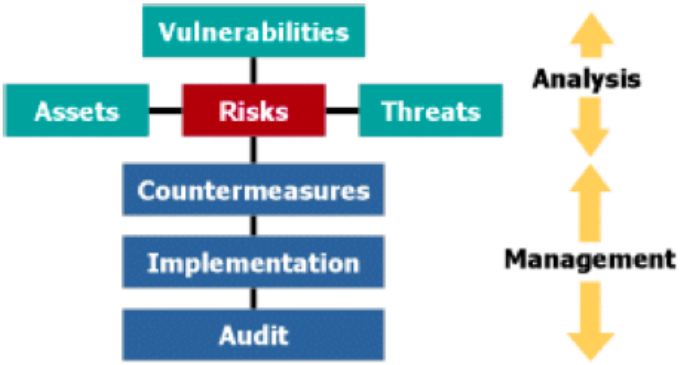


Figure 2: The CRAMM methodology

2.2.4 The NIST framework for Managing Information Security Risk

The National Institute of Standards and Technology (NIST) of the United States' (U.S.) Department of Commerce, has developed a risk management framework tailored specifically for the needs of information systems' security (NIST, 2011, ch. 1,p 1). The framework draws on standards and guidelines established also in the ISO 31000:2009 framework for risk management, thus certain similarities are expected. The framework deals with things like defining the components of risk management which include i) the framing of risk, which aims to establish the general environment where strategic decisions about risk need to be made, ii) the assessment of risk by the organisation based on the frame developed earlier; this is performed by identifying the threats to the organisation, the internal or external vulnerabilities and the possible harm/impact the organisation can have once these threats exploit certain vulnerabilities, iii) the organisation's response to risk, which includes the development of alternative actions to tackle risk, the evaluation of those, the decision on which ones to select based on the organisation's risk tolerance set in the framing and the actual implementation of those actions and iv) lastly the monitor of risk over time to verify that the planned actions are consonant with existing regulation, guidelines and standards; assess the effectiveness of these actions against reality and identify possible new risks from changes in the environment where these actions and the systems they are planned to protect operate.

2.2.5 The OCTAVE approach to Risk Assessment

OCTAVE stands for Operationaly Critical Threat, Asset and Vulnerability Evaluation and it is a risk assessment methodology developed by researchers at Carnegie Mellon University in the U.S. (Alberts, Dorofee, Stevens, & Woody, 2003). It is described by its creators as a risk based strategic assessment and planning technique with a focus on information security. Unlike other risk management frameworks where they handle risk on a continuous basis throughout the lifecycle of the organisation, OCTAVE is an evaluation activity, it has a specific beginning and end. Should the organisation want to perform another run it should start from scratch. It sets certain criteria on how to identify, analyse

and evaluate risk. The aim of the framework is to balance between the security practices of the organisation and the operational risk it may face.

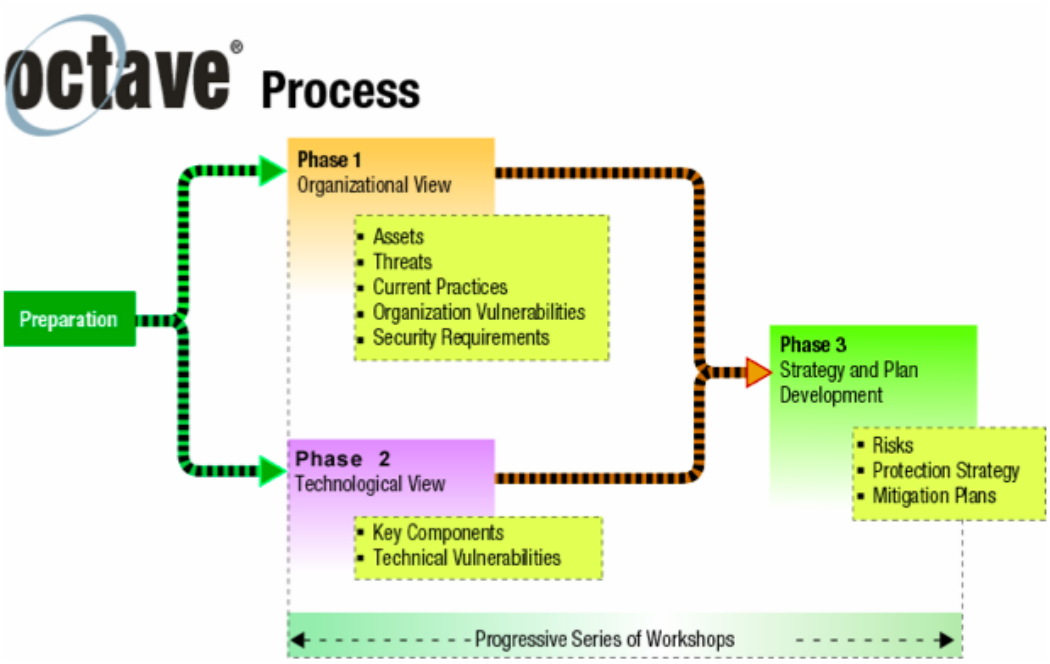


Figure 3: The OCTAVE risk assessment Process

As shown in Figure 3 it consists of the preparation and three phases:

Preparation is done when the organisation decides to start with the risk assessment and an interdisciplinary team to conduct it is formed.

Phase 1 aims to build threat profiles for the organisational based on the critical assets of the organisation. First the organisation needs to decide on what is important related to information-assets, then decide which of these are critical, set the security requirements for each and identify the threats for each asset.

Phase 2 aims to identify the vulnerabilities in the information infrastructure as a whole. Thus identifying the network paths and the classes of ICT components related to each critical asset.

Phase 3 develops a security strategy and plan for the organisation based on risks that are identified and mitigation plan decided to address them.

Later the team has developed an additional framework, OCTAVE-S, which is tailored for smaller sized organisations and it consists of five process similar to the phases of OCTAVE (Carnegie-Mellon University, Software Engineering Instution, 2014).

Process S1: Identify Organisational Information, by defining a set of measures which will be the base to evaluate the impact of risk to the organisation, identifying the assets and evaluating the security practices related to them.

Process S2: Create Threat Profiles, by selecting the critical assets, setting the security requirements of those and identifying the possible threats.

Process S3: Examine Computing Infrastructure in Relation to critical Assets, by examining the paths to access the critical assets and analyse processes related to technology

Process S4: Identify and Analyse Risks, by evaluating the probability and impact of threats

Process S5: Develop Protection Strategy and Mitigation Plans, by examining the current protection strategy, selecting appropriate mitigation measures, develop these, identify the necessary changes to the protection plan and any additional future steps.

An additional framework to the OCTAVE series is the OCTAVE Allegro, shown in Figure 4, developed later from the ISACA institution in an effort to simplify and streamline the process of risk assessment (Caralli, Stevens, Young, & Wilson, 2007). It consists of four phases (Panda, 2009):

Phase 1: To establish Risk Measurement Criteria by defining the organisational drivers that will be used to measure the effect of a risk to the organisation.

Phase 2: Create Assets Profiles, developing profile for the information assets and identifying where they are located.

Phase 3: Identify the threats, by recognising areas of concern in the information assets and the possible threat scenarios.

Phase 4: Identify and Mitigate Risks, by identifying possible risks, analysing them and selecting a mitigation approach.

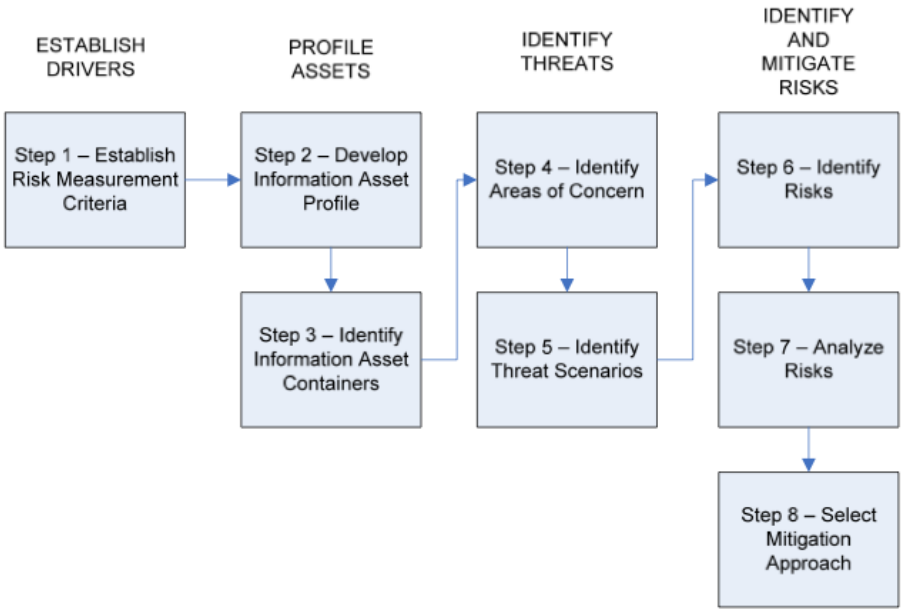


Figure 4: The OCTAVE Allegro methodology

As we can observe and is expected, the three methods share similar characteristics like at the initial stages where the organisation needs to set the environment where risk assessment will take place or the selection of the assets that are critical for the operation or the value generation of the organisation from early on.

2.2.6 The Risk IT Framework

The Risk IT Framework is developed by the former Information Systems Audit and Control Association now known only by its acronym, ISACA (ISACA, 2009). The framework is aimed at handling risk related to ICT of an organisation. It is related to both risk of implementation of ICT projects (software and hardware) but also to risk around the security of ICT assets. The framework draws from already existing frameworks developed by ISACA, COBIT a framework for control and governance of business driven, ICT based services and VAL IT a framework aimed to help organisations to maximise their return on investment from ICT solutions. The framework can be seen in Figure 5.

Figure 5: The RISK IT Framework by ISACA organisation

It consists of several processes that are grouped in three domains:

Risk Governance where the environment that risk management will be performed is set, like the risk appetite and tolerance of the organisation, the risk culture and

the people who are responsible and accountable for the processes or just need to be aware and part of the communication flow.

Risk Evaluation where the impact of risk on the business functions of the organisation is estimated. Then certain risk scenarios are created to test the frequency of these occurring and the impact to the organisation.

Risk Response where specific Key Risk Indicators (KRI's) are defined to measure the susceptibility of the organisation to certain risks. Then an identification of possible responses needs to be made to either avoid, reduce, share or transfer, or accept the risk. A decision of what type of response is appropriate for each risk follows.

risk assessment is part of Risk Governance only as a single process that aims to identify the value generating assets of the organisation and potential threats to them. It produces an overview of the major risk factors for the organisation and are later the foundation for the risk scenarios.

2.3 Cybercrime

In this section we give a short description of the birth of the internet and how it could be used with malicious purposes along with what actions can be characterised as cybercrime.

2.3.1 The internet as a venue to perform criminal activities

The internet was first introduced to be an open communication standard to facilitate academic research purposes by the Defence Advanced Research Projects Agency (DARPA). The first envisioning of it was more or less as it is now in its current state, a global network of interconnected computers that could access data and software from any location (Leiner et al., 2009). The effort started as a way to access files that were remotely stored in a different computer and to facilitate communication among researchers. The first remote network connection was established in 1965 (Leiner et al., 2009). Since then the internet has been increasingly becoming a very important part of modern life in both private and business life. This means that most of the devices we use today are somehow connected to the internet to deliver or enhance their functionality.

However, the proliferation of the internet meant from early on that a lot of computer systems were now easily accessible by people other than the owner or user of that computer. That person could have legitimate access to the computer or he/she could be an external threat that tried to gain illegitimate access to it and retrieve information not intended for him/herself or perform other type of damage to the device itself or to the network. With the help of computers and the internet, traditional criminal activities have found a new venue for execution, while newer forms of criminal activity have emerged. One can hardly think of a criminal activity with the use of computers that is not using the internet as the medium to reach the target.

Also, according to researchers like Grabosky and Clough (Grabosky, 2001; Clough, 2011),cybercrime is the best application of the maxim that crime follows opportunity. The internet and our increasing reliance on devices that are connected to it provide an easily accessible

target for criminal activity, regardless whether the target is an individual or an organisation. In addition the devices that are connected to the internet can be part of a network within the internet, used unwillingly to attack another network.

Moreover, the standards which were developed initially to achieve the connection between remote computers, are based on the sending and receiving of data packages, a technique introduced by Kleinrock (Kleinrock, 1961).

2.3.2 Current status of the definition and typology of cybercrime

Academic research around cybercrime is quite young and because of the medias fondness of the criminal activities related to technology, the term was more or less imposed without first defining exactly what type of activities can be considered as cybercrime. Cybercrime is a term invented and used mainly by the media, legal disciplines and only later by academics to describe a criminal activity that is related with technology (Hunton, 2009; Wall, 2001, 2010). The word is a compound one from the words cyber and crime. According to Wall (Wall, 2010) cyber has its origin from the Greek word "kybernetes" which means the person who governs. The term cyber became quite easily a term to describe the digital word of technology i.e. cyberspace. Since recently, cybercrime is becoming a big priority for both private and public organisations, considering that the consequences of such criminal activity can be quite severe, thus motivating them to take action to monitor and defend against such. Therefore, it is only by chance that the term cybercrime has also a relative linguistic connotation to the phenomenon (Wall, 2010).

Recent research has focused on trying to define what types of criminal behaviour may be under the scope of the term cybercrime, with some researchers arguing that perhaps cybercrime is not a new type of crime and current legal frameworks are adequate enough to battle these offences (Kleve, De Mulder, & Van Noortwijk, 2011; Wall, 2010). The difficulty in coming up with a definition of cybercrime derives mainly from the fact that in some cases a certain activity or the means used to perform this activity may not be considered illegal in all countries (Cross, 2008; Hunton, 2009). Some activities can be just unacceptable behaviour that may not be prosecuted at all or with different scale and punishment among various jurisdictions.

One of the early definitions for cybercrime comes in the form of just computer crime when the proliferation of the internet was at its early stages and originates from a legal practitioner in 1989. Donn B. Parker, in an effort to help the US Department of Justice tackle the new phenomenon of that time (Parker, 1989). The main characteristic of computer crime is that it is a business or white-collar crime committed inside or with the help of a computer. Parker distinguishes three types of computer crimes:

1. Crimes where the computer is actually the target of a physical attack,
2. Computer related crimes where the criminal activities require computer related knowledge for their perpetration, investigation and prosecution and
3. Computer abuse crimes which include not necessarily criminal activities, but also behaviors involving computer knowledge where an individual could have gained something while another suffered or could have suffered loss.

The networked nature of cybercrime is only implied by the use of a computer system, while the definition goes as far as to include also crimes where the use of a computer is necessary for the prosecution procedure, probably because the computer would be an incidental aspect to the committing of the crime.

Clough recognises three types of criminal behaviour when trying to provide a definition for cybercrime (Clough, 2011) :

1. Crime in which the computer or the network itself is the target of the attack.
2. Existing crimes where the computer is just a tool to commit these crimes.
3. Crimes where the use of a computer is incidental to the execution of crime itself, but may still provide evidence useful for the law enforcement purposes.

On the first type of criminal behaviour in general belong activities that aim to render a network or a certain node of the network as ineffective and for example make a website of an organisation inaccessible for a certain period of time, or deface it by placing content other than that the owner intended (Grabosky, 2001).

On the second type of criminal behaviour belong traditional criminal activities that with the help of computers and the internet have found a new way to achieve their purpose. As discussed the internet provides access to a lot of possible targets, thus i.e. a potential hacking attempt to compromise a banks database to get access to customers information can have a very big impact based on the expertise of the offender and the vulnerabilities of the banks ICT infrastructure in place.

What is more troubling is that the same offender with the same tools with little additional customisation can attack more than one target consequently in a short period of time. Thus, the impact of a single offender can be quite high while the probability of a successful attack may be low depending on the defences in place. The probability that the same offender will try to mimic the attack to another network can be considered high, thus even more increasing the magnitude of such criminal behaviour.

The third type of cybercrime according to Clough, cannot be considered as a type of criminal behaviour related to the use of technology. The technology in this situation is used for purposes other than that of the execution of the crime, but rather perhaps for coordinating the criminal activity itself or keeping a record of the activities. Although such occasions may prove extremely useful when taking legal action against the criminals, it can hardly be categorised as criminal activity. It would be similar to calling a technology crime every crime that was organised with the help of a telephone landline or mobile phone when they were first introduced. The use of technology here, as with the definition of Parker, is merely incidental and thus it would be too much of a generalisation to include it under the term cybercrime.

According to Cross (Cross, 2008) the UN definition of cybercrime can be considered in two different contexts, a narrow and a broader one. The narrow definition is that cybercrime refers to any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. The broader definition

is that cybercrime is any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network. Both terms are more in tandem with the first two definitions of Clough stated above. They identify the usage of a computer system to perform the criminal activity and also that a computer or a network can be the target including the data contained within. Also they recognise that a computer may also serve as a tool to commit already existing criminal activities like fraud, intellectual property and identity theft. They also prefer to ignore the incidental aspect of computer usage in a criminal activity.

David Wall initially tried to provide a framework to help researchers to identify and categorise criminal activities that can be considered as cybercrimes (Wall, 2001). His framework is considered as quite comprehensive and relevant to understand the role of modern technology in criminal activities (Holt & Bossler, 2014). The framework consists of four categories (Wall, 2001; Holt & Bossler, 2014):

1. cyber-trespass
2. cyber-deception/theft
3. cyber-porn and obscenity and
4. cyberviolence

Cyber-trespassing is considered any unwanted or illegal crossing of set boundaries of ownership either salient or invincible. This is typical in cases as described earlier when individuals or organisations attempt to access a computer system or network on which they do not have legitimate access rights. This categorisation includes also the creation and distribution of malware that can serve in automating the process of infiltration. In this case the attack on a system may not necessarily be live, but can happen at a later time when a malware has been installed and/or executed.

The second category cyber-deception/theft refers to the stealing of data or items of value either from individuals or from organisations. This could be the unauthorised copy and distribution of intellectual property like patents, multimedia, business sensitive information etc. Another criminal activity under this category could be to digitally impersonate a person to acquire legal or illegal goods; using stolen data like ID and credit card information. This category is very closely related to cyber-trespassing, since in order for a criminal to acquire these data before using them he/she needs to infiltrate a computer system or database where this information is stored.

The third category of cybercrime is cyber-porn and obscenity. The offences under this typology are varying from the computer being the medium to communicate, plan and organise these offences to the distribution of sexually explicit material. This is a typical example of activities that are on the thin line of being characterised as crimes among various jurisdictions. For example not all sexual expressions and fetishes are considered as illegal in all countries or the providing of such as a commercial service to customers. Of course there are cases like pedophilia and the distribution of online sexual material, which is illegal in all countries. Under this typology computers are just the medium to perform

the crime and do not target other computers or networks. This is a typical example of existing criminal activities, which have found a new venue to operate.

The last category in Walls framework is cyberviolence, including behaviour that aims at causing harm to individuals in the real or virtual environment. Cyber-stalking/harassment and bullying have gathered some spotlights in the news the past years due to suicide incidents of teenagers that were targeted by such behaviors. Another activity could be the use of social media to promote civil unrest and infuse terror to the general population (Wall, 2001).

As we can see the first framework of Wall aims to categorise cybercrime with respect to their relation to existing criminal activities; perhaps in an effort to help law practitioners to tackle the new at that time phenomenon of cybercrime. He later defines further categorisation for these offences into only three categories that are more related to the role of the technology itself than that to the crime committed. These are:

1. Crimes that take into advantage exploits in ICT, computer integrity crimes,
2. Crimes that target the content of computers, computer related crimes and
3. Computer content related crimes, criminal activities related to the distribution of pornographic material and/or dissemination of hate material (Wall, 2004, 2010).

The last category still refers to a certain type of criminal activity perhaps because of the scale and magnitude of it. The first two categories are also comparable to the first two behaviors of Cloughs definition for cybercrime.

Only later did Wall provide a definition for what can be considered cybercrime. He considers cybercrimes: "criminal or harmful activities that are informational, global and networked and are to be distinguished from crimes that simply use computers. They are the product of networked technologies that have transformed the division of criminal labor to provide entirely new opportunities and new forms of crime which typically involve the acquisition or manipulation of information and its value across global networks for gain" (Wall, 2007).

2.4 Critical infrastructure

Modern societies in the developed or developing world are depending on various services for the their normal operation and that of their households. These services include, but are not limited to the provision of electricity, gas, fresh water, sewage and water treatment, landline communication etc. Besides these fundamental services, several more exist that contribute to the normal functioning of a society like healthcare, transportation networks, banking and financing, emergency services etc. The more developed a nation the more complex services that are considered essential or basic can be recognised within a society. These services are widely referred to as infrastructures and are basically the backbone that fuel our daily life operations. For example for the U.S. infrastructure is "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of

essential goods and services" (Rinaldi, Peerenboom, & Kelly, 2001). According to the Organisation for Economic Co-operation and Development (OECD), infrastructure includes tangible assets and/or to production or communication networks, plus the intangible assets like products and services offered by the former (Gordon & Dion, 2008).

One can easily understand the severeness of a situation where one of these infrastructures was unable to provide the services it was designed to, due to unexpected reasons outside of our influence. All the services based on that infrastructure would be inaccessible to citizens, government agencies or other infrastructures as well. This is of most significance since one infrastructure is not a stand alone silo of services but it is rather dependent on other infrastructures as well, while several more infrastructures may be dependent on that one (Rinaldi et al., 2001). The downtime of one infrastructure could have various implication to the provision of its services and towards other infrastructures as well. The dependences between infrastructures and the consequences of a downtime can have, according to Rinaldi, nth order layers of effects. For example in the case of a disruption in the power grid distributing electricity, a first order effect could be a downtime in the oil production facilities which could to lead to a second order effect, the shortage on jetfuel, which in turn would lead to a third order effect the cancelation or rescheduling of commercial flights (Rinaldi et al., 2001). In addition as Boin and McConnell argue, modern infrastructures are so complex and tightly interdependent that small disruptions in their operation could lead to major crises. These crises due to the complexity and interdependence of the infrastructures could easily escape geographical and functional barriers and affect the wider population within a nation, or other nations as well (Boin & McConnell, 2007).

According to Rinaldi et al. there are four types of interdependencies among the infrastructures (Rinaldi et al., 2001):

Physical Interdependency when the states of two infrastructures depend on the material output of the other,

Cyber Interdependency when the state of an infrastructure depends on information transmitted through the information infrastructure.

Geographic Interdependency when a local adverse event can affect the state of infrastructures, then these are geographically interdependent.

Logical Interdependency when the state of one infrastructure depends on another's state in a way that is not physical, cyber or geographical, then these infrastructures are logically interdependent.

The adverse effects from the downtime or underperformance of an infrastructure can be generally categorised in (Stamp et al., 2003):

1. Physical Impacts, which include direct consequences like injury or the loss of human life, property damage or damage to the environment etc.

2. Economic Impacts, a second order effect from the physical ones including economic loss to the owner of the infrastructure that could transfer also from the local to the national economy.

3. Social Impacts, a second order effect from the physical ones, like the loss of confidence in the state and government that could lead to civil unrest or extremism.

As we can understand the consequences of a non-functioning or under performing infrastructure can be quite severe and are not always apparent. Thus, the protection of these infrastructures against unwanted events that could obstruct their normal operation is of outmost importance for any society.

However, not every single infrastructure can be protected to the same level, since not every single one is as crucial to the normal operation of a nation. For example some infrastructures can stay out of service for days or even weeks without heavily disrupting the normal daily activities while with others even with a downtime of a few hours the consequences could be quite severe for normal daily operations like the provision of electricity discussed before. An effort to protect all the infrastructures to the same level of security could very likely be redundant in some cases, but it would also mean an enormous amount of resources to achieve it. Therefore, the infrastructures that are most critical must be recognised and protected to a level in accordance to the severity of the consequences of their downtime. Such infrastructures are referred to as critical infrastructures (CI) and should have a prominent part in the contingency plans of most organisations.

Specifically among various governments different definitions of what is a critical infrastructure exist. For the United States (U.S.) critical infrastructures are "the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole." (Rinaldi et al., 2001; Moteff & Parfomak, 2004).

European Union (E.U.) defines critical infrastructure as "an asset, system or part thereof located in member states that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a member state as a result of the failure to maintain those functions." (Hämmerli & Renda, 2010).

For the OECD critical infrastructure is one "that provides essential support for the economic and social well-being, for public safety and for the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far-reaching damage" (Gordon & Dion, 2008). Church et al. define critical infrastructure as "those elements of infrastructure that, if lost, could pose a significant threat to needed supplies (e.g., food, energy, medicines), services (e.g., police, fire, and emergency medical services (EMS)), and communication or a significant loss of service coverage or efficiency" (Church, Scaparra, & Middleton, 2004).

2.4.1 Critical Information Infrastructure

As already discussed, the infrastructures described in the previous section rely on ICT systems, both hardware and software, for their normal operations. Especially with the

advent of technology previously manual labour like the turning of valves to release a water flow in an electricity producing factory, has been replaced by sophisticated electromechanical equipment, able to perform this operations from a remote location. These systems are called Process Control System (PCS) or SCADA systems (Stamp et al., 2003).

In the past, these systems used to be based on simple connections between a terminal and a remote sensor or actuator, usually located in close proximity and without connectivity to the internet. As already discussed in Section 1, the need for companies to modernise their facilities in order to cut costs and be more efficient lead them to have more centralised control structures and demand even more remote capabilities for the SCADA systems, including also the capability to connect to the corporate network and the internet. Therefore, the security of these networks against attacks from the internet has become a serious concern for infrastructure owners. And as also Amanallah et al. mention the security of the network of the infrastructure owner is reflected on the security of the SCADA network. Johnson mentions that even if the SCADA network is separated from the corporate intranet or internet, there should be a connection point on a computer system on a higher level where traffic from these would aggregate. The information systems supporting these control mechanisms which in turn support the functioning of the entire infrastructure are referred to as critical information infrastructure (CII). We can observe that the definition of critical infrastructure provided in the previous subsection from Church, Scaparra and Middleton is broad enough to include also critical information infrastructures.

According to Hämmerli critical information infrastructure is "Information and Communication Technology systems that are essential to operations of national and international Critical Infrastructures" (Hämmerli & Renda, 2010). OECD identifies the differences in the definition of critical information infrastructure among its member states and provides only with a generic understanding of what CII is for all members. Thus, it is in general information components supporting the critical infrastructure, information infrastructure supporting essential components of government functions and essential to the national economy (OECD DSTI/CICCP, 2007). At a later year the organisation tries to force a definition that is more similar to that of the critical infrastructures; so in 2008 they propose that critical information infrastructures are "those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy" and are identified through a risk assessment process performed by government institutions (OECD DSTI/CICCP, 2008).

2.5 From cybercrime to cyberwarfare

In the previous section we elaborated briefly on the consequences of a downtime or underperfomance of a critical infrastructure for a nation or the society. However we did not address the issue of the actor and the political implications of these attacks. Who could potentially benefit from such a situation where some major national operations are disrupted for an undefined amount of time? Such critical components may be the target of another nation or terrorist group among others, who can exploit such disruptions in many different ways (Nicholson et al., 2012). This is better understood if we consider for example the case of the war between Russia and Georgia in 2008. During the 5 day pe-

riod that it lasted there where physical and non-physical attacks against Georgia. Russia launched a series of cyber attacks that disrupted the function of some government sites providing vital information to citizens, but also disrupting the country's internet traffic further hurdling the communication and information flow among government agencies and to the western world (Beidleman, 2009).

In such a situation we do not merely deal with cybercrime, but we have a more directed attack towards specific targets, a nation's critical infrastructure, with the intention to compromise a country's ability to normally operate and perhaps defend against an attacker.

What a country can do against these attacks is to deter the intentions of possible attackers and defend itself in case the former does not work and a cyberattack occurs by reducing the capabilities of the attacker (Liff, 2012). The deterrence can be in a form of statements like for example in the U.S. where they have stated that any kind of attack against the U.S. either physical or non-physical will be addressed with military force, and with nuclear weapons in its arsenal, such a threat can act as a deterrent. Cyberdefence can be all types of information security mechanisms employed to protect the critical information infrastructure against unwanted intrusion of unauthorised personnel and against cyber attacks intending to damage the critical infrastructure. Both the attack and defence capabilities of a country are referred to as warfare. With respect to cyberwarfare specifically we have some definitions below. The lack of a definition from the European Union is somewhat odd.

According to Liff, "first, the term cyberwarfare applies strictly to computer network operations (CNO) whose means if not necessarily its indirect effects are non-kinetic. Second, it does not include operations in cyberspace that constitute psychological warfare. Third, and most importantly, cyberwarfare is conceptualised as including only computer network attacks (CNA) with direct political and/or military objectives - namely, attacks with coercive intent and/or as a means to some strategic and/or brute force end - and computer network defence (CND)" (Liff, 2012).

For the U.S. cyberwarfare "can include defending information and computer networks, deterring information attacks, as well as denying an adversarys ability to do the same. It can include offensive information operations mounted against an adversary, or even dominating information on the battlefield" (Hildreth, 2001).

Parks and Duggan provide with a definition which is a sum of two definitions to better understand the context of cyberwarfare. Thus, "cyberwarfare is the sub-set of information warfare that involves actions taken within the cyber world. The cyber world is any virtual reality contained within a collection of computers and networks. There are many cyber worlds, but the one most relevant to cyber-warfare is the internet and related networks that share media with the internet" (Parks & Duggan, 2011).

War is a political act of violence and is a way to coerce a nation in doing or not doing something according to another actor's will (Von Clausewitz, 2004; Liff, 2012). Recent events in regards to cyberwarfare (e.g. Stuxnet) had shown us that violence is not necessarily a characteristic of modern warfare. Liff argues that the cyberwarfare capabilities

owned by a country may slightly increase the occurrence of cyberwar, since they cost less than physical war for weaker actors, with cyber attacks the attackers can confuse the target that another nation is behind the attack and when used as a surprise attack before a physical attack it may change the power balance in favour of the attacker (Liff, 2012). A lot of nations are realising that and have started developing their cyberwarfare arsenal for potential use, with the U.S., France, Israel, Russia and China leading in the race (Nicholson et al., 2012).

However, some researchers argue that the term cyberwarfare is exaggerated and does not consist an act of war (Rid, 2012). Rid argues that an act of war should potentially be lethal, instrumental and have political motivation. Cyberwarfare is merely a new way to perform the classic warfare types of subversion, sabotage and espionage. Nonetheless, since the purpose of this thesis is not to argue on the appropriateness of the term or not, we shall consider that cyberwarfare exists and it is a new type of warfare. Thus, a potential attack to the critical infrastructure of a nation, through the critical information infrastructure supporting it, can be considered as an act of war.

2.6 Working Definitions

In this subsection we will provide the working definitions of the major terms to be used for the rest of this thesis.

2.6.1 Risk

Summarising the previous section we could say that for the purpose of this thesis a definition of risk should take into consideration the aspect of human life, or be broad enough to include it, the uncertainty of future events, the deviation from a set or desired future state and the likelihood of occurring along with the impact or magnitude of the deviation. Therefore, as a working definition for this thesis the one from ISO organisation is more appropriate.

The ISO definition is risk is the effect of uncertainty on objectives and then there are the accompanying explanatory notes for the practitioner to better understand the meaning and be able to assess which events or unknown situations should be considered as incidents that can affect an organisations objectives. It may not specifically mention the potential for human lives losses, but using it in a broader context it may as well include it. For example one of the objectives could be the avoidance of human casualties. Especially for the unknown according to ISO, it is the deficiency of relevant information for a future event that may occur which define it. This is worth noting since an organisation needs to be proactive when trying to identify and assess risk even if it can always imagine or predict future situations, which may derail its set objectives.

2.6.2 Risk assessment

Among the various frameworks stipulated earlier in Section 2.2, a selection of the one we will work with for this thesis needs to be made. The ISO documentation is proprietary and not freely available to download for usage and application, thus we exclude it from

our selection. CRAMM is also not a free software to access and thus it is also excluded.

The IRGC, NIST and Risk IT frameworks are quite extensive and initiate the process of risk assessment from a high level within the organisation. The IRGC framework gives a holistic approach to the process and thus it is quite vague when you actually get to implement it. The Risk IT is quite analytical with thorough documentation, but it requires knowledge of the other two frameworks developed by ISACA, the COBIT and VAL IT. Thus we exclude these two from the selection.

The NIST framework is also quite extensive with good supporting documentation but since OCTAVE is tailored just for the purpose of ICT security, and specifically the Allegro version since it is more refined and streamlined approach, we will select this framework to conduct the risk assessment for our case study.

2.6.3 Cybercrime

For the purpose of this thesis a suitable definition for cybercrime has also to be decided. As it has already been discussed, the current academic work so far was initially aimed at explaining to the laymen what a crime that involves a computer is. As also Holt and Bossler mention, the research has focused to help mainly legal practitioners to understand the complexity of cybercrime and the differences to the conventional crimes, rather than providing a single agreed definition (Holt & Bossler, 2014). David Wall is one of the early researchers to address the issue although he initially only developed a characterisation framework and later worked on a definition.

As we have already discussed also the use of the internet as a delivery mechanism for the attack is fundamental. Thus, we cannot speak of an attack to a computer without considering the networking aspect that such an attack involves. Also, the incidental use of computers to organise or create a records log of activities should not be the case for our definition. Moreover, we should bear in mind that the purpose of this thesis does not involve the taking legal action against the offenders; the possible characterisation of an offence as criminal or not should not be of significance in our definition.

Thus, we conclude that the more suitable definition is that provided by Wall (Wall, 2007), "Cybercrimes are criminal or harmful activities that are informational, global and networked and are to be distinguished from crimes that simply use computers". The definition clearly sets itself apart from the crimes where the computer is just an incidental aspect of the crime and recognises the networked nature of the use of technology. It further identifies the new opportunities cubercrime reveals for offenders either in new types of criminal activities of in new ways to perform existing ones. Furthermore, the target of the criminal activity is the information that is held by computers system either to manipulate them or just because of their significance to the owning organisation.

2.6.4 Critical Infrastructure and Critical Information Infrastructure

In Section 2.4.1 we have seen various definition about what critical infrastructure and the critical information infrastructure that supports it. For the purpose of this thesis we consider critical infrastructures according to OECD, the infrastructure "that provides

essential support for the economic and social well-being, for public safety and for the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far-reaching damage" (Gordon & Dion, 2008).

For the critical information infrastructure we require a definition that is clear enough and separates it from that of the critical infrastructure in general. We are interested only in the ICT infrastructure that supports the critical infrastructure, thus we need a definition that identifies this distinction and relation between critical and ICT infrastructures. Therefore, for our purposes critical information infrastructures are according to Hämmerli "Information and Communication Technology systems that are essential to operations of national and international Critical Infrastructures" (Hämmerli & Renda, 2010).

2.6.5 Cyberwarfare

We shall conclude our working definitions section with the definition of cyberwarfare, from the ones discussed in Section 2.5, that most suits our purposes.

We require a definition that describes and identifies the actions that could happen over a computer network with possible military and political coercive results. Firstly, the definition of the term proposed by Parks and Duggan is focusing mainly on describing the space where the actions of cyberwarfare occur. However, they do not describe what these actions are. Secondly, the U.S. definition is broad enough to describe the actions and the space they occur like for example the battlefield as was the case with the Georgia - Russia war. Lastly, the definition by Liff is the most elaborate, clearly describing the nature of the actions of cyberwarfare and their coercive intent.

Thus for the current thesis we will use the definition by Liff: "first, the term cyberwarfare applies strictly to computer network operations (CNO) whose means if not necessarily its indirect effects are non-kinetic. Second, it does not include operations in cyberspace that constitute psychological warfare. Third, and most importantly, cyberwarfare is conceptualised as including only computer network attacks (CNA) with direct political and/or military objectives - namely, attacks with coercive intent and/or as a means to some strategic and/or brute force end - and computer network defence (CND)" (Liff, 2012).

3 Risk Assessment

In the following sections we will perform a risk assessment for the critical infrastructure of the power plant using the OCTAVE Allegro approach as discussed in Section 2.6.2.The critical infrastructure and critical information infrastructure will be described and identified, along with its vulnerabilities and possible threats. A plan to mitigate these risks will be proposed, thus concluding the risk assessment.

3.1 Describing the Critical Infrastructure

For the purpose of this thesis we shall consider that the critical infrastructure is already known, located in Germany and it is the provider of the fundamental product required for almost all basic daily operations, namely electricity. More specifically a power plant fuelled by lignite is our candidate. This is in tandem with the report from Federal Ministry of Economics and Technology (BMWi) that shows the dependency of Germany in these power plants (Federal Ministry of Economics and Technology Editing team JWB 2013, 2013). Especially with the the decision of Germany to decommission its nuclear power plants by 2022 (The Guardian, 2011), the importance of lignite fuelled power plants may rise significantly to support the electricity needs of the country. As we can see in Figure 6 (Federal Ministry of Economics and Technology Editing team JWB 2013, 2013, Diagram 20), the main source to power the plants in 2012 is lignite followed by renewable sources, hard coal, nuclear power and natural gas. There is a steady increase in the amount of renewable sources but future increase may not be enough to compensate for the shutdown of nuclear plants. Thus, we assume that lignite powered power plants are some of the critical components of the energy supply for the near future.

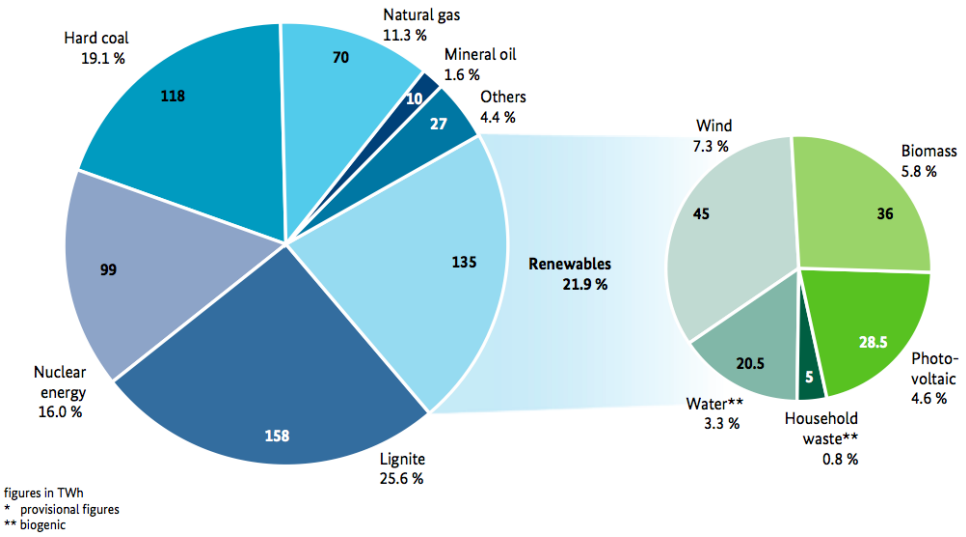


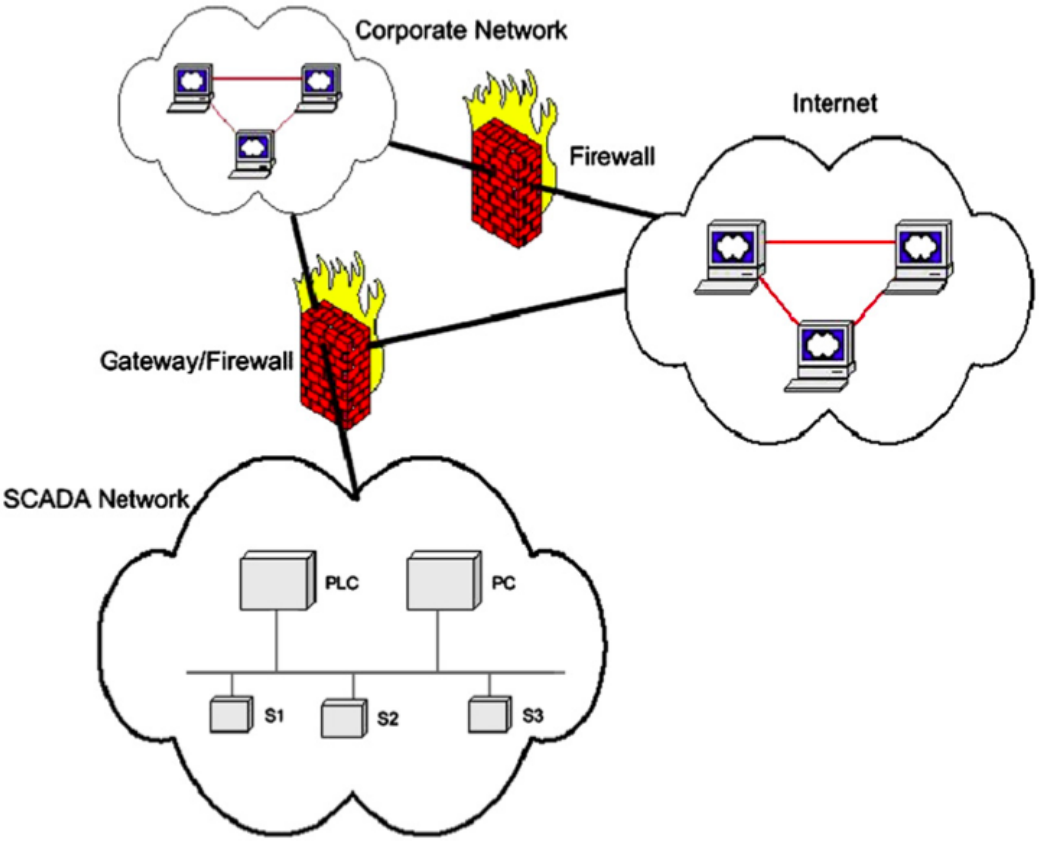
Figure 6: Gross electricity generation in Germany in 2012

The plant has two production lines operating at 90% of their net capacity. We assume that the power plant has a net capacity of 4.000 MW able to produce 8 billion kWh. This amounts to approximately 5% of the total energy needs of Germany. This particular power plant serves 3 million customers of which 10% is enterprise ones, like other industries with

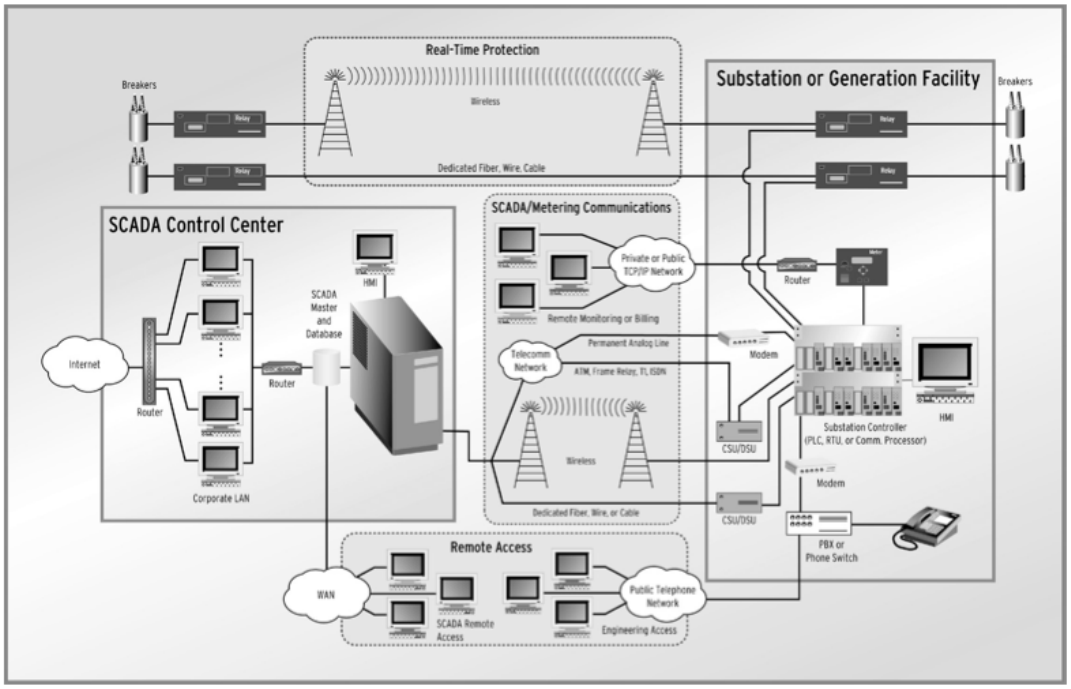
production facilities, offices of business headquarters etc. Of the 8 billion kWh, 4 billion are sold to other distributors, 2.5 billion are sold to enterprise customers and 1.5 billion are sold to commercial customers (households).

3.1.1 Describing the Critical Information Infrastructure

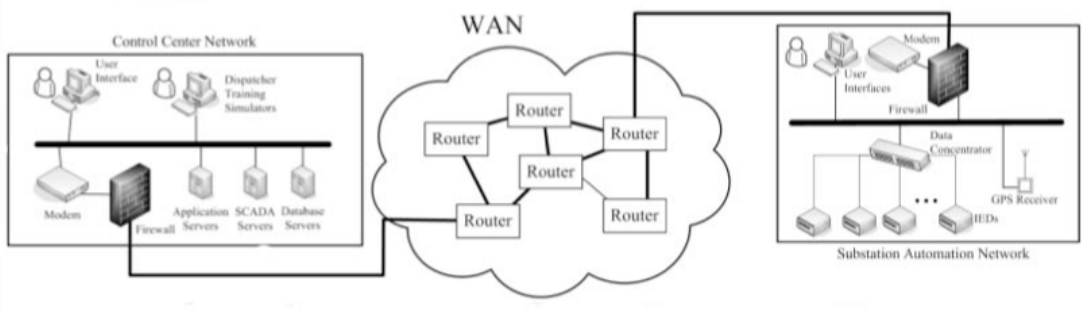
As we discussed in Section 2.4.1 any infrastructure is based on some ICT components for the operation of some electromechanical equipment defining the state of each component and in total that of the plant. These states depend on the input of these components and the outputs transmitted to other components in the electromechanical and ICT infrastructure. Usually to control these mechanisms there is a SCADA control centre established somewhere physically with close proximity to the infrastructure. However, due to the need for remote control of the mechanisms from quite distant locations, infrastructure owners have implemented connections through the internet or through their corporate network that has access to the internet as well. In Figure 7 we can see some examples of SCADA networks (Sridhar & Manimaran, 2010; Igure et al., 2006; Risley, Roberts, & Ladow, 2003).



(a) (Igure et al., 2006)



(b) (Risley et al., 2003)



(c) (Sridhar & Manimaran, 2010)

Figure 7: Some examples of SCADA networks

In Figure 7a we see that the SCADA network is directly connected to the corporate network and to the internet through a gateway that acts also as a firewall. The SCADA network consists of some servers, personal computers and a Programmable Logic Controller (PLC). Both a PC and a PLC can control actuators through the SCADA software (Igure et al., 2006). In Figure 7b we can see that the SCADA network, according to the authors, encapsulates also the corporate network and have direct access to the internet. It consists of some PCs and a server acting as the primary host of the SCADA software and as a database. The information is fed to a so called Human-Machine-Interface (HMI), a PC used to control the actuators through the SCADA software (Risley et al., 2003). In Figure 7c the SCADA network consists again of some servers for databases, applications and SCADA software purposes and two PCs one of which is used for testing, training and simulation (Sridhar & Manimaran, 2010).

We can observe that the SCADA control centre can be just any typical personal computer network setup with access to the internet and/or the corporate network, but it has

installed some sophisticated software to specifically operate the electromechanical equipment responsible for the state of the infrastructure. Connected to this network additional ICT infrastructure and networks may exist to facilitate the communication of the SCADA software with the equipment and the general operation of the plant. For our purposes we will consider as Critical Information Infrastructure the SCADA control centre since it can define the state of operation of the infrastructure and any malevolent cyber attack to the infrastructure may have as a target the underperfomance or complete powering down of the plant for an indefinite and unknown period of time. In addition since it has direct connection to the internet it can be an entry point for an attack aiming to compromise its operation Our interest will be limited only to the personal computers that form the network, they have connection to the internet and have SCADA software installed.

For the purpose of this thesis we assume that the SCADA network is as shown in Figure 8. It consists of 5 workstation, where at three of them the SCADA software is running while among those three, two of them are servers. They are connected to the internet through a gateway.

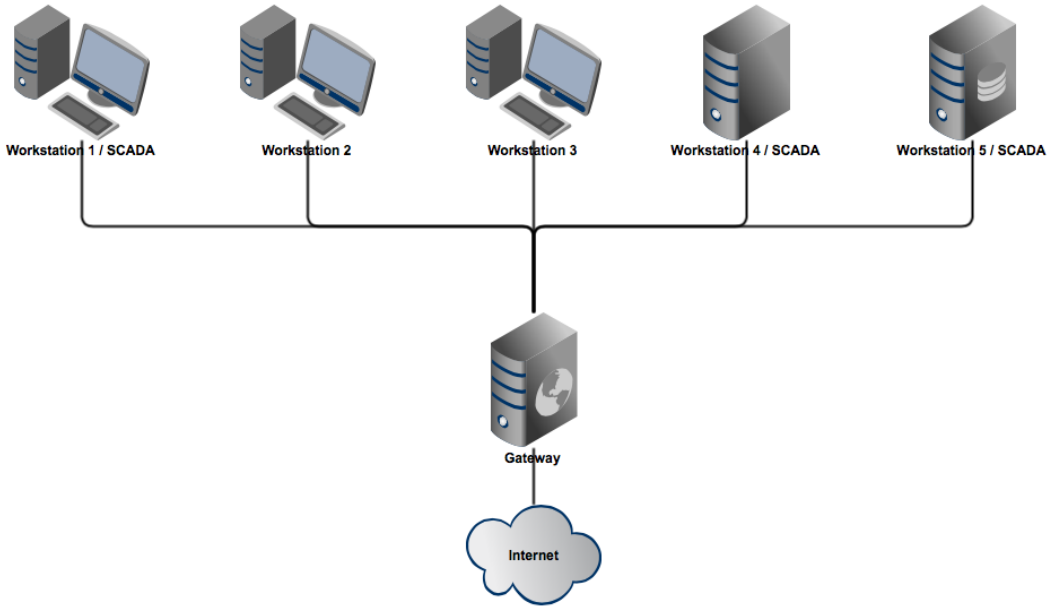


Figure 8: The virtual network simulating a SCADA Control centre

3.2 Conducting the OCTAVE Allegro Risk Assessment

The steps that were described in Section 2.2.5 and Figure 4 are presented in the following sections in regard to our critical infrastructure. More specifically as discussed in Section 3.1 our critical infrastructure is a thermopower plant fuelled by lignite and the critical information infrastructure supporting it is as we have shown in Figure 8. We will use the templates provided by the OCTAVE Allegro approach (Caralli et al., 2007, p. 65) making assumptions about the possible threat scenarios and their impact. It is important for the reader to know that OCTAVE Allegro uses the term information asset and critical information asset to refer to information infrastructure and critical information

infrastructure. In the following subsections we use the two terms alternately to avoid repetition.

3.2.1 Step 1 - Establish Risk Measurement Criteria

The first step aims to establish what could be the impact of a risk on the business strategy and objectives. This step consist of two activities, in the first one we define a set of qualitative and quantitative measures in order to evaluate the effect of risk on the critical information infrastructure. In the second activity we prioritise the impact areas according to their importance for the infrastructure owner.

Activity 1
We will consider the impact areas proposed by OCTAVE Allegro in the relevant worksheets. These are the:

- Reputation and Customer Confidence
- Financial
- Productivity
- Safety & Health
- Fines & Legal penalties
- User defined

In Table 2 we can see what we consider as an impact to reputation and customer confidence for the infrastructure owner in three scales: low, moderate and high.

Table 2: Risk Measurement Criteria - Reputation and Customer Confidence

Allegro Worksheet 1	**Risk Measurement Criteria – Reputation and Customer Confidence**		
Impact Area	**Low**	**Moderate**	**High**
Reputation (commercial)	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and no more than 100K € in worktime and money is required to recover.	Reputation is irrevocably destroyed or damaged and up to 300K € in worktime and money is required to recover.
Reputation (enterprise)	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and no more than 300K € in worktime and money is required to recover.	Reputation is irrevocably destroyed or damaged and up to 700K € in worktime and money is required to recover.
Customer Loss (commercial)	Less than 5% reduction in customers due to loss of confidence	5 to 10% reduction in customers due to loss of confidence	More than 10% reduction in customers due to loss of confidence
Customer Loss (enterprise)	Less than 2% reduction in customers due to loss of confidence	2 to 5% reduction in customers due to loss of confidence	More than 5% reduction in customers due to loss of confidence

We take into consideration four criteria, reputation for commercial and reputation for enterprise customers, customer loss for commercial and customer loss for enterprise customers. With these criteria we set different monetary values or percentages in the three scales as shown in Table 2.

In Table 3 the criteria for the Financial impact area are shown. We consider the operating costs, the earnings before interest, taxes, depreciation and amortisation (EBITDA) and one-time financial losses. We represent this with different percentages and monetary values in the three scales.

Table 3: Risk Measurement Criteria - Financial

Allegro Worksheet 2	**Risk Measurement Criteria – Financial**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 2% in yearly operating costs	Yearly operating costs increase by 2 to 5%.	Yearly operating costs increase by more than 5%.
EBITDA	Less than 3% yearly EBITDA loss	3 to 5% yearly EBITDA loss	Greater than 5% yearly EBITDA loss
One-Time Financial Loss in Euro	One-time financial cost of less than 25K €	One-time financial cost of 25 to 200K €	One-time financial cost greater than 200K €

In Table 4 the criteria for the Productivity impact area are shown. We consider the loss of productivity, fuel shortage of lignite, the normal operation of the boiler and the turbine. We represent this with days or hours of disruption to each criterion with the values as shown in the three scales.

Table 4: Risk Measurement Criteria - Productivity

Allegro Worksheet 3	**Risk Measurement Criteria – Productivity**		
Impact Area	**Low**	**Moderate**	**High**
Productivity loss	up to 1 hour lost productivity	1 up to 8 hours lost productivity	more than 8 hours lost productivity
Fuel shortage (lignite)	2 days disruption in supply	between 2 and 5 days disruption in supply	More than 5 days disruption in supply
Boiler operation	1 boiler down for 5 hours	1 boiler down for 5 up to 8 hours	1 boiler down for more than 8 hours
Turbine operation	1 turbine down for 4 hours	1 turbine down for 4 up to 8 hours	1 turbine down for more than 8 hours

In Table 5 the criteria for the Productivity impact area are shown. We consider the aspect of human life, the health of employes regarding injuries on work related accidents and health regarding the working conditions, like heat, flying ash etc. We represent this with the values as shown in the three scales.

Table 5: Risk Measurement Criteria - Safety & Health

Allegro Worksheet 4	**Risk Measurement Criteria – Safety and Health**		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to staff members' lives	A staff member has suffered some minor injuries with the need to be hospitalised	A staff member has died due to a work accident
Health (injuries)	Staff members have suffered some minor injuries without the need to be hospitalised	Staff members have suffered some minor injuries, but with the need to be hospitalised	Staff members have suffered severe injuries and need to be hospitalised
Health (working conditions)	Working conditions have become a little more adverse	Working conditions have become quite adverse threating staff members' health	Working conditions have become very adverse threating staff members' lifes. Production needs to be halted until working conditions are improved

In Table 6 the criteria for the Fines & Legal Penalties impact area are shown. We consider the fines, lawsuits and investigations by 3rd party associations for labor rights, security, health and safety. We represent this with the values as shown in the three scales.

Table 6: Risk Measurement Criteria - Fines & Legal Penalties

Allegro Worksheet 5	**Risk Measurement Criteria – Fines and Legal Penalties**		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than 100K € are levied.	Fines between 100K € and 200K € are levied.	Fines greater than 200K € are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than 200K € are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between 200K € and 400K € are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than 400K € are filed against the organization.
Investigations (Security, Health & Safety, Employee Associations)	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.

In Table 7 we have the possibility to consider another impact area other than those proposed by OCTAVE Allegro. However, we will not consider any additional impact area thus this worksheet will be left intentionally blank.

Table 7: Risk Measurement Criteria - User Defined

Allegro Worksheet 6	Risk Measurement Criteria – User Defined		
Impact Area	**Low**	**Moderate**	**High**

Activity 2

Our next activity is to prioritise the impact areas mentioned in the previous acidity according to their importance to the operation of the power plant shown in Table 8.

Table 8: Risk Measurement Criteria - User Defined

Allegro Worksheet 6	Impact Area Prioritization
Priority (1 high - 5 low)	**Impact Areas**
3	**Reputation and Customer Confidence**
2	**Financial**
4	**Productivity**
5	**Safety and Health**
1	**Fines and Legal Penalties**
	User Defined

We consider the impact area of Safety and Health to the personnel as the most critical and it is directly affected during the operation of the power plant. Any abnormal operation of the power plant or even an unscheduled shut down could have severe implications. Productivity is the next most important area since any losses in output power could cause problems to the commercial and enterprise customers of the power plant while potentially indirectly affecting also their safety and health. One example could be a warehouse that uses cranes to move bulk and heavy packages around its facilities. An energy outage could endanger the lives of the personnel there because of the sudden stoppage of the cranes.

Third in order is the reputation and customer confidence, where some negative reactions could be expected from customers; especially enterprise ones since electricity is paramount for their normal operations and any outage could be linked to possible productivity losses. The effort to win back these customers could be significant while some damage to the company name could be expected. Next in order to less important is the financial impact. Although the consequences to the revenue and profit (EBITDA) could be severe due to a prolonged underperformance or shutdown of the power plant, nonetheless the areas mentioned earlier are considered more important. while any productivity losses in the power plant could attract some regulating bodies for investigations.

3.2.2 Step 2 - Develop Information Asset Profile

With this step we will identify the information assets of the power plant and identify the critical ones formulating the critical information infrastructure. It consists of 8 activities.

We have already described the critical information infrastructure in Section 3.1.1 so we will continue with that selection, but for the sake of the risk assessment we will brainstorm on what could be an information asset for the power plant and which one could be critical.

Activity 1
Our first activity is to list the potential information assets of the power plant and decide on the critical one or ones. The information assets could be for example:

- the ERP software that is used for the business functions of the power plant and the workstations or servers it resides. It stores all the suppliers' and customers' data, has pricing info and the agreements with other distributors for electricity. It is used by Accounting (AC), Human Resource (HR), Plant Engineering, Sales and Distribution (SD), Quality and Supply Chain (SC) departments.

- the Siemens WinCC software and the workstations or servers it resides (the SCADA control centre). It is responsible for the operation of the power plant from a technical perspective. All the components of the infrastructure are controlled and monitored by this software. It is also used for drafting reports on the production yields and fuel consumption. It is used by Electricity Production, Quality, Environmental and Health and Safety departments.

- the simulation software used to test and evaluate new production scenarios and the workstations or servers it resides, interactions among new components and maintenance activities on the current ones. It is used by Plant Engineering - Installation department.

The information assets mentioned above are just an indication and listing them all would be irrelevant to the scope of this thesis.

Activity 2
Our next activity is to assess the critical information asset/infrastructure from the ones listed earlier. A disruption or unavailability of the ERP software could have significant consequences to the business functions of the power plant since it could lead to unauthorised disclosure of employee data, wrong invoices sent to customers, wrong pricing calculated in the invoices, payments to suppliers issued on wrong bank accounts etc. All these could have a sever financial impact to the infrastructure owner with potential costly legal implications. It could also disrupt the supply of lignite to fuel the power plant, but still it does not affect directly the normal operation of the power plant.

A disruption or unavailability of the simulation software could affect the operation of Plant Engineering and could cause the postponing of planned maintenance activities, but this is not directly affecting the normal operation of the power plant.

Lastly a disruption or unavailability of the Siemens WinCC software could have severe direct implications to the normal operation of the power plant possibly affecting the health and safety of the personnel working there and indirectly that of its customers, plus any government agencies depended on the electricity output of the plant. Thus, we shall consider this information asset as the most critical one, our critical information infrastructure of the power plant.

Activity 3
With this activity we start gradually filling information for the critical information infrastructure on worksheet 8 of OCTAVE Allegro, starting with the its name. As we mentioned it is the SCADA control centre, including the Siemens WinCC software and the workstations and servers it resides in.

Activity 4
Next activity is to explain the reasoning behind our selection of the critical information infrastructure. As we mentioned, the SCADA control centre is very important because it defines the state of the components and consequently that of the whole critical infrastructure.

Activity 5
Our next activity is to place a small description of the critical information infrastructure. Thus, this information asset consists of 5 workstation (two are servers), 3 of which have the Siemens WinCC software running. It receives data from all the monitoring and controlling devices in the power plant. It also controls their operation, by means of fuel flow and supply, boiler temperature, water and steam flow etc.

Activity 6
Now we need to identify the departments in the organisation that have ownership of the SCADA centre. These are the Plant Production and Plant ICT Maintenance Departments.

Activity 7
The next activity is to define the security requirements of the information asset with respect to confidentiality, integrity, availability and other like regulatory requirements. We need also to define which personnel is affected and has access to view and modify it. For our purposes we assume that the security level of the employees in the power plants is defined by the department they belong to and the level of security clearance they have, ranging from 1 (lowest) to 5 (highest).

Activity 8
The last activity is to define what is the most important security requirement for the information asset, whether it is confidentiality, integrity, availability or another one. For our purpose we consider that the most important is the availability of the critical information infrastructure for reasons explained earlier.

The outcome of all the activities of this step can be seen on Table 9

Table 9: Critical Information Asset Profile

Allegro Worksheet 8	**Critical Information Asset Profile**		
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*	
SCADA control centre	This information asset is important because it defines the state and operation of all the components in the power plant	This information asset consists of 5 workstation, 3 of which have the Siemens WinCC software running. It receives data from all the monitoring & controlling devices in the power plant. It also controls their operation, by means of fuel flow and supply, boiler temperature, water and steam flow etc.	
(4) Owner(s) *Who owns this information asset?*			
The information asset is owned by the Plant Production and Plant ICT Maintenance Departments			
(5) Security Requirements *What are the security requirements for this information asset?*			
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Access to the asset is restricted to members with level 3 and higher clearence of Electricity Production and level 4 and higher clearence ICT-SCADA	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Only members of ICT-SCADA with level 5 clearence can introduce add ons, repair or update the asset	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The asset is available through the SCADA centre of operations in the plant to level 3 and higher Electricity Production members	
	This asset must be available for **24** hours, **7** days/week, **52** weeks/year.	There is a scheduled downtime for backups and maintenance of 4 hours on 08:00 hours every Saturday. During that time the backup system is online for the operation of the plant	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	It complies to the ISO/IEC TR 27019 standard which is adopted also by VDE	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	❑ Integrity	☑ Availability	❑ Other

3.2.3 Step 3 - Identify Information Asset Containers

Next step in our risk assessment is to identify the containers where the critical information infrastructure resides. These can be technical, physical or people. All containers can be external or internal to the organisation. This step has one activity.

Activity 1

We shall use the OCTAVE Allegro worksheets 9a, 9b and 9c for this activity. The outcome can be seen Tables 10, 11 and 12

Table 10: Information Asset Risk Environment Map (Technical)

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Internal	
Container Description	**Owner(s)**
1. The SCADA centre resides in a setup of 5 workstations, on three of them the Siemens Simatic software is running	Electricity Production & ICT-SCADA
2. Infrastructure intranet: All data from controlers and actuators to the SCADA centre and information panels are transferred through this intranet	Electricity Production, Maintenance Infrastructure & ICT SCADA
3. Log files of SCADA activities and reports, hourly, daily, monthly and yearly data from controlers actuators, production yields	Electricity Production
External	
Container Description	**Owner(s)**
1. The Internet: it is used to access remotely the databases of the SCADA centre for reporting reasons	German ISP

Table 11: Information Asset Risk Environment Map (Physical)

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Internal	
Container Description	**Owner(s)**
1. Documentation and reports of daily production yields	Electricity Production
2. Manuals and handbooks for normal operation and crisis situations	Electricity Production, ICT-SCADA & Auditing
3. Documentation and reports of key activities of SCADA software	Electricity Production, Auditing
External	
Container Description	**Owner(s)**
1.	

Table 12: Information Asset Risk Environment Map (People)

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
1. Electricity Production employees with level 3 and higher security clearance	Electricity Production
2. ICT-SCADA employees with level 4 and higher security clearance	ICT-SCADA
3. Auditing employees	Auditing
External Personnel	
Contractor, Vendor, Etc.	**Organization**
1.	

3.2.4 Step 4 - Identify Areas of Concern

Our next step is to identify the areas of concerns to the information asset, namely the threats that could affect it. It consists of one activity, where using the worksheet 10 (Information Asset Risk Worksheet) of Allegro, we document as much as we can detailed information about the threat. Because this worksheet is used also by Steps 5, 6 and 7 we provide the outcome in Step 7. Only threats originating from outside of the organisation will be considered. For example it is no concern for our purposes malevolent attacks initiated by a disgruntled employee.

Activity 1

In this activity we have identified 5 types of threats that could affect our critical information infrastructure. These are a distributed denial of service attack (DDoS), port scanning, a malevolent software like a virus or malware, zero days exploits and a hardware defect. For each threat we make assumptions on who is the actor, what are his/hers means, his/hers motives, what could be the undesired outcome to the critical information infrastructure and what security requirements are endangered by the threat.

3.2.5 Step 5 - Identify Threat Scenarios

In this step we will use the questionnaires provided by Allegro, in an effort to identify additional threats than those in Step 4. It consists of three activities.

Activity 1

In the first activity we try to answer the questionnaires provided by Allegro. The questionnaires draw on the containers identified in Step 3 in Section 3.2.3 and state questions on whether an individual internal or external to the organisation, or another type of threat could have unauthorised intended or unintended disclosure of information, modification, effect on availability or destruction of the information asset.

In Table 13 we answer the questions about two scenarios. The first is the case where a person internal to the organisation would cause intentionally or unintentionally damage to the critical information infrastructure. As we discussed we do not assume that such a scenarios is possible in our case. While, a person external to the organisation (like a hacker or a hostile nation) could have interest to disclose information, modify, interrupt or destroy the information asset.

Table 13: Threat Scenario Questionnaire 1 - Technical Containers

Threat Scenario Questionnaire 1	**Technical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

In Table 14 we answer the questions about different threat scenarios like a software defect, a system crash etc. We assume that threats like a power supply disruption, problems with the communications (intranet and internet) and natural disasters are out of our scope.

Table 14: Threat Scenario Questionnaire 1 - Technical Containers (continued)

Threat Scenario Questionnaire – 1 (cont)	**Technical Containers**				
Scenario 3: In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes: ⟨ Unintended disclosure of your information asset ⟨ Unintended modification of your information asset ⟨ Unintended interruption of the availability of your information asset ⟨ Unintended permanent destruction or temporary loss of your information asset					
A software defect occurs	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A hardware defect occurs	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur (Intranet)	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur (Internet)	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	No	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

In Table 15 we answer the questions about the physical containers of the information asset. Again we assume that the case of an individual person internal to the organisation is not a threat to the physical container.

Table 15: Threat Scenario Questionnaire 1 - Physical Containers

Threat Scenario Questionnaire – 2	**Physical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	Yes (accidentally)	Yes (intentionally)
Modified so that it is not usable for intended purposes?	**No**	Yes (accidentally)	Yes (intentionally)
Interrupted so that it cannot be accessed for intended purposes?	**No**	Yes (accidentally)	Yes (intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	Yes (accidentally)	Yes (intentionally)
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	No	Yes (accidentally)	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	No	Yes (accidentally)	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	No	Yes (accidentally)	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	Yes (accidentally)	**Yes (intentionally)**

In Table 16 we answer the questions about other threats to the physical containers of the information asset like natural disasters.

Table 16: Threat Scenario Questionnaire 1 - Physical Containers (continued)

Threat Scenario Questionnaire -2 (cont)	**Physical Containers**				
Scenario 3: In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes: ⟨ Unintended disclosure of your information asset ⟨ Unintended modification of your information asset ⟨ Unintended interruption of the availability of your information asset ⟨ Unintended permanent destruction or temporary loss of your information asset					
Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Table 17: Threat Scenario Questionnaire 1 - People Containers

Threat Scenario Questionnaire – 3	**People**		
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

In Table 17 we answer the questions about threats to the people container of the information asset. Again we assume that such a threat is out of our scope.

Activity 2
Next activity is to create new Information Asset Risk Worksheets (worksheet 10) based on the answers we gave in the questionnaires of the previous activity. We assume that the threats we identified in Step 4 in Section 3.2.4 are covering the threats identified in the current step.

Activity 3
The last activity of this step is to assign a probability of occurrence to the threat scenarios identified in the previous steps. The values are qualitative and quantitative: Low (25%), Medium (50%) and High (75%).

3.2.6 Step 6 - Identify Risks

In this step we try to assess what could be the consequences of the threats to the critical information infrastructure. It consists of one activity.

Activity 1
We make assumptions about the consequences the threats could have on the information asset . For example a DDoS attack could make the critical information infrastructure unavailable to the personnel for several hours or even days and it could leave it open and vulnerable for further exploits by the actors of the attack.

3.2.7 Step 7 - Analyse Risks

In this step we assess what is the severity of the threats' consequences to the impact areas defined in Step 1 - Activity 2 in Section 3.2.1. This step consists of two activities.

Activity 1
In the first activity we assign qualitative and quantitative values for the severity of the threat: Low (1), Medium (2) and High (3).

Activity 2
In the second activity we multiply the values in Activity 1 with the priority value (1 to 5) we assigned in the Step 1 - Activity 2 in Section 3.2.1. The results for each impact area are summed up to make up a score for this particular threat. The threat score shows us the severeness of the effect of a threat to the critical information infrastructure.

The outcome of Steps 4 to 7 is for each threat an Information Asset Risk Worksheet that shows us the probability of the threat occurring and a score indicating its severeness to the information asset. This is more obvious if we have a look in Tables 18, 19, 20, 21 and 22.

Table 18: Information Asset Risk DDoS attack

Allegro - Worksheet 10a	Information Asset Risk Worksheet			
Information Asset Risk / Threat	Information Asset	SCADA control centre		
	Area of Concern	*A DDoS attack occurs targeting the SCADA control centre. The gateway crashes exposing the workstations to other forms of malevolent attacks.*		
	(1) Actor *Who would exploit the area of concern or threat?*	Terrorist group, hostile nation or hacker		
	(2) Means *How would the actor do it? What would they do?*	Using the internet and a botnet to perform DDoS attack		
	(3) Motive *What is the actor's reason for doing it?*	Gain unauthorised access and modify or crash the Siemens WinCC software		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ☑ **Destruction** ❑ **Modification** ☑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the respective authorised employees can control and modify the Siemens Simatic		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High (75%)**	❑ **Medium (50%)**	❑ **Low (25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A DDoS attack can affect heavily the operation of the SCADA control centre and lead to further attacks or exploitations	Reputation & Customer Confidence (3)	Low (1)	3
	Financial (2)	Low (1)	2
A DDoS attack may cause problems to the workstations for some hours or days	Productivity (4)	High (3)	12
	Safety & Health (5)	High (3)	15
Some fines can be expected from business and commercial customers	Fines & Legal Penalties (1)	Low (1)	1
	User Defined Impact Area		
		Relative Risk Score	**33**

In Table 18 we see the information for a potential DDoS attack to the information asset. This threat has a high probability of occurring while having moderate effects to the organisation in total, but quite severe to the asset itself. The actors could be a terrorist group, a hostile nation or a simple hacker using a botnet to perform the attack. Their motives could be to modify or crash the Siemens WinCC software running in the asset with the ultimate purpose of damaging components of the critical infrastructure. The main concern here is that a DDoS attack could last for some hours potentially crippling the workstations of the SCADA control centre for even longer and render them vulnerable for further exploits.

Table 19: Information Asset Risk hardware defect

Allegro - Worksheet 10b	Information Asset Risk Worksheet			
Information Asset Risk	Information Asset	SCADA control centre		
	Area of Concern	*A hardware defect on the actuators or the workstations of the SCADA control centre occurs*		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Accident, Terrorist group, hostile nation or hacker		
	(2) Means *How would the actor do it? What would they do?*	Using a virus or remote exploit, after a DDoS attack has occurred, an interested party could cause a hardware defect		
	(3) Motive *What is the actor's reason for doing it?*	Gain unauthorised access and damage one of the acuators or one of the workstations		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure**	☑ **Destruction**	
		❑ **Modification**	☑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	The actuators and workastations of the SCADA control center must be available 24/7/365		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High (75%)**	□ **Medium (50%)**	☑ **Low (25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A hardware defect can have high financial consequences due to the cost of repair and unavailability of the infrastructure	Reputation & Customer Confidence (3)	High (3)	9
	Financial (2)	Medium (2)	4
A hardware defect could hinder productivity for an indefinite amount of time depending on the defect.	Productivity (4)	High (3)	12
	Safety & Health (5)	High (3)	15
Some fines can be expected from business and commercial customers	Fines & Legal Penalties (1)	Low (1)	1
	User Defined Impact Area		
		Relative Risk Score	**41**

In Table 19 we see the information for a potential hardware defect to the information asset. This threat has a low probability of occurring while having severe effects to the organisation in total and to the asset itself. The actors could be an accident, a terrorist group, a hostile nation or a simple hacker. If we exclude the case of an accident, this is not exactly an attack but more the outcome of another threat materialising, that of a malware for example targeting to damage the hard drives of the workstation. Their motives could be to modify or crash the workstations of the asset with the ultimate purpose of damaging components of the critical infrastructure. The main concern here is that such an attack could have significant consequences since a workstation going offline could jeopardise the operation of the Siemens WinCC software and could take time to replace it and set it up.

Table 20: Information Asset Risk port scanning

Allegro - Worksheet 10c	Information Asset Risk Worksheet			
Information Asset Risk / Threat	Information Asset	SCADA control centre		
	Area of Concern	*Scanning of the workstations of the SCADA control centre for open ports or ports used by Siemens WinCC for further exploit*		
	(1) Actor *Who would exploit the area of concern or threat?*	Terrorist group, hostile nation or hacker		
	(2) Means *How would the actor do it? What would they do?*	Using the internet to perform port scanning, an information gathering technique		
	(3) Motive *What is the actor's reason for doing it?*	Gain unauthorised access and detect vulnerabilities		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ☑ **Destruction** ❑ **Modification** ☑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the respective authorised employees can control and modify the Siemens Simatic		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High (75%)**	❑ **Medium (50%)**	❑ **Low (25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A port scanning can be used to detect vulnerabilities in OS and the services running on the OS of the SCADA control centre for further exploit	Reputation & Customer Confidence (3)	Low (1)	3
	Financial (2)	Low (1)	2
Such exploits could be unauthorised remote access to infect with malware	Productivity (4)	Low (1)	4
	Safety & Health (5)	Low (1)	5
Some fines can be expected from business and commercial customers	Fines & Legal Penalties (1)	Low (1)	1
	User Defined Impact Area		
		Relative Risk Score	**15**

In Table 20 we see the information for a potential port scanning attack to the information asset. This threat has a high probability of occurring while having little effects to the organisation in total and to the asset itself. The actors could be a terrorist group, a hostile nation or a simple hacker using freely available tools to perform the attack. Their motives could be to gain unauthorised access and scan the workstations for vulnerabilities with the ultimate purpose of damaging components of the critical infrastructure. The main concern here is that a port scanning attack is an information gathering attack about what ports are open and which services are using them in order to exploit this for further attacks like remote access to infect the system with malware.

Table 21: Information Asset Risk malware

Allegro - Worksheet 10d	Information Asset Risk Worksheet			
Information Asset Risk / Threat	Information Asset	SCADA control centre		
	Area of Concern	*A malicius software is affecting the operations of the workstations. It may alter the function of Siemens WinCC, make it unavailable to the designated users or extract data*		
	(1) Actor *Who would exploit the area of concern or threat?*	Terrorist group, hostile nation, hacker		
	(2) Means *How would the actor do it? What would they do?*	A malicius software is installed to one of the workstations of either the SCADA control centre or of the corporate intranet		
	(3) Motive *What is the actor's reason for doing it?*	Gain unauthorised access and modify or crash the Siemens Simatic software or the OS of the workstations		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ☑ **Destruction** ❑ **Modification** ☑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the respective authorised employees can control and modify the Siemens Simatic. Not all data are meant for disclosure outside the organisation		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High (75%)**	☑ **Medium (50%)**	□ **Low (25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
A malware can potentialy have long lasting effects until it can be identified and properly removed.	Reputation & Customer Confidence (3)	Low (1)	3
	Financial (2)	Medium (2)	4
Malware targeting specifically Siemens software or actuators can severely disrupt the operation of the SCADA control centre and of the power plant.	Productivity (4)	High (3)	12
	Safety & Health (5)	High (3)	15
Some fines can be expected from business and commercial customers	Fines & Legal Penalties (1)	Low (1)	1
	User Defined Impact Area		
		Relative Risk Score	**35**

In Table 21 we see the information for a potential malware attack to the information asset. This threat has a medium probability of occurring while having moderate effects to the organisation in total, but quite severe to the asset itself. The actors could be a terrorist group, a hostile nation or a simple hacker using freely available tools to perform the attack. Their motives could be to gain unauthorised access and infect the workstations with malware with the ultimate purpose of damaging components of the critical infrastructure. The main concern here is that new malware is not easy to identify if its signature does not exist in the antivirus' database. Certain malware like Stuxnet are known to be targeting specific components of the infrastructure operated by the Siemens WinCC software by replacing the readings of the actuators with false data and ordering them to operate in other than their normal operation. So far the removal of such viruses can be a long and tedious process.

Table 22: Information Asset Risk zero day exploits

Allegro - Worksheet 10e	**Information Asset Risk Worksheet**			
Information Asset Risk / Threat	Information Asset	SCADA control centre		
	Area of Concern	*A software defect on the MS Windows OS or the Siemens WinCC software is exploited to crash or modify the software. Workstations are not patched to the latest updates*		
	(1) Actor *Who would exploit the area of concern or threat?*	Terrorist group, hostile nation or hacker		
	(2) Means *How would the actor do it? What would they do?*	Using a virus or remote access after a DDoS or port scanning attack has occurred		
	(3) Motive *What is the actor's reason for doing it?*	Gain unauthorised access and modify or crash the Siemens Simatic software or the OS of the workstations		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ☑ **Destruction** ❑ **Modification** ☑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only the respective authorised employees can control and modify the Siemens Simatic		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High (75%)**	❑ **Medium (50%)**	❑ **Low (25%)**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area (Priority)	**Value**	**Score**
A software crash on the Simatic or OS it could lead to miss on readings about malfunctions of the infrastructure or cause them. It would hinder productivity possibly to a halt affecting distribution. Some financial loss is expected	Reputation & Customer Confidence (3)	Low (1)	3
	Financial (2)	Medium (2)	4
A software crash on the Simatic or OS it could lead to miss on readings about malfunctions of the infrastructure or cause them. It would hinder productivity possibly to a halt and jeopardise the health & safety of the personnel	Productivity (4)	High (3)	12
	Safety & Health (5)	High (3)	15
Some fines can be expected from business and commercial customers	Fines & Legal Penalties (1)	Low (1)	1
	User Defined Impact Area	-	
		Relative Risk Score	**35**

In Table 22 we see the information for a zero day exploit attack to the information asset. This threat has a high probability of occurring while having moderate effects to the organisation in total, but quite severe to the asset itself. The probability is high because most of the workstations in the SCADA control centre are old MS Windows versions and not at their latest patch level. The actors could be a terrorist group, a hostile nation or a simple hacker. This is a typical attack occurring after a port scanning and/or DDoS attack has occurred. Their motives could be to gain unauthorised access with the ultimate purpose of damaging components of the critical infrastructure. The main concern here is similar to that of malware since it could lead to software crashes, infection with malware etc.

3.2.8 Step 8 - Select Mitigation Approach

The last step of the OCTAVE Allegro approach to risk assessment is to decide on how the organisation will react to the threats identified in the previous steps. The organisation can:

- Accept the risk, meaning that no action will be done to address the risk and its consequences if it materialises.
- Defer, meaning that the organisation will not react to the risk nor accept it, but it will continue with its analysis to gather additional information on the risk and its consequences.
- Mitigate the risk, meaning a course of action will be decided and implemented to reduce or negate the consequences of the risk materialising.
- Transfer, meaning the organisation decides to transfer the risk by means of an insurance policy against such an event with a third party.

This step consists of three activities.

Activity 1
The first activity is to create a risk matrix based on the outcome of steps 4 to 7, with which we assigned to each threat a probability of occurrence and a score indicating the threats severeness to the critical information infrastructure. The risk matrix can be seen in Figure 9.

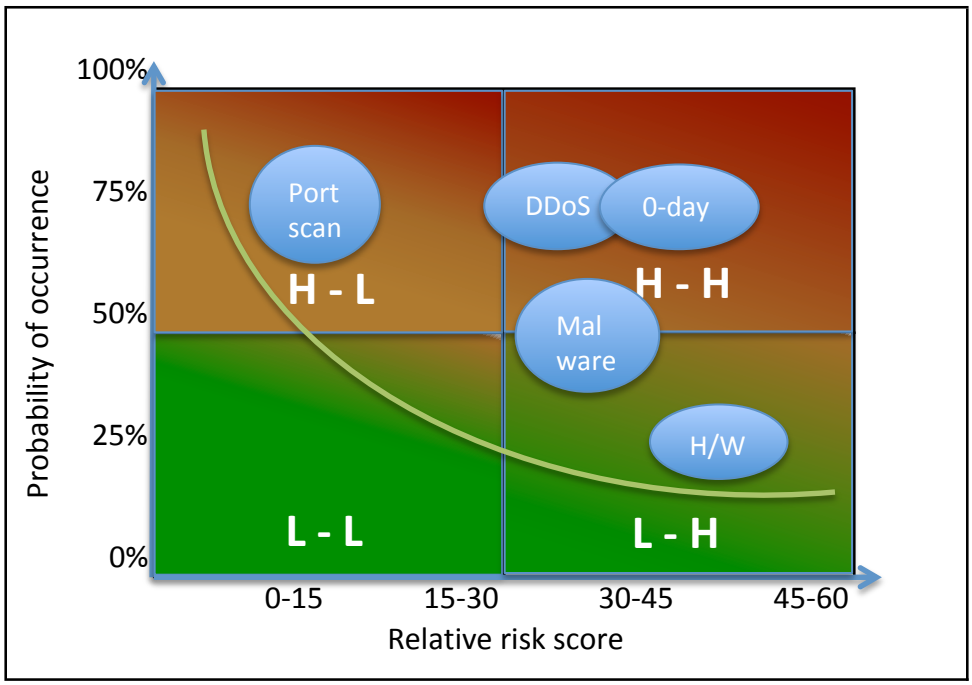


Figure 9: Risk Matrix

On the X-axis we plot the score of each threat and on the Y-axis the probability of occurrence. With the median values the matrix is divided in 4 quadrants. The lower left is

the low probability - low threat score, the lower right is the low probability - high threat score, the upper left is the high probability - low threat score, and the upper right is the high probability - high threat score.

Activity 2
In the second activity we have to decide on what the reaction of the infrastructure owner will be. Either accept, mitigate, defer or transfer the risk. We decide to mitigate all the threats identified to prevent them from materialising or reducing their effect to the critical information infrastructure.

Activity 3
With the third activity we develop a reaction plan or strategy to each of the threats we decided to mitigate. The outcome of all the activities can be seen in Tables 23, 24, 25, 26 and 27.

Table 23: Mitigation for DDoS

(9) Risk Mitigation DDoS *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical: gateway	Install Intrusion Detection System (IDS)		
Technical: gateway	Analyse network traffic and identify suspicious IP communications		
Technical: gateway	Have a reasonably sufficient bandwidth with the Internet Service Provider (ISP) to withstand the attack.		
Technical: gateway	Automatically block for some period of time IPs that sent out frequent and large amount of packages.		
Technical: gateway	If the attack is persistent block all incoming internet traffic		

A possible mitigation plan to defend against a potential DDoS attack could involve actions taken on the gateway of the SCADA control centre. These could be for example the presence of intrusion detection systems (IDS), that can alert the owner of potential malevolent traffic and could even block some of that traffic or divert it. This is a safe strategy since the control centre is not relying on the internet to function, but mainly employees to extract data for reporting purposes. Another strategy would be to have enough available bandwidth from the internet service provider (ISP) to absorb the malevolent traffic. In this case an assessment needs to be made on what is adequate bandwidth since such a solution can be costly and the extra bandwidth will be idle during most of the operating hours of the control centre and used only when a DDoS attack occurs.

Table 24: Mitigation for Hardware defect

(9) Risk Mitigation Hardware defect *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical: actuators	Have always the designated amount of spare parts and components in case of a hardware break down		
Technical: Workstations	Have the backup system (BCP) up to date and ready to go live within maximum one hour.		
Technical: Workstations	Try to eliminate the problem at it source, perhaps a virus.		

In the case of a hardware defect in the SCADA control centre, we should always have some spare parts/components readily available to replace them. These of course could be limited to the ones that have a high delivery time from the manufacturer and are critical to the safety of the infrastructure and thus of the employees. In such a case also the backup system of Business Continuity Plan(BCP) should be available to become operational in an hour. Lastly we should try to avoid the defect happening at its source which could be for example a virus.

Table 25: Mitigation for Port scanning

(9) Risk Mitigation Port scanning *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical: gateway	Install Intrusion Detection System (IDS)		
Technical: gateway	Analyse network traffic and identify suspicious IP communications, e.g. broad range of connections requests on different ports by a signle IP		

To help us defend against port scanning attacks we could rely on an IDS and identify suspicious communications with the IPs of the SCADA centre from external IPs.

Table 26: Mitigation for Malware

(9) Risk Mitigation Malware *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical: MS Windows	Make sure antivirus software is installed on all workstations. Perform check whether it is on the latest licensed version and with the signature database updated.		
Technical: MS Windows	Be in contact with Kaspersky to get informed on new vulnerabilities that need to be patched.		

A good mitigation strategy in the case of malware is of course the presence of an antivirus software. Although it is effective against known malware, depending on the identification technique it is using, it can recognise also new ones. Nonetheless, existing known malware can still be harmful for the SCADA control centre. For the strategy to properly work it is paramount that the virus database of the software and the software itself is regularly updated with new versions and patches from the developer.

Table 27: Mitigation for Zero day exploits

(9) Risk Mitigation Zero day exploits *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Technical Simatic	Be in contact with Siemens to apply patches for known vulnerabilities		
Technical MS Windows	Be in contact with Microsoft to apply patches for known vulnerabilities		
Technical developer system	Thoroughly test these against the delevor copy of the SCADA control centre		

With respect to zero days exploits there is little the infrastructure owner can do to mitigate. By definition these are exploits not known to the OS or software developer so they are hard to identify and can only be addressed post an exploit has been used. The owner must be in regular communication with the developer to be informed about new vulnerabilities discovered and assess how can they affect the operations of the SCADA control

centre. Of course all updates need to be tested in a developer copy of the centre and not in the production version.

4 Design of the experiment

As we discussed in Section 2.4 some fundamental products or services are provided by organisations usually identified as critical infrastructure. Nowadays these facilities are operated by electromechanical equipment that is controlled by SCADA software installed on specific control centres. The purpose of this thesis is to identify the cyber threats that exist to critical infrastructures that have their SCADA control centres connected to the internet. This is of most importance given the escalation of cyber-attacks between nations and especially the precedence of the Stuxnet virus. A virus that targeted, attacked and damaged specific infrastructure components of the Iranian uranium enrichment facilities thus, forcing Iran to abandon its nuclear programme (Liff, 2012).

Research so far has focused on custom made computer simulations based on estimations or with software tools designed to simulate large networks and their traffic, in most cases the attacks that are known, directed and specific rather than unknown, random and blind, something you could expect in real life.

For example Liljenstam et al. present the Real-time Immersive Network Simulation Environment (RINSE) to simulate generic network operations that can be used to model attacks and defences to a network and their research is not specific to SCADA networks (Liljenstam et al., 2005). Cohen uses computer simulation to model cyber attacks and defences on a network using a cause and effect model. His research is also not speclificaly related to SCADA networks (Cohen, 1999).

McQueen et al. create a methodology for risk a reduction estimation on a SCADA control centre. A so called compromise graph is created based on vulnerabilities and estimation about time-to-complete successful attacks. The methodology is applied to a SCADA setup using the graph created (McQueen, Boyer, Flynn, & Beitel, 2006). Sridhar and Manimaran use simulation in order to assess the impact of attacks to disrupt the normal function of a SCADA control centre. These attacks are data integrity attacks aiming to send false signals to the components operated by the SCADA software (Sridhar & Manimaran, 2010). Ten, Liu, and Manimaran also use computer simulation with probabilities to model a SCADA control centre and its vulnerabilities on three levels: systems, scenarios and access points (Ten, Liu, & Manimaran, 2008). Davis et al. use computer simulation to model a SCADA control centre that receives data from the infrastructure and RINSE to simulate the network operation. The attacks are directed through RINSE (Davis et al., 2006).

With this experiment we will mimic the real life setup of a SCADA control centre and assess what types of threats exist that can target it specifically, by setting up workstations that are part of the SCADA network and have a SCADA software installed and running 24/7 in a controlled environment.

Our intention is to create three virtual networks with five virtual machines each, that are connected to the internet through a gateway (the workstation hosting the experiment) and each network has a different level of security ranging from minimum and medium to best possible. On three of the machines, the Siemens SCADA WinCC software shall be installed to simulate the setup of a SCADA control centre. The duration of the experi-

ment will be fifteen (15) calendar days (five (5) calendar days for each virtual network). Afterwards, all three networks will be put offline.

In order to exclude from the parameters of the experiment the level of the network security awareness of the personnel, the SCADA network will be idle. Thus, no activities will be performed on the workstations by some designated actors or agents like sending and receiving of email, web browsing, file downloading, execution of software etc. Only the Workstations will be operating with the software described in the next sessions running on a 24/7 basis.

4.1 Setting up the iconic SCADA network

In our effort to identify the possible threats that a SCADA control centre may face in real life, we will create three virtual networks consisting of five personal computers (workstations) each, running different Microsoft Windows Operating Systems (OS). The experiment is conducted at the facilities of Universität der Bundeswehr München at the Informatik 1 Department. The workstations will be created on VMware Workstation 10 running on Ubuntu Server (host workstation) These computers have access to the internet through the host as shown in Figure 8. The network is replicated two times (so in total three virtual networks) in order to simulate different security levels. The security level of each network is determined by the level of patching for each OS. The host is having the role of the gateway for the network.

Any operating system or software is hardly free of exploits in its source code, hackers know this and continuously try to find these exploits in order to design and launch new malware and types of attacks to take advantage of these. The only thing the developers can do is try to patch these exploits while in parallel avoid creating new ones by issuing regular software updates along the lifetime of an OS or software.

Our intention is to create a so called "honeypot" or "honey net" that also simulates the setting of a SCADA control centre. A "honeypot" or "honey net" is a network setup with deliberate vulnerabilities to attract the cyber threats we want to observe. That means older version of MS Windows with services running that are known to be exploitable for malicious purposes.

In Table 28 we can see the final setup of the three virtual networks and the respective IP addresses, while the following sections describe their function and selection.

Table 28: Setup of the virtual machines

Virtual Network 1 (VN1)		Minimum additional protection					
Client description	**OS**	**Patch level**	**Antivirus**	**Firewall**	**Software**	**Services**	**IP address**
WS1	Windows XP Professional DE	Service Pack 3	none	Yes (Built in)	Siemens WinCC Professional V12		80.237.252.242
WS2	Windows NT DE	none	none	No	none		80.237.252.243
WS3	Windows 2000 Professional DE	none	none	No	none		80.237.252.244
WS4	Windows Server 2008 Std Ed. SP1	Service Pack 1	none	Yes (Built in)	Siemens WinCC Professional V12	Active Directory Domain Services, DNS, File services, Web Server (IIS), FTP server	80.237.252.245
WS5	Windows Server 2008 Std Ed. SP1	none	none	Yes (Built in)	Siemens WinCC Professional V12	File services, Web Server (IIS), FTP server	80.237.252.246

Virtual Network 2 (VN2)		Medium additional protection					
Client description	**OS**	**Patch level**	**Antivirus**	**Firewall**	**Software**	**Services**	**IP address**
WS1	Windows XP Professional DE	Service Pack 3	Kaspersky 6.0.0	Yes (Built in)	Siemens WinCC Professional V12		80.237.252.242
WS2	Windows NT DE	Service Pack 4	none	No	none		80.237.252.243
WS3	Windows 2000 Professional DE	Service Pack 2	none	No	none		80.237.252.244
WS4	Windows Server 2008 Std Ed. SP1	Service Pack 1	Kaspersky 6.0 for Servers	Yes (Built in)	Siemens WinCC Professional V12	Active Directory Domain Services, DNS, File services, Web Server (IIS), FTP server	80.237.252.245
WS5	Windows Server 2008 Std Ed. SP1	none	Kaspersky 6.0 for Servers	Yes (Built in)	Siemens WinCC Professional V12	File services, Web Server (IIS), FTP server	80.237.252.246

Virtual Network 3 (VN3)		Best possible protection					
Client description	**OS**	**Patch level**	**Antivirus**	**Firewall**	**Software**	**Services**	**IP address**
WS1	Windows XP Professional DE	Service Pack 3 + Updates	Kaspersky 14	Yes (Built in)	Siemens WinCC Professional V12		80.237.252.242
WS2	Windows NT DE	Service Pack 6 + Updates	Kaspersky 6	No	none		80.237.252.243
WS3	Windows 2000 Professional DE	Service Pack 4 + Updates	Kaspersky 7	No	none		80.237.252.244
WS4	Windows Server 2008 Std Ed. SP1	Service Pack 1+Updates	Kaspersky 6.0 for Servers	Yes (Built in)	Siemens WinCC Professional V12	Active Directory Domain Services, DNS, File services, Web Server (IIS), FTP server	80.237.252.245
WS5	Windows Server 2008 Std Ed. SP1	Service Pack 1 + Updates	Kaspersky 6.0 for Servers	Yes (Built in)	Siemens WinCC Professional V12	File services, Web Server (IIS), FTP server	80.237.252.246

4.1.1 Operating System selection

In a critical infrastructure provider normally you would not expect some very sophisticated ICT, but rather some old hardware systems running on older versions of operating systems, because it simply just works. The ICT components of the critical information infrastructure are too sensitive to the operation of the facility to patch, upgrade and test continuously, since this is translated to potential downtime, underperfomance of the facility and unknown side effects to the operation and communication of other components of the infrastructure (Johnson, 2010). Consequently, we expect to find some older versions of Windows OS and not at their latest patch level. This validates also our selection of OS for the "honeypot"

Therefore, for the three virtual networks the workstations we will install some older versions of Windows OS, like Windows 2000 Professional, Windows XP Professional, Windows NT 4.0 and Windows Server 2008. Although, we would not expect them to be in the latest patch level, the VN3 will simulate the best possible environment in terms of security. Thus, all OS will be updated with the latest updates from Microsoft.

Another factor limiting the selection of the OS for our workstations is also the requirements specified by the SCADA software we will use, that are described in Section 4.1.3.

4.1.2 Firewall

A firewall software is already included in most recent versions of Windows OS, but not in older ones. In particular Windows XP and Windows Server 2008 R2 have firewall included and we will verify that it is activated. Windows NT 4.0 and Windows 2000 Professional do not include a firewall.

4.1.3 Additional software and services selection

In addition to the selection of the OS and the firewall described earlier it is needed to have additional software and services installed on the workstations of the virtual networks simulating the SCADA network. The most important of course is the SCADA software itself. The additional software and services for the three virtual networks will be identical, namely the same distribution, version and level of patches.

SCADA software

There is not sufficient academic literature to argue the selection of a specific SCADA software against another so we will make some assumptions for our selection. Siemens is a German multinational company involved in the development of such software but also producer of the electromechanical equipment that is set to control, it is also a big contractor for many public projects in Germany. Thus, we would expect Siemens equipment to be used quite often in infrastructures like power plants in Germany accompanied by the relevant Siemens SCADA software. In addition, the Siemens SCADA software was specifically targeted by the Stuxnet virus to damage Iran's nuclear programme (Liff, 2012), thus contributing to the setup of our "honeypot".

Therefore, the Siemens WinCC Professional (TIA Portal) V12 software will be installed and will be running on a 24/7 basis on all the workstations of the virtual network. A trial version of the WinCC software will be installed and ran with the default settings. A demo project provided by Siemens will be launched in the Siemens TIA Portal and executed in runtime. The demo project is located at Siemens' support website (Siemens Automation, 2014a).

According to Siemens the OS requirements for the software are the following (Siemens Automation, 2014b):

- Windows XP Professional SP3
- Windows 7 Professional/Enterprise/Ultimate SP 1 (32 Bit)
- Windows 7 Professional/Enterprise/Ultimate SP 1(64 Bit)
- Microsoft Windows Server 2003 Standard Edition R2 SP2 (32 Bit)
- Microsoft Windows Server 2008 Standard Edition SP2 (32 Bit)
- Microsoft Windows Server 2008 Standard Edition R2 (64 Bit)
- Microsoft Windows Server 2008 Standard Edition R2 SP1 (64 Bit)

Services
Windows Server 2008 R2 comes with the Microsoft Internet Information Services (IIS) preinstalled after the installation of the OS. A platform known for vulnerabilities regarding network security. To justify its presence in a SCADA control centre, IIS can be used to develop web applications to access remotely files in the server. Also an FTP service role will be installed under IIS used also for the remote access of files and documents in the server.

Another service that will be installed is the DNS server function. Along with the Active Directory Domain service, that will be installed, they can be used to assign specific names for the workstations in the network to their IP address. DNS servers are known to attract or be part of DDoS attacks, either unwillingly by replying to spoofed request packets, or because they have been infected by malware (Alomari, Manickam, Gupta, Karuppayah, & Alfaris, 2012).

4.1.4 Building up the virtual networks

The workstation hosting the experiment is a virtual server hosted by Hosteurope.de running Ubuntu Server 14.04 LTS,. The host is running VMware Workstation 10.0.2 build-1744117. The IP of the host is 91.250.87.185. Due to limitations on the global availability of IPv4 addresses, only one subnet (80.237.252.240/29) was assigned from Hosteurope.de and thus used consequently for each network. Meaning that the first network was assigned the IP range 80.237.252.242-80.237.252.246, put online for 5 days then put offline and the range was assigned to the second network and then to the third. Below the steps to build the virtual networks are mentioned.

Virtual Network 1 (VN1) :

VN1-WS1 Windows XP Professional SP3 VN1 : Install Windows XP Professional DE with Service Pack 3 and Siemens WinCC software. During the experiment the software will be executed and running.

VN1-WS2 Windows NT 4.0 VN1 : Install Windows NT 4.0 DE

VN1-WS3 Windows 2000 Professional VN1 : Install Windows 2000 Professional DE.

VN1-WS4 Windows Server 2008 Standard SP1 x32 EN VN1: Install Windows Server 2008 Standard SP1 x32 EN, install Siemens WinCC Professional EN (at this point clones are created for the next workstation and VN2 and VN3), install DNS server role, install FTP service role under the Web server role (IIS).

VN1-WS5 Windows Server 2008 Standard SP1 x32 EN VN1 2 : Clone VN1-WS4, install Siemens WinCC software (at this point clones are created for VN2 and VN3), install FTP service role under the Web server role (IIS) and Active Directory Domain Services.

Virtual Network 2 (VN2) :

VN2-WS1 Windows XP Professional SP3 VN2 : clone VN1-WS1, install Kaspersky 6. antivirus software.

VN2-WS2 Windows NT 4.0 SP4 VN2 : clone VN-WS2, install Service Packs 1, 2, 3 and 4.

VN2-WS3 Windows 2000 Professional SP2 VN2 : use the clone from VN1-WS3, install Service Pack 2.

VN2-WS4 Windows Server 2008 Standard Edition SP1 x32 VN2 : use the clone of VN1-WS4, install Kaspersky 6 antivirus for servers, install DNS server role, install FTP service role under the Web server role (IIS).

VN2-WS5 Windows Server 2008 Standard SP1 x32 EN VN2 2 : use the clone from VN1-WS5, install Kaspersky 6 antivirus for servers, install FTP service role under the Web server role (IIS) and Active Directory Domain Services.

Virtual Network 3 (VN3) :

VN3-WS1 Windows XP Professional SP3 VN3 : clone VN1-WS1, install all latest Windows updates up to 26.05.2014, install Kaspersky 14 antivirus software.

VN3-WS2 Windows NT 4.0 SP6 VN2 : clone VN1-WS2, install Service Packs 5 and 6, install Internet Explorer 6 (this was necessary for the installation of the antivirus), install Kaspersky 6 antivirus.

VN3-WS3 Windows 2000 Professional SP4 VN3 : clone VN1-WS3, install Service Pack 4, install Kaspersky 7 antivirus.

VN3-WS4 Windows Server 2008 Standard Edition SP1 x32 VN3 : use the clone from VN1-WS4, install latest Windows updates, install Kaspersky 6 antivirus for servers, install DNS server role, install FTP service role under the Web server role (IIS).

VN3-WS5 Windows Server 2008 Standard SP1 x32 EN VN3 2 : use the clone from VN1-WS5, install all latest Windows updates up to 26.05.2014, install Kaspersky 6 antivirus for servers, install FTP service role under the Web server role (IIS) and Active Directory Domain Service server role.

4.2 Data gathering

As we mentioned earlier, for the gathering of the data we will use the linux OS of the host who is acting as a gateway for the virtual machines. We will use the "tcpdump" command of linux that captures all traffic to the ethernet port of the host. This is suitable for us since the virtual machines are running in VMware workstation in bridged mode with the host, meaning they are directly connected to the internet through the ethernet port of the host.

5 Results

In the following sections we will present the results from the experiment, after each of the virtual networks was online for five (5) calendar days. For each network we received three files, the first one was approximately 2.59Gb, the second 2.85Gb and the third 547.2Mb. The results are analysed with the open source software Wireshark.

5.1 Data cleaning

The files we received from the host after each virtual network was put offline included the network traffic of the IPs of the virtual machines and that of the host. From the files we need to exclude the traffic of the host itself since it is not in the scope of our research. Since the files were too large to load them and analyse them in Wireshark, it was more suitable to extract from each file the network traffic for each IP address. Thus, for each network from each file, five additional files were created that included only the traffic of the respective IP address.

After each file was analysed to identify malevolent traffic captured, our focus turned to the VMs where the Siemens WinCC software was running. In order to identify if specific malevolent network behaviour was targeting them, we filtered all the traffic that was directed to the ports used by the software during runtime. The ports that are used by the software are TCP ports 80, 102, 4840, 52601 and UDP ports 135, 137, 138, 161 and 162 (Siemens AG Industry Sector, 2013, p. 59). Therefore, we created additional files for each VM containing only the traffic to these ports.

5.2 Macroscopic level of analysis: generic types of attacks

We analyse first, the results from all networks with Wireshark using the I/O graph function of the software and set it to display on the Y-axis the packet/tick and on the X-axis the time with a tick interval of 10 minutes and 10 pixel per tick. This way we have better resolution on the graph and the packets can be grouped by 10 minutes intervals to better visualise the density of them. We then focus on the picks of the graph for each file that indicate a number of packets of more than 50. For the data analysis purposes we consider all suspicious network traffic as attacks; even port scanning or NBSTAT queries mentioned later that are mainly information gathering techniques.

At this level of analysis, we can group the attacks we identified in three major categories: Denial of Service (DoS), Distributed Denial of Service (DDoS) and port scanning. The outcome can be seen in Table 29.

A DoS attack occurs when a host computer (attacker) is sending a very big amount of packet requests in a short period of time (usually a few seconds), independent of the protocol used for the communication, to another host (victim) with the intend to disrupt the victim's normal operation. When in this attack a lot of different attackers are targeting the same victim then we have a DDoS. Port scanning is a form of information gathering technique usually occurring before the actual attack.

Table 29: Types of attacks identified and categorised to D=DoS, Dd=DDoS and P=port scanning, in the three network setups.

	Types of Attacks	WS1 (242)	WS2 (243)	WS3 (244)	WS4 (245)	WS5 (246)
VN1	Day 1	D	-	N/A	-	D
	Day 2	D, D, D, P	D, D, D, D, P	N/A	D, D, D, P	D, D, P
	Day 3	D, D	-	N/A	D	-
	Day 4	P	P	N/A	D, D, P	D, D, P
	Day 5	-	D, D, D	N/A	D, D, D, Dd	D, D
VN2	Day 1	P	D, D, P	N/A	D, D, Dd, Dd, Dd, Dd, Dd, Dd, Dd, Dd, Dd, Dd,	P
	Day 2	-	-	N/A	D, Dd, Dd, Dd, Dd, Dd, Dd, Dd, Dd	D
	Day 3	P	D, D, P	N/A	D, Dd, Dd, Dd, Dd, Dd, Dd, P	D, P
	Day 4	D	D	N/A	D	D, D, D, D, D
	Day 5	-	-	N/A	D	-
VN3	Day 1	D, D	D	D	D	D, D
	Day 2	-	-	-	D	D
	Day 3	-	-	-	-	-
	Day 4	-	-	H	D	D, D
	Day 5	-	D	D	D, D, D	D, D

In Table 29 in each cell the category of the attack is indicated and the frequency with which it occurred for each day of the experiment and for each VM. For example for the VN2-WS4 on the first day, 2 DoS attacks were identified along with 10 DDoS. For VN1-WS1 on the second day, 3 DoS attacks and one port scanning were identified in the data.

Among the DoS attacks more specific types of attack were identified. These are the following and we will refer to them as generic types of attacks:

- TCP SYN flood, where the attacker is exploiting the way a TCP connection is established between a client and a host computer (Alomari et al., 2012). The client send a TCP request with the SYN flag to connect to the host, the host replies to the client with a TCP request with the SYN, ACK flags and then the client sends back a TCP request with the ACK flag. In the case of an attack the client sends only the TCP SYN request without sending the TCP SYN, ACK request. Thus the host is keeping the connection open until it receives the TCP ACK request. If a lot of these connections are piling up then the resources of the host are depleted causing it to crash or refuse further new connection requests.

- SMB flood, where the attacker again tries to flood the victim with packet requests using the SMB or SMB2 protocol, which is used for sharing of files, printers or ports in a network (Miller, 2009). These requests can be for random user access to files, random file creation or request etc.

- DNS flood, where an attacker uses the Domain Name Service (DNS) protocol to flood the victim with requests (Alomari et al., 2012). For the protocol to be used there needs to be a DNS service running in the host as it is the case for the WS4 and WS5 VMs. The client then sends a request to retrieve the information about the IP address of a specific website, the host then sends the request to the third party server that the website is registered and the third party server replies with the information which is then transmitted back to the client.

- DCE/RPC flood, where the attacker uses another protocol called Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) to flood the victim with requests and limit its resources. With this protocol the attacker requests remote access to the victim as administrator (Pang, Yegneswaran, Barford, Paxson, & Peterson, 2004).

- TCP RST flood, this attack is similar to the TCP SYN flood, but the client is sending TCP requests with the RST, ACK flag (Alomari et al., 2012). This tells the host to reset the connection after it has sent the TCP SYN request.

- TCP PSH flood, this attack is again similar to the previous one where the attacker is using again the TCP protocol, but send TCP requests withe PSH, ACK flags (Alomari et al., 2012). With these flags the client is indicating the host to pass through any data that is being sent to the host for processing.

- PHP flood, is a path traversal attack that tries to identify the file structure in a host computer and also requests for php files that may contain sensitive information like password lists, user accounts etc (*Path Traversal Attack*, 2014).

Besides the DoS attacks also some DDoS attacks occurred in the VMs during the experiment. These were using only the DNS protocol as the venue of the attack. More details can be seen in Table 30. The numbers in the cells are in ixj form, where i indicates the number of the day when the attack has occurred and the j indicates the frequency of occurrence on that day. For example, for the VN1WS4 machine the SMB flood occurred two times in day 2 two times in day 4 and two times in day 5.

Port scanning, is an information gathering technique, that usually happens before an actual attack occurs (Miller, 2009). With this an attacker can gain information on what ports are open in the victim and potentially what applications are using them.

Table 30: Types of attacks identified based on the method used, in the three network setups.

	Types of Attacks	DoS								DDoS
		TCP SYN flood	SMB flood	DNS flood	DCE/RPC flood	TCP RST flood	TCP PSH flood	PHP flood	Port Scanning	DNS flood
VN1	WS1 (242)	0	0	0	2x1, 3x1	1x1, 2x2, 3x1	0	0	2x1, 4x1	0
	WS2 (243)	0	5x1	0	0	2x2	2x2, 5x2	0	2x1, 4x1	0
	WS4 (245)	0	2x2, 4x2, 5x2	5x2	2x1, 3x1	0	0	0	2x1, 4x1	5x1
	WS5 (246)	0	2x2, 4x2, 5x2	0	1x1	0	0	0	2x1, 4x1	0
VN2	WS1 (242)	0	0	0	4x1	0	0	0	1x1, 3x1	0
	WS2 (243)	0	1x1, 3x1, 4x1	0	1x1	0	3x1	0	1x1, 3x1	0
	WS4 (245)	0	4x1, 5x2	1x2, 2x1	3x1	0	0	5x1	1x1, 3x1	1x10, 2x8, 3x5
	WS5 (246)	0	3x1, 5x3	0	2x1	5x1	0	5x1	1x1, 3x1	0
VN3	WS1 (242)	1x1	0	0	1x1	0	0	0	0	0
	WS2 (243)	0	5x1	0	1x1	0	0	0	0	0
	WS3 (244)	0	5x1	0	1x1	0	0	4x1	0	0
	WS4 (245)	0	2x1, 4x1, 5x3	0	1x1	0	0	0	0	0
	WS5 (246)	0	1x1, 2x1, 4x2, 5x2	0	1x1	0	0	0	0	0

As we mentioned earlier, the results from the VN1WS3 and VN2WS3 are not taken into consideration at this point since for this analysis step the size of the data file was to large for a proper loading and processing with Wireshark.

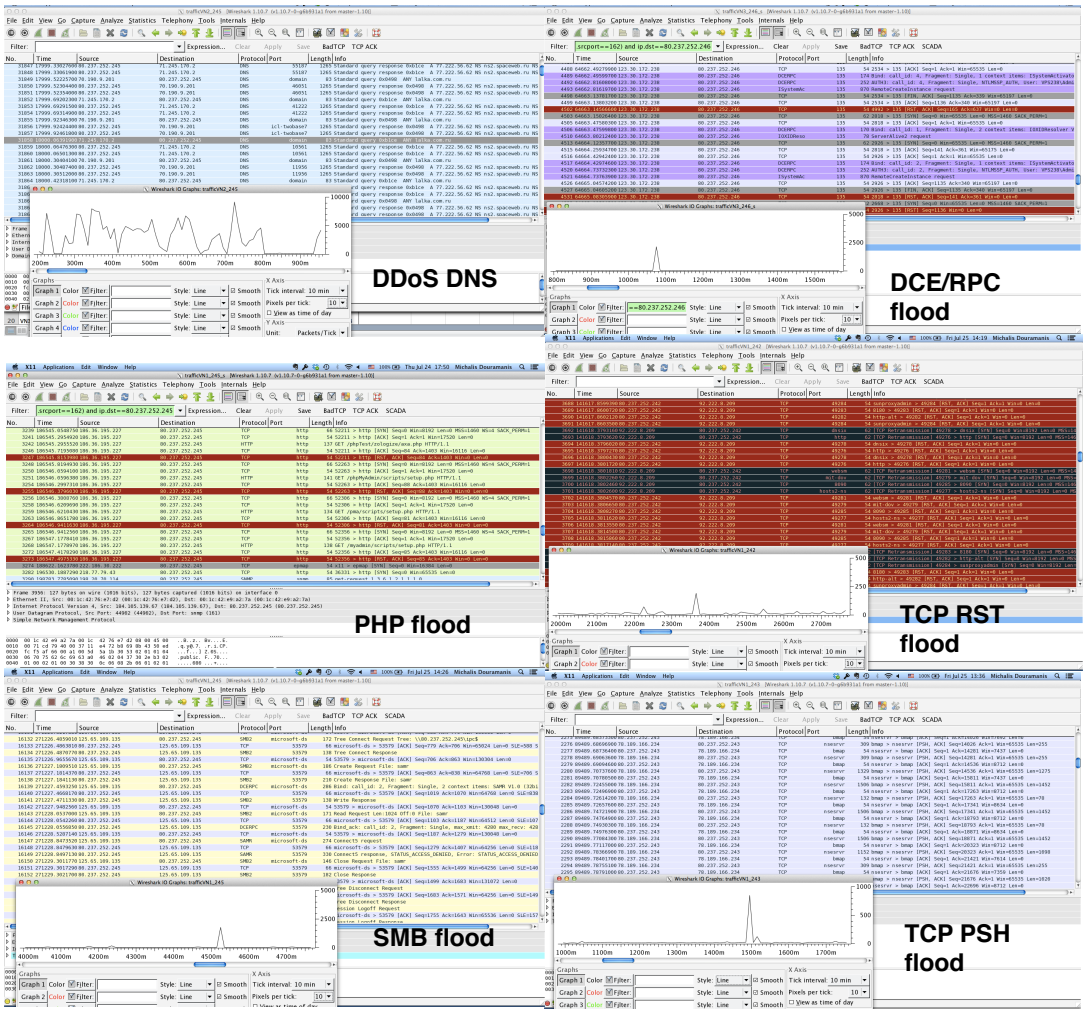


Figure 10: Examples of the attacks identified based on the method used as displayed in Wireshark.

In Figure 10 we can see the display of the software and some examples of the attacks we identified in the network capture files. For example, we can see for some DDoS DNS attacks a lot of requests coming from multiple IPs to the IP of our VM (80.237.252.245) to resolve the IP address of a Russian website. A lot of packets are arriving within 1 second and we can see from the graph that the average is 5000 packets grouped in 10 minutes intervals. Similarly the other attacks have the same principle, a lot of requests arriving closely one after the other in a very short duration and they are exploiting different communication protocols.

In Figures 11, 12 and 13 we visualise with histograms the number of generic attacks by type, that the VMs for each virtual network (VN) have attracted for the 5 day duration of each VN.

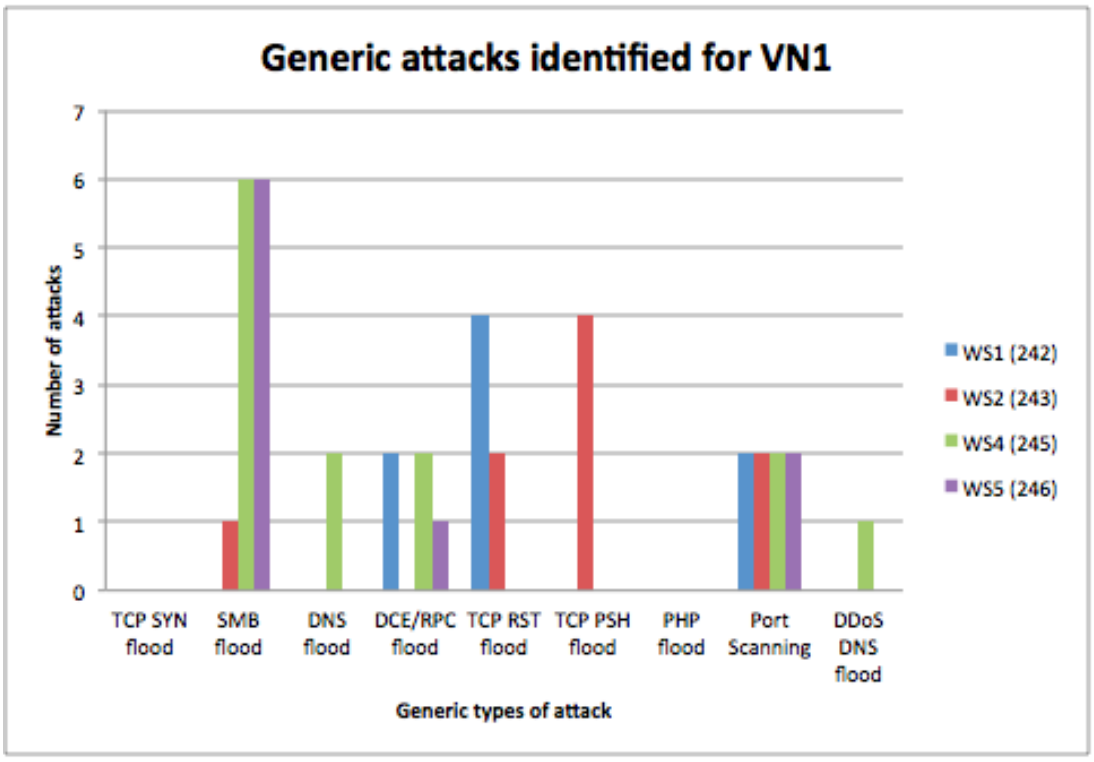


Figure 11: Histogram of the number of attacks the VMs of VN1 have attracted during the 5 days

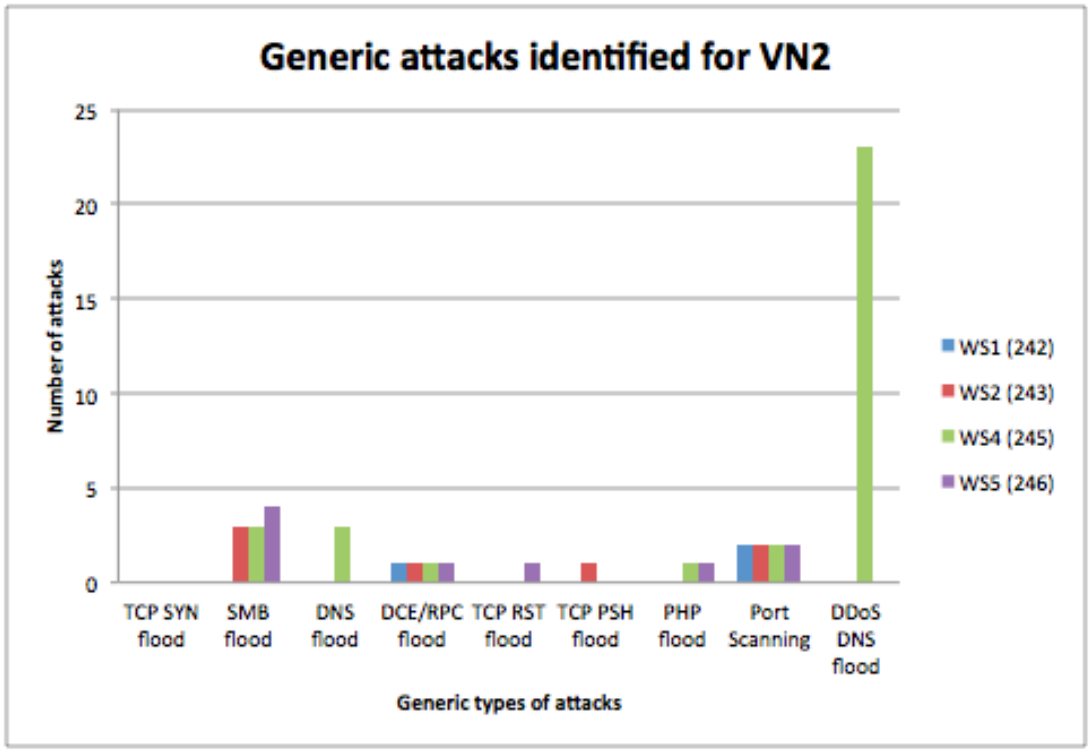


Figure 12: Histogram of the number of attacks the VMs of VN2 have attracted during the 5 days

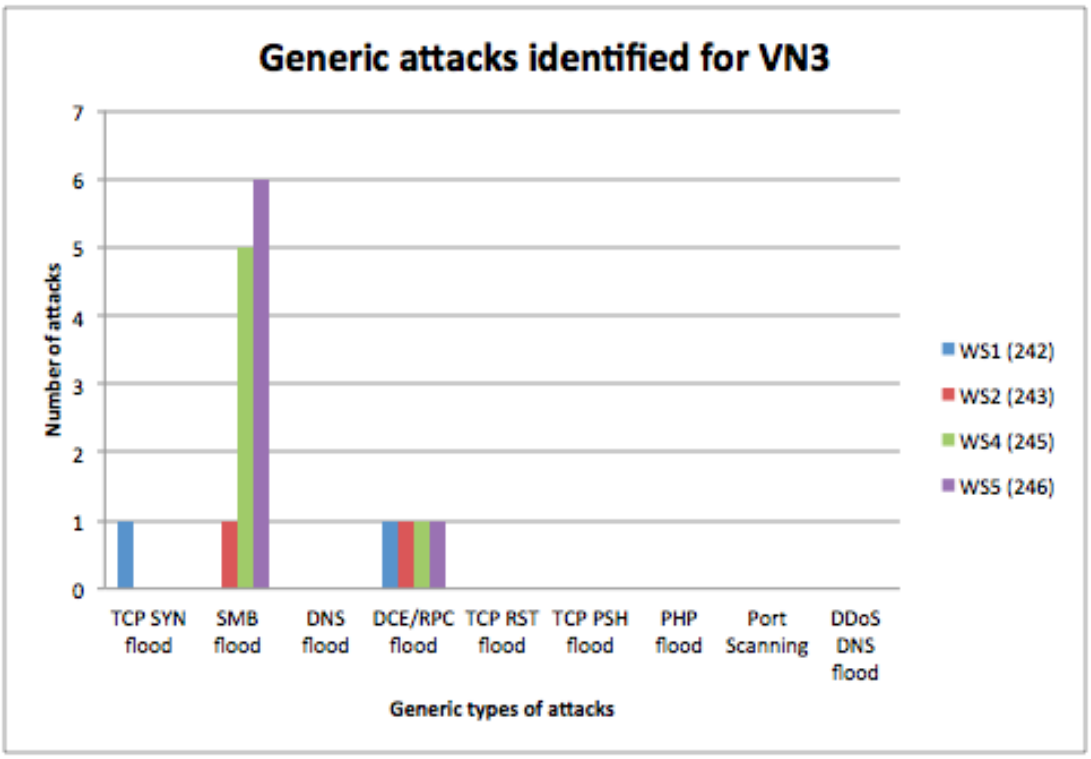


Figure 13: Histogram of the number of attacks the VMs of VN3 have attracted during the 5 days

In Figure 14 we can see the total number of attacks by type for all the VMs for each virtual network during the 5 day duration of the experiment for each VN.

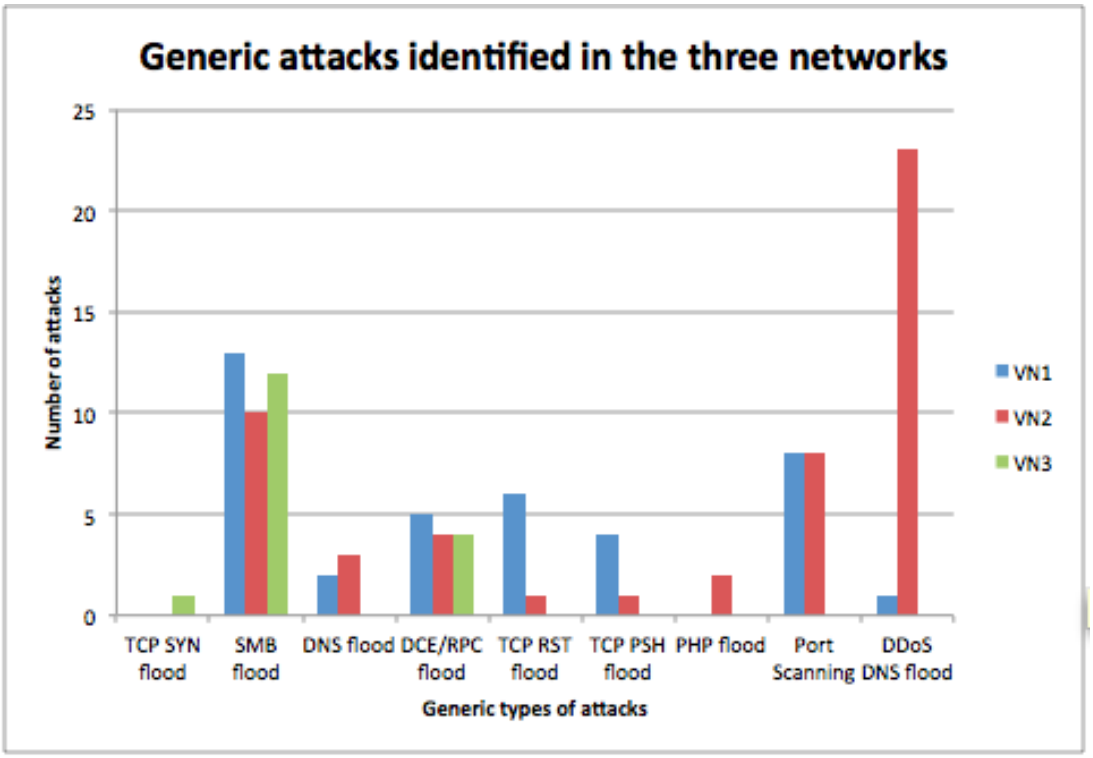


Figure 14: Total number of attacks for the virtual networks that have attracted during the 5 days duration

5.3 Microscopic level of analysis: focus on network captured on the ports used by Siemens WinCC

Our next step is to try to figure out whether there are specific attacks that target the VMs where the Siemens WinCC software is running in runtime. To do this we filter for the VMs WS2, WS4 and WS5 in all networks the traffic that is using the ports that are also used by the Siemens software. As we mentioned these are TCP ports 80, 102, 135, 4840, 52601 and UDP ports 137, 138, 161 and 162. Some of these ports are common like the TCP 80, 135 and UDP 137, 161. Thus, any malevolent behaviour on these ports may not be directly indicating the Siemens software as being a target of the attack.

Our findings revealed malevolent traffic only on TCP 80, 135 and UDP 137 ports. No network traffic or no suspicious network traffic was captured in the rest of the ports. We also observe that most of the attacks where carried using UDP protocols with the exception of the VMs WS4 and WS5 where TCP protocol based attacks were more prevalent.

At this point we did the same filtering of port based network traffic also on the VMs that were not having the Siemens WinCC software installed in order to assess whether some types of attacks could be automated, targeting randomly targets accessible in the internet without discrimination. The findings based on the protocol used can be seen in Figures 15, 16 and 17

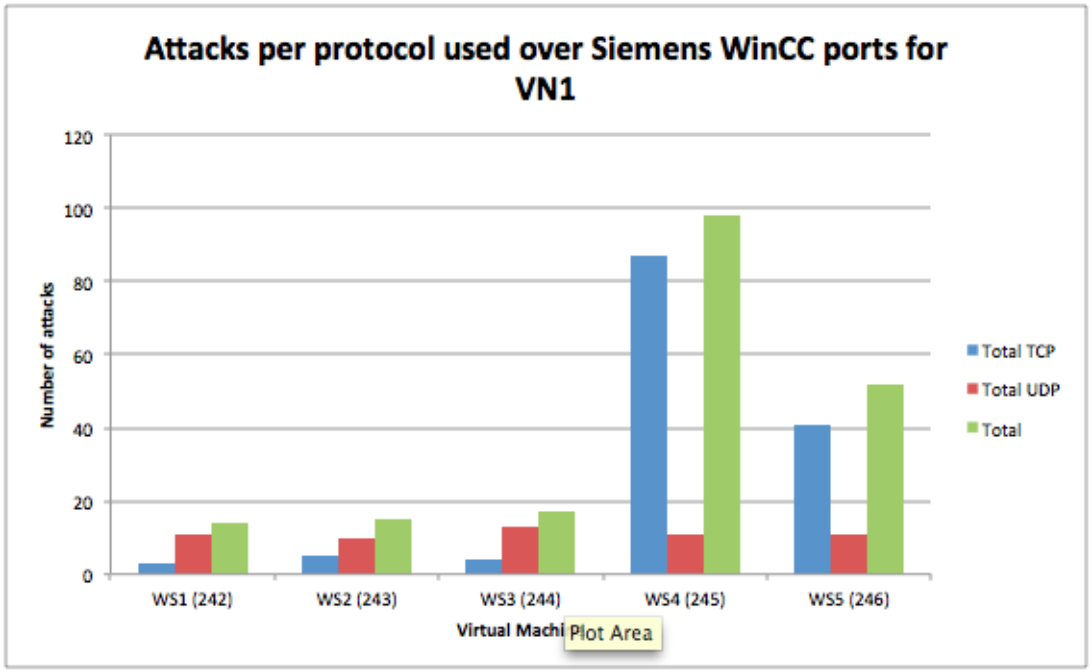


Figure 15: Histogram of number of attacks for VN1, based on the protocol used over Siemens WinCC ports for the whole duration of the experiment

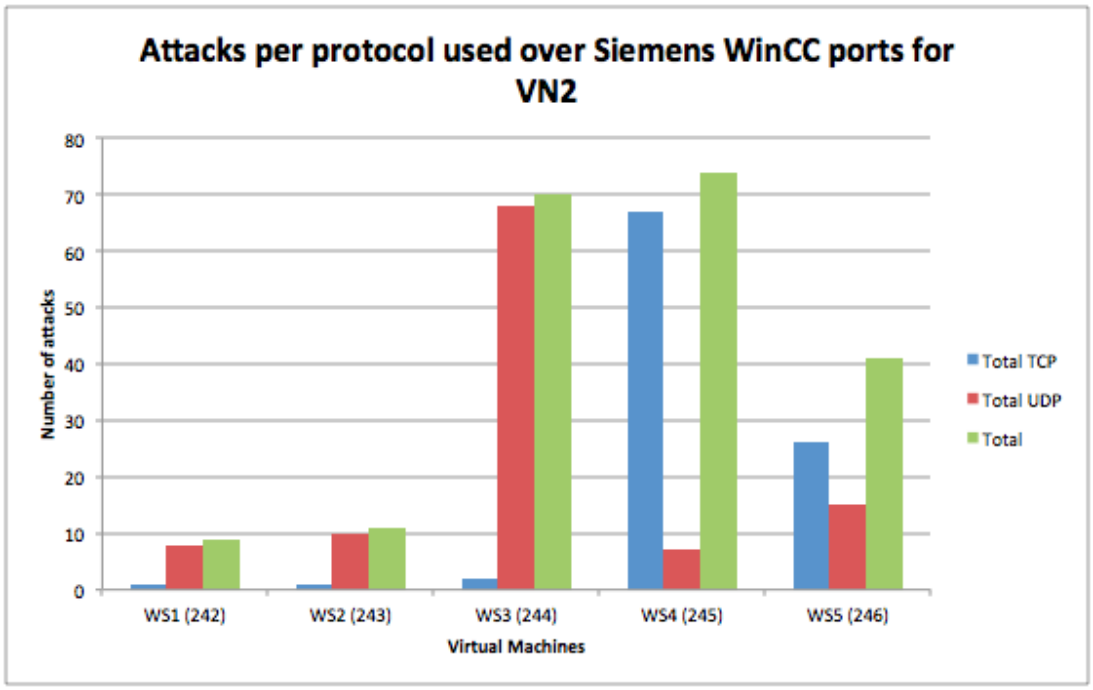


Figure 16: Histogram of number of attacks for VN2, based on the protocol used over Siemens WinCC ports for the whole duration of the experiment

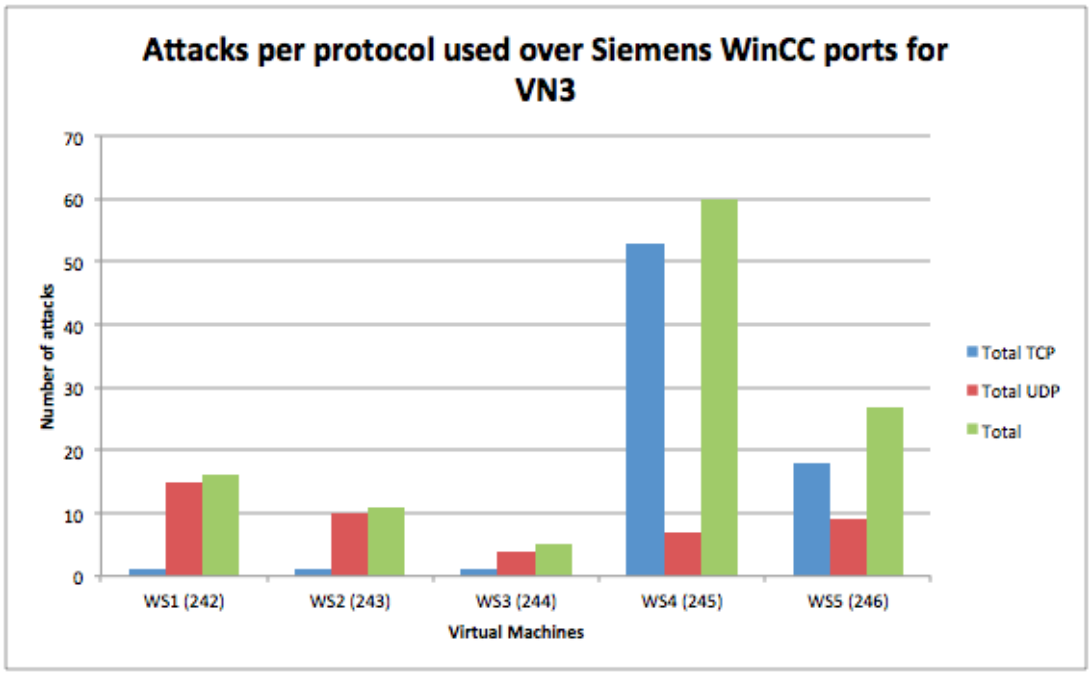


Figure 17: Histogram of number of attacks for VN3, based on the protocol used over Siemens WinCC ports for the whole duration of the experiment

In Figure 18 we see the number of attacks depending on the protocol used for all three networks per network.

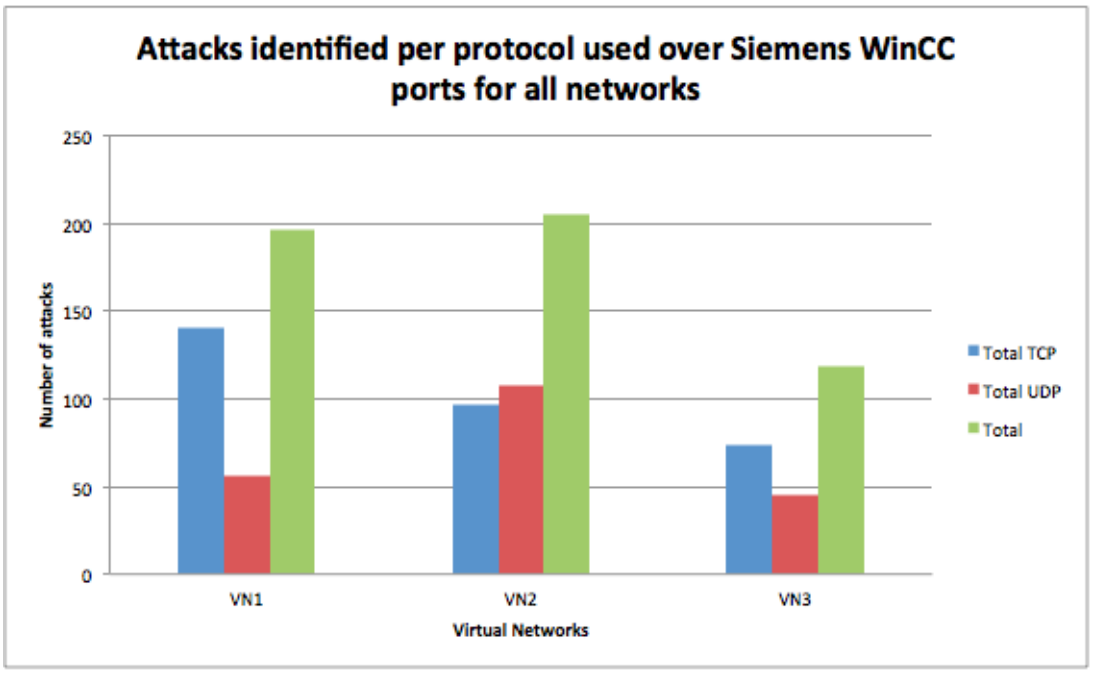


Figure 18: Histogram of number of attacks, based on the protocol used over Siemens WinCC ports for all the networks and the whole duration of the experiment

The findings based on the ports used by the attacks can be seen Figures 19, 20 and 21.

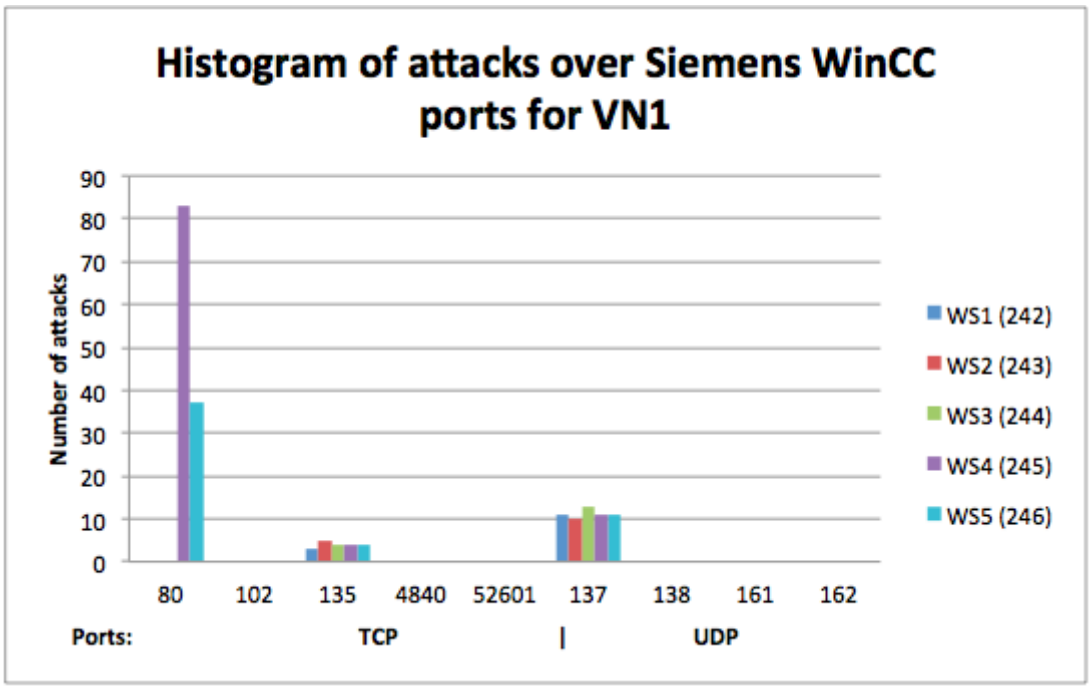


Figure 19: Histogram of number of attacks for VN1 over Siemens WinCC ports for the whole duration of the experiment

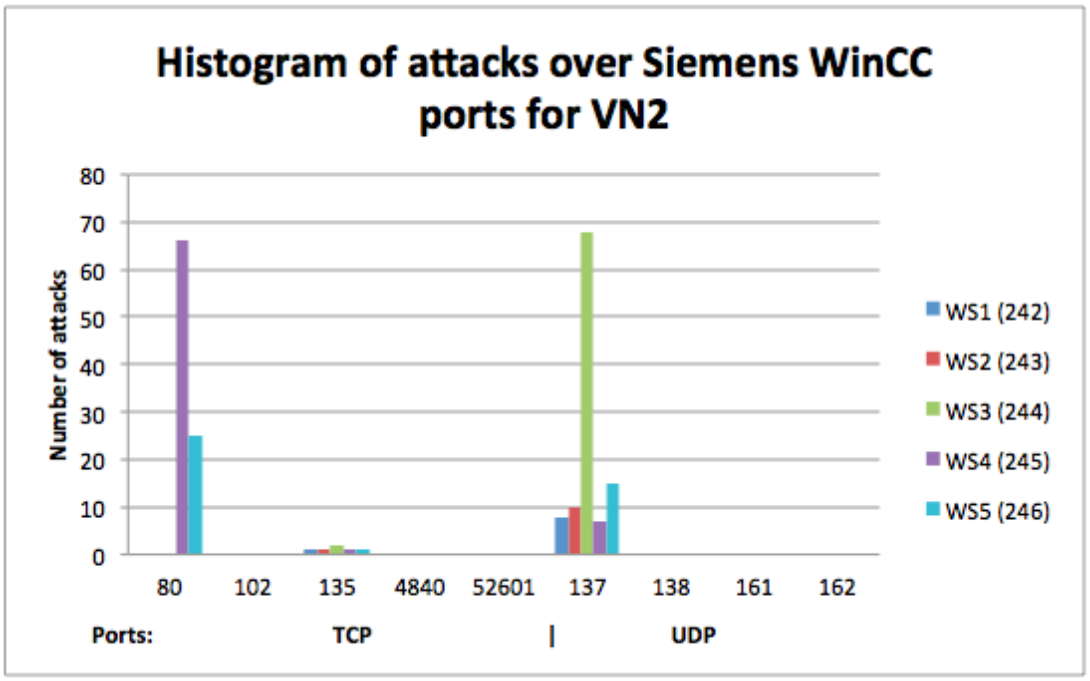


Figure 20: Histogram of number of attacks for VN2 over Siemens WinCC ports for the whole duration of the experiment

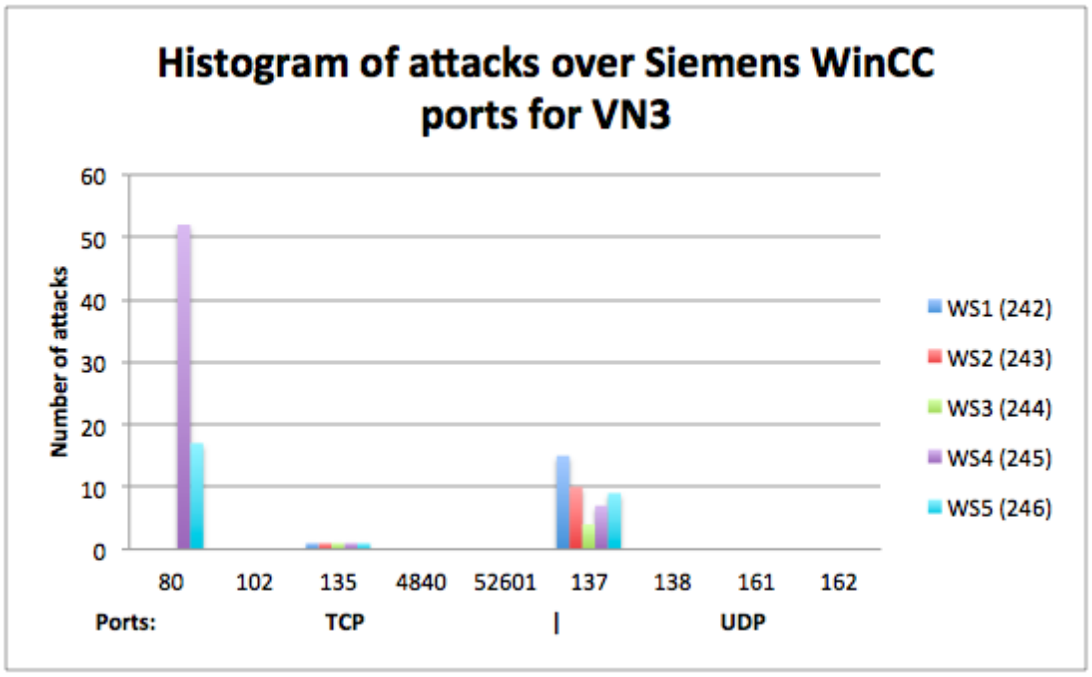


Figure 21: Histogram of number of attacks for VN3 over Siemens WinCC ports for the whole duration of the experiment

In Figure 22 we can see the total number of attacks for the three networks that were captured over the specified ports.

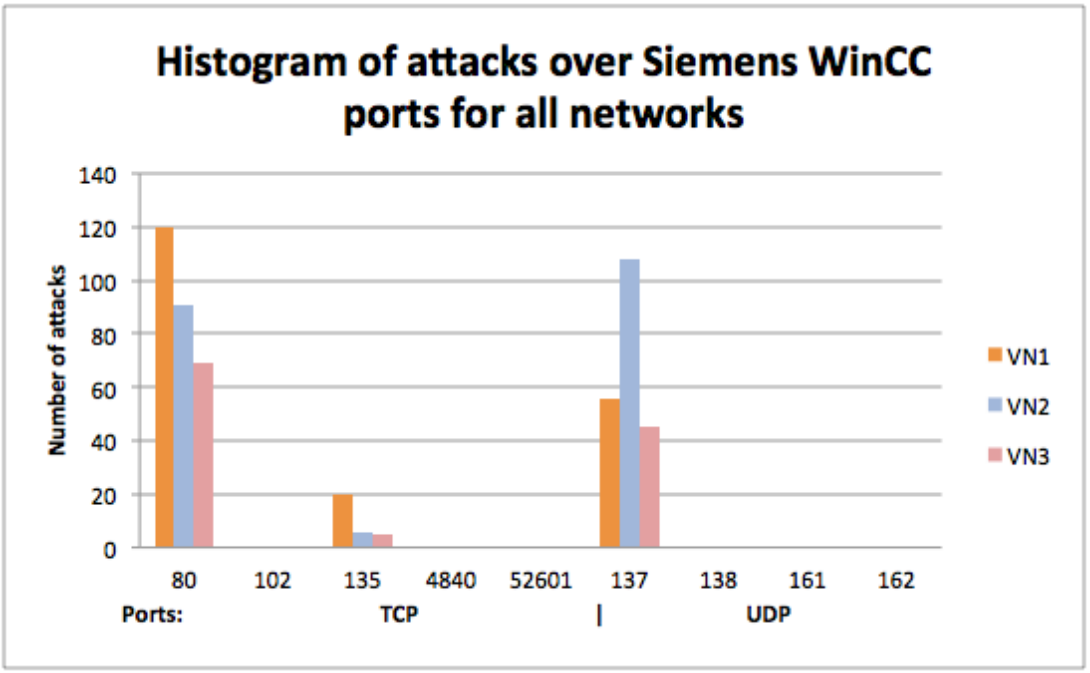


Figure 22: Histogram of number of attacks for all three networks over Siemens WinCC ports for the whole duration of the experiment

With this step of analysis we identified some types of attacks that were also earlier identified in Section 5.2 and also some new ones. These types of attacks which where identified over these ports are listed below:

- Code injection, where an attacker (client) sends a hyper text transfer protocol (HTTP) request to the victim (host) to post a file in its system (Liang, Liang, & Li, 2009). This could be any kind of malware with the effort to compromise the host.

- DCE/RPC, this is similar to the DCE/RPC flood we mentioned earlier in Section 5.2 but the attacker is making random single attempts rather than flooding the victim with requests.

- DCE/RPC flood, as we mentioned in Section 5.2.

- Dfind, this is a vulnerability scanner that sends HTTP requests to the victim that have a header like "w00tw00t.at.ISC.SANS.DFind:". This is similar to port scanning as it gathers information from the victim (Miller, 2009).

- HTTP HEAD flood, this again an attack using the HTTP protocol where the attacker is requesting from the victim some random files that are secure shell encrypted (SSH). The header is for example similar to "HEAD /.ssh/authorized_keys HTTP/1.1".

- PHP, this is similar to the PHP flood we mentioned earlier in Section 5.2 but the attacker is making random single attempts rather than flooding the victim with requests.
- PHP flood, as we mentioned in Section 5.2.
- NBSTAT, this an information gathering technique, where an attacker is using the NBSTAT command of MS Windows to request the names of various hosts (*NetBIOS NBStat Query*, 2014).

In Table 31 we can see these attacks on which VMs and which days have occurred. Again the numbers in the cells are in *ixj* form, where *i* indicates the number of the day when the attack has occurred and the *j* indicates the frequency of occurrence on that day. For example, for VN2WS5 the PHP attack occurred one time in day 1, two times in day 2 and one time in day 5.

Table 31: Types of attacks identified based on the method used, over the Siemens WinCC ports in the three network setups.

	Types of Attacks	Code injection (80)	DCE/RPC (135)	DCE/RPC flood (135)	Dfind (80)	HTTP HEAD flood (80)	PHP (80)	PHP flood (80)	NBSTAT (137)
VN1	WS1 (242)	0	1x1	1x1, 3x1	0	0	0	0	1x1, 2x4, 3x2, 4x2, 5x2
	WS2 (243)	0	1x2, 2x1, 3x1, 4x1	0	0	0	0	0	1x1, 2x3, 3x1, 4x2, 5x3
	WS3 (244)	0	1x1, 2x2	2x1	0	0	0	0	1x1, 2x12
	WS4 (245)	3x10	1x2	2x1, 3x1	1x1, 2x4, 3x2	3x1, 5x1	1x20, 2x19, 3x4, 4x1, 5x20	0	1x2, 2x5, 3x2, 4x1, 5x1
	WS5 (246)	3x10	1x1, 2x1, 4x1	1x1	1x2, 2x4, 3x2	3x1, 5x1	1x11, 2x5, 4x1	0	1x1, 2x6, 3x2, 4x1, 5x1
VN2	WS1 (242)	0	0	4x1	0	0	0	0	1x2, 2x1, 3x1, 4x2, 5x2
	WS2 (243)	0	0	1x1	0	0	0	0	1x2, 2x2, 3x2, 4x2, 5x2
	WS3 (244)	0	1x1	1x1	0	0	0	0	1x2, 2x1, 3x1, 4x9, 5x55
	WS4 (245)	2x10, 4x5	0	3x1	1x1, 4x2	0	1x9, 2x10, 3x20, 4x9	0	1x3, 2x1, 3x1, 4x2
	WS5 (246)	2x10, 4x5	0	2x1	1x1, 4x2, 5x3	0	1x1, 2x2, 5x1	5x1	1x4, 2x2, 3x2, 4x2, 5x5
VN3	WS1 (242)	0	0	1x1	0	0	0	0	1x8, 2x2, 3x2, 4x1, 5x2
	WS2 (243)	0	0	1x1	0	0	0	0	1x1, 2x1, 3x3, 4x2, 5x3
	WS3 (244)	0	0	1x1	0	0	0	0	1x4
	WS4 (245)	0	0	1x1	1x2, 2x3, 3x1, 4x1, 5x1	0	1x12, 2x15, 3x9, 4x8	0	1x2, 3x2, 4x3
	WS5 (246)	0	0	1x1	1x2, 2x3, 3x1, 4x1, 5x1	0	3x5, 4x4	0	1x2, 3x5, 4x1, 5x1

In Figures 23, 24 and 25 we can see the number of the types of attacks for each VM for the different networks, that where captured over the specified ports.

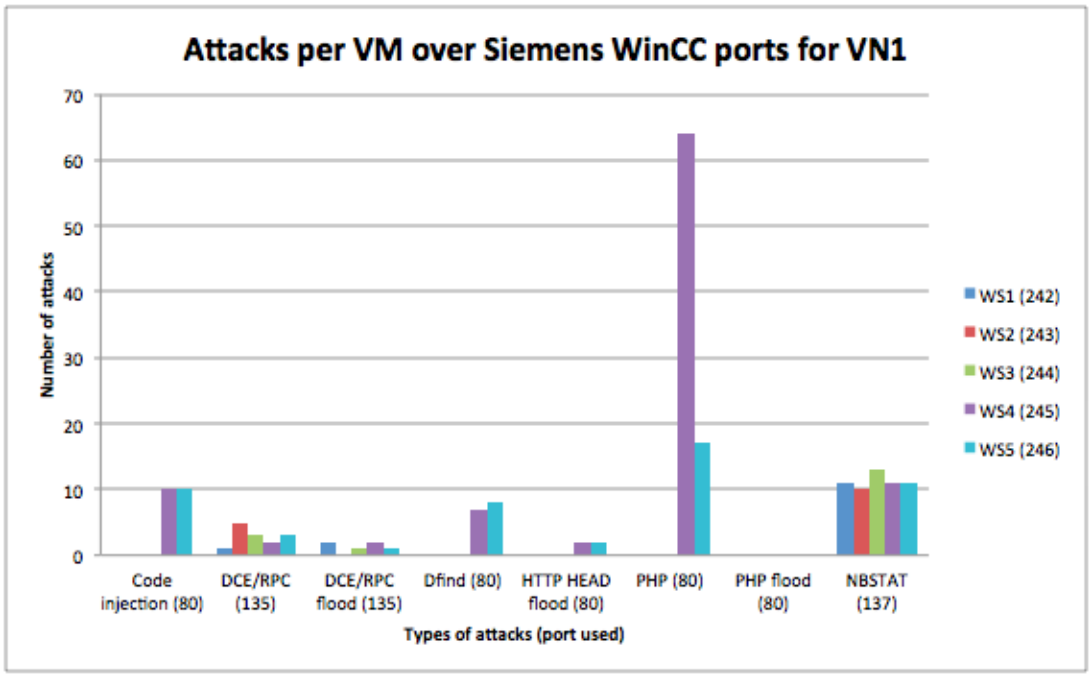


Figure 23: Histogram of number of attacks for VN1 over Siemens WinCC ports, based on the type, for the whole duration of the experiment

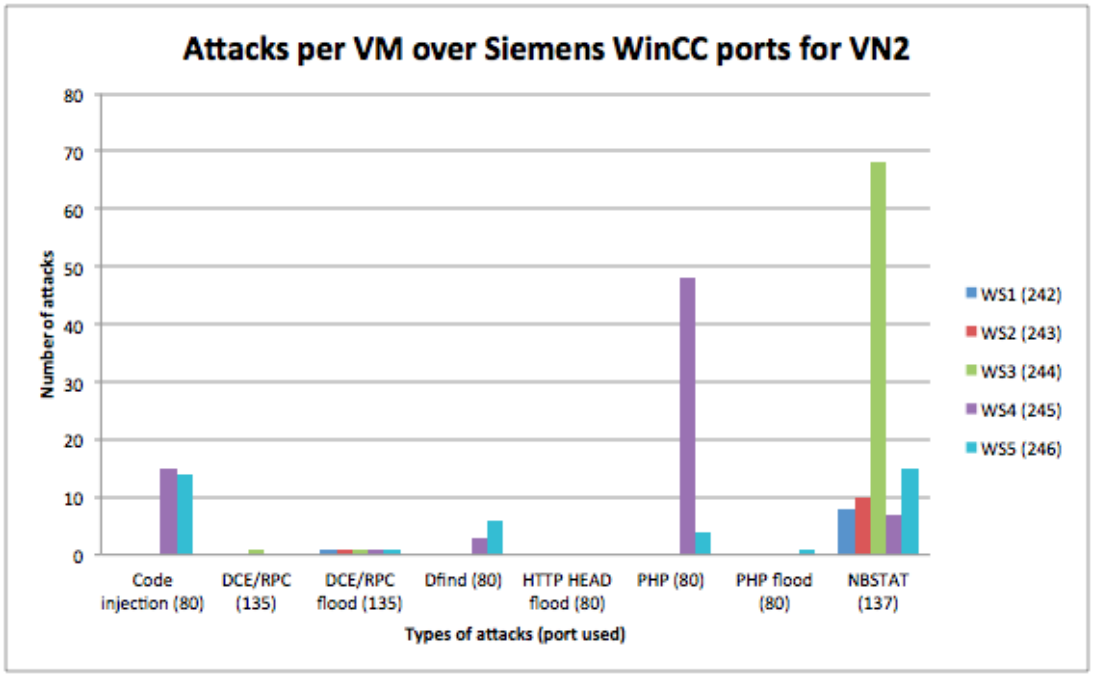


Figure 24: Histogram of number of attacks for VN2 over Siemens WinCC ports, based on the type, for the whole duration of the experiment

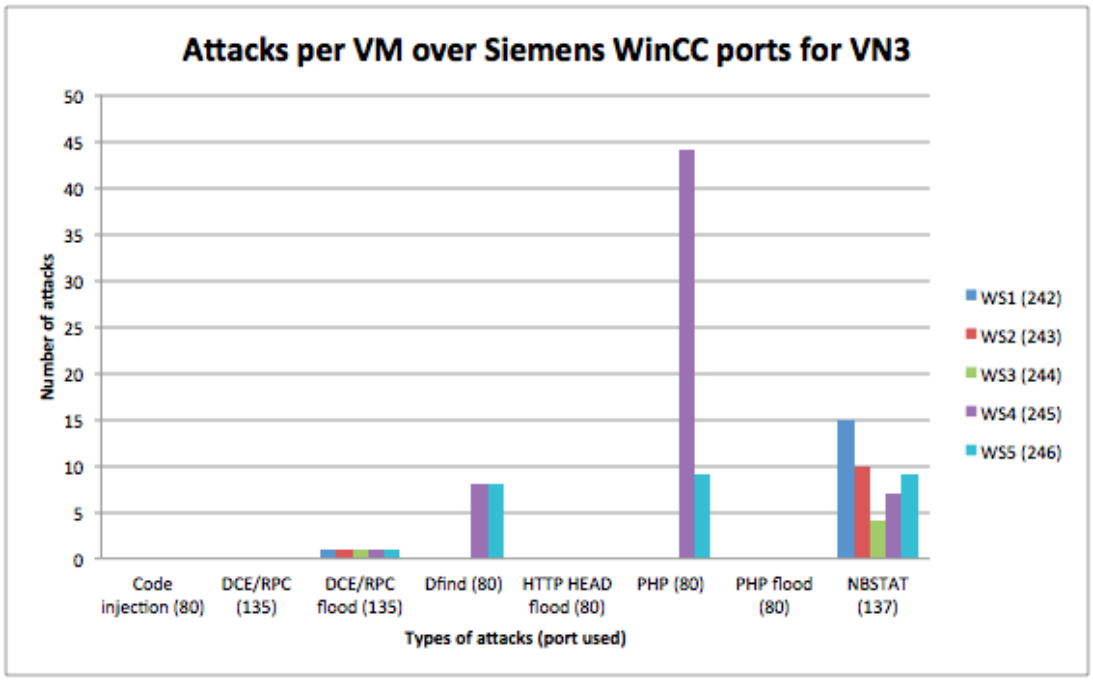


Figure 25: Histogram of number of attacks for VN3 over Siemens WinCC ports, based on the type, for the whole duration of the experiment

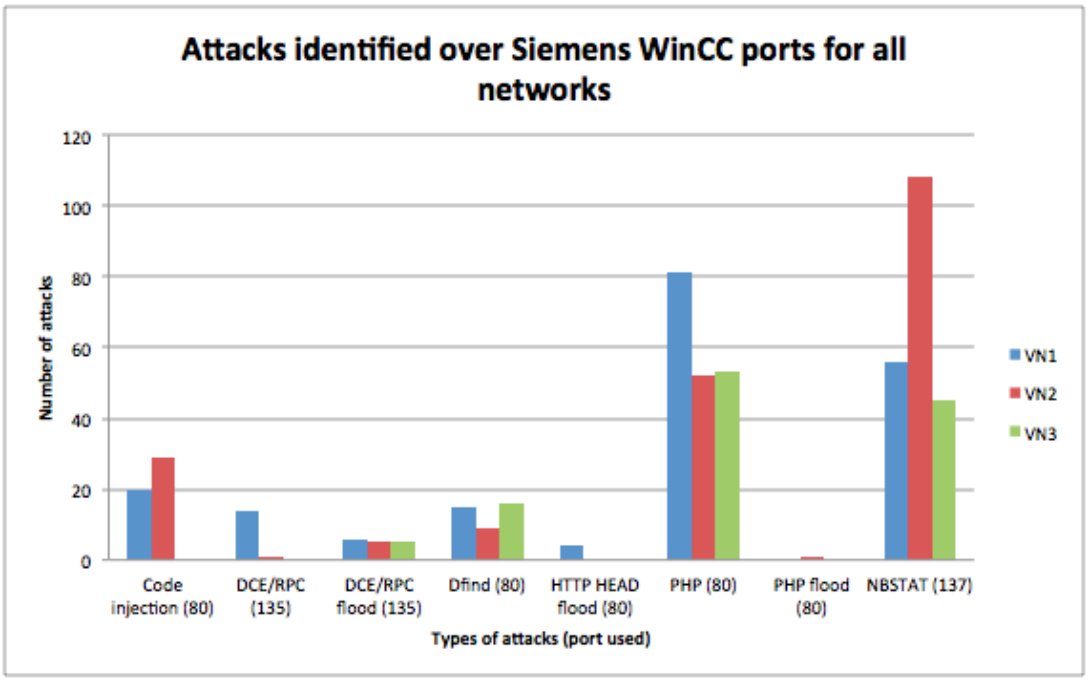


Figure 26: Histogram of number of attacks identified over Siemens WinCC ports, based on the type, for all the networks and the whole duration of the experiment

5.4 Identification of unique hostile IP addresses

Our next task in the analysis of the data is to identify the IPs targeting our virtual machines for each network and from where they are originating. The number of hostile IPs

for VN1 are 38, for VN2 91 and for VN3 43 IPs.

We then try to identify the country of origin for each IP from the data captured and with geoip databases installed with Wireshark. The results can be seen in Figures 27, 28 and 29.

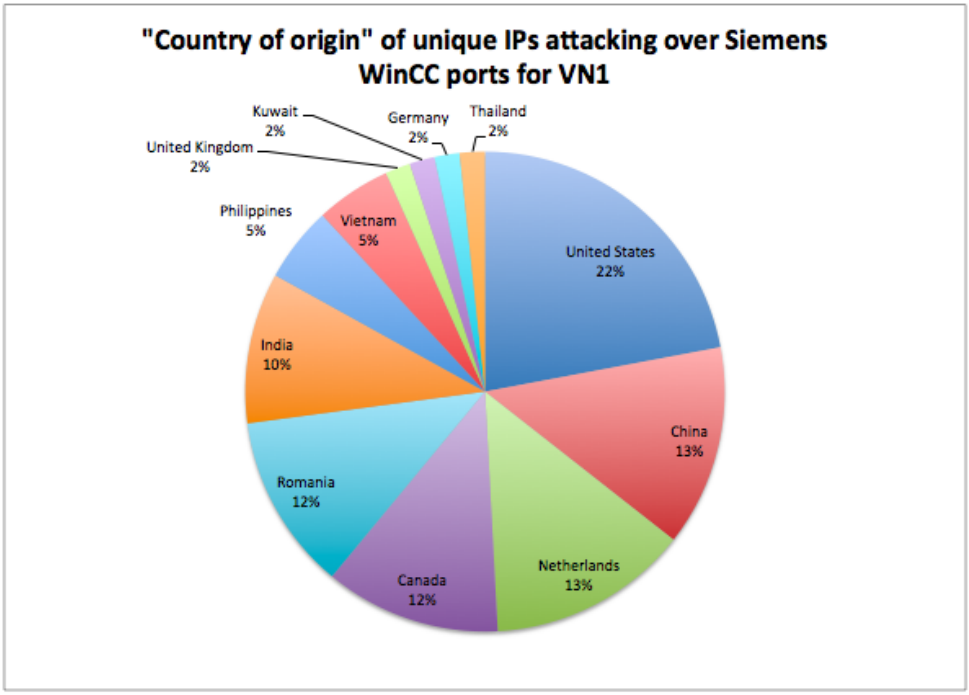


Figure 27: Country of origin of unique IPs targeting VN1 over Siemens WinCC ports

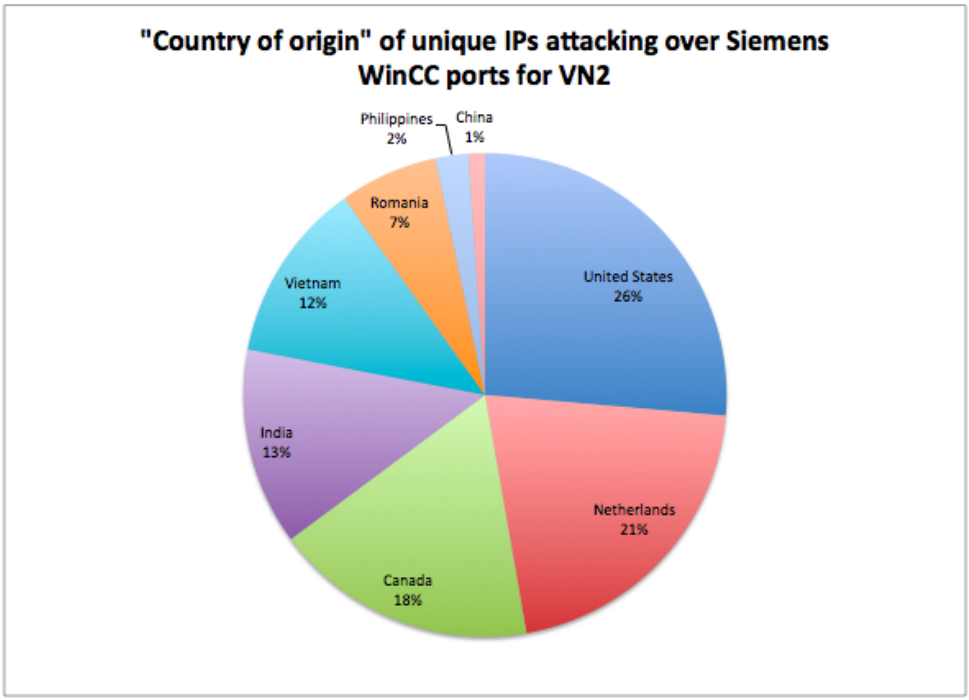


Figure 28: Country of origin of unique IPs targeting VN2 over Siemens WinCC ports

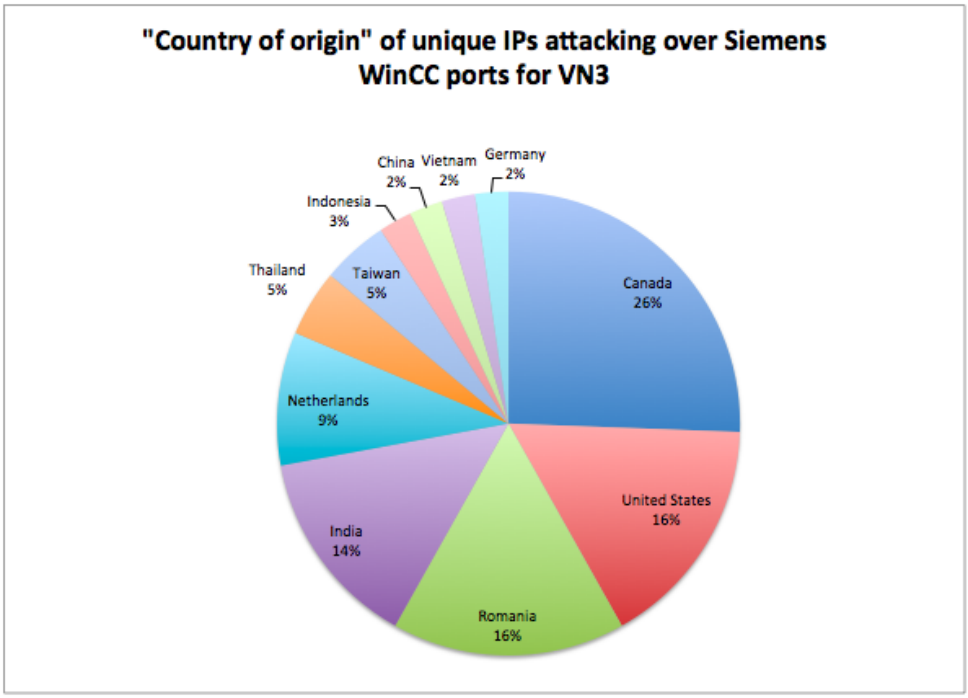


Figure 29: Country of origin of unique IPs targeting VN3 over Siemens WinCC ports

These figures though, cannot be considered as 100% accurate since in most cases of network attacks, the attackers "spoof" their original IP address falsifying it and replacing it with that of another innocent client computer. Thus we cannot be sure that these IPs are also the ones performing the attack. This is basically done to avoid detection and keep the interest and efforts of law enforcing agents away from them and the systems they are using.

As a final step of our analysis we try to identify IPs that are targeting only specific VMs among the same virtual network and IPs that target only the WS1, WS4 and WS5 which are the ones that have the Siemens software installed and running in runtime. Our findings are the following and can be also seen in Table 32:

- there is no unique IP that is targeting only the three workstations with the SCADA software.
- among the 38 hostile IPs for VN1, 14 are targeting only one VM
- among the 91 for VN2, 20 are targeting only one VM
- among the 43 for VN3, 13 are targeting only one VM

Table 32: Unique IPs targeting only one VM or the VMs with the SCADA software running

	No of unique hostile IPs	No of unique hostile IPs targeting only one VM	What are the targets	No of unique hostile IPs targeting WS1, WS4 and WS5
VN1	38	14	WS3, WS4	0
VN2	91	20	WS2, WS3, WS4, WS5	0
VN3	43	13	WS1, WS2, WS3, WS4, WS5	0

6 Discussion, limitations and future work

After we have presented the results in the previous section we need to interpret them and try to assess whether our research question has been answered. We remind the reader that the research question is "what cyber threats can a SCADA network centre attract?".

On a macroscopic level we saw that some typical malevolent behaviour involves DoS and DDoS attacks and port scanning. These are quite common especially taking into consideration that DoS attacks occurred in all the VMs of all the networks at least once in one day of the experiment. These attacks vary according to the different types of communication protocol like TCP and UDP and then also along the subprotocol used. We identified TCP flood requests with various flags set, SMB floods, DCE/RPC floods and DNS flood requests which use the UDP protocol etc. The most common attack among the three virtual networks are the SMB floods, the DCE/RPC floods and port scanning, while some other where specifically identified on certain VMs like the DDoS DNS flood on WS4, but this was expected since it was the only VM having a DNS service running. The WS4 and WS5 VMs, the ones that are also MS Windows Servers attracted most of the attacks as we can see if we compare Figures 11, 12 and 13. Another remark is that most of these generic attacks occurred in VN1 and VN2. If we take a closer look at Table 30 we can see that the DDoS DNS attack on the VN2WS4 is actually a continuation of the attack on the day 5 of VN1WS4 and continued to VN2WS4 on days 1,2 and 3.

As we can see in Figures 11, 12 and 13, from the generic types of attack identified, the most common was port scanning, which occurred in al VMs for VN1 and VN2, and the SMB flood requests which occurred on the WS2, WS4 and WS5 VMs in all three networks. The DCE/RPC flood also occurred in all 4 VMs that we analysed at this step (WS3 was not included due the data file size). In Figure 14 we can observe that VN1 and VN2 have attracted almost all types of generic attacks, while VN3 only three; the TCP SYN flood, SMB flood and DCE/RPC flood. This is expected since VN3 has all the latest patches for the OSs. Only the SMB flood occurrence is still quite high compared to the other two.

From our microscopic level of analysis and Figures 15, 16 and 17 we observe that in most of the VMs the attacks were carried out using the UDP protocol with the exception of WS4 and WS5 where TCP based attacks were more prevalent in all three networks (we remind the reader that at this point the results of WS3 are included in the analysis). If we look at the total picture in Figure 18 we see that the VN1 and VN2 have attracted most of the attacks, while VN1 has attracted more TCP based attacks. These attacks are mainly using port 80 as we can see in Figures 19, 20 and 21 and the method is a PHP flood (TCP port 80 based) as we can see in Figures 23, 24 and 25. Some attacks are targeting specifically the WS4 and WS5 that have Windows Server 2008 as an operating system and these are the code injection, PHP and PHP flood and Dfind (TCP port 80 based). The DCE/RPC, DCE/RPC flood and NBSTAT attacks (TCP port 135 and UDP port 137 based) are occurring in all 5 VMs irrespective of their OS. In Fgure 22 and 26 we see that VN1 and VN2 still attract more attacks that occurred over the ports Siemens WinCC uses. Again VN1 and VN2 have attracted almost all types of attacks, 6 out of 8, while VN3 has attracted half, 4 out of 8. The most prevalent attack in all networks is the NBSTAT and PHP.

In Figures 27, 28 and 29 we observe that most attacks occurred from developing countries while there is also a big number of attacks coming from developed ones. However as we mentioned these graphs need to be treated with caution, since the IP of the attacker may be "spoofed", falsifying its original one(s).

We end our analysis with the identification of the unique hosts in each VN that was targeting specific VMs in Table 32. We could not identify any unique IPs that were targeting specifically the VMs having the Siemens WinCC software. Thus, we can say that perhaps these attacks are somehow random or automated from infected personal computers that scan the internet for vulnerable hosts and attack them randomly, in order to infect them and further exploit them. There are some attacks that are targeting specifically the WS4 and WS5, but most probably because of their Windows Server 2008 operating system, while the third VM that has the SCADA software, has attracted only DCE/RPC and NBSTAT attacks, attacks that have occurred in all VMs, in almost all networks as we can see in Figures 23, 24 and 25.

To summarise our discussion, we can say that there are cyber threats that can target a SCADA network centre. These attacks vary based on the method they use and also the internet communication protocol they utilise to deliver their payload. However, we could not identify any types of attacks or hosts targeting specifically our VNs for the fact that they were mimicking a SCADA network. This is obvious given also the fact that no malevolent network behaviour was recored in all the ports that the Siemens WinCC software is using, but mostly on the common ones.

6.1 Limitations of current research and future work

Certain limitations of the current research and the design of the experiment can be identified, that could have affected the results registered during the experiment.

To begin with, our VMs were virtual machines running on host that was also itself a virtual machine. This perhaps could be identified by an attacker by detecting the VMware services that were installed and ran in the VMs during the experiment, deciding not to bother with them by guessing their role as a "honeypot".

Moreover, the Siemens WinCC Professional software that we installed in the VMs is a trial version and for the runtime we had a demo project running, freely available by Siemens. Perhaps certain functionalities were not included that could have made the software more visible in the internet. The requirements for operating systems for the software to run, limited our choice for the starting patch level for some of them. For example for the MS Windows XP we had to have it updated to Service Pack 3 from VN1 in order to install the software. This remained unchanged to VN2 and only to VN3 we updated the OS.

In addition, the IPv4 addresses we received from the provider of the the host were registered to the name of the author and not for example to an infrastructure owner, making our VMs less likely to attract the interest of an attacker targeting SCADA networks.

Lastly, the limited availability of IPv4 addresses could have greatly affected our results. Our method was to have the same IPs for the VMs in all the three networks. For a potential attacker this meant that each VM was the same personal computer that was merely updated or not after some time. This practically meant that each VM was online for 15 days with a few hours interval every five days, where some VMs were updated. This remark is also strengthened by the results at Table 30 where we saw that the DDoS DNS attack on WS4 was a continuation of the same attack from VN1 to VN2.

We propose to further explore the field of network security for SCADA networks from the aspect of the threats existing in the internet. Future work could possibly address the current limitations of our research and try to identify threats that are specific to the nature of a SCADA network centre.

7 Conclusion

We started our research with an exploration in the academic literature of the definition of risk and decide that a definition of the term involves the effect of uncertainty on our objectives. In the case of a critical infrastructure that is supported by a critical information infrastructure these uncertainties could be the cyber threats originating from the internet and our objectives the unobstructed operation and availability of the critical infrastructure. We further defined some of the major terms of our research like the critical infrastructure and critical information infrastructure, risk and risk assessment, cybercrime and cyberwarfare.

We tried to assess the cyber threats with the help of the OCTAVE Allegro risk assessment methodology, a method tailored to the needs of ICT security. We made some assumptions about the type of the critical infrastructure and the critical information infrastructure supporting it and came up with some potential cyber threats from the internet.

We decided to design and conduct an experiment to identify the cyber threats that exist in real life for a critical information infrastructure, in our case a SCADA network centre. Based on existing previous work in the academic literature we decided instead of a computer simulation to design an experiment that is mimicking the real life setup of a SCADA network centre with the help of virtual machines as closely as our resources could allow.

The results of the experiment and our analysis have revealed that certain varying cyber threats exist, but we could not identify specific threats that were targeting our setup as a SCADA network centre. Thus, the threats we identified can be considered as relevant to any network setup and not only to our SCADA setup.

Certain limitations of the current study regarding the design of the experiment could be identified, like the limitation on the availability of IP addresses, the registration of these IPs to an individual instead of an organisation like an infrastructure owner, the software running on the VMs was trial version with a demo project and the fact that we incorporated virtual machines instead of actual workstations.

Nonetheless, we can assume that our research question is answered by the research we conducted, but additional future research addressing our limitations should be performed since these cyber threats can greatly affect the normal operation of a critical infrastructure and consequently that of a nation and its citizens.

References

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. *Pittsburgh, PA, Carnegie Mellon University*.

Alomari, E., Manickam, S., Gupta, B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *... Journal of Computer ...*, *49*(7), 24–32.

Amanullah, M., Kalam, A., & Zayegh, A. (2005). Network security vulnerabilities in SCADA and EMS. In *Transmission and distribution conference and exhibition: Asia and pacific, 2005 ieee/pes* (pp. 1–6).

ANSI=ASSE Z690.1–2011. (2011). Vocabulary for Risk Management. Washington DC. *American National Standards Institute*.

Aven, T. (2007, June). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety*, *92*(6), 745–754. doi: 10.1016/j.ress.2006.03.008

Aven, T. (2010, June). On how to define, understand and describe risk. *Reliability Engineering & System Safety*, *95*(6), 623–631. doi: 10.1016/j.ress.2010.01.011

Beidleman, S. W. (2009). *Defining and deterring cyber war* (Tech. Rep.). DTIC Document.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50–59.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007, May). *Introducing OCTAVE Allegro: Improving the information security risk assessment process* (Tech. Rep. No. CMU/SEI-2007-TR-012). Carnegie-Mellon University, Software Engineering Institution.

Carnegie-Mellon University, Software Engineering Instution. (2014, 04). *The OCTAVE-S Method.* Retrieved 04.04.2014, from http://www.cert.org/resilience/products-services/octave/octave-s-method.cfm

Church, R. L., Scaparra, M. P., & Middleton, R. S. (2004). Identifying critical infrastructure: the median and covering facility interdiction problems. *Annals of the Association of American Geographers*, *94*(3), 491–502.

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, *37*(4), 671–680.

Cohen, F. (1999). Simulating cyber attacks, defences, and consequences. *Computers & Security*, *18*(6), 479–518.

Cross, M. (2008). *Scene of the Cybercrime.* Burlington, MA: Syngress.

Davis, C., Tate, J., Okhravi, H., Grier, C., Overbye, T., & Nicol, D. (2006). SCADA cyber security testbed development. In *Proceedings of the 38th north american power symposium (naps 2006)* (pp. 483–488).

DHS Risk Steering Committee. (2010). *DHS Risk Lexicon* (Tech. Rep. No. September). Washington D.C.: U.S Department of Homeland Security.

Dietz, E., Scott Frey, R., and Rosa, E. (1996). *Risk, Technology, and Society.* R.E. Dunlap and W.

ENISA. (2014, 04). *European Union Agency for Network And Information Security.* Retrieved 02.04.2014, from http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html

Federal Ministry of Economics and Technology Editing team JWB 2013. (2013, January). *2013 Annual Economic Report, Competitiveness – the key to growth and jobs in Germany and Europe* (Tech. Rep.). Federal Ministry of Economics and Technology (BMWi), Public Relations.

Gordon, K., & Dion, M. (2008, May). Protection of 'Critical Infrastructure' and the role of investment policies relating to national security. *Investment Division, Directorate for Financial and Enterprise Affairs, Organisation for Economic Cooperation and Development, Paris*(40700392).

Grabosky, P. N. (2001). Virtual criminality: old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249.

Hämmerli, B. M., & Renda, A. (2010). *Protecting critical infrastructure in the EU*. Centre for European Policy Studies Brussels.

Hildreth, S. A. (2001). Cyberwarfare..

Holt, T. J., & Bossler, A. M. (2014, January). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40. doi: 10.1080/01639625 .2013.822209

Hunton, P. (2009, November). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law and Security Review*, *25*(6), 528–535. doi: 10.1016/j.clsr.2009.09.005

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, *25*(7), 498–506.

ISACA. (2009). *THE RISK IT Framework*.

ISO. (2009). Risk Management - vocabulary. *Guide 73:2009*.

Johnson, R. E. (2010). Survey of scada security challenges and potential attack vectors. In *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for* (pp. 1–5).

Kleinrock, L. (1961). Information flow in large communication nets. *RLE Quarterly Progress Report*, *1*.

Kleve, P., De Mulder, R., & Van Noortwijk, K. (2011, April). The definition of ICT Crime. *Computer Law and Security Review*, *27*(2), 162–167. doi: 10.1016/j.clsr .2011.01.004

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22–31.

Liang, Z., Liang, B., & Li, L. (2009). A system call randomization based method for countering code-injection attacks. *International Journal of Information Technology and Computer Science (IJITCS)*, *1*(1), 1.

Liff, A. P. (2012, June). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, *35*(3), 401–428. doi: 10.1080/01402390.2012.663252

Liljenstam, M., Liu, J., Nicol, D., Yuan, Y., Yan, G., & Grier, C. (2005). Rinse: The real-time immersive network simulation environment for network security exercises. In *Principles of advanced and distributed simulation, 2005. pads 2005. workshop on* (pp. 119–128).

Luko, S. N. (2013, July). Risk Management Terminology. *Quality Engineering*, *25*(3), 292–297. doi: 10.1080/08982112.2013.786336

McQueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A. (2006). Quantitative cyber

risk reduction estimation methodology for a small SCADA control system. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on* (Vol. 9, pp. 226–226).

Miller, B. S. (2009). *Analysis of Attacks on Web Based Applications*. Unpublished master's thesis, College of Engineering and Mineral Resources at West Virginia University.

Moteff, J., & Parfomak, P. (2004, October). *Critical infrastructure and key assets: definition and identification* (Tech. Rep.). Congressional Research Service, The Library of Congress.

NATO Science and Technology Organization. (2008, September). *Improving common security risk analysis* (Tech. Rep. No. RTO-TR-IST-049). NATO.

Netbios nbstat query. (2014, August). Retrieved 03.08.2014, from http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20588

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, *31*(4), 418–436.

NIST. (2011, March). *Managing information security risk* (Tech. Rep. No. NIST Special Publication 800-39). Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930: National Institute of Standards and Technology.

OECD DSTI/CICCP. (2007). *Development of Policies for Protection of Critical Information Infrastructures* (Tech. Rep.). Organisation for Economic Co-operation and Development, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy.

OECD DSTI/CICCP. (2008). *OECD Recommedation of the Council on the Protection of Critical Information Infrastructures* (Tech. Rep.). Organisation for Economic Co-operation and Development, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy.

Panda, P. (2009). The octave® approach to information security risk assessment. *ISACA Journal*, *4*.

Pang, R., Yegneswaran, V., Barford, P., Paxson, V., & Peterson, L. (2004). Characteristics of internet background radiation. In *Proceedings of the 4th acm sigcomm conference on internet measurement* (pp. 27–40).

Parker, D. B. (1989). *Computer crime: criminal justice resource manual*. US Department of Justice, National Institute of Justice, Office of Justice Programs.

Parks, R. C., & Duggan, D. P. (2011). Principles of cyberwarfare. *IEEE Security & Privacy Magazine*, *9*(5), 30–35.

Path traversal attack. (2014, August). Retrieved 03.08.2014, from http://en.wikipedia.org/wiki/Directory_traversal_attack

Purdy, G. (2010). Iso 31000: 2009—setting a new standard for risk management. *Risk analysis*, *30*(6), 881–886.

Renn, O. (1998). Three decades of risk research: accomplishments and new challenges. *Journal of risk research*, *1*(1), 49–71.

Renn, O. (2005). RISK GOVERNANCE: towards an integrative approach. *Geneva: International Risk Governance Council*.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, *21*(6), 11–25.

Risley, A., Roberts, J., & Ladow, P. (2003). Electronic security of real-time protection and scada communications. *Schweitzer Engineering Laboratories, SEL*.

Rosa, E. a. (1998, January). Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, *1*(1), 15–44. doi: 10.1080/136698798377303

Siemens AG Industry Sector. (2013, July). WinCC Professional V12.0 SP1 [Computer software manual]. Postfach 4848, 90026 Nürnberg, Germany.

Siemens Automation. (2014a, July). *Siemens WinCC Demo project RT.* Retrieved 27.05.2014, from https://support.automation.siemens.com/WW/llisapi.dll?func=ll&objid=73468169&nodeid4=20229806&caller=view&lang=en&siteid=cseus&aktprim=4&objaction=csopen&extranet=standard&viewreg=WW

Siemens Automation. (2014b, May). *Siemens WinCC system requirements.* Retrieved 27.05.2014, from https://www.industry.siemens.com/topics/global/en/tia-portal/hmi-sw-tia-portal/wincc-tia-portal-es/system-requirements/pages/default.aspx?HTTPS=REDIR

Sridhar, S., & Manimaran, G. (2010). Data integrity attacks and their impacts on SCADA control system. In *Power and energy society general meeting, 2010 ieee* (pp. 1–6). IEEE.

Stamp, J., Dillinger, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. *SAND2003-1772C. Sandia National Laboratories*.

Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for scada systems. *Power Systems, IEEE Transactions on*, *23*(4), 1836–1846.

The Guardian. (2011). *Germany to shut all nuclear reactors.* Retrieved 30.05.2011, from http://www.theguardian.com/world/2011/may/30/germany-to-shut-nuclear-reactors

UK Cabinet Office. (2002). Risk : Improving government ' s capability to handle risk and uncertainty. *Strategy Unit Report, UK*(November).

Von Clausewitz, C. (2004). *On war*. Digireads. com Publishing.

Wall, D. S. (2001). *Crime and the Internet*. London: Routledge.

Wall, D. S. (2004, December). What are Cybercrimes? *Criminal Justice Matters*, *58*(1), 20–21. doi: 10.1080/09627250408553239

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity.

Wall, D. S. (2010). The internet as a conduit for criminal activity. *Information Technology and The Criminal Justice System*(March), 77–98.