Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector

by

Ruth Østgaard Skotnes

Thesis submitted in fulfillment of
the requirements for degree of
PHILOSOPHIAE DOCTOR
(PhD)

University of
Stavanger

Faculty of Social Sciences

2015

University of Stavanger
N-4036 Stavanger
NORWAY

www.uis.no

ISBN: 978-82-7644-616-6

ISSN: 1890-1387

Preface

This thesis documents the work carried out during my PhD study at Centre for Risk Management and Societal Safety (SEROS), Department of Media, Culture and Social Sciences, University of Stavanger (UiS). Completing the thesis has been a challenging, but extremely rewarding process. Many people have contributed during the process, and I am very thankful for their help and support.

First of all, I would like to thank my main supervisor, Professor Ole Andreas Engen from SEROS at UiS, for all his help, encouragement, and support during my PhD study. I am also grateful for his constructive feedback, and for encouraging me to take control of my project and make my own decisions. I also thank my co-supervisor, Lise Hellebø Rykkja, Post doctor from the Department of Administration and Organization Theory at the University of Bergen (UiB), for her feedback and insightful comments.

Next, I would like to thank Roger Steen, Arthur Gjengstø, and the rest of the contingency planning department of the Norwegian Water Resources and Energy Directorate (NVE), for all their information and support during my PhD study. Furthermore, I would like to thank the representatives from Forum for informasjonssikkerhet i kraftforsyningen for their help with the pilot study of my survey questionnaire, and for inviting me to attend their conference. I am also very grateful to all the managers and employees in the Norwegian network companies that took the time to answer my survey.

Thank you to all my colleagues and friends at UiS, you have made the university a great place to work! I especially want to thank Professor Preben H. Lindøe and Post doctor Sindre Høyland for reading the final draft of my thesis and giving me valuable feedback. I also thank Professor Knud Knudsen for his help with the statistical analysis, and Bjørn-Tore Blindheim for reading through early drafts of my thesis and providing helpful comments.

Thank you to my family and friends, and a special thank you to my wonderful parents for all their help and encouragement.

Finally, warm thanks to my two beautiful daughters, Sofie and Ella, and my husband, Thomas Yvan – I dedicate this thesis to you. Thank you, Sofie and Ella, for your patience and understanding when your mum was away at work or busy staring at the computer screen. And thank you most of all, Thomas Yvan, for being encouraging, understanding, patient, and supportive. You were always there to listen when I was frustrated, you believed in me, and helped take care of our family – I could not have done this without you.

Stavanger, 2015.

Ruth Østgaard Skotnes

Summary

The generation, transmission, and distribution of energy are among the most vital prerequisites for the functioning of modern societies (Antonsen et al., 2010). Today, information and communication technology (ICT) is used to monitor, control, and operate power generation plants and power distribution within electric power supply systems (Patel and Sanyal, 2008). Process control systems, e.g., supervisory control and data acquisition systems (SCADA systems) and other ICT systems used within electric power supply systems, are vulnerable to a multitude of physical, electromagnetic, and logical threats, both natural and man-made (Rodal, 2001). The recent trends are toward more general purpose software solutions; and toward use of the Internet for communication related to operations and management of remote processes and production systems. This increases efficiency and cooperation, saves time, and reduces costs. However, this also makes formerly isolated ICT systems vulnerable to a set of threats and risks they have not been exposed to before (Line and Tøndel, 2012).

Since the early 1990s, the energy sectors of Western societies have been through a process of institutional restructuring, where large state-owned monopolies have been divided into several independent organizations (Antonsen et al., 2010). Emergent control technologies, making intensive use of ICT, have been useful for dealing with the new situation of enlargement, open access, progressive integration of electricity markets, and intensification of cross-border trade. However, the full application of these technologies has demanded a new approach to system design and operation, and their integration within existing control infrastructures and practices has been a challenge (The GRID Consortium, 2007).

With this background as a point of departure, the thesis examines several important elements of safety and security management systems which have been emphasized in previous research (Rasmussen, 1997; Hagen, Albrechtsen, and Hovden, 2008; Renn, 2014; Aven et al., 2004), i.e., government risk regulation, the use of technical standards for safety and security, risk perception among managers and employees, management commitment to safety and security, and awareness creation and training with regard to safety and security. The aim of the study is to follow up on previous research on challenges for safety and security management and to explore, describe, and discuss challenges for safety and security management of network (distribution/grid) companies within the electric power sector that arise due to the increased use of ICT to monitor, control, and operate electric power production and distribution. Thus, the main aim of the thesis is to answer the following question:

- What challenges for safety and security management of network companies within the electric power sector have arisen in light of the increased use of ICT to monitor, control, and operate electric power production and distribution?

Specific research questions have been derived from the main aim, and these research questions are addressed in the four articles included in the thesis.

The context for the study is the Norwegian electric power supply sector, and the research questions are answered by presenting results from a survey sent to 137 network (distribution/grid) companies in Norway, supplemented by results from interviews, observation studies, and document studies. The thesis focuses on companies involved in transmission and distribution of electricity, and

not generation (production). The generation system in the Norwegian electric power supply consists of many power stations distributed over the whole country. The structure is thus relatively robust, and the dependence on individual plants is small (Fridheim, Hagen, and Henriksen, 2001). However, a failure in the electricity networks and the transmission and distribution of electricity to critical infrastructures and important societal functions, as well as to individual households, would have a huge impact on societal safety (and security).

This thesis concentrates on organizational safety and security (risk) management within electric power supply network companies. However, network companies run critical national infrastructure, and the safety and security management of these companies can thus affect societal safety and security. Safety and security management of network companies is also affected by national regulations, and there is no longer a clear distinction between national regulations and safety and security management of network companies. Ideas about internal control and risk management have been increasingly commingled, and risk management and regulation are no longer seen as broadly contrasting methods of assuring safety and security (Power, 2007).

The results of the study show that finding the best balance between the use of detailed, prescriptive regulation versus functional regulation (self-regulation/internal control) as principles for controlling risk and ensuring safety and security is a challenge for the safety and security management of the network companies. Next, the thesis finds that technical standards for management of ICT safety and security pose a challenge for the network companies. These standards have both strengths and weaknesses, and both use and non-use of these standards can lead to challenges for the safety and security management of the network companies. The study also suggests that users (both managers and employees) of ICT systems (including SCADA systems) within the electric power supply network companies perceive the risk of attacks on or malfunctions in these systems as low, which can present a challenge for the safety and security management of the companies. Furthermore, the study finds a statistically significant correlation between management commitment to ICT safety and security and implementation of awareness creation and training measures in the companies; however, the use of awareness creation and training measures for ICT safety and security varies quite a bit among the network companies. The lack of awareness of a danger might lead to weak vigilance by users and a greater potential for abuse, which can be a challenge for safety and security management. The thesis also highlights that one main factor – complexity – influences all the different challenges studied.

The theoretical framework for the thesis (i.e., the sociotechnical perspective and institutional organizational theory) has helped to contextualize the studied phenomena, highlight aspects and elements that are important to consider in relation to safety and security (or risk) management, and show that many different factors can lead to challenges for safety and security management at every level of the sociotechnical system. The thesis illustrates why it is important to consider human, technological, *and* organizational factors, as well as the dynamic interaction between these factors. It is especially important to consider cultural-cognitive factors and be aware of how these elements affect safety and security management. Institutional organizational theory contributes to illustrate that there is no clear distinction between organizations and their environments and that many socially constructed and institutionalized aspects can influence organizations and create important challenges. Regulative (regulations), normative (technical standards), and cultural-cognitive

(sensemaking, risk perception, commitment, and awareness) processes are connected in complex and changing mixtures, and these processes shape organizational structures and activities. The use of institutional organizational theory also sheds light on the important fact that many issues related to safety and security seem to be taken for granted.

Contents

Part I

1. Introduction

Today, information and communication technology (ICT) is increasingly becoming a part of all critical infrastructures (Line and Tøndel, 2012) and ICT is used for various power system applications, such as monitoring and control, protection coordination, and other vital functions. While these system applications have the potential for further improving system operation, flexibility, security margins, and overall cost, they are also subject to threats, both malicious and accidental, which are not fully understood and thus introduce additional vulnerabilities. The application of ICT systems contributes to increase power system vulnerabilities in a worldwide scenario where malicious threats against large and complex infrastructures are increasing (The GRID Consortium, 2007).

The current research is conducted in light of these risks and vulnerabilities, and the thesis focuses attention on challenges for safety and security[1] management of network (distribution/grid) companies due to increased use of ICT in the electric power supply sector, i.e., the authorities' regulation of risk (managers' and employees' attitudes toward these regulations), the use (or non-use) of technical standards for ICT safety and security, risk perception among users (both managers and employees) of ICT systems regarding threats to and vulnerabilities in these systems, and management commitment, awareness creation, and training measures for ICT safety and security within these companies.

The electric power supply is often said to be the most critical infrastructure in modern society, providing the basic infrastructure for all kinds of service production that depends on computers and electronic communication services (Hagen and Albrechtsen, 2009a). Today, critical infrastructures are increasingly connected and interconnected, and failures of critical infrastructures can represent a threat to people, the economy, and societal functions, as well as to national security (Hokstad, Utne, and Vatn, 2012). Since the early 1990s, the energy sectors of Western societies have also been through a process of institutional restructuring, where large state-owned monopolies have been divided into several independent organizations (Antonsen et al., 2010). Emergent control technologies, making intensive use of ICT, have been useful for dealing with the new situation of enlargement, open access, progressive integration of electricity markets, and intensification of cross-border trade. However, the full application of these technologies has demanded a new approach to system design and operation, and their integration within existing control infrastructures and practices has been a challenge (The GRID Consortium, 2007).

In today's power systems, ICT is involved at every level and in virtually all functions. Consequently, malfunctions of ICT or malicious attacks on the ICT systems that monitor, control, and operate power generation plants and power distribution within the electric power supply system can have serious impacts on the physical grid and result not only in a major financial disaster but also in devastating damage to public safety and health (Patel and Sanyal, 2008).

The context for the empirical studies in the thesis is the Norwegian electric power supply sector. The Norwegian power system is almost entirely based on hydropower generation (98%-99%); it also uses combined cycle gas turbine production and wind power. During the last three decades, the

[1] The area of risk research has traditionally distinguished between the terms "safety" and "security" – this, in addition to other important concepts (i.e., risk, uncertainty, vulnerability, complexity, and safety and security management) will be further elaborated in Chapter 4.

Norwegian electric power supply system has become more complex due to large-scale implementation of new technology (i.e., electronic components and ICT systems). Furthermore, the advanced metering infrastructure (AMI), and later the smart grid, are being introduced in the Norwegian electric power system, as in other Western countries. This is expected to further increase the vulnerability of ICT systems used in electric power supply systems. According to the "Cyber Security Strategy for Norway" (Regjeringen, 2012a), threats related to ICT-based espionage and sabotage have increased in recent years, and we now must expect sophisticated attacks aimed at critical societal information, including ICT systems that operate industrial processes and critical infrastructure (Regjeringen, 2012b).

1.1 Structure of the thesis

The thesis consists of two parts. Part I is structured in the following way: Section 1.2 outlines the research aim, how the challenges that constitute the focus areas in this thesis were selected, and the research questions that form the basis for the four studies (articles) that are part of the thesis. Chapter 2 describes the background and context of the thesis, and Chapter 3 provides an overview of related research. Chapter 4 discusses concepts that are essential for theoretical discussions of challenges for safety and security management. Chapter 5 outlines the theoretical framework chosen for this study, and Chapter 6 describes the research design and data collection methods applied in the thesis. Chapter 7 summarizes the research results from each of the four articles included in the thesis, and Chapter 8 presents a discussion of the research results related to the main research aim presented in the introduction. Chapter 9 discusses the contributions of the thesis, provides recommendations for measures that can be used to reduce the challenges for safety and security management of network companies and improve the safety and security of their ICT systems, and offers suggestions for future research.

Part II presents the four research articles included in the thesis:

Article 1: Skotnes, R. Ø. and Engen, O. A. (2015), Attitudes toward risk regulation – Prescriptive or functional regulation?, *Safety Science,* Vol. 77, pp. 10–18.

Article 2: Skotnes, R. Ø. (2012), Strengths and weaknesses of technical standards for management of ICT safety and security in electric power supply network companies, *Journal of Risk and Governance*, Vol. 3, Iss 2, pp. 119-134.

Article 3: Skotnes, R. Ø. (2015), Risk perception regarding the safety and security of ICT systems in electric power supply network companies, *Safety Science Monitor,* Vol. 19, Iss 1, article 4.

Article 4: Skotnes, R. Ø., (2015), Management commitment and awareness creation – ICT safety and security in electric power supply network companies, *Information & Computer Security*, Vol. 23, Iss 3, pp. 302 – 316.

1.2 Research aim, selection of focus areas, and research questions

This section outlines the research aim for the thesis, how the challenges that constitute the focus areas in the thesis were selected, and the research questions that form the basis for the articles included in the thesis.

1.2.1 Research aim

The aim of this thesis is to follow up on previous research on challenges for safety and security management and to explore, describe, and discuss challenges for safety and security management of network (distribution/grid) companies within the electric power sector that arise due to the increased use of ICT to monitor, control, and operate electric power production and distribution. I have chosen to focus on companies involved in transmission and distribution of electricity, and not generation (production). The generation system in the Norwegian electric power supply consists of many power stations distributed across the country. The structure is thus relatively robust, and the dependence on individual plants is small (Fridheim, Hagen, and Henriksen, 2001). However, a failure in the electricity networks and the transmission and distribution of electricity to critical infrastructures and important societal functions, as well as to individual households, would have a huge impact on societal safety (and security).

Thus, the main aim of the thesis is to answer the following question:

- What challenges for safety and security management of network companies within the electric power sector have arisen in light of the increased use of ICT to monitor, control, and operate electric power production and distribution?

Specific research questions have been derived from the main aim, and these research questions are addressed in the articles included in the thesis.

This thesis focuses on organizational safety and security (risk) management within electric power supply network companies. However, network companies operate critical national infrastructure, and the safety and security management of these companies can thus affect societal safety and security. Safety and security management of network companies is also affected by national regulations, and there is no longer a clear distinction between national regulations and safety and security management of network companies. Ideas about internal control and risk management have been increasingly commingled, and risk management and regulation are no longer seen as broadly contrasting methods of assuring safety and security (Power, 2007).

1.2.2 Selection of challenges and research questions

To select which types of challenges to focus on in this thesis, a combination of several approaches was used. First, I performed a review of previous literature on related problem issues and relevant documents (e.g., regulations, guidelines, reports, newspaper articles). In addition, I conducted two exploratory interviews with representatives from the contingency planning department of the Norwegian Water Resources and Energy Directorate (NVE) and observation studies at two conferences on ICT safety and security for the electric power supply sector to determine what representatives from both the authorities and the industry considered to be challenges related to the research aim of this thesis. I chose to discuss elements of safety and security (or risk) management systems that previous research has identified as important for ensuring ICT safety and security (Rasmussen, 1997; Hagen, Albrechtsen, and Hovden, 2008; Lindøe, Baram, and Renn, 2014; Aven et al., 2004). Last, factor analysis of survey data results also guided selection of the specific challenges discussed in this thesis. All these approaches will be thoroughly described in the following chapters.

1.2.3 Research questions

This research project includes four empirical studies (presented in four articles) with their own research questions, which all discuss important elements of safety and security management systems and important challenges for safety and security management of network companies due to the increased use of ICT.

Article 1:

Attitudes toward risk regulation – prescriptive or functional regulation?

The aim of the first article was to address attitudes toward the use of functional versus prescriptive risk regulations. The context for the study was the use of functional internal control regulations for ICT safety and security in network companies within the Norwegian electric power supply sector.

Previous research has shown that ambiguity of results of internal control regulations may be explained by organizational size, where large companies have been seen as better suited to implement internal control than smaller companies (Hovden, 1998; Lindøe, 2001). However, the results of my survey revealed no statistically significant differences between large and small network companies regarding their attitude toward the internal control regulations for ICT safety and security in the Norwegian electric power supply sector. Managers and employees in both large and small network companies had diverging views on and varying attitudes toward internal control regulations, depending on the specific question asked.

Hence, the following research question was discussed in the article:

- What can explain varying attitudes toward the use of functional internal control regulations as the principle for regulating risks?

Article 2:

Strengths and weaknesses of technical standards for management of ICT safety and security in electric power supply network companies

The aim of the second article was to study the use of technical standards for management of ICT safety and security in electric power supply network companies and to discuss the following research question:

- What are strengths and weaknesses of technical standards for management of ICT safety and security?

Article 3:
Risk perception regarding the safety and security of ICT systems in electric power supply network companies

The aim of the third article was to provide insight into risk perception among users of ICT systems within electric power supply network companies and to discuss factors that can influence users' risk perception. Perceived risk (i.e., subjective risk judgments) can be influenced by several factors and may deviate from "objective" risk. According to Rundmo (1996), biased perception of risk can cause misjudgments of potentially hazardous risk sources, and in a report from the project "Emerging systemic risks in the 21st century," the Organization for Economic Cooperation and Development (OECD) pointed to risk perception itself as one factor that can delay or exaggerate precautionary measures (OECD, 2003).

The following research question was examined in this article:

- What factors can influence the risk perception of users (managers and employees) within electric power supply network companies regarding the risk of malfunctions in or attacks on their ICT systems?

Article 4:
Management commitment and awareness creation – ICT safety and security in electric power supply network companies

The aim of the fourth article was to follow up on previous research by studying the degree of management commitment to ICT safety and security within network companies in the electric power supply sector, implementation of awareness creation and training measures for ICT safety and security within these companies, and the relationship between these two variables.

Previous research has advocated for more training, awareness creation, and management commitment regarding ICT safety and security (Johnson, 2006; Hagen, Albrechtsen, and Hovden, 2008; Hagen, 2009; Hagen and Albrechtsen, 2009a). These studies have suggested that management involvement is important for the safety work within companies. If the management is engaged, it will be aware of the need for information security measures to comply with the law and assure that safety and security measures are implemented. The success of safety and security management systems often depends on the commitment of all staff, and all members must be aware of their responsibility for safety and security. Otherwise, the safety and security mechanisms may be bypassed or diminished by employees.

This article followed up on previous research that has shown a positive relationship between management commitment to ICT safety and security and implementation of awareness creation and training measures. The article addressed the following research questions:

- To what degree is the management of network companies in the electric power supply sector committed to the safety and security of their organizations' ICT systems?
- To what extent are awareness creation and training measures for ICT safety and security implemented within network companies in the electric power supply sector, and what type of measures are implemented?

2. Background and context

This chapter provides a description of the background and empirical basis for the problems of interest and the research context for the thesis.

2.1 ICT systems and information security

A central part of ICT is the information processed by the system. An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications (Swanson et al., 2010).

The work to protect ICT systems is usually called information security. The most common definition of information security involves the properties of confidentiality, integrity, and availability:

- *Confidentiality* means that the information is not made available or disclosed to unauthorized individuals, entities, or processes.
- *Integrity* means safeguarding the accuracy and completeness of assets so that no unauthorized modification can be made to the information or the system that handles the information.
- *Availability* means that information is accessible and usable on demand by an authorized entity (Line and Tøndel, 2012).

However, information security is not strictly a technical issue. Hagen (2009) defined information security as essentially a management responsibility that includes using all available resources – human, technological, and organizational – to ensure availability of information and that there is only authorized access to and modification of companies' information assets.

2.2 Critical infrastructures

As previously mentioned, the electric power supply is often said to be the most critical infrastructure in modern society; it provides the basic infrastructure for all kinds of service production that depends on computers and electronic communication services (Hagen and Albrechtsen, 2009a). Modern societies rely on the effective functioning of critical infrastructure networks to provide public services, enhance quality of life, sustain private profits, and spur economic growth. However, this growing dependence is accompanied by an increased sense of vulnerability to new and future threats, such as terrorism, climate change, and cyber attacks. According to Boin and McConnel (2007), the degree and criticality of critical infrastructures is bound to differ across systems and cultures, but it is widely thought that a breakdown of one or more of these critical systems has the potential to cause very serious problems. Furthermore, an infrastructural breakdown may present challenges that are well beyond the routine contingency planning[2] and management capacities of public authorities.

[2] Planning in advance for extraordinary scenarios allows organizational responders (at both operational and political levels) to shift gears, applying the procedures and rules of "crisis management" rather than those of "business as usual." Anticipation of what may happen, coupled with the prior allocation of resources, personnel, equipment, crisis control rooms, tasks, responsibilities, and decision guidance/rules, is assumed to maximize the chances of a successful response in the event of a crisis. Broadly, such preparations are often

Background and context

Definitions of the term critical infrastructure vary widely, ranging from hardware such as cables and wires to networks for the generation and supply of energy sources (Boin and McConnel, 2007). Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and its economy. Since the word infrastructure refers to physical assets, other terms are often introduced focusing on what to achieve, such as societal critical functions. Societal critical functions can be defined as functions that are essential to ensure the basic needs of a society. The basic needs point to what is considered essential in a society, such as food, water, heating and cooling, and safety and security (Vatn, Hokstad, and Utne, 2012).

Various societal critical functions are required to ensure that the basic needs of society are fulfilled. The Norwegian Directorate for Civil Protection (DSB) has proposed to limit critical functions to those functions where (1) a loss of the function for seven days or more will threaten basic needs and (2) such a loss occurs under disadvantageous conditions and/or in combination with other events. Based on this argument, the societal critical functions are water supply, food supply, heat supply, life and health, financial security, national security, crisis management, and law and order. The societal critical functions depend on infrastructure components. To some extent, infrastructure components may be replaced by substitutes; hence, their criticality depends on the organization of infrastructure components in the society. The following basic infrastructure components are often considered: electric power grids, ICT networks, water and sewage networks, telecommunication networks, and networks of roads, railways, and harbors. Finally, several input factors are required to provide the infrastructure elements and/or the societal critical functions, including labor, energy, ICT services, other services, transportation, telecommunication, and goods and products (Vatn, Hokstad, and Utne, 2012).

The interdependencies between infrastructures can be strong, and several types of dependencies should be taken into account. Three types of interdependencies and possible failures are:
(1) Cascading failures, where a failure in one infrastructure causes disturbances in another infrastructure; in this situation there is a functional relationship between two or more infrastructures (e.g., water supply is dependent on electricity for water treatment), (2) Escalating failures, where failure in one infrastructure worsens an independent disturbance in another infrastructure; for example, a breakdown in the metro is significantly worse if a main road is unavailable due to a fire in a tunnel, and (3) Common cause failures, where two or more infrastructures are disrupted at the same time due to a common cause; for example, a fire in a culvert may cause interruption of electricity, water, and telecommunication at the same time (Vatn, Hokstad, and Utne, 2012).

When categorizing dependency and interdependency between critical infrastructures, the term functional interdependency is used in situations where there are cascading failures, the term impact interdependency is used in situations where there are escalating failures, and the term geographical dependency is used in situations where there are common cause failures. The term geographical dependency is used to explain such failures because one or several elements of the infrastructures are in close proximity so that external threats may knock out several infrastructures at the same time (Vatn, Hokstad, and Utne, 2012).

referred to as contingency planning (or emergency response planning) and are widely considered to be an essential role of public authorities (Eriksson and McConnell, 2011).

Rinaldi, Perenboom, and Kelly (2001) presented another framework of six dimensions to describe and analyze interdependencies: (1) type of interdependencies, (2) surroundings, (3) coupling and response behavior, (4) infrastructure characteristics, (5) type of failures, and (6) state of operation. In addition, they defined four categories of interdependencies: (1) Physical interdependency, that is, physical coupling between inputs and outputs. An example is that a commodity produced/modified by an infrastructure is required by another infrastructure to function. (2) Cyber interdependency, that is, the state of the infrastructure depends on the information transmitted through the information infrastructure, (3) Geographical interdependency, where one or several elements of infrastructures are in close proximity so that one event (e.g., fire) creates disturbances to the infrastructures, and (4) Logical interdependency, where two or more infrastructures have reciprocal effects without any physical, geographical, or cyber interdependency.

According to Olsen, Kruke, and Hovden (2007), an infrastructure is critical if its failure would lead to unacceptable human or economic consequences and affect societies' capabilities of rescue, response, and recovery. Critical infrastructures are systems upon which we build new systems (e.g., of production). Understanding the interconnections between critical infrastructures is a demanding task, and this is even more the case when one includes organizational contexts. Many organizational challenges have to be addressed when analyzing and managing risks that involve several infrastructure sectors. A few decades ago, most critical infrastructures in the OECD countries were publicly owned and run by integrated utility companies. However, this started to change in the late 1980s with the dawn of a new era of public governance called new public management (NPM). Since then, NPM has influenced most public sectors, though to varying degrees in different countries (Almklov, Antonsen, and Fenstad, 2012).

Broadly put, NPM is the introduction of a set of principles and methods for organizing from the private sector into the public sector. Functional splitting, outsourcing of work processes, and full-blown privatization are the most typical organizational changes. New organizational forms confront existing forms as society faces new challenges. The NPM-based reforms of the 1980s and 1990s encouraging decentralization and structural devolution have increasingly been supplemented by arrangements that emphasize the need for more coordination across sectors and levels, labeled post-NPM, Whole of Government, or Joined Up Government (Lango, Lægreid, and Rykkja, 2011). Nevertheless, decentralization still influences many critical infrastructures, and the infrastructures of today are often run by networks of private and public entities rather than single utility companies. Consequently, the number of organizations that need to be involved to map, analyze, and manage risks that cross sectors is increasing. The organizational changes also imply that work is managed and coordinated in ways that imply a stricter focus on efficiency and accountability with regard to core tasks and responsibilities. Technologies have become increasingly interconnected at the same time that the organizations managing them have become increasingly fragmented (Almklov, Antonsen, and Fenstad, 2012).

2.3 Electric power supply systems

According to De Bruijne (2006), the generation, transmission, and distribution of electricity in many ways constitute the veins and arteries of Western societies. These societies also become increasingly dependent on electricity as different infrastructures become increasingly interdependent (referred to in Antonsen et al., 2010). According to Fridheim, Hagen, and Henriksen (2001), the electric power system is a good example of mutual dependency in complex technological systems. In case of a power outage, most services stop, and a prolonged interruption of power supply (blackout) may have consequences for many critical functions in society. This can result in a major financial disaster and in damage to public safety and health (Patel and Sanyal, 2008).

Electricity is produced, or generated, by the turning of turbines. Once the turbines generate the electricity, its voltage is significantly increased by passing it through step-up transformers. Then the electricity is routed to a network of high-voltage transmission lines capable of efficiently transporting electricity over long distances. At the electric distribution substations that serve private homes, the electricity is removed from the transmission system and passed through step-down transformers that lower the voltage. The electricity is then transferred to local electric networks of distribution lines and delivered to homes. There, the electricity's voltage is lowered again by a distribution transformer and passed through the electric meter into people's home network of electric wires and outlets (KAEC, 2014). The function of the power grid is to transport electricity from producers to consumers in the volume and at the time requested by consumers. Electricity must be generated the same second it is consumed. Consequently, a vital feature of the power system is establishing a balance between total generation and total consumption of power at all times, a so-called instantaneous balance (FACTS, 2013).

From around 1990 onward, the electricity industries in Western countries have been subjected to a massive institutional restructuring. Traditionally, the generation, transmission, and distribution of electricity were assembled in vertically integrated utilities, often state owned. However, since the late 1980s and early 1990s, all countries in Western Europe have, to various degrees, taken steps toward liberalizing their electricity industries. In this context, the term liberalization refers to attempts to introduce competition into some or all segments of the industry and to remove barriers to trade and exchange. The large, state-owned organizations have been divided into several smaller units, which are increasingly exposed to competition. The transition from being an infrastructure monopoly to becoming a form of "infrastructure market" represents a significant institutional restructuring of the industry (Antonsen et al., 2010).

Through this liberalization, the organizations responsible for the production and transmission of electrical energy have, to a large extent, gone from being bodies regulated by governments to being organized more like private companies subject to more indirect regulation. This process is commonly referred to as deregulation, but according to Antonsen et al. (2010), it would more accurately be described as "re-regulation" because the introduction of market forces often results in additional regulation. The development of privatization, liberalization, and deregulation is part of the aforementioned general trend of public sector restructuring that is heavily influenced by the ideal of NPM. A myriad of organizational variants exists, but the drift toward management by market mechanisms and commoditization of services is a common denominator. The objective of such restructuring is to improve cost-efficiency by introducing competition, and this is a radical shift from the traditional mode of organizing critical infrastructures. Competition has led to a focus on cost reductions and a more efficient use of assets. However, low investment levels, loss-of-supply incidents, and society's increasing dependence on electricity have shifted the focus toward the quality and security of the supply in many Western countries.

Today, ICT is used to monitor, control, and operate power generation plants and power distribution within electric power supply systems (Patel and Sanyal, 2008). Intricate interdependencies are probable outcomes of the computerization and automation of infrastructures of the last decades. In the digital age, society's critical infrastructures rely on the functioning of ICT systems, as ICT software and hardware are integrated in the ability of other sectors to uphold their services. Computers and software depend on electricity, but the very same computers and software are strongly integrated in the production of electricity. The existence of such "feedback loops" means that the potential for cascading effects will be increasing at the same time that the intersections between infrastructures are becoming more and more opaque. This combination may lead to surprising interactional effects, and it is thus a vulnerability of increasing importance (Almklov, Antonsen, and Fenstad, 2012).

Emergent control technologies, making intensive use of ICT, have been useful for dealing with the new situation of enlargement, open access, progressive integration of electricity markets, and intensification of cross-border trade. However, the full application of these technologies has demanded a new approach to system design and operation, and their integration within existing control infrastructures and practices has been a challenge (The GRID Consortium, 2007).

2.4 Process (industrial) control systems

ICT infrastructure is used for controlling critical processes in other infrastructures, for example, through process (industrial) control systems (Line and Tøndel, 2012). Process control systems is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems and other control system configurations often found in the industrial sectors and critical infrastructures. Process control systems are typically used in industries such as electric power supply, water and wastewater, oil and natural gas, chemical, transportation, and food and beverage. These control systems are critical to the operation of highly connected and mutually dependent critical infrastructures (Stouffer, Falco, and Scarfone, 2011).

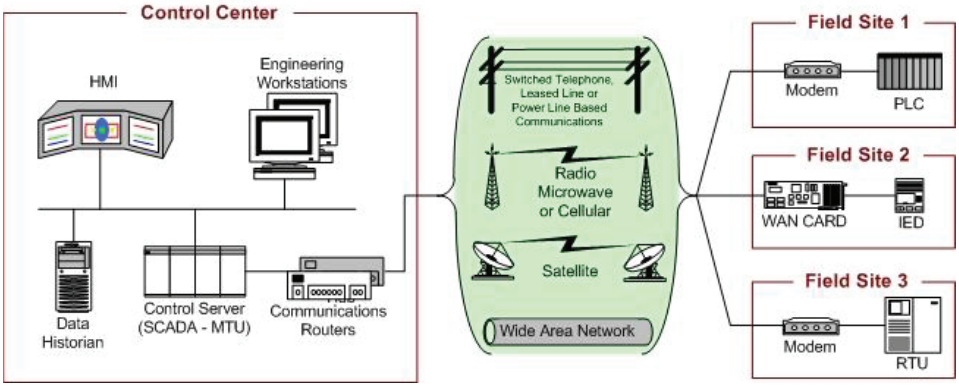
Figure 1 shows the general layout of a SCADA system. SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as electrical power grids, water distribution and wastewater collection systems, oil and natural gas pipelines, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions (Stouffer, Falco, and Scarfone, 2011).

SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control. SCADA systems integrate data acquisition systems with data transmission systems and human-machine interface (HMI) software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automated or performed by operator commands. SCADA systems consist of both hardware and software. Typical hardware includes a master terminal unit (MTU) placed at a control center, communications equipment (e.g., radio, telephone line, cable, satellite), and one or more geographically distributed field sites consisting of either a remote terminal unit (RTU) or a programmable logic controller (PLC), which controls actuators and/or monitors sensors (Stouffer, Falco, and Scarfone, 2011).

Initially, process control systems had little resemblance to traditional information technology (IT) systems in that process control systems were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As process control systems are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities and being designed and implemented using industry standard computers, operating systems, and network protocols, they are starting to resemble IT systems. While this integration supports new IT capabilities, it also provides significantly less isolation for process control centers from the outside world than predecessor systems, creating a greater need to secure these systems. Security solutions have been designed to deal with these security issues in typical IT systems, but special precautions must be taken when introducing these same solutions to process control systems environments. In some cases, new security solutions are needed that are tailored to the process control system environment (Stouffer, Falco, and Scarfone, 2011).

Although some characteristics are similar, process control systems also have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that the logic executing in process control systems has a direct effect on the physical world. Process control systems have unique performance and reliability requirements and often use operating systems and applications that typical IT personnel may consider unconventional. The goals of efficiency sometimes conflict with safety and security in the design and operation of control systems (Stouffer, Falco, and Scarfone, 2011).

Figure 1. SCADA System General Layout, NIST (Stouffer, Falco, and Scarfone, 2011).



2.5 Threats to electric power supply companies' ICT systems

The evolution of ICT systems and their use within critical infrastructures has radically changed the threats to such infrastructures, and the increased dependence on ICT in critical infrastructures has resulted in the need to properly address the interdependencies that exist between these infrastructures and the ICT systems (Line and Tøndel, 2012). As previously mentioned, the logic executing in process control systems has a direct effect on the physical world, including significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impacts to a nation's economy, and the compromise of proprietary information (Stouffer, Falco, and Scarfone, 2011). Downtime is increasingly critical, and our society has become more vulnerable to even short interruptions to systems and networks, increasing the importance of having a secure and robust ICT infrastructure (Regjeringen, 2012a).

Whereas the traditional ICT systems used in infrastructures were proprietary and not connected to the outside world, the recent trends toward more general purpose software solutions and increased networking have radically changed the benefits and risks involved (OECD, 2006; Line and Tøndel, 2012). Utilizing the Internet for communication related to operation and management of remote processes and production systems increases efficiency and cooperation and saves time and money in localization and correction of faults and errors. Using commercial off-the-shelf (COTS) components (e.g., MS Windows) in control systems further reduces costs. However, the increased use of publicly available ICT systems instead of proprietary solutions, and the increased connectivity between different types of networks, makes formerly isolated ICT systems vulnerable to a set of threats and risks they have not been exposed to before.

According to Line and Tøndel (2012), the introduction of ICT results in an increased need to consider incidents caused by attackers and not only failures that occur by accident. The offline proprietary systems traditionally had an attack surface close to zero, as an attacker would have to be geographically in the same place as the target system and have detailed technical knowledge of the system to be able to do harm. However, today, when connecting these proprietary systems to the outside world through ICT networks, this is no longer the case as the systems can be accessed from any location. In addition, the increased use of COTS systems results in production systems being easier targets. Although detailed technical knowledge is still required, there are far more experts of COTS systems worldwide than there are experts of proprietary systems.

A threat is a potential incident; thus, it has not yet occurred (Hagen, 2009). According to Line and Tøndel (2012), threats to ICT systems can be divided into three main categories: (1) *unintentional incidents* that are possible due to weaknesses in the ICT system, unfortunate employees, or external incidents, (2) *general attacks* that are not directly aimed at a particular ICT system, but rather attack ICT systems in general, and (3) *targeted attacks* that are directed toward a particular enterprise or system. Unintentional incidents occur by sheer accident. Examples include lightning, power failures, fire, disk crashes, communication failures, erroneous backups, and mistakes made by employees (Line and Tøndel, 2012). Employees can unintentionally misuse software, web mail, or e-mail and import infected information, or they can disclose confidential or sensitive information unintentionally (Hagen, 2009). Any lack of competence regarding how the systems should be used, and also the reliance on key personnel, can be a potential vulnerability (Line and Tøndel, 2012). Likewise, fire or flooding can destroy electronic equipment (Hagen, 2009).

General attacks are not aimed at a particular ICT system, but rather target a number of different ICT systems. Examples include the high volume of malicious software found on the Internet. Such software may, for instance, aim to gain access to computer resources or get hold of personal information like usernames/passwords and credit card numbers (so-called phishing). Although they do not directly target a system, they can still do a lot of harm, and the risk from general attacks increases as COTS components are incorporated into the systems and as connectivity increases. Typical high-risk activities include employees surfing on the Internet from systems with critical functionality (e.g., production systems), remote access to control systems, and connecting portable units (e.g., laptops, USB sticks) to critical systems (Line and Tøndel, 2012).

Targeted attacks are launched with the intent to harm one particular system or organization. They can range from physical attacks (e.g., in the form of burglary or vandalism of personal computers (PCs) and other ICT equipment that is not physically secured) to attacks performed via the Internet. The perpetrators may be located far away, but it is also possible for insiders to attack via the ICT systems. Disgruntled employees can intentionally misuse ICT resources and disclose information, and the consequences of insider attacks can be worse than the consequences of external attacks (Johnson, 2006; Hagen, 2009). Internal vandalism, theft, or misuse of the organization’s ICT resources by its own employees can be difficult to detect. This is partly because many businesses have bad or poor operating and administrative procedures or management is not entirely aware of what system privileges employees actually have. Internal attacks against a computer network can also be more difficult to detect than external attacks (Regjeringen, 2012a). Furthermore, physical attacks can be combined with online attacks. Some attacks will only be possible if the attackers have detailed knowledge of the ICT systems and thus require skilled and dedicated attackers. Such attacks may be unlikely but can still have a huge impact (Line and Tøndel, 2012).

There are many security measures on the path from the Internet to any process control system, and it is unlikely that any outside player would be able to breach these defenses and gain access to the critical ICT systems in the electric power supply. However, since logical connections exist between the different ICT systems, skilled hackers may be able to penetrate defenses. When an attacker has exploited vulnerabilities, the threat becomes an incident or a security breach. Potential attackers can exploit weaknesses of employees, the organization, the network architecture, and physical security. External attackers can use the inherent weaknesses in human nature and trick employees into performing actions that lead to security breaches (social engineering) or attempt extortion. External attackers can also prey on weaknesses in network architecture and use software to perform automated attacks (Hagen, 2009). An external attacker can break into a process control (SCADA) system as well and take control of production and distribution processes through, for example, a back door installed earlier by malware (Line and Tøndel, 2012).

Attacks can be both economically and politically (e.g., espionage, sabotage) motivated or just be performed as jokes, and attacks can use malicious software (malware) such as viruses, worms, and Trojan horses. Attacks can be distributed attacks (e.g., viruses) or targeted attacks (e.g., hacking). The Internet enables criminals to commit crimes from locations far away and escape in a nanosecond. Denial-of-service (DoS) attacks are typical examples of external automated attacks that rely on connections in the Internet architecture (Hagen, 2009). Threats to process control systems can come from numerous sources, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, and malicious intruders, and from natural sources like system complexities, human errors and accidents, equipment failures, and natural disasters (Stouffer, Falco, and Scarfone, 2011).

In addition, reductions in staff and expertise within the power companies as a result of the restructuring and deregulation of the sector have led to increasing dependence on external competence. All enterprises that outsource their ICT operations must trust a third party and its employees and systems. Important security risks include weak preparation before signing the contract and weaknesses in follow-up management and the audit process. Work by external suppliers may often be carried out online, and this increases the need to tie all the different participants of the electric power supply together in a massive ICT network. The Internet has become an increasingly important part of this network (Hagen, Fridheim, and Nystuen, 2005).

2.5.1 Examples of cyber attacks and blackouts

Worldwide, there have been several incidents of cyber attacks during the last few years. The U.S. government identified the Titan Rain attacks on companies, national laboratories, and military targets well before 2003. Attackers from the Netherlands also successfully compromised some 34 U.S. defense sites in 1990 (Johnson, 2014). In 2009, President Barack Obama declared America's digital infrastructure to be a "strategic national asset," and in May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM) to defend American military networks and attack other countries' systems. The European Union (EU) has established the European Network and Information Security Agency (ENISA), and there are further plans to significantly expand ENISA's capabilities. The United Kingdom has also set up a cyber security and "operations center" based in the Government Communications Headquarters (GCHQ), the British equivalent of the National Security Agency (NSA) (Open Security Alliance, 2014). Furthermore, North Atlantic Treaty Organization (NATO) members developed the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in 2008 (Johnson, 2014).

Background and context

In February 2010, top American lawmakers warned that the "threat of a crippling attack on telecommunications and computer networks was sharply on the rise"; according to the Lipman Report, numerous key sectors of the U.S. economy along with those of other nations are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education, and government, all of which now depend on computers for daily operations. The federal government of the United States also admits that the electric power transmission is susceptible to cyber warfare, and in 2009 President Obama stated that "cyber intruders have probed our electrical grids." In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials, even though China denies this (Open Security Alliance, 2014).

The last decade has seen a growing number of cyber attacks, for instance, on Estonia (2007), Belarus (2008), Lithuania (2008), Georgia (2008), and India (2009) (Johnson, 2014). In July 2009, a series of coordinated DoS attacks was launched against major government, news media, and financial websites in South Korea and the United States. In 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation. In addition, a group calling itself the Indian Cyber Army hacked websites belonging to the Pakistan Army and others belonging to different ministries. In 2011, the South Korean company SK Communications was hacked, resulting in the theft of the personal details (including names, phone numbers, home and e-mail addresses, and resident registration numbers) of up to 35 million people. Recent reports with respect to cyber security suggest that cyber attacks against U.S. governmental institutions are imminent. As predicted, a massive cyber attack in the form of a DoS attack hit the EU and U.S. computer systems on February 11, 2014, in protest of the recent spying by the NSA (TBSMUN, 2014).

Several attacks on ICT systems have had major consequences for critical infrastructures. In July 2010, a new and advanced piece of malware, Stuxnet, was detected. This was the first occurrence of malware specifically targeted at process (industrial) control systems. Its goal was to reprogram systems of a specific type and hide any changes. It exploited vulnerabilities in a Windows-based software program used in industrial settings. Most Stuxnet infections were detected in Iran, where five organizations were specifically targeted. However, since Stuxnet was able to self-replicate, it also infected computers outside the target organizations and all over the world. Thus, Stuxnet is an example of a targeted attack that also resulted in a general attack. Stuxnet also demonstrated that it is possible to attack critical infrastructure, even infrastructure that is not connected to the Internet (Line and Tøndel, 2012).

In November 2009, an attack targeting the energy sector (oil, power, and petrochemical companies) was identified. This attack seemed to originate from China and was given the name Night Dragon. The goal appeared to be to collect information related to competitive proprietary operations and financial details regarding field bids and operations. In January 2008, several cities experienced power outages caused by hackers breaking into computer systems related to the power supply. Little information about this incident has been disclosed, but the motive is said to be extortion. The Slammer worm occurred in 2003 as a piece of malware exploiting a vulnerability in the Windows

Internet information server. Slammer infected a computer network at a nuclear power plant in Ohio, disabling a safety monitoring system for nearly five hours (Line and Tøndel, 2012).

The OECD report "Reducing Systemic Cybersecurity Risk" (2011)[3] concluded that very few single cyber-related events have the capacity to cause a global shock. However, the authors argued that governments nevertheless need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events, both accidental and deliberate. There are significant and growing risks of localized misery and loss as a result of the compromise of computer and telecommunications services. In addition, reliable Internet and other computer facilities are essential in recovering from most large-scale disasters (OECD, 2011b).

Natural incidents or technical failures are also realistic sources of power blackouts, and we have many examples of this from the last decade (Hagen, Fridheim, and Nystuen, 2005). Several countries have experienced major electrical blackouts, and these have highlighted the society's vulnerability and contributed to rising questions about the regulation and organization of the electricity sector. California experienced a major crisis in 1999, and the rolling blackouts, skyrocketing electricity prices, and lasting under-supply of electrical power exposed how vulnerable the society had become. The U.S. and Canada experienced blackouts in 2003 that affected 50 million people. The United Kingdom (U.K.) also experienced large loss-of-supply incidents in 2003 in London and Birmingham. In both cases, the supply was restored to all customers within an hour, but the incidents caused significant disruptions of activities, particularly for transport systems. In 2005, Sweden experienced severe damage to electricity lines in southern Sweden, caused by Hurricane Gudrun. These reports on major blackout events all underline the integrated nature of the power supply in the causal chain (e.g., in the case of cascading events) leading up to the events or in the restoration of supply (Antonsen et al., 2010).

2.5.2 Advanced Metering Infrastructure and Smart Grids

ICT systems within electric power supply systems in the Western world are also becoming increasingly vulnerable due to the introduction of AMI and the smart grid. AMI is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers. Customer systems include in-home displays, home area networks, energy management systems, and other customer-side-of-the-meter equipment that enable smart grid functions in homes, offices, and factories. Time-based rate programs include different types of electricity pricing options for customers that are made possible by AMI and sometimes include customer systems (Smart Grid, 2014).

Smart grid is a term coined for a wide range of solutions for the electricity grids of the future (Fosso et al., 2014). According to Baumeister (2010), the current electrical power grid is an out-of-date infrastructure. It has met our needs in the past; however, as our society advances technologically, so do our expectations of our electrical power delivery system. The smart grid reflects a movement to bring the electrical power grid up-to-date so it can meet the current and future requirements of its customers. However, updating the electrical power grids could introduce new security vulnerabilities into the systems.

[3] The report is part of the broader OECD study, "Future Global Shocks" (OECD, 2011a).

Smart grids introduce ICT components into the power distribution grid (e.g., sensors for monitoring and control, smart meters, two-way communication). Smart grids connect power plants and system control centers with all households, businesses, and buildings all over the country, as well as abroad. The power industry is thus moving toward a situation where the power distribution depends on ICT, while the ICT infrastructure itself depends on power. Such an evolution within critical infrastructures makes ICT an integrated part of all other industries, and it is thus not possible to make a clear distinction between the ICT systems and the industries that utilize these systems (Line and Tøndel, 2012).

According to Line and Tøndel (2012), there is an increasing need to include ICT in all the electric power supply companies' risk assessments. In the smart grid vision, ICT systems are a part of the power distribution, monitoring and influencing the whole service delivery. As a result, it becomes obsolete to make a clear separation between, for example, ICT and power, ICT and oil/gas, and ICT and water distribution. All infrastructures are based on ICT, and specific ICT competence is therefore necessary in operations and management, in addition to competence related to the core business of the specific infrastructure. The electric smart grid promises increased capacity, reliability, and efficiency through the marriage of cyber technology and the existing electricity network. On the other hand, the scale and complexity of the smart grid, along with its increased connectivity and automation, make the task of cyber protection particularly challenging (Kundur et al., 2010).

2.6 Societal safety and security

As mentioned in section 2.2, an infrastructure is considered critical if its failure would lead to unacceptable human or economic consequences and affect societies' capabilities of rescue, response, and recovery. This links the notion of critical infrastructures closely to the concept of societal safety and security. As previously stated, this thesis focuses on organizational safety and security (risk) management within electric power supply network companies. However, network companies run critical national infrastructure, and the safety and security management of these companies can thus affect societal safety and security. Safety and security management of network companies is also affected by national regulations, and there is no longer a clear distinction between national regulations and safety and security management of the network companies. Ideas about internal control and risk management have been increasingly commingled, and risk management and regulation are no longer seen as broadly contrasting methods of assuring safety and security (Power, 2007).

In most industrial countries, the end of the Cold War marked a change in focus from preparedness for war to an increasing focus on civil society's own vulnerability, safety, and security. This vulnerability stems from changes in the composition of hazards and new distributions of risk (Beck, 1992; OECD, 2003). To meet these new threats and changing risks, there was a need for new analytical concepts and for establishing borders between societal safety and other safety-related areas, such as national security, sustainable development, human security, and incident management. The concept of societal safety was developed in Norway during the last decade and has been defined as the "society's ability to maintain critical social functions, to protect the life and health of the citizens and to meet the citizen's basic requirements in a variety of stress situations" (White Paper 17 (2001-02) Societal Safety; referred to in Olsen, Kruke, and Hovden, 2007).

According to Olsen, Kruke, and Hovden (2007), societal safety may be considered a process of applying scientific principles and practices to dealing with threats, dangers, risks, losses, and other dynamic side effects of modern society. It aims to be a systematic approach to understanding and responding to social problems such as accidents, emergencies, crises, and disasters, whether they are intentional or caused by accidents (and whether they originate within the organization or outside in the organization's environment). Societal safety therefore entails coordination, organization, and assignment of clear roles to different actors at the international, national, and local levels.

NordForsk (2013) used the concept of societal security, which has a similar definition: "(…) the ability of a society to sustain vital societal functions and secure its population's life, health, needs and basic values under extraordinary stresses, known as crises." The difficult but widely embraced concept of "resilience" may capture the essence of what is required to meet the grand challenges relating to societal security in the future. NordForsk defined resilience as "… the capability of a social system (e.g. an organization, city or society) to proactively adapt to and recover from both expected and unexpected disturbances."

There is still disagreement about what the phenomenon of societal safety (and/or societal security) should include. In this thesis, I have chosen to use the term societal safety *and* security, define it by assessing events and stresses in light of a few general criteria, and understand societal safety and security as a combination of society's resilience and vulnerability toward threats and stressors, as well as society's ability to maintain trust in vital functions and institutions (Olsen, Kruke, and Hovden, 2007). Vulnerability is defined in different ways, depending on different research traditions, but it is most often conceptualized as being constituted by components that include exposure to perturbations or external stresses, sensitivity to perturbations, and the capacity to adapt. Vulnerability can be defined as society's inability to resist or manage hazards and threats, and society's vulnerability can be defined as vulnerabilities across sectors and governance levels (Rasmussen, 1997). Trust is essential for maintaining a resilient society and can be seen as the glue that maintains the functionality of important societal institutions. Trust in central societal functions is an important topic for understanding how people perceive different threats and society's ability to handle unwanted events. Hence, trust, and not only the functionality (dependability) of critical societal functions, is paramount for maintaining societal safety and security. Consequently, lack of trust can be a societal vulnerability in itself (Juhl, 2009).

2.7 Societal context – societal safety and security in Norway

Norway is a parliamentary democracy and a unitary state with 5 million inhabitants. The country has a multi-party system that results in coalition governments or a single party coming into power. As in most European countries, there are three administrative levels: a national level (central government), a regional level (19 counties), and a local level (429 municipalities). The Norwegian central government consists of 16 different ministries, including the Prime Minister's Office. A ministry works as a secretariat for the political staff, manages agencies, and is responsible for administrative tasks within its portfolio. The ministries at the central level are relatively small. Agencies report to different ministries and are located outside the ministries (Lægreid and Rykkja, 2013).

In Norway, three crucial principles guide the authorities responsible for internal safety and security: the principle of liability, the principle of decentralization, and the principle of conformity (or similarity). However, according to Christensen, Lægreid, and Rykkja (2012), the liability and decentralization principle in particular create tensions between different coordination forms. The liability principle implies that every ministry and authority is responsible for internal security and safety within its own sector. This is closely related to the doctrine of individual ministerial responsibility and emphasizes strong sector ministries and vertical coordination. The decentralization principle, on the other hand, emphasizes that a crisis should be managed at the lowest operational level possible. Here, specialization by geography is an important organizing concept, and local democracy and authority are relatively strong values in the Norwegian polity. Consequently, the county governors and municipalities are given an important function in risk assessment and crisis management (Lango, Lægreid, and Rykkja, 2011). A fourth principle relating to rescue services is also relevant. A principle of collaboration implies mobilization of the private sector and civil society organizations to enhance the capacity to handle disasters and major crises (Christensen, Lægreid, and Rykkja, 2012).

However, these principles also lead to an important (organizational) paradox: The principle of liability implies strong vertical coordination. The decentralization principle, on the other hand, implies strong horizontal coordination across sectors at a low level. The principle of conformity (or similarity) creates further organizational pressure in that it stresses that the organizational forms in a crisis situation should be as similar to the daily organizational forms as possible, which can be particularly difficult to maintain in “extraordinary” crises. According to Christensen, Lægreid, and Rykkja (2012), it is crucial to supplement existing formal organizations with improvisation and create temporary organizations when a major disaster occurs.

The most important developments in Norwegian internal security and safety policy since the Cold War have been the gradual strengthening of the Ministry of Justice and Public Security’s overall coordination responsibilities and the establishment of new directorates, agencies, and more ad hoc organizational arrangements under the ministry. This includes establishment of the Directorate for Civil Protection and Emergency Planning (DSB). Strong sectoral ministries and relatively weak super-ministries responsible for coordination across ministerial areas characterize the central government in Norway. The Prime Minister’s Office has traditionally been small with weak coordination power due to the principle of individual ministerial responsibility, which means that each minister bears the ultimate responsibility for actions within the ministry and subordinate agencies. Specialization by purpose or task is a dominant principle, making it difficult to establish coordinated arrangements across ministerial areas (Christensen, Lægreid, and Rykkja, 2012).

Nevertheless, Norway is characterized by a consensus-oriented and collaborative decision-making style. This may modify both vertical and horizontal fragmentation. Cooperative arrangements of consulting and participating and compromises are more common than confrontations. Norway is also a high trust society, where generalized trust among citizens, as well as citizens’ trust in government and mutual trust relations between politicians and bureaucrats and between different public bodies, is generally high. Added to this, Norway is regarded as a safe haven on the periphery of Europe, where until 2011[4] there had not been any major crises or terrorist attacks. High trust also

[4] On July 22, 2011, Norway was struck by a terror attack of unprecedented magnitude. A bomb explosion in the Central Government Complex destroyed several central ministries and, at the same time, a terrorist shot a large number of young people from the Labor Party’s youth organization attending a camp on the island of

characterizes the field of crisis management and internal security (Christensen, Lægreid, and Rykkja, 2012).

In Norway, the Ministry of Justice and Public Security has overall responsibility for national security in peacetime, including a coordination role with regard to the protection of critical networks and systems. DSB, the technical arm of the ministry, has an underlying department dedicated to national contingency planning which elaborates contingency plans and risk and vulnerability assessments. In less severe or cross-cutting crises, responsibility lies with the authorities within the sector or administrative level most affected, according to the liability principle. The Cabinet Crisis Council supports the government during severe crises and is normally summoned by the most affected ministry. The Council has five permanent members, comprising the top-level staff (director-generals) with the Prime Minister's Office, the Ministry of Justice and Public Security, the Ministry of Defense, the Ministry of Health and Care Services, and the Ministry of Foreign Affairs. In particularly severe crises, the heads of all the ministries can be summoned. Constitutional and ministerial responsibility still rests with each ministry (Lango, Lægreid, and Rykkja, 2011).

The Crisis Support Group, an administrative resource designated to support the lead ministry, is summoned in certain demanding crisis situations. The main operative units under the Ministry of Justice and Public Security are the Directorate of the Police (PD), the Police Security Service (PST), and the Joint Rescue Coordination Centers. At the local level, police districts are responsible for tactical decisions and operations. The PD is responsible for the professional direction and follow-up of the police and can assist the local chief of police in a crisis situation. There are 2 main rescue coordination centers and 28 local branches (Lango, Lægreid, and Rykkja, 2011). The Norwegian National Security Authority (NSM) coordinates preventive ICT security measures in Norway (OECD, 2006). NSM is responsible for taking protective measures against espionage, sabotage, and terrorism, as well as for supporting affected agencies by identifying and managing hostile ICT incidents. The Norwegian Intelligence Service (NIS) is responsible for assessing the intentions and capabilities of foreign actors and PST is responsible for preventing and investigating incidents where there is suspected involvement by foreign states, as well as for assessing threats to Norway and Norwegian interests (NSM, 2011). Last, several public agencies, which report to different ministries, are responsible for supervision and inspections to ensure that enterprises follow regulatory requirements.

2.7.1 Organizational context - the Norwegian electric power supply sector

The Norwegian power system is almost entirely based on hydropower generation (around 98%-99%); it also uses combined cycle gas turbine production and wind power. Hydropower is the production of electricity based on water, and the volume of water and the head determine the potential energy in a waterfall (FACTS, 2013). Norway is the world's sixth largest hydropower producer and the largest hydropower producer in Europe.

The Norwegian power grid is separated into the transmission grid, the regional grid, and the distribution grid. The transmission grid comprises the highways of the power system that link producers and consumers in a nationwide system. The transmission grid also includes international

Utøya. In total, 77 people died, and many were seriously injured. The attack was a terrible shock in a country seen as a peaceful and open democracy that had never experienced anything like this before (Rykkja, Fimreite, and Lægreid, 2011).

interconnectors, which make it physically possible to export and transport power as needed. The transmission grid has high capacity; the voltage level is normally 300 to 420 kV, but some power lines are 132 kV in certain parts of the country. The transmission grid is about 11,000 km. The regional grid is the link between the transmission grid and the distribution grid, and it covers about 19,000 km. The distribution grid consists of the local power grids that normally supply power to end users, such as households, services, and industry. The distribution grid has a normal voltage of up to 22 kV, but the voltage is reduced to 230 V for delivery to the general electricity consumer. The distribution grid over 1 kV is just under 100,000 km. Large power generation plants can be connected to the transmission grid, while smaller generation units can be connected to either the regional grid (small wind farms or small-scale power plants) or the distribution grid (minor small-scale power plants). Minor consumers are connected to the distribution grid while major consumers, such as power-intensive industry, can be directly connected to the regional or transmission grids (FACTS, 2013).

Norway began restructuring its electricity industry in 1991, with the unbundling of activities and the establishment of an open market which other Nordic countries joined during the second half of the 1990s. Restructuring and deregulation of the electric power supply sector was undertaken to intensify price competition and increase efficiency (Antonsen et al., 2010). Throughout the Norwegian energy business, integrated companies have, by law, been separated into network/grid companies (owning and operating the grid) and energy and brokering firms. Electric grid operations are closely connected activities that are separated by law to avoid undesirable cross-subsidizing between grid operation (network companies), which is a natural monopoly, and production, which is not (Almklov, Antonsen, and Fenstad, 2012).

Building power grids is expensive; the average cost per transported unit declines with increased use of the grid until it approaches maximum capacity. This means that it is not profitable for a society to build parallel power lines when there is sufficient transport capacity in the existing lines. Parallel lines can also lead to inappropriate land use and disfigure the landscape unnecessarily. One consequence of the network companies' natural monopoly is that users are tied to their local network company. The authorities have established extensive monopoly supervision to prevent the network companies from exploiting this position and to regulate the network companies' activities. The goal is to ensure that users do not pay too much for the grid, while also making sure that grid investments are sufficient to ensure capacity and quality. Grid companies engaged in operations other than grid activities must maintain separate accounts for their monopoly operations. The monopoly supervision aims to ensure that costs related to the generation and sale of electricity are not charged to the grid activities (FACTS, 2013).

Figure 2 shows the state organization of energy and water resources activities in Norway. The Storting (Norwegian parliament) defines the political framework for energy and water resources management in Norway. The government has executive authority and exercises this through various ministries:

- The Ministry of Petroleum and Energy has the overall administrative responsibility.
- The Ministry of the Environment is responsible for the external environment and planning legislation.
- The Ministry of Finance is responsible for power plant taxation, various taxes on energy, and the state's expenditures.
- The Ministry of Trade and Industry has ownership responsibility for Statkraft SF (FACTS, 2013).

The Ministry of Petroleum and Energy has the overall responsibility for managing the energy and water resources in Norway. The ministry's job is to ensure that this management is carried out according to the guidelines provided by the Storting and the government. The ministry's Energy and Water Resources Department has ownership responsibility for the state-owned enterprises Enova SF and Statnett SF (FACTS, 2013). NVE holds the managing responsibility according to the Energy Act (1990) and the Water Resources Act (2000), makes individual decisions, and performs preparatory procedures in cases to be resolved by the Ministry of Petroleum and Energy. NVE has the legislative power to issue regulations for companies within the electric power supply sector, is responsible for supervision, and performs regular inspections to ensure compliance with regulations (NVE, 2014a). In addition, NVE is responsible for issuing licenses. A license is a document granting permission to a specified company to develop and run power stations, dams, and power lines outlined in the license, including conditions and rules of operation (NVE, 2014b).

Enova is a state-owned enterprise that manages the assets in the Energy Fund[5]. Enova's objective is to promote environmentally friendly conversion of energy consumption and generation and to develop energy and climate technology. Statnett is a state-owned enterprise responsible for building and operating the central (main) electricity grid. The enterprise is the transmission system operator (TSO) for and owns more than 90% of the transmission grid. Statnett is the system coordinator for both the short and long term, which entails responsibility for ensuring the instantaneous power balance, as well as facilitating satisfactory quality of supply throughout the country (FACTS, 2013).

[5] The Energy Fund is financed via a small additional charge to electricity bills. In addition, the Energy Fund has been allocated the proceeds from "The "Green Fund for Climate, Renewable Energy and Energy Efficiency Measures" (http://www.enova.no/om-enova/rammebetingelser/lover-og-regler/vedtekter-for-energifondet/vedtekter-for-energifondet/257/308/) (accessed 11 September 2015).

Figure 2. State organization of energy and water resources activities in Norway (from FACTS, 2013).

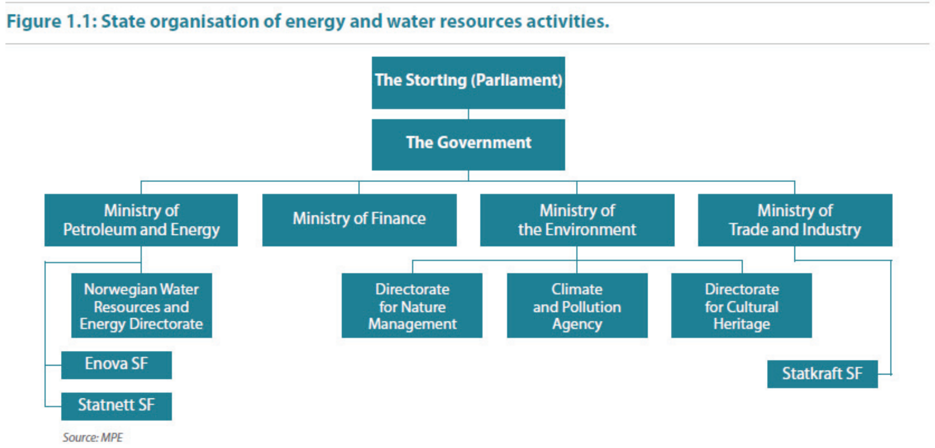


Figure 1.1: State organisation of energy and water resources activities.
The Storting (Parliament)
The Government
Ministry of Petroleum and Energy
Ministry of Finance
Ministry of the Environment
Ministry of Trade and Industry
Norwegian Water Resources and Energy Directorate
Directorate for Nature Management
Climate and Pollution Agency
Directorate for Cultural Heritage
Enova SF
Statnett SF
Statkraft SF
Source: MPE

The Norwegian power sector is characterized by a large number of stakeholders within different areas of activity. The sector is organized around power generation, grid, and trading. In addition, considerable numbers of district heating suppliers have also been established over the last 10 years. Public bodies are considerable owners in the sector (e.g., about 90% of Norwegian hydropower production is owned by public entities). The combination of considerable public ownership and a diversity of stakeholders is distinctive for the Norwegian power sector (FACTS, 2013). In this study, I have chosen to focus on ICT safety and security in *network companies* (distribution/grid companies) because a failure in the electricity networks/grids and the transmission and distribution of electricity to critical infrastructures and important societal functions, as well as to individual households, would have a huge impact on societal safety (and security).

As mentioned, Statnett is the transmission system operator in Norway. Thus, Statnett must ensure a balance between generation and consumption of electricity at all times. The enterprise is responsible for prudent socioeconomic operation and development of the transmission grid and is subject to the NVE’s monopoly supervision. Statnett is responsible for continuously assessing and developing necessary policy instruments to ensure instantaneous balance in severe power situations. These policy instruments include agreements on energy options in consumption and use of reserve power plants. Statnett is also responsible for continuously assessing whether new policy instruments are necessary to ensure the instantaneous balance in a better manner than currently provided. Furthermore, Statnett plays a key role in development and operation of cross-border interconnectors. This includes extensive cooperation with transmission system operators and regulators in other European countries (FACTS, 2013).

Norway is part of a joint Nordic power market with Sweden, Denmark, and Finland, which is in turn integrated in the European power market through interconnectors to Germany, the Netherlands, Estonia, Poland, and Russia. The transmission system operators cooperate through the European Network of Transmission System Operators for Electricity (ENTSO-E). Nord Pool Spot AS organizes the physical power trading on the Nordic power exchange. Nord Pool Spot is owned by Nordic transmission system operators, who have the largest ownership interests, and transmission system operators in Estonia and Lithuania. The Latvian system operator will become an owner when the Latvian power market opens (FACTS, 2013).

As previously stated, all power producers, grid owners, and/or traders must have a license from NVE. In 2012, 183 companies produced power in Norway, and 58 were solely producers. The 10 largest production companies by megawatts (MW)-installed capacity in Norway in 2012 controlled more than 75% of the country's mean production capacity and installed about 74% of the overall capacity. As of December 31, 2010, 154 companies were carrying out grid activities at one or more levels (distribution grid, regional grid, or main (transmission) grid). Of these, 44 were pure grid (network) companies. Most network companies are wholly or partially owned by one or more municipalities, while Statnett, which owns about 90% of the main grid, is owned by the state. Private companies, county authorities, and municipalities also own parts of the main grid, and municipalities and county authorities own most of the regional grids and distribution grids. There are private ownership interests within all activity areas: production, grid activity, and trading. Foreign ownership interests are relatively limited in the Norwegian power supply, but some foreign companies have been granted trading licenses in Norway. In addition to production companies and network companies, there are also trading companies that purchase power in the market for re-sale, vertically integrated companies that engage in activities within power production, power transmission, and/or power trading, and district heating companies (FACTS, 2013).

The Power Supply Preparedness Organization (PSPO) includes all the units undertaking production with appurtenant watercourse regulation, transmission, and distribution of electrical power and district heating pursuant to the Energy Act. The PSPO prepares, establishes, and maintains a structure giving all relevant levels in the power supply system tasks and responsibilities so as to efficiently handle extraordinary situations in the power supply system and appurtenant watercourse structures. According to NVE, 137 of the companies included in the PSPO in 2012 were classified as network (distribution/grid) companies (some practicing both monopoly and competitive activities). Of these 137 network companies, 10 were registered as having more than 100 employees. Furthermore, 23 of the network companies were organized in large corporate groups with several subsidiaries or daughter companies. NVE classifies installations into three classes according to their importance for the nation's power supply system. Class 1 is for installations of lesser importance, class 2 is for installations of importance to maintenance of the power supply system at the county level or for operation of regional grids, and class 3 is for installations of importance for the power supply system in a part of the country or region, for operation of the central (main) grid, or for large population groups, important infrastructure, or other special considerations (NVE, 2013).

2.7.2 Threats to Norwegian network companies' ICT systems

In 2008, a group was established to coordinate efforts by NIS, PST, and NSM to achieve a more comprehensive understanding and assessment of the ICT risk scenario in Norway. This group has fostered a great deal of cooperation, which has led to the uncovering of major challenges. According to them, the digitization of Norwegian society makes the dependence on ICT and the Internet a strategic challenge. In peacetime, the greatest threat to Norwegian interests is the theft of commercial data and intellectual property. Such thefts could affect, for example, the country's competitive advantage, the ability to compete, the ability to negotiate, decision-making, stock market prices, industrial performance, and infrastructure. Foreign parties could also infect systems with malware that, in a time of crisis or conflict, could be used to disrupt or destroy systems and processes so as to limit the Norwegian government's room to maneuver. Several countries have developed offensive capacities that in a crisis situation can destroy essential services and critical infrastructure. This means that political and economic decision-making processes, as well as defense capabilities, might be affected by a data attack (NSM, 2011). According to PST's annual threat assessment for 2012, there is a danger that foreign intelligence services' computer and Internet-based intelligence activity could severely affect Norwegian intelligence targets (PST, 2012). In addition, NIS presented a report on national security in February 2013 and, according to its security threat assessment, cyber terror is one of the main threats to national security (NIS, 2013).

The Norwegian Business and Industry Security Council (NSR) serves the Norwegian business sector in an advisory capacity on matters relating to crime and works actively to prevent loss (NSR, 2014). NSR conducts the Norwegian Computer Crime and Security Survey (Mørketallsundersøkelsen) through the Computer Crime Committee (Datakrimutvalget). The survey's goal is to map out the scope of data crime and ICT safety and security incidents in Norwegian organizations, the awareness of ICT safety and security, and the scope of implemented ICT safety and security measures. Results from the 2012[6] survey showed an increasing gap between threats and safety and security measures in Norwegian organizations at the same time that ICT dependence is increasing (NSR, 2012).

In December 2012, the Norwegian government launched the Cyber Security Strategy for Norway (Regjeringen, 2012a). According to the action plan that accompanied this national strategy, the Norwegian authorities' annual threat assessments ascertained that threats related to ICT-based espionage and sabotage have increased in recent years and, as previously mentioned, we now must expect sophisticated attacks aimed at critical societal information, including ICT systems that operate industrial processes and critical infrastructure (Regjeringen, 2012b). In addition, the Data Protection Authority, NSM, and Office of the Auditor General have revealed weaknesses in risk assessments conducted by public administration. They pointed out that existing security measures are often unsystematic and fragmented and that information security efforts neither have enough support from management nor are well integrated into business management (Regjeringen, 2012a).

Furthermore, in 2013, one of the largest Norwegian newspapers, Dagbladet, published a series of articles called “Null CTRL” (“No CTRL”). The newspaper articles examined online devices in Norway and revealed how a lack of computer security can affect us all at home, at work, and in public spaces. The newspaper has so far alerted the authorities and network owners and/or providers of more than 2500 Norwegian control systems (used in, for example, the armed forces and the health, oil, and transport sectors) connected to the Internet with little or no protection. NVE has also been interviewed in connection with these articles and has warned that the vulnerability of ICT systems used in electric power supply systems is expected to increase during the next few years because of the implementation of AMI (smart meters) in all Norwegian households by 2019 and, later, the smart grid (Dagbladet, 2013). Moreover, a report from 2012 on terror toward the U.S. electrical grid concluded that a few well-informed persons may be able to black out large areas over a long period of time, with devastating and life-threatening consequences. According to NVE, this threat is just as great for Norway as for the U.S. (Teknisk Ukeblad, 2012).

[6] The Norwegian Computer Crime and Security Survey from 2012 was the eighth survey conducted by NSR.

The Norwegian Computer Emergency Response Team (NorCERT) is a department of NSM, and one of the organization's principle tasks is to coordinate response to cyber attacks on critical infrastructure in the public and private sectors in Norway (OECD, 2006). According to NorCERT, there are a lot of challenges, both technical and organizational, when it comes to ICT safety and security in the organizations within the Norwegian electric power supply system. Examples of technical challenges include that safety and security in closed systems is falling behind according to the current risk picture, patching can be a challenge for production systems, operational networks are linked to other ICT networks in the organizations, wireless communication (Bluetooth) has been introduced, and operational networks are increasingly linked to the Internet. Examples of organizational challenges are a lack of communication between the ICT department and operational departments in the organizations, ICT often having a low priority in the safety management of the organizations, many organizations lacking a comprehensive overview of their own safety and security status, and many organizations lacking procedures and routines for handling ICT safety and security incidents and incident reporting that results in weak management commitment.[7]

Mnemonic AS is one of the largest providers of IT information security services within the Nordic region and has been hired by many Norwegian network companies to assess their ICT safety and security. According to representatives from Mnemonic, they hear a lot of the same claims from the organizations that hire them. These claims are: "We are not a target for attacks," "We have never experienced an attack on our ICT systems," "Our SCADA systems are completely isolated from the Internet or other ICT systems," and "We are very good at following Microsoft's programs for updating the systems." However, according to Mnemonic, techniques for attacking SCADA systems have already found their way to online "hacker manuals" such as Metasploit, there is a lot of evidence of attacks on these types of systems, it is possible to use USB sticks and go online from the computers used for the process control systems, and there are always some computers that for some reason do not have their systems updated (e.g., the computer is too old, the computer is mostly not in use).[8]

As in other countries, the electricity sector in Norway has experienced an increased focus on profitability stemming from the deregulation in 1991. Maintenance practices, investment level, the organization of activities, and the interface between government bodies have been important discussion topics in Norway. Critics have questioned whether restructuring and outsourcing have led to deterioration of the network companies' competence to maintain a reliable system. Network companies must have the competence necessary to fulfill their roles as service buyers, including high-quality specifications and control routines, and ensure their ability to coordinate efforts during major breakdowns. Reduced local knowledge and personnel, in combination with an aging infrastructure, are areas of concern (Antonsen et al., 2010).

[7] "Det nasjonale IKT-trusselbildet" ("The national ICT threat picture"), Torgeir Vindsnes, Norwegian National Security Authority. Presentation at conference – "Kraft IS 2011: Informasjonssikkerhet i kraftsektoren" ("Information security in the electric power supply sector"), November 9-10, 2011.

[8] «Hvor vanskelig er det egentlig å ta over elementer i prosessnettet uten utdelte tilganger?» ("How difficult is it really to take over elements in a process control network without access rights?"), Espen Martinsen, Mnemonic. Presentation at conference – "Kraft IS 2011: Informasjonssikkerhet i kraftsektoren" ("Information security in the electric power supply sector"), November 9-10, 2011.

In 2014, NSM uncovered an extensive cyber attack on companies in the Norwegian oil and energy sector. The attack consisted of e-mails carrying malware and, according to NSM, its detection systems showed that these e-mails were sent to around 50 Norwegian companies. Statnett, the transmission system operator in Norway, was one of the companies attacked; however, one of Statnett's employees was vigilant and reacted to both the content and the sender of the e-mail. Nevertheless, NSM found that Norwegian companies are not doing what they should to ensure better security in their ICT systems. Most companies do not keep a log of access to their systems, which means they do not know whether an attack has occurred (e.g., if they have a virus in their systems) and, if they should find a virus, they have no possibility of tracing its origin or effects. According to NSM, the cyber attack in 2014 was the biggest attack in Norway's history, but it has not been taken seriously by Norwegian companies. The extent of hacking, espionage, and other serious computer crimes was expected to double from 2013 to 2014, but most Norwegian companies did not check whether they had been exposed to espionage. Five hundred companies in the Norwegian oil and energy sector received a warning from NSM and were advised to check for malware in their systems, but only 27 companies reported back to NSM that they had found malware, even though at least 50 companies were actually attacked. Thus, NSM recommends increased monitoring and control of ICT systems and increased awareness of ICT safety and security among the companies' employees.

2.7.3 Regulation of safety and security in the Norwegian electric power supply sector

Compliance with regulation of ICT safety and security is a challenge for safety and security management of the network companies discussed in this thesis. Therefore, this section provides a brief description of the regulation of safety and security (which includes ICT safety and security) in the Norwegian electric power supply sector. Safety and security in the Norwegian electric power supply system is based on functional regulation (enforced self-regulation), where internal control[9] is essential. Hence, risk management is required by law, in the Internal Control Regulation (1997),[10] and for the electric power supply sector the requirement for risk management is further reinforced through several different regulations. Contingency planning is regulated by the Energy Act (1990),[11] the Energy Act Regulations,[12] and the Contingency Planning Regulations.[13]

Several regulations require organizations to have an information security management system (e.g., Electronic Public Administration Regulations) that apply to the entire public sector. Regulations relating to the Personal Data Act apply to both the private and public sector. In addition, the Norwegian Security Act[14] applies to the entire public sector and parts of the private sector. Several regulations state that security efforts must be tailored to the risk. Thus, it is crucial for organizations to conduct comprehensive risk and vulnerability analyses[15] (Regjeringen, 2012a). ICT safety and

[9] Internal control gives companies responsibility to monitor and implement an updated safety (and security) management system (see sections 5.4.1.1 and 5.4.1.2).

[10] January 1, 1997: Regulation concerning Systematic Health, Environment and Safety Activities at Enterprises (Internal Control Regulation).

[11] Act no. 50 of June 29, 1990.

[12] REG. no. 1990 of December 7, 1990.

[13] Reg. No. 1157 of December 7, 2012: Regulations relating to contingency planning in the power supply system.

[14] Act no. 10 of March 20, 1998: Regulations relating to Protective Security Services.

[15] In this thesis, I have chosen to use the term risk and vulnerability *analysis* because this term closely resembles the term used in the contingency planning regulations for the Norwegian electric power supply (i.e.,

security is further reinforced through §6 and §7 of the contingency planning regulations for the electric power supply system. Furthermore, NVE develops regulatory guidelines for the contingency planning regulations. The guidelines are to be continually developed and quality assured based on feedback from the electric power supply companies.

2.8 Summary

The electric power supply is said to be the most critical infrastructure in modern societies, and our societies are vulnerable to the consequences of damage and breakdowns in the electric power supply systems. ICT systems are critical infrastructures in themselves, and these critical infrastructures are in turn used for controlling critical processes in other infrastructures through, for example, process (industrial) control systems (e.g., SCADA systems). After the introduction of NPM, technologies have become increasingly interconnected at the same time that the organizations managing them have become increasingly fragmented. SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control. Although some characteristics are similar, these process control systems also have characteristics that differ from traditional ICT systems, which mostly stem from the logic executing in process control systems having a direct effect on the physical world. This direct effect leads to significant risk to humans, the environment, and the economy. SCADA systems support many aspects of our day-to-day lives and, in many cases, are critical to our well-being and the very existence of our economy (Nicholson et al., 2012).

The shift from proprietary hardware to standardized and less expensive operating systems and security products, with commonly known vulnerabilities, has dramatically increased the number of systems subject to attack. SCADA systems are vulnerable to several different types of attacks (both intentional and unintentional) and malfunctions, and threats to process control systems can come from numerous sources. The last decade has seen a growing number of cyber attacks and attacks on ICT systems have had major consequences for critical infrastructures. Natural incidents or technical failures are also realistic sources of power blackouts, of which there are many examples from the last decade. Furthermore, ICT systems within electric power supply systems in the Western world are also becoming increasingly vulnerable due to the introduction of AMI and the smart grid. The context for the studies of different challenges for safety and security management of network companies due to the increased use of ICT is the Norwegian electric power supply sector. As in other Western countries, Norwegian network companies' ICT systems are vulnerable to a number of threats, both natural and man-made.

risiko- og sårbarhetsanalyse). However, the term risk and vulnerability *assessment* often describes the same process and will be used in this thesis when referring to other research.

3. State of the art

This chapter provides an overview of related research on problem issues similar to those discussed in the current study.

3.1 Research on ICT safety and security

Information and communication have experienced tremendous technological changes in the past decades. However, according to the OECD (2006), security considerations were largely overlooked in the early phases of development of technologies and products. Most companies currently have a system portfolio that is far more complex than just a few years ago. ICT is now part of almost all new products and systems, and it is often taken for granted that these new products and systems will interact seamlessly with other systems and across organizations and sectors. It is a challenge to keep track of all the interdependencies and potential vulnerabilities. The increasing complexity of systems and networks has also made it more difficult for procurers of ICT systems to set clear and precise security requirements (Regjeringen, 2012a).

Several different terms are commonly used when discussing ICT safety and security and threats to ICT systems (e.g., information technology, IT safety and security, information security, computer safety, computer crime, data safety, cyber safety, cyber security, cyber threats, cyber crime, cyber terror, logical threats). In this thesis, I mainly use the term ICT safety and security, but different terms are used when referencing other research studies. According to Siponen and Oinas-Kukkonen (2007), research on information security has traditionally been dedicated to technological aspects and more research on the non-technical aspects is needed. Von Solms (2001) stated that information security has moved away from its singularly technical image and now includes a wide range of facets (e.g., organizational, technical, legal), all of which must be considered in creating a secure environment (referred to in Hagen, 2009). However, according to Dhillon and Backhouse (2001), computer and information security has focused mainly on technological solutions to prevent vulnerabilities and attacks and has not yet fully adopted a sociotechnical approach[16] that addresses human and organizational aspects of computer and information security (referred to in Kraemer, Carayon, and Clem, 2009).

According to Hansen and Nissenbaum (2009), the concept of cyber security appeared on the post-Cold War agenda in response to a mixture of technological and changing geopolitical conditions. Cyber security was first used by computer scientists in the early 1990s to highlight a series of insecurities related to networked computers, but the concept moved beyond a mere technical conception of computer security when proponents urged that threats arising from digital technologies could have devastating societal effects. These warnings were increasingly validated throughout the 1990s by prominent American politicians, private corporations, and the media. The terrorist attacks in the U.S. on September 11, 2001, further spurred attention to computers, information technology, and security, as well as questions of digital infrastructure protection, electronic surveillance, terrorists' use of hacking, and the Internet as a networked platform for communication across and against states (Latham, 2003, referred to in Hansen and Nissenbaum,

[16] A thorough description of the sociotechnical perspective on risk management will be given in section 5.2.

2009). Central to cyber security is the manner in which the referent objects of “the network” and “the individual” are linked to national and regime/state security.

Issues related to ICT safety and security have been mentioned in many studies of risk, safety, security, and organization. According to Rasmussen (1997), the rapid development of ICT leads to a high degree of integration and coupling of systems and the effects of a single decision can have dramatic effects that propagate rapidly and widely through the global society. Weick (2001) claimed that the use of computer systems has created unusual problems in sensemaking for managers and operators (employees) and, according to Leonardi and Barley (2010), one of the most critically important questions for students of organizing is: How is the shift to a computational infrastructure shaping the way people work and organize? These issues will be explored further in Chapter 5.

Line and Tøndel (2012) suggested that several problems related to the security of ICT systems are rooted in the quality of existing solutions. Experience shows that software contains a lot of vulnerabilities, some of which attackers can use to perform general untargeted attacks. Several nations are developing computer network attack (CNA) capabilities so as to shut down ICT systems or manipulate critical data. The ICT industry itself has started to address many of these security concerns (Hagen, Fridheim, and Nystuen, 2005). Soon after a vulnerability is identified, software producers often develop a corrective “patch” that they make available free of charge. Applying software patches to computers can protect information systems from an estimated 95% of all intrusions. However, patch application is still far from being immediate and universal. ICT administrators often find it difficult to keep up-to-date with corrective patches, and the time lag between the moment a vulnerability is announced (and a patch made available) and the moment hackers start to exploit it is also shrinking (OECD, 2006).

According to Albrechtsen and Hagen (2009), the widespread use of computers has made it increasingly important to attend to the human element of information security. Humans threaten the security level by accidental and intentional failures and by social engineering attempts and deliberate malicious acts. However, at the same time, humans are also an important resource to prevent incidents and individuals’ information security performance is influenced by a wide range of formal and informal factors (e.g., security technologies, formal organizational structures, education, awareness, values and norms, social relations and interactions).

3.2 Research on risk regulation

Hovden (1998) studied the introduction of internal control of safety as the main principle for controlling safety in Norway from the 1980s. The Norwegian experiment with the so-called internal control reform was an attempt to develop new approaches and means to cope with new challenges of misfits between technology and regulation, partly caused by the rapid development of production and information technology. At the end of the 1990s, the contents and results of the Norwegian internal control of safety, health, and environment (SHE) reform was ambiguous and included a mixture of successes and failures in implementing the reform. In 1993, more than 90% of the big companies classified as high hazard industries by authorities had established internal control systems according to the regulations. However, small enterprises and the service sector were far behind the big hazard industries in complying with the intentions of the reform. The auditing methods used by the authorities and within the enterprises were mainly based on the principles of quality assurance.

These methods seemed to best fit big, stable bureaucratic organizations and gave lower ratings to flexible dynamic organizations and small enterprises with few formal procedures.

Lindøe (2001) discussed the integration of occupational health, environment, and safety management with management systems. In Norway, internal control includes occupational health and safety (OSH) and the external environment practices. Thus, the term health, environment, and safety (HES) was used in the revision of the internal control regulations from 1997. Results from one study showed that in contrast to the bigger industries there seemed to be a mismatch between the HES requirements and small and medium-size enterprises (SMEs). These findings were consistent with results from other countries reporting that a successful implementation of occupational health and safety management (OSHM) depended on the specific characteristics of the enterprises. Large companies with a bureaucratic form, clear lines of authority, and expertise in OSH should be well suited to such implementations. Implementing OSHM in SMEs, on the other hand, was also reported to be difficult in other countries. One argument was that the internal control system was not able to adjust to radical changes in employment and labor market relations; however, Lindøe (2001) found that the process may succeed under certain conditions.

In 2013, an expert group appointed by the Norwegian government reviewed the regulatory strategy and the health, safety and environment (HSE) regulations for the Norwegian petroleum (oil and gas) sector through an extensive interview study with relevant organizations and agencies. The relationship between functional and prescriptive risk regulations is an area of conflict between the different actors within this industry. The industry in general considers the functional regulations as well functioning and wants as few detailed requirements as possible. However, contrary to this, the labor unions and the government want to increase the minimum requirements. New companies within the industry are also requesting more guidance and detailed requirements from the authorities (Engen et al., 2013).

3.3 Research on technical standards for ICT safety and security

Previous research has shown that even though information security guidelines are of a prescriptive nature and an imperative for the users, users still often fail to apply the guidelines as intended. This result suggests that the guidelines may not be effective in influencing human behavior and attitudes (Hagen, Albrechtsen, and Hovden, 2008). According to Brunsson and Jacobsson (2000), practicing a standard is mostly about adapting practice so that the standard describes it with reasonable accuracy. Substantial differences may exist between presentation and practice, between formal structure and actual operations, and between what people say and what they do. Actors may have dual systems that are decoupled from each other, and they may argue that they follow a standard while not doing so in practice. However, standardizers (e.g., national standards organizations) do not seem to notice this phenomenon, or at least they seldom discuss it in public. Standardizers seem to assume that standards that change presentation always change practice.

According to Hagen (2011), International Organization for Standardization (ISO) standards 27001 and 27002 provide a good framework for developing a management system for information security, and in addition they provide management commitment and ensure that routines and plans are in place. However, these technical standards are still no guarantee that a company will achieve a good effect because the standards say nothing about the quality of each individual measure. Awareness regarding ICT safety and security among the companies' managers and employees is also necessary, and management needs to focus on ICT safety and security and demonstrate commitment to these issues both through their activities and through a dedicated budget.

The aforementioned expert group that reviewed the regulatory strategy and the HSE regulations for the Norwegian petroleum sector in 2013 also discussed the use of technical standards. The guidelines to the regulations in the Norwegian petroleum industry refer to recognized technical standards as a way to meet functional requirements. However, with a steadily growing number of technical standards, considerable knowledge and technical skill are required to use them, and renewing these standards also requires a lot of resources. The technical standards used in the petroleum industry are developed by Norwegian, foreign, and international organizations (e.g., Standards Norway/NORSOK, American Petroleum Institute, ISO), and several of the interview groups in the study found the regulatory regime to be too complicated, with overlapping of standards in some areas. A number of actors in the industry struggled with the complexities of the standards and claimed that this complexity leads to unnecessary additional costs and diminished efficiency. Some of the interview groups also felt that the technical standards were not sufficiently updated and were not keeping up with the fast-paced technological and organizational development (Engen et al., 2013).

3.4 Research on risk perception

According to Andersson (2011), individuals make well-informed decisions and expose themselves to an optimal risk level if they have accurate perceptions of risk (i.e., knowledge of the true levels of risk they face). To some extent, perceived risk is a reflection of “objective” (real) risk, especially when risks are well known (Sjöberg, 2000). Humans are influenced by their surroundings, and the environment affects cognition as well as behavior and individual decisions. Perceived risk concerns how an individual understands and experiences a phenomenon (Oltedal et al., 2004).

Several factors influence risk perception. Whether people perceive a risk the same as technical risk estimates (most often calculated from statistics and probability distributions) depends on subjective probability. Heuristics, probability judgment biases, and frequent media exposure influence the level of perceived risk (Sjöberg, 2000). Tversky and Kahneman (1974) introduced a program of research on judgment under uncertainty which has come to be known as the heuristics and biases approach. They suggested that intuitive predictions and judgments are often mediated by a small number of distinctive mental operations, called judgmental heuristics. These heuristics are often useful, but they sometimes lead to characteristic errors or biases (referred to in Kahneman and Tversky, 1996). Kahneman and Tversky (1979) criticized expected utility theory as a descriptive model of decision making under risk and developed an alternative model, called prospect theory. When faced with a complex problem, people employ a variety of heuristic procedures to simplify the representation and valuation of prospects (referred to in Tversky and Kahneman, 2000). Examples of perceptual biases include biases in people’s judgments of time saved by increasing the speed of an activity (Svensson, 2008). Time gain is one motivator for drivers to speed up, and in turn speeding increases the risk of having an accident (Eriksson, Svensson, and Eriksson, 2013).

Several studies have found that company size influences risk perception within companies (Eakin, 1992; Hasle and Limborg, 2006; Hagen, Sivertsen, and Rong, 2008). Hagen, Sivertsen, and Rong (2008) presented a selection of findings from the Norwegian Computer Crime and Security Survey from 2006. According to their study, smaller businesses are less likely to have extensive security arrangements in place. The constraints of small businesses include that they generally do not have the diverse ICT staff typical of larger companies, and many managers in small businesses also have little understanding of information security threats and risks. Smaller enterprises may, however, be exposed to several kinds of computer crime incidents due to weaknesses in access control measures and data protection.

All enterprises that outsource their ICT operations have to trust a third party and its employees and systems. According to Hagen (2009), important security risks include weak preparation before signing the contract and weaknesses in the follow-up management and audit process. When outsourcing ICT functions, it is important for the contract to include requirements regarding access control, confidentiality, technical safety and security measures, availability, access to documentation, economic liability for incidents, and possible sanctions if the requirements are not followed. However, the Norwegian Computer Crime Survey (2012) found a steady decline (for both public and private enterprises) in all of these areas from 2008 to 2012, though larger organizations seemed to set stricter requirements for their vendors (suppliers). These findings suggest that managers not only outsource functions but also the responsibility for ICT safety and security, which are worrying results. Only half of the enterprises answered that they had allocated internal resources with ICT knowledge to follow up on the contracts with and deliveries from their vendors and subcontractors. This does, in turn, support the claim that the enterprises are not thorough enough when it comes to monitoring the quality of the services they purchase, which might affect risk perception.

According to Mearns et al. (1997), a relationship exists between risk perception and accident involvement, and having had an accident or having experienced an attack can influence the current perception of risk. In a study of fishermen’s risk perception (subjective assessments of risks), Brooks (2005) found that they did not consider it necessary to conduct emergency procedures (e.g., capsize, abandon ship) and that this may be related to the absence of capsizes in recent times. According to Goodhue and Straub (1991), it often takes a major loss from computer abuse to initiate or reinforce security management.

How a security incident is handled can depend on how serious the security violation is perceived to be (Hagen, 2009). According to Hagen, the way employees interpret (make sense of) a security situation depends on the extent of their security knowledge. According to Besnard and Arief (2004), humans may be biased in perceiving actual levels of risk and rarely have exhaustive knowledge of the systems with which they interact. The Norwegian Computer Crime and Security Survey from 2012 found that Norwegian enterprises, especially their managers, lack knowledge of ICT safety and security and do not have an overview of threats and incidents. This may explain why many of the enterprises have not implemented available safety and security measures or focused on their organization’s safety and security culture.

According to Sjöberg (2000), the risk target is of paramount importance in risk studies; people do not make the same estimate when they rate the risk to themselves, to their family, or to people in general. Risk denial is an important feature, and this phenomenon has been related to what has been called unrealistic optimism. People tend to estimate the general risks to be larger than the personal risks. Familiarity with the source of danger, control over the situation, and the dramatic character of the events can also influence risk perception (Oltedal et al., 2004).

Marek et al. (1985) measured “feelings of safety” (risk perception) in four occupational groups working on the Norwegian Statfjord A platform and found that each group lived and worked in its own “worlds of risks.” Mearns et al. (1998) measured perceptions of the job situation (e.g., work pressure, job security, risk-taking at work), risk perception, satisfaction with safety measures, and safety attitudes in a survey of 722 UK offshore employees on 10 different installations. They concluded that employees’ responses to the questionnaire reflected different safety climates as evidenced by perceptions of the state of safety on each installation and, furthermore, perceptions of the safety climate were also, in part, determined by the particular subculture to which the individuals belonged (both referred to in Mearns, Flin, and O’Connor, 2001). The concepts of safety climate and safety (or security) culture will be further discussed in section 5.5.3.

Goodhue and Straub (1991) studied the level of security concern among ICT system users and focused on users’ perceptions of the security of their systems. Previous studies found that neither end-users nor information security staff believed that there were persuasive reasons to be concerned about security. This lack of concern was alarming in the face of mounting empirical evidence that a significant number of security breaches has occurred. A lack of awareness of the danger might lead to weak vigilance by users and a greater potential for abuse.

3.5 Research on users of ICT systems and management commitment, awareness creation, and training with regard to ICT safety and security

According to Hagen (2009), the success of an information security program depends on the commitment of all staff (users of ICT systems), and all members of an organization must be aware of their responsibility for security. Albrechtsen (2008) demonstrated how organizations can measure cultural aspects such as awareness, behavior, and management commitment by using surveys and experiments (referred to in Hagen, 2009). The effectiveness of an organization’s security culture has been evaluated by measuring compliance with the existing security policy and written guidelines. Administrative measures and documents may, however, be taken for granted, and one of the major challenges for a safety and security management system is to enhance the behavior of people (both management and employees) (Johnson, 2006). The effectiveness of a safety and security policy has been assumed to depend on the way the safety and security contents are addressed in the policy document and how the content is communicated to users (Höne and Eloff, 2002, referred to in Hagen, 2009). A safety and security policy is not effective unless it is supported by management (Kemp, 2005, referred to in Hagen, 2009).

3.5.1 Users of ICT systems

According to Dhillon and Backhouse (2000), the role, responsibility, and integrity of users are important principles of information security management. A user can be characterized as a person with legitimate access to the organization’s information (and communication) systems (referred to in Albrechtsen, 2007), such as end-users, security officers, managers, and designers (Besnard and Arief, 2004). Users play an important role in the information security performance of organizations through their security awareness and cautious behavior (Albrechtsen, 2007).

According to Albrechtsen (2007), a user’s view on information security is created by several interlocking organizational, technological, and individual factors. The context of a user’s work may create information security trade-offs (e.g., individuals tend to emphasize efficient and least-effort work instead of loss prevention). Social norms and interactions at the workplace influence individual understanding of information security, and the quality of information security management also affects users' awareness, motivation, and behavior. Technological information security solutions influence users, and individual factors such as motivation, knowledge, attitudes, values, and behavior also influence individual views on information security. Last, but not least, how people perceive risk is a part of the explanation of users' view on information security.

Albrechtsen and Hovden (2009) conducted a study of a possible information security digital divide between information security managers and users of ICT systems. A digital divide in information security can be viewed as consisting of existing differences with regard to information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships, any or all of which can result in differences in information security performance among individuals. Albrechtsen and Hovden pointed out that users can cause adverse incidents through malicious or unintentional behavior. Users often assume that the responsibility for ICT safety and security rests with the technology and with the ICT safety and security managers, and they do not realize the benefits of ICT safety and security measures. In addition, users often trade off ICT safety and security against efficiency and functionality, which can be caused by efficiency demands, emphasis on minimum-effort work, and poor quality of ICT safety and security training and education resulting in insufficient skills and knowledge. For employees, the responsibility for acting in a manner that is safe and secure for the organization comes on top of other demands they face in their everyday work.

The important role of ICT system users has also been emphasized in studies of safety and security in electric power supply systems. From 2001 to 2008, Roe and Schulman (2008) conducted a longitudinal analysis of California's electricity system (California Independent System Operator). This system is the transmission manager of California's high-voltage electrical grid, one of the largest, most complex, and economically important electricity systems in the world. One of their key conclusions was that the reliability of these types of electricity systems depends on the performance of skilled control room operators (users of ICT systems) handling disturbances and variations. An implicit consequence of this was also an accompanying reliance on the functioning of ICT equipment, such as sensors and remote controls (process control systems/SCADA systems) without which these professionals cannot operate (Almklov, Antonsen, and Fenstad, 2012).

3.5.2 Management commitment to ICT safety and security

According to Rasmussen (1997), management's commitment to safety and security has been a major problem and led to the related efforts of society to control management incentives through safety and security regulation. Research on safety climate has also indicated that the safety levels of organizations are influenced by managers' attitudes toward safety and the perceived priority given to safety training (Antonsen, 2009). As previously mentioned, the safety climate represents employees' perceptions of organizational support, particularly management's commitment to safety in the organization. According to Skogdalen and Tveiten (2011), managing an organization's safety requires a long-term approach focused on the key determinants of the safety culture, and one of the prime factors is the degree of management commitment to safety at all levels, from first-line supervisors to managing director. Managers should also check whether their safety commitment is being transmitted to others and, according to Flin, O'Dea, and Yule (2002), this can be achieved with the use of safety climate surveys.

Hagen (2009) argued that information security should be embedded in all management processes and should include incident reporting and organizational learning. Organizational policies and user guidelines require the commitment of top-level managers and should be directly linked to the company's business strategies. The top management must demonstrate commitment to ICT safety and security through its activities and through a dedicated budget. An organization's safety and security policy should contain a letter of commitment from the top management showing commitment to ICT safety and security within the organization and assign the responsibilities of each member of the organization, particularly line management, top management, and safety and security professionals (Johnson, 2006).

3.5.3 Awareness creation and training

According to Furnell (2007), one of the essential aspects of good information security management is an effective security culture that includes consistent, appropriate attention to employee security awareness, training, and education (referred to in Hagen, 2009). A lack of safety and security awareness by users has been cited as the top obstacle for effective ICT safety and security. If people (management and employees) do not handle and protect ICT systems in a safe and secure manner, even the best technologies will be ineffective.

Previous research has also suggested that the impact of ICT safety and security breaches coming from people inside an organization is bigger than all other sources combined (Johnson, 2006; Hagen, 2009). Hagen and Albrechtsen (2009a) performed a comparative study of the regulation of information security and the impact on top management commitment in the electric power supply sector versus the finance sector in Norway. Their results showed that a larger number of electric power supply companies reported incidents typically caused by insiders (e.g., abuse of ICT systems, unintentional use violating security) compared with financial companies. The researchers found that higher organizational security awareness corresponded with less exposure to insider threats. The results of the study also showed that high management engagement corresponded with a high degree of adopted security measures and a lower degree of insider incidents.

According to Albrechtsen and Hovden (2009), both the ICT safety and security managers and the end-users of ICT systems that were interviewed in their study agreed that end-users often do not have the knowledge or skills needed for safe and secure behavior. Both groups believed this shortcoming to be the result of insufficient training. Users of ICT systems often do not realize the benefits of information security; they consider practicality and efficiency as far more important in their work. Both the interviewed managers and end-users also agreed that the best measures to raise awareness regarding ICT safety and security were interactive, face-to-face measures (e.g., personal meetings or presentations). However, this type of measure was also among the least frequently used approaches by the companies in the study. Formal one-way communication methods, such as information material and electronic information (e.g., screen savers, e-mail messages, leaflets) were extensively used because these measures are simple and cheap.

Albrechtsen and Hovden (2009) found that employee participation is valuable for measures influencing user performance as well as for other parts of information security management. Practical learning (through interaction) rather than formal education is likely to be the most effective way to improve knowledge on how to act safely and securely. Thomson and von Solms (1998) argued that social psychological principles must be introduced to improve the effectiveness of security awareness programs. The use of role-playing exercises and the use of examples related to the employee's own work situation were suggested as good techniques to achieve information security awareness among users of ICT systems. Use of e-learning can also strengthen individual security awareness and behavior. Hagen and Albrechtsen (2009b) discussed the effects of a computer-based security training program (using e-learning software) which was introduced in a multinational commercial organization in 2008. The study documented significant improvements in information security knowledge, awareness, and behavior of the employees who participated in the training program.

Johnsen (2012) studied key safety and security challenges in a complex industrial setting, i.e., the use of integrated operations (IO) in the Norwegian onshore and offshore petroleum sector. IO is a new technology that involves the integration of traditional ICT systems with the process control systems (SCADA systems) used in production, and the systems are distributed between onshore and offshore. Johnsen's research was performed through a survey of all 46 offshore oil and gas installations in the North Sea, and one result found in the data analysis and discussions was an absence of systematic knowledge sharing and awareness training. Information about undesirable ICT/SCADA incidents had not been shared among the relevant stakeholders, and systematic awareness training related to ICT/SCADA security had not been performed. According to Johnsen, this would affect both anticipation and attention and might reduce the resilience of the system. Jaatun et al. (2009) also studied the use of IO within the petroleum industry on the Norwegian Continental Shelf. Although the petroleum sector has experienced few incidents in relation to its SCADA systems, being unprepared for higher risk factors and new and unforeseen threats will, according to their study, be very costly in an industry that depends on virtually no downtime for its productions systems.

As previously mentioned, the Data Protection Authority, NSM, and Office of the Auditor General have revealed weaknesses in risk assessments conducted by Norwegian public administration. They pointed out that existing security measures are often unsystematic and fragmented and that information security efforts neither have enough support from management nor are well integrated into business management (Regjeringen, 2012a). According to the action plan for the Cyber Security Strategy for Norway (2012), awareness regarding ICT safety and security has significant potential for improvement among top management, middle management, and employees in many organizations.

Similarly, results from the national Norwegian Computer Crime and Security Survey from 2012 showed an increasing gap between threats and safety and security measures in Norwegian organizations at the same time that ICT dependence is increasing. According to the survey, citizens, employees, and managers in Norwegian enterprises/organizations should be safety and security conscious and must increase their knowledge of ICT safety and security. Everyone should have access to information regarding safety and security challenges and safety and preventive measures, and everyone needs to understand that measures must be implemented. Organizations need to have the necessary procurement expertise for purchasing new ICT tools and services, using external consultancy, and outsourcing enterprise services. Recommendations from the survey included establishing an ICT safety and security culture in organizations through continuous training and awareness creation activities for all employees; ICT safety and security awareness and knowledge among managers must also be increased.

4. Conceptual clarifications

This chapter provides an overview of and discusses several concepts that are essential for theoretical discussions of challenges for safety and security management (i.e., risk, vulnerability, uncertainty, complexity, safety and security). In the literature, these concepts are used in various ways and there exists no common accepted terminology (Vatn, Hokstad, and Utne, 2012). However, the concepts of risk, uncertainty, vulnerability, and complexity are often seen as closely linked, and these concepts are again closely linked to the concepts safety and security.

4.1 Risk, uncertainty, vulnerability, and complexity

The concept of risk can be given many different definitions which represent different ways of looking at risk. In this thesis, I have chosen to understand the concept of risk as a perspective from which to analyze the uncertain consequences of future developments and changes in societies. Uncertainty refers to the difficulty of predicting the occurrence of events and/or their consequences, and uncertainty may result from an incomplete or inadequate reduction of complexity (Aven and Renn, 2010). However, as mentioned previously, it is important to acknowledge that perceived risk (i.e., subjective risk judgments) can be influenced by several factors, which will be further discussed later in this thesis.

Specific uncertainties become risk objects that need to be managed, and organizations can be seen as processors of uncertainty. According to Power (2007), institutionalized (cultural) frames underwrite social accounts of the control and manageability of risks. The organization of uncertainty involves the creation of ideal frames for the management of issues under the description of risk; organizations must be seen to act as if the management of risk is possible. Visions of risk manageability constitute a new space of responsibility and actionability; the organization of uncertainty in the form of risk management designs and standards is related to expectations of governance and demands for defendable, auditable processes. Since the mid-1990s, there has been an expansion in discourses of risk and its management and, according to Power, the dominant discourse of risk management has shifted from the logic of calculation to that of organization and accountability; this represents a shift from a discipline with its foundations in analysis and calculation to a more general governing framework both for risk analysis and for management in general.

The concept of vulnerability relates to complexity and interdependencies in technological and social systems. As stated in section 2.6, vulnerability is defined in different ways depending on different research traditions, but it is most often conceptualized as constituted by components that include exposure to perturbations or external stresses, sensitivity to perturbation, and the capacity to adapt. Vulnerability can be defined as society's inability to resist or manage hazards and threats, and society's vulnerability can be defined as vulnerabilities across sectors and governance levels (Rasmussen, 1997). Vulnerability is closely linked to concepts of risk (Renn, 2008); however, public policies to mitigate the impacts of unwanted events still differ depending on whether they focus on reducing risk or reducing vulnerability. Risk-based approaches do not depend on reduction of vulnerability for their success (Sarewitz, Pielke, and Keykhah, 2003), and society's ability to manage events through ordinary routines can be strongly influenced by vulnerability in critical technological and social systems (i.e., how these systems influence and depend on each other).

According to Aven and Renn (2010), the degree of complexity and uncertainty are two aspects that can be used to distinguish between different types of risk problems (situations). Here complexity refers to the difficulty of identifying causal links between a multitude of potential causal agents and specific effects, and uncertainty refers to the difficulty of predicting the occurrence of events and their consequences. The National Institute of Standards and Technology (NIST) is a part of the U.S. Department of Commerce and responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets in the U.S. NIST has developed a guide to process control systems security, and one of the threats to process control systems listed in this guide is complexity. As previously mentioned, process control networks are often more complex than traditional ICT networks and require a different level of expertise (e.g., control networks are often managed by control engineers, not ICT personnel). Process control systems can have very complex interactions with physical processes, and consequences in the process control system domain can manifest in physical events (Stouffer, Falco, and Scarfone, 2011).

Some unwanted events can have cascading effects far beyond the system in which they occurred, which means that single events can affect several societal functions simultaneously. Events in technological and social systems can thus spread quickly to other sectors and/or systems. Among the best examples of complex technological systems are the focus areas of this thesis: energy supply systems and ICT systems, or failure in such systems, that depend on energy and ICT (e.g., financial systems, transport systems, hospitals) (OECD, 2003). Cyber risk can be seen as a systemic risk, an emerging risk, and a possible transboundary crisis. Systemic risks are risks that affect the systems on which society depends. According to the OECD, changes likely to affect risks and their management in the future may occur in four contexts: demography, the environment, technology, and socioeconomic structures. These will reshape conventional hazards and create new ones, modify vulnerability to risks, transform the channels through which accidents spread, and alter society's response. Furthermore, cyber crime, terrorist attacks, and some natural catastrophes call for a critical look at both the safety and security of networked systems and the social infrastructure that makes them vulnerable. The sheer complexity of today’s world requires a broad approach to the subject of systemic risks (OECD, 2003). Systemic risks cross the boundaries between different infrastructure sectors, as well as different levels in those sectors (Almklov, Antonsen, and Fenstad, 2012).

The International Risk Governance Council (IRGC, 2010) has defined emerging risk as “a risk that is new, or a familiar risk in new or unfamiliar conditions. Emerging risks are issues that are perceived to be potentially significant but which may not be fully understood and assessed.” Definitions vary according to the sector under scrutiny. Emerging risks may challenge efforts to maintain societal security based on cross-sectorial and multi-level governance. According to the OECD report “Future Global Shocks – Improving Risk Governance” from 2011, shocks in the future may arise from previously unknown hazards for which there are no data and no model for likelihood and impacts, the so-called unknown-unknown events. The working definition of future global shocks in this report is “a rapid onset event with severely disruptive consequences covering at least two continents” (OECD, 2011a). Important examples of these future global shocks are cyber risks, as well as pandemics, financial crises, and geomagnetic storms.

According to Ansell, Boin, and Keller (2010), in recent years crises and disasters have become increasingly transboundary in nature. Examples of transboundary crises are epidemics, financial crises, ice storms, and oil spills. These crises affect multiple jurisdictions, undermine the functioning of various policy sectors and critical infrastructures, escalate rapidly, and morph along the way. Energy blackouts and cyber attacks are also considered transboundary crises. All crises and disasters require a rapid response which must be delivered under conditions of collective stress and deep uncertainty. Nevertheless, according to Ansell, Boin, and Keller, these challenges become more difficult to manage when a crisis spreads across geographic borders and policy boundaries. More participants become involved, and these participants tend to be more dispersed, have more divergent agendas, and be less acquainted with each other.

As previously mentioned, based on numerous examples, failures in one infrastructure can lead to disruptions in other infrastructures and in the process lead to serious human, material, and economic consequences. The existence of such cascading effects highlights the tight couplings between various infrastructures and also the degree of complexity that makes these interconnections difficult to identify and manage (Almklov, Antonsen, and Fenstad, 2012).

4.2 Safety and security

Risk research has traditionally distinguished between the terms safety and security, but their meaning can vary considerably from one context to another. This can lead to serious misunderstandings when individuals from different technical communities collaborate. According to Piètre-Cambacédès and Chaudet (2010), the critical infrastructure protection domain is particularly prone to such difficulties. Safety and security are core, omnipresent concepts in the domain at both policy and technical levels, and the complexity of critical infrastructure systems involves the coordination of multiple actors from multiple engineering disciplines. Each discipline has its own understanding of the terms safety and security (e.g., the meaning of security to an electrical engineer differs from the meaning to a computer scientist, and both meanings differ from the meaning to a nuclear expert).

Piètre-Cambacédès and Chaudet found that two relevant and representative distinctions can be identified (the SEMA referential framework). The first is the system versus environment distinction (S-E), where security is concerned with the risks originating from the environment and potentially affecting the system, whereas safety deals with the risks arising from the system and potentially affecting the environment. The second is the malicious versus accidental distinction (M-A), where security typically addresses malicious (intentional) risks, while safety addresses purely accidental (unintentional) risks (p. 59).

According to Piètre-Cambacédès and Chaudet, the power grid sector and data (ICT) networks provide good examples of multiple definitions that can be clarified by SEMA. Electrical transmission and distribution networks are highly technical systems that evolve rapidly and involve diverse security and safety issues and challenges. In the power grid sector, the involved actors have different backgrounds, making it a good example of a thematic area that is full of traps and potential ambiguities with regard to the terms safety and security. The term safety is consistently used in the sector to denote the prevention of accidental harm from the power system and its components to humans and the environment. The term security is much more ambiguous. From a strict electrical engineering perspective, security is usually understood as the ability to survive disturbances (e.g., short-circuits, unanticipated loss of system elements) without interruptions in customer service. The nature of the cause is usually not considered. The malicious dimension is not explicitly excluded but is considered marginally, and the impact of the system on the environment is not in scope because it is treated as a safety aspect. Nevertheless, growing critical infrastructure protection concerns which were reinforced in the aftermath of the attacks of September 11, 2001, have led to numerous efforts to address malicious risks, especially regarding terrorist and external threats. In this perspective, the term security is associated with a different meaning which is often delimited by the malicious versus accidental distinction.

As previously stated, the increased dependence of the power grid on ICT coupled with the global interest in the AMI and smart grid has introduced new types of malicious risks. Cyber security concerns have caused the term security to be viewed in another manner. Moreover, internal threats are in some cases treated as separate issues. All critical infrastructures are highly dependent on telecommunications and data networks, and the protection of these assets is referred to as critical information infrastructure protection. Consequently, use of the terms security and safety in this context reflects the pervasiveness of telecommunications and data networks in the various critical infrastructure sectors and varies accordingly. The Internet Engineering Task Force (IETF), recognized as one of the principal technical bodies in the Internet domain, gives no relevance to the malicious versus accidental distinction. Safety is seen as a system-to-system issue, whereas security is potentially much broader. Definitions of security in the ISO/International Electrotechnical Commission (IEC) series of standards on information security also cover malicious and accidental aspects. However, the ISO/IEC documents (technical standards) do not mention safety, which may explain the conceptual width given to the term security (Piètre-Cambacédès and Chaudet, 2010).

Avoiding ambiguities in the meaning of the terms security and safety can be important for system design, risk assessment, policy-making, and collaborative research. With regard to safety, the importance of information-sharing and learning from previous accidents is often emphasized; however, secrecy is often emphasized when it comes to security issues (especially according to the malicious versus accidental distinction). Methods and tools involved in risk assessments can also be highly dependent on the chosen distinctions. For example, stochastic modeling is a well-established method for assessing accidental risks in industry, whereas it is unusual to model malicious behavior using this method because of its very different nature (Piètre-Cambacédès and Chaudet, 2010).

Using the malicious versus accidental distinction, Sivertsen (2007) argued that studies of risk and vulnerability in ICT systems should discuss both safety and security (p. 16) and, according to Aven (2007), both accidental threats (hazards) and threats of intentional origin need to be covered when discussing the massive use of ICT devices, the complexity of modern infrastructures, and the increasing interconnectedness among systems and organizations. According to the OECD, governments are vulnerable to a wide range of unwanted cyber events, both accidental and deliberate (OECD 2011b), and the U.S. NIST emphasizes that the personnel responsible for operating, securing, and maintaining the process control system must understand the important link between safety and security (Stouffer, Falco, and Scarfone, 2011). Furthermore, according to the Norwegian Computer Crime and Security Survey (2012), it is possible for data to fall into the wrong hands and be misused and manipulated without it being the result of a deliberate attack (NSR, 2012).

Many definitions of safety build on the idea that safety can be linked to risk – the lower the risk the higher the safety, and vice versa; however, this idea has also been challenged by several researchers. Aven (2014), for his part, held that for broad risk perspectives, which highlight uncertainties beyond probabilities and expected values, safety *can in fact* be considered the antonym of risk, and safe can be defined by reference to acceptable risk. An example of such a risk perspective is risk understood as uncertainty about and severity of the consequences of an activity (Aven and Renn, 2010), that is, the risk perspective applied in this thesis. According to Aven, seeing safety as the antonym of risk leads to simple and easily understandable definitions of safety, and we avoid the introduction of a double set of definitions for risk and safety and safe. However, this common platform for the risk and safety concept needs to be based on sufficiently broad risk perspectives that give due attention to the uncertainties. Using this risk interpretation, we acknowledge that being safe is a subjective judgment dependent on institutional processes to determine what is acceptable risk and what is not.

According to Aven, there is no problem technically to extend the safety definition (of safety as the antonym of risk) to also include intentional situations and events, as the risk concept does not distinguish between intentional and unintentional. The same might be said about the system versus environment distinction, and it may not be possible to make a clear distinction between safety and security. Accordingly, this thesis discusses both safety and security. Both safety and security issues are important with regard to ICT systems, which are vulnerable to both attacks and accidents (e.g., technical malfunctions), and risks that may arise within the organizations and in the organizations' environment. The focus in this project is on organizational risk (which affects societal safety and security), and not on occupational safety and health (HSE) and personal risk. However, as mentioned earlier, threats to organizations operating critical infrastructure may also lead to serious consequences for public safety, security, and health.

4.3 Safety and security (risk) management

According to Aven et al. (2004), the term safety (and/or security) management system (or risk management system) can be used to describe all measures that are implemented to achieve, maintain, and develop a level of safety and security in accordance with defined safety and security goals. According to Boin and McConnell (2007), preventing all extreme threats from materializing is not possible. We cannot know every conceivable "worst case" that may unfold, and there are political, cognitive, informational, cultural, and resource barriers to being able to prevent any possible threat to our critical infrastructures. The same is said about information security: Much vulnerability may be minimized or eliminated through management, operational, or technical controls as part of the organization's resiliency effort; however, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability (Swanson et al., 2010). Organizations must *attempt* to develop broad and comprehensive defenses for all relevant threats, to identify successful attacks and their consequences, and to plan for extraordinary incidents with potentially large consequences.

Rasmussen (1997) discussed risk management in a modern dynamic society and introduced the sociotechnical system involved in risk management. Many levels of politicians, managers, safety officers, and work planners are involved in the control of safety (and security) by means of laws, regulations, rules, and instructions that are formalized means for the control of hazardous physical processes. The purpose is to motivate workers and operators (employees) and to educate them, guide them, or constrain their behavior by rules and equipment design so as to increase the safety of their performance. In addition to the use of regulations, rules, and instructions, Rasmussen discussed cognitive control of behavior and, according to him, important questions with regard to risk management were: Will decision makers be committed to safety? Is management prepared to allocate adequate resources to the maintenance of defenses? Do regulatory efforts serve to control management priorities properly? Are decision makers aware of safety constraints? A more thorough description of the sociotechnical perspective on risk management will be given in section 5.2.

According to Power (2007), the organization of uncertainty in the form of risk management designs and standards is related to expectations of governance and demands for defendable, auditable processes. Public demands for risk regulation and greater transparency and accountability in risk handling have led to a shift from risk analysis to risk governance, a shift toward a form of risk governance that is more corporate in form and constitutes the governance of risk management. Risk governance refers to a complex of coordinating, steering, and regulatory processes conducted for collective decision-making involving uncertainty. The term governance comprises both the institutional structure (formal and informal) and the policy process that guides and restrains collective activities of individual groups and societies. Its aim is to avoid, regulate, reduce, or control risk problems (Renn, 2014).

As previously mentioned, ideas about internal control (functional self-regulation) and risk management have been increasingly commingled, and risk management and regulation are no longer seen as broadly contrasting methods of assuring safety and security (Power, 2007). Regulatory agencies seek to harness organizations' risk management systems as regulatory assets (Ayres and Braithwaite, 1992, referred to in Scheytt et al., 2006), and incentives of various kinds can be used to get organizations to internalize regulatory objectives, including the promise of a lower burden of inspection (Scheytt et al., 2006). Risk management is a part of the risk-governing process and is based on different regimes, that is, the set of rules and standards that govern the handling of risk in a specific regulatory context (Renn, 2014).

Traditionally, industrial safety has focused its effort on preventing incidents that had occurred in the past. More recently, the aim has become to identify and evaluate potential threats before they realize their catastrophic potential (Mearns et al., 1997). Safety (and security) management programs often include risk and vulnerability assessments, management strategies, training, information, and technical design (Aven et al., 2004). In earlier years, risk and vulnerability analyses of technological systems (e.g., the electric power supply system) were mostly concentrated on technical factors, but during the last decades human and organizational factors have also become important parts of the analysis (Fridheim and Hagen, 2007). Organizations have to implement different preventive measures based on the results of the risk and vulnerability analysis.

According to Hood et al. (2002, referred to in Renn, 2014), risk management for technological systems requires technological, organizational, and behavioral measures for reducing risks:

- *Technological measures* relate to the inclusion of active and passive safety devices.
- *Organizational measures* include emergency and contingency plans, guidelines, monitoring requirements, and provisions for assuring accountability and competence.
- *Behavioral measures* include all educational and training efforts to improve personal performance, increase sensibility toward safety issues, and strengthen the feeling of responsibility and accountability among the staff (safety culture).

With regard to information security management (ICT safety and security), Hagen, Albrechtsen, and Hovden (2008) also distinguished between technical security measures and organizational security measures. Technical security measures comprise firewalls, antivirus software, passwords, spyware, and malware protection, for example. In addition, a wide range of different organizational information security measures and activities exists. Hagen, Albrecthsen, and Hovden categorized these measures into four main groups:

- *The security policy*, which is the foundation of any security regime. This policy specifies the strategies behind an organization's information security approach through a written document, directly linked to the overall strategy of the company.
- *Procedures and controls,* which are directly derived from the security policy. This group of measures consists of documents guiding individual and organizational behavior such as user instructions, security plans, and non-disclosure agreements, as well as control and follow-up activities of the documented systems.
- *Administrative tools and methods* include both proactive and reactive means such as asset classification, risk analysis, audits, and incident reporting systems.
- *Creation and maintenance of security awareness*, which includes both individual and collective activities, that is, education and awareness-raising initiatives (e.g. e-mails, pamphlets, mouse pads, formal presentations, e-learning, discussion groups).

According to Leveson et al. (2009), organizational factors play a role in almost all accidents and are a critical part of understanding and preventing them. Technologies enable growth and promise global prosperity but may also cause major disruptions and undesirable long-term consequences. We need to understand not only the technologies, but also the organizations and institutions that implement, sustain, and co-evolve with the technologies. The way safety is managed in an organization, or regulated by a regulatory authority, depends heavily on the beliefs and assumptions that managers and safety professionals have concerning organizational behavior and safety (Reiman and Rollenhagen, 2011). In this thesis, I have chosen to study several important elements of safety and security management systems which have been identified in previous research (Rasmussen, 1997; Hagen, Albrechtsen, and Hovden, 2008; Renn, 2014; Aven et al., 2004); i.e., government risk regulation, the use of technical standards for safety and security, risk perception among managers and employees, management commitment to safety and security, and awareness creation and training with regard to safety and security.

5. Theoretical foundations

This chapter starts with a summary of various theories within the safety science field, and then goes on to describe the main theoretical framework of this thesis (i.e., the sociotechnical perspective and institutional organizational theory). Last, different theories about regulation, standards, sensemaking, risk perception, safety culture, and management commitment and awareness are explored in relation to the theoretical framework.

5.1 Safety science

Safety science can be viewed as knowledge about safety-related issues and the development of concepts, theories, principles, and methods to understand, assess, communicate, and manage safety (Aven, 2014). Certain theories have been popular in the safety science community in recent decades, as evidenced by their widespread citation. Three theories in particular are often cited: normal accident theory, high reliability theory, and resilience engineering (Hopkins, 2014).

Charles Perrow introduced the normal accidents theory in 1984. He detailed the concepts of coupling and complexity and claimed that failures may be inevitable as systems grow increasingly complex. The main problem is that it is impossible to predict the widespread impacts if one system component fails. Systems can be described by their complexity and by the tight coupling of their components and processes. Perrow's framework was not initially designed to address infrastructure interdependencies; however, his key concepts can be instrumental in highlighting some of the challenges related to infrastructure interdependencies. Coupling can refer to the degree of interconnectedness in technological systems (i.e., the extent to which failures are able to escalate rapidly and spread to other parts of the system or other technological systems). The concept of complexity here refers to the nature of interactions between parts of a system or between infrastructures. In a system of complex interactions, its processes will be characterized by "unfamiliar sequences, unplanned and unexpected sequences, and either not visible or immediately comprehensible" (Perrow, 1984, referred to in Almklov, Antonsen, and Fenstad, 2012).

In relatively simple systems – where only a few elements and their relationships and interconnections are well understood – it is relatively easy to determine how an event will propagate. This is not the case in complex systems. Indeed, it can be extremely difficult to understand propagation in complex systems because they are "composed of many parts that interact with and adapt to each other and, in so doing, affect their own individual environments and, hence, their own futures. The combined system-level behavior arises from the interactions of parts that are, in turn, influenced by the overall state of the system. Global patterns emerge from the autonomous but interdependent mutual adjustments of the components" (OECD, 2009). According to Hagen, Fridheim, and Nystuen (2005), most societal services and critical infrastructure adhere to Perrow's description of complexity and tight couplings, and this is especially true for critical ICT systems. Large interconnected infrastructures are characterized by high complexity, and ICT is both a critical infrastructure in itself and at the same time an important component of other critical infrastructures, which further increases the complexity (Line and Tøndel, 2012).

One can argue that several critical infrastructures are becoming both more tightly coupled to each other and *at the same time* more interactively complex (Almklov, Antonsen, and Fenstad, 2012). According to Utne, Hassel, and Johansson (2012), the largest challenge when it comes to modeling and simulating interdependent infrastructures is the vast complexity. Even if we only consider a single infrastructure, the complexity is significant. Extrapolating this to the system of systems, a set of interdependent critical infrastructures, the complexity is manifold. According to Leveson (2004), technology today (especially digital technology) is changing faster than the engineering techniques to cope with the new technology are being created. Lessons learned over centuries about designing to prevent accidents may be lost or become ineffective when older technologies are replaced with new ones. The time to market for new products has significantly decreased, and carefully testing systems and designs to understand all the potential behaviors and risks before commercial and scientific use is often no longer possible. Interactive complexity is increasing in the systems we are building, and we are designing systems with potential interactions among the components that cannot be thoroughly planned, understood, anticipated, or guarded against. Thus, the degree of uncertainty is also high (Aven and Renn, 2010), which can create challenges for safety and security management of organizations.

The theory of high reliability organizations (HROs) is another widely known theory, popular both inside and outside academia. HROs have been seen as organizations that operate with hazardous technology in a "nearly accident-free" manner or with many fewer accidents than might have been expected (Hopkins, 2014). For Weick and Sutcliffe (2001), HROs (which they called "mindful organizations") manage the unexpected through five processes:

- Preoccupation with failures rather than successes
- Reluctance to simplify interpretations
- Sensitivity to operations
- Commitment to resilience
- Deference to expertise, as exhibited by encouragement of a fluid decision-making system

Together these five processes produce a collective state of mindfulness (referred to in Hopkins, 2014).

According to Roe and Schulman (2008), the study of reliability in critical systems is the study of strategic balances that must be struck between efficiency and reliability, between learning by trial and error and the prevention of risky mistakes, and between maximizing our anticipation of shocks and maximizing our resilience to recover after them. High reliability management also concerns how these balances are achieved and sustained. Roe and Schulman's framework for understanding high reliability management highlights the crucial role of reliability professionals – control room operators, key technical department heads, and support personnel. Their special cognitive skills and flexible performance modes maintain reliable operations even in the face of widely varying and unpredictable conditions. Westrum (1992) argued that organizations conducting potentially hazardous operations need requisite imagination (i.e., a diversity of thinking and imagining that matches the variety of possible failure scenarios). Having this requisite imagination characterizes high reliability organizations. High reliability organizations can manage and sustain almost error-free performance despite operating in hazardous conditions where the consequences of errors could be catastrophic. According to Westrum (2004), these organizations can also be described as having a generative culture. A generative culture requires that alignment, awareness, and empowerment replace suspicion, isolation, and passivity. An open and generative culture will mean better uptake of innovations and better response to danger signals.

A third perspective that has become popular in recent years is resilience engineering (Hopkins, 2014). According to Hollnagel et al. (2010), resilience engineering can be defined as the “intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (p. xxxvi). The development of resilience engineering has focused on four abilities that are essential for resilience: the ability to (a) respond to what happens, (b) monitor critical developments, (c) anticipate future threats and opportunities, and (d) learn from past experience, successes as well as failures. Working with the four abilities provides a structured way of analyzing problems and issues, as well as of proposing practical solutions (concepts, tools, and methods). According to Hopkins (2014), resilience engineering is quite similar to HRO theory.

5.2 Sociotechnical dimensions of safety

As shown in the previous section, the past 30 years of research on accidents have built an understanding of ensuring safety that goes beyond technical rationality and traditional engineering models. In 1997, Rasmussen introduced a sociotechnical perspective, where stressors from the environment affect the organizations’ management. Sociotechnical systems involved in risk management include several levels ranging from legislators through managers and work planners to system operators. These systems are stressed by the fast pace of technological change, by an increasingly aggressive, competitive environment, and by changing regulatory practices and public pressure. According to Rasmussen, risk management must be modeled by cross-disciplinary studies, considering risk management to be a control problem and serving to represent the control structure involving all levels of society, which requires a system-oriented approach (Rasmussen, 1997).

Figure 3 shows Rasmussen’s (1997) model of the sociotechnical system. At the top of the sociotechnical system, society seeks to control safety through the legal system, where safety has a high priority but so have employment, production, and trade balance. Legislation makes explicit the priorities of conflicting goals and sets boundaries of acceptable human conditions. The next level is authorities and industrial associations, workers (trade) unions, and other interest organizations. Here the legislation is interpreted and implemented in rules to control certain hazardous activities for certain employees. The rules must also be interpreted and implemented in the context of particular companies, where the work processes and equipment applied can be considered. Many details from the local conditions and processes need to be added to make the rules operational. At the bottom level are design of the productive and potentially hazardous processes and equipment and the development of standard operating procedures for the relevant operational states, including disturbances.

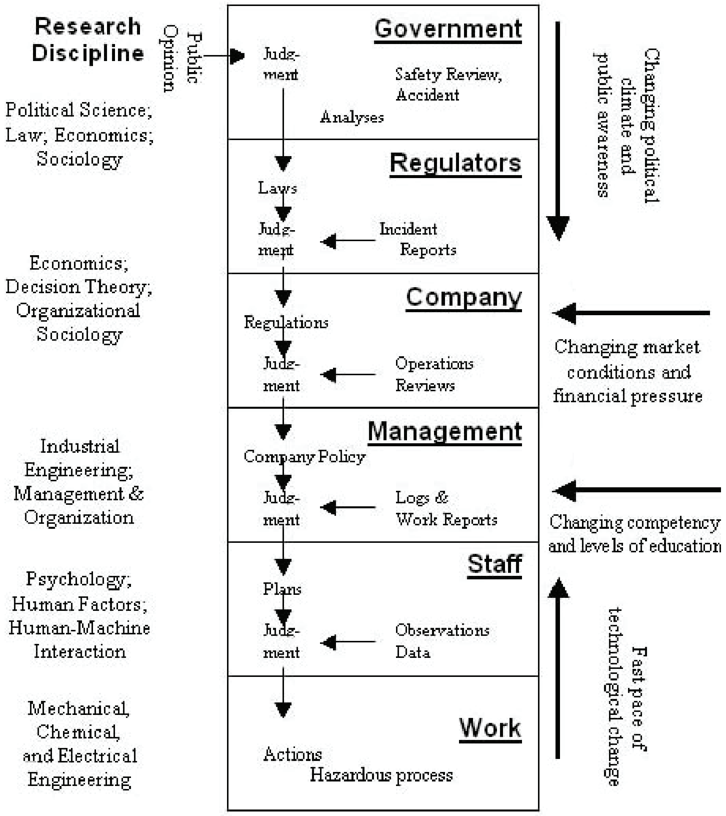
According to Rasmussen, the usual approach to modeling sociotechnical systems was by decomposition into elements that are modeled separately. However, he emphasized the need for more studies of the vertical interaction among the levels of sociotechnical systems with reference to the nature of the technological hazard they are assumed to control. In addition, practically speaking, laws, rules, and instructions are never followed to the letter. As previously mentioned, legislation and rules must be interpreted and implemented in the context of particular companies, and modifications of instructions are repeatedly found. The study of decision making cannot be separated from a simultaneous study of the social context and value system in which it takes place and the dynamic work process it is intended to control. Thus, it is important to include cognitive science in studies of risk (or safety and security) management (e.g., processes of sensemaking, perception, awareness, and commitment).

Using the sociotechnical approach we have to consider factors related to man, technology, and organization (MTO) in investigations of accidents or attacks in the past and in the risk assessment of the future (Johnsen, 2012). According to Albrechtsen and Hovden (2007), information security is a less mature field than industrial safety when it comes to sociotechnical approaches. Hagen (2009) argued that research on information security management has much to learn from the sociotechnical theoretical approach when it comes to dealing with the human factor in organizations. Good information security performance can be achieved through a dynamic interaction among technology, individuals, and organizational factors. However, according to Dyreborg (2006), it is important to expand on the sociotechnical perspective so that it opens up to understand that not only does the environment influence organizations, organizations also influence their environments.

According to Dyreborg (2006), research on risk and safety has evolved from being dominated by a formal rational perspective through a bounded rational perspective to a cultural open perspective where social and cultural factors increasingly are seen as important for the understanding and analysis of safety. This corresponds well with Reason's (1997) discussion of three approaches to safety management: the person model directed at reducing personal injury events, the engineering model focusing on the human-machine interface and system reliability, and the organizational model that deals with the integrity of defenses and broader systemic factors (p. 239). Dyreborg argued that it is important to develop a better understanding of the mechanisms that can influence organizational safety and that preferences and decisions are related not only to individuals but also to social and cultural mechanisms. In addition, research on organizational safety should apply an open organizational perspective to be better able to capture the increasing importance of the external dynamic boundaries for organizations' management of safety. It is important to understand organizational safety (and security) in connection with the organizations' environment, as well as how interactions play out in practice between organizations and their environment on the one side and between organizations and individuals/groups on the other.

Thus, my research in this thesis is consistent with the sociotechnical perspective on risk (or safety and security) management where stressors from the environment affect the organizations' management, and I include and discuss several levels of the sociotechnical system from legislators/regulators (regulatory authorities) through managers and employees. The socio-technical approach means that we must explore theories from several research domains (Johnsen, 2012). In the present study, I have chosen to apply institutional organizational theory to expand on the sociotechnical perspective. As in the sociotechnical perspective, the institutional organizational perspective (an open organizational perspective) emphasizes regulative, normative, and cognitive aspects that can influence safety and security management. In addition, I explore theories from industrial safety and elements from information security research.

Figure 3. Collaboration in the sociotechnical system to improve risk management according to Rasmussen (1997) (from Johnsen, 2012).


Research Discipline
Political Science; Law; Economics; Sociology
Economics; Decision Theory; Organizational Sociology
Industrial Engineering; Management & Organization
Psychology; Human Factors; Human-Machine Interaction
Mechanical, Chemical, and Electrical Engineering
Public Opinion
Government
Judg-ment
Safety Review, Accident Analyses
Regulators
Laws
Judg-ment
Incident Reports
Company
Regulations
Judg-ment
Operations Reviews
Management
Company Policy
Judg-ment
Logs & Work Reports
Staff
Plans
Judg-ment
Observations Data
Work
Actions
Hazardous process
Changing political climate and public awareness
Changing market conditions and financial pressure
Changing competency and levels of education
Fast pace of technological change

5.3 Institutional organizational theory – organizations and their environments

Organizational forms affect which issues get attention and which are ignored, how the issues are grouped together, and how they are separated. Organizational arrangements therefore have vital importance for risk management. Furthermore, external pressures, developments, and shocks (crises) may well be influential and result in new perceptions and organizational or procedural changes (Lango, Lægreid, and Rykkja, 2011). Many approaches to understanding the relationship between organizations and uncertainty (risk) focus on the organization-environment relationship (Power, 2007). In this thesis, I have chosen to apply institutional organizational theory (or organizational institutionalism) as part of my theoretical framework, which emphasizes that organizations are open systems strongly influenced by their environments. Organizations are embedded in society and are affected by institutions, ideas, rules, and legitimate patterns of action that are generally taken for granted. Attention is directed toward forces that lie beyond the organizational boundary in the realm of social processes (Brunsson and Jacobsson, 2000; DiMaggio and Powell, 1983, 1991; Hoffman, 1999). Organizations and environments are interdependent; environments influence organizations but organizations also influence environments, and thus the sharp distinction between organization and environment is blurred (Power, 2007).

Modern societies contain many complexes of institutionalized rules and patterns (e.g., products of professional groups, the state, public opinion), and these are seen as socially constructed realities which provide frameworks for the creation and elaboration of formal organizations (Scott, 1998). The roots of the social constructionist approach are found in the social phenomenology of Alfred Schutz, and in Berger and Luckman's (1966) *The social construction of reality,* which challenged realist approaches by arguing that rationalized social and economic laws are subjective social phenomena derived from experience rather than objective natural phenomena revealed through experience (Dobbin, 1994). Organizations are not seen as conforming to institutional demands, but as making sense of them, adapting them, enacting them, and working upon them (Glynn, 2008, referred to in Greenwood et al., 2008).

The use of institutionalism with other theories and topics rather than in isolation is, according to Greenwood et al. (2008), a conspicuous and significant strength. Institutional theory has an important capacity to stimulate contextualization. It aids us in contextualizing the phenomena we study, whether that context encompasses regulatory, historical, political, cognitively tacit, or socially embedded settings. Such contextualization (which includes the understanding that knowledge is socially constructed within a broader context) is a distinguishing feature of institutional theory and research. In this thesis, institutional organizational theory is mainly used to contextualize and structure the studied phenomenon (i.e., challenges for safety and security management).

According to Engen and Olsen (2010), changes in technological systems are characterized by a complex institutional embeddedness. The environmental contexts in which organizations exist are constantly changing, and at an increasing rate. These changes lead to increasing complexity, especially under the impact of fast-paced technological change. Future threats to society are not limited to specific sectors or areas, but stem from complex interactions among economic, technological, social, and cultural factors (Olsen, Kruke, and Hovden, 2007). Moreover, a growing consensus suggests that micro-electronically based information technologies are altering the way we live, work, communicate, and organize our activities. Orlikowski and Barley (2001) argued that information technology research can benefit from incorporating institutional analysis from organization studies, and organization studies can benefit by following the lead of information technology research in taking the material properties of technologies into account. Technologies are embedded in complex interdependent social, economic, and political networks and are consequently shaped by such broader institutional influences. At the same time, changes are occurring in the nature of work and organizing that cannot be understood without taking into account changes in the technological infrastructure on which economic and organizational activity rests. It is important to consider both the technological changes and the institutional contexts that are reshaping economic and organizational activities.

Institution is a complex concept, and institutional scholars have not reached agreement on its definition. Different institutional scholars accord priority to different institutional elements. In the introduction chapter to *The SAGE Handbook of Organizational Institutionalism*, Greenwood et al. (2008) used the term to refer to "(…) more or less taken-for-granted" repetitive social behavior that is underpinned by normative systems and cognitive understandings that give meaning to social exchange and thus enable self-producing social order" (p. 5). Since the conceptual beginnings of modern organizational institutionalism in the late 1970s, the term institution has acquired two different meanings: institutions as cultural models and institutions as regulatory frameworks. Scott (1995) brought order to the various strands of institutional analysis by distinguishing between the regulative, normative, and cultural-cognitive "pillars" or elements/aspects that underpin institutions (Greenwood et al., 2008). According to Scott (2008), "Institutions are comprised of (sic.) regulative, normative and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life" (p. 48). This thesis builds on Scott's definition of institution.

According to Scott, institutions are transported by various carriers – cultures, structures, and routines – and operate at multiple levels of jurisdiction (Hoffman, 1999) from the world system to interpersonal interaction. Although rules, norms, and culture-cognitive beliefs (symbolic systems) are central ingredients of institutions, the concept must also encompass associated behaviors and material resources. Rules, norms, and meanings arise in interaction and are preserved and modified by human behavior. Institutions impose restrictions by defining legal, moral, and cultural boundaries, setting off legitimate from illegitimate activities. However, institutions also support and empower activities and actors; they provide guidelines and resources for taking action (Scott, 2008). The institutional influences on organizational behavior can take several forms, but taken together they guide the interpretation of issues as they emerge and persist (Hoffman, 1999).

The institutional aspects (or pillars) are not operationally distinct, but rather overlap; development of one aspect influences the development of other aspects (Hoffman, 1999). However, Scott acknowledged that the cultural-cognitive pillar provides the deeper foundations of institutional forms (i.e., the infrastructure on which not only beliefs, but also norms and rules rest). Scott also urged researchers to specify which pillars are operative in which settings, how they unfold, and with what effects (Scott, 2004, referred to in Greenwood et al., 2008).

The regulative aspects of institutions most commonly take the form of regulations, which guide organizational action and perspectives by coercion or threat of legal sanctions. The normative aspects of institutions generally take the form of rules-of-thumb, standard operating procedures, occupational (technical) standards, and educational curricula. Their ability to guide organizational action and beliefs stems largely from social obligation or conformance to norms. The cognitive (or cultural) aspects of institutions embody symbols (words, signs, and gestures), cultural rules, and frameworks that guide understanding of the nature of reality and the frames through which that meaning is developed. Organizations will often abide by them without conscious thought (Hoffman, 1999); that is, they take them for granted. Institutions are viewed as including both formal structures and informal rules and procedures that structures conduct (Scott, 2008).

Greenwood et al. (2008) were somewhat critical of the definition of institutions as regulatory frameworks of states and professional agencies. According to them, accounts of how regulatory agencies (institutions) shape organizational behavior are incomplete institutional explanations unless they show how regulatory frameworks embody, enact, or transmit taken-for-granted societal norms and values. Otherwise, referring to regulatory frameworks as “the institutional context” risks confusing institutional theory with resource-dependence or political-economy explanations. However, they still conclude that in the interests of guarding the epistemological pluralism the scope of contributors to institutional theory’s growth seems to indicate they favor the broader construct definition of institutions put forward by Scott. Scott’s definition increased specificity but encouraged continued application of institutional theory to multiple levels, topics, and settings.

Institutions exist at the level of the individual, the organization, the field, and the society, but organizational institutionalism has primarily been interested in institutions and institutional processes at the level of the organization and the organizational field (Greenwood et al., 2008). An organizational field refers to those organizations that, in the aggregate, constitute a recognized area of institutional life (DiMaggio and Powell, 1991). Organizations operate within fields (or societal sectors) that shape, constrain, and empower them, but are also influenced by the interests and activities of their own participants. The concept of the organizational field builds on the more conventional concept of industry, but adds to this focal population other and different organizations that critically influence their performance, and this includes regulators. The concept of organizational field expands the framework of analytic attention to encompass relevant actors and governance structures that empower and constrain the actions of participants in a delimited social sphere (Scott, 2008).

Ultimately, organizational institutionalists believe that organizations are penetrated by environments and deeply embedded in institutional contexts. A given organization is supported and constrained by institutional forces. Moreover, a given organization incorporates a multitude of institutionalized features in the form of symbolic systems, relational systems, routines, and artifacts (e.g., technology) within their own boundaries. Hence, according to Scott (2008), it is appropriate to speak of the extent to which organizational components or features are institutionalized, and these views are shares by all or the great majority of institutional theorists. In addition, the subset of theorists endorsing a cultural-cognitive perspective has added an additional assertion: The very concept of an organization as a special-purpose, instrumental entity is a product of institutional processes – constitutive processes that define the capacities of collective actors, both generally and as specialized subtypes.

According to the theoretical approach employed in this thesis, technology’s effects on organizations are socially constructed. Artifacts can be defined as a discrete material object, consciously produced or transformed by human activity under the influence of the physical and/or cultural environment. Artifacts are created by human ingenuity to assist in the performance of various tasks. The most important characteristic of artifacts is that they all embody both technical and symbolic elements (Suchman, 2003, referred to in Scott, 2008). Users draw on familiar schemas and frames to make sense of a new technology. The formal organization can be considered an institution with accompanying rules and instructions for its incorporation and employment in a social setting. Institutions are taken for granted in that they are both treated as relative fixtures in a social environment and accounted for as functional elements of that environment (Jepperson, 1991). Once a technology is developed and deployed, it tends to become reified and institutionalized, losing its connection with the human agents that constructed it and gave it meaning, and appears to be a part of the objective, structural properties of the organization (Roberts and Grabowski, 1996).

Institutions can shape technological trajectories, but technologies can also shape organizations (Leonardi and Barley, 2010). Technology can be defined as "the process whereby actors (or teams) operate tools to solve certain tasks" (Engen and Olsen, 2010, p. 336). According to Hughes (1992), technology is a core element in technological systems. A technological system is defined as a complex of cultural, organizational, and technological phenomena jointly focused on a particular productive or political goal (e.g., the system for generating, distributing, and using electricity). As mentioned in Chapter 3, Leonardi and Barley (2010) argued that one of the most critically important questions for students of organizing is: How is the shift to a computational infrastructure shaping the way people work and organize? By computational infrastructure, they suggested that work done in organizations is increasingly accomplished via ICT that store, transmit, and transform information. Organizations often come to take for granted the way a technology should be used. Network companies might, for instance, take for granted that process control systems (e.g., SCADA systems) are used to improve system operations and not be adequately aware of the additional vulnerabilities introduced by using these ICT systems.

5.4 Regulative and normative aspects

Regulation is central to any discussion of the relationship between organizations and the management of risk (Scheytt et al., 2006). Organizations are embedded in society, which makes them susceptible to rules that come from their environment (Brunsson and Jacobsson, 2000). Regulation can be seen as being inherently about the control of risks; however, a number of core challenges lies at the heart of any regulatory decision on the handling of risk, ranging from the definition and identification of risks and critical debates about the principles inherent in any regulatory activity to fundamental questions on the appropriate institutions for risk regulation. How risk is perceived and what regulatory solutions are proposed are fundamentally shaped by underlying worldviews and understanding of cause-effect relationships (Baldwin, Cave, and Lodge, 2012). A substantial variation in risk regulation approaches is evident from one domain to another in an international context, between states within the same area of risk, and across policy domains within a national context (Hood, Rothstein, and Baldwin, 2001).

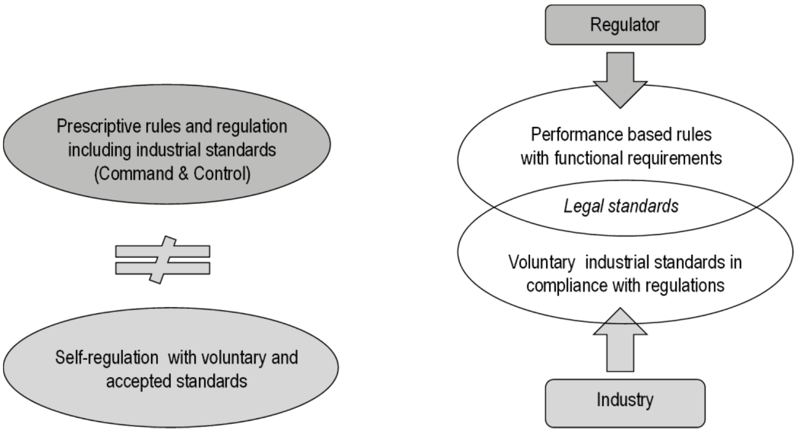
From an organizational institutional perspective, legislation can be seen as a reflection of cognitive schema that is historically contingent. In some studies, organizations have instrumentally invoked or evaded the law and looked to the law for normative and cognitive guidance as they sought their place in a socially constructed cultural reality. These studies discussed how policies and practices become constructed as enhancing efficiency, and thus as "rational" behavior, and eventually are taken for granted. These studies did not assume that new practices/models exist. Instead, they pointed to the reciprocal relationships involving professions, regulators, and organizational managers in constructing business models in response to ambiguous legislation. According to Scott (2004), this implies a transmutation over time of regulative into normative and cultural-cognitive elements (referred to in Greenwood et al., 2008).

Some groups of researchers within organizational institutionalism have focused not on the role of the state, but on the emergence of “soft” regulations. For these theorists, the institutional change of interest is the displacement of coercive, state-level regulations by more voluntary regulations such as standards, rankings, and accreditations. These softer regulatory structures are developed and applied by non-governmental agencies and elicit compliance because they provide legitimacy (Greenwood et al., 2008).This research can be linked to research on risk regulation. During past decades, a marked change has occurred in the way safety legislation is framed in many industrialized countries. The current trend is toward functional rules that emphasize the required outcomes of safety management, allowing considerable freedom on the part of organizations to identify the means by which these ends will be achieved (Reason, 1997).

Modes of risk regulation can be seen as a discussion of the pros and cons of rule compliance versus risk management (Hopkins, 2011), with a distinction between “hard regulation” based on “command and control” with prescriptive rules and “soft regulation” with concepts coined as “self-regulation” (Sinclair, 1997; Short and Toffel, 2010) and “meta-regulation” (Gilad, 2010), for example. Command and control regulation was for a long time the dominant type of government regulation and has often resulted in a complex web of legislation, agency rules, permit procedures, standards, judicial decisions, and other enforceable policies underpinned by a variety of sanctions. Command and control regulation has been referred to as an instrumental model of regulation, a deterministic regulation regime, detailed regulation, and prescriptive regulation. Despite its position as the dominant policy response, command and control has routinely been subjected to criticism, which has sparked considerable interest in various types of regulatory alternatives. These range from the replacement of command and control with economic incentives to the greater use of property rights and markets, as well as information-based strategies, voluntarism, and self-regulation (Sinclair, 1997).

An important question is whether these modes of regulation represent a dichotomy or whether they are complementary, as presented in Figure 4. The argument in this thesis follows Sinclair (1997), stating that the dichotomy is false. These modes represent two extremes or ideal types. In practice, risk regulation regimes combine responsibilities and roles in a public-private partnership with a top-down approach with legal, binding norms and a bottom-up approach with industrial (technical) standards and “best practices.” The use of legal standards becomes a “linking pin” that brings the two approaches together, as indicated in the right-hand part of Figure 4.

Figure 4. Two modes of risk regulation.


Prescriptive rules and regulation
including industrial standards
(Command & Control)
≠
Self-regulation with voluntary and
accepted standards
Regulator
Performance based rules
with functional requirements
Legal standards
Voluntary industrial standards in
compliance with regulations
Industry

5.4.1.1 Functional regulations

Function-based regulation relies on some form of discretionary criteria that are considered legal standards and provides some special interpretation challenges. The term legal standard refers to words or phrases in a law claim that stipulate a scale or norm beyond the law (i.e., a particular practice, widespread attitudes in the community, or other conditions that change with time). All the while these phenomena change over time, the contents of the law do not. The use of legal standards aims to achieve an appropriate regulation of complex fields in constant development. It can also be seen as an expression of respect for the importance of expert knowledge to ensure safety and quality in key areas of society. Legal standards are likely to safeguard the goal of safety and quality better than if they had been fully formulated in laws and regulations. The underlying measure of the legal standards is based on an understanding of the issues, terminology, and solutions that are understood in the professional and scientific community. Through stakeholder involvement in the process of developing these norms, the use of legal standards may enjoy greater legitimacy than rules based on legal terminology and legal text (Lindøe and Engen, 2013).

A consistent application of a function-based regulation requires a comprehensive and systematic review of how the various provisions are to be understood and how the appropriate standards should be used to meet the requirements. Procedures must provide relationships between laws and regulations and technical/professional standards to comply with the laws and provide predictability in relation to supervisors' evaluations. For regulatory authorities and inspectors, this can be a demanding and comprehensive system to maintain because it requires that the standards keep pace with developments and new knowledge. Comprehensive guidelines may also be an excuse for companies to not take responsibility in monitoring and implementing new and recognized expertise and scientific knowledge (Lindøe and Engen, 2013).

5.4.1.2 Internal control

When using functional internal control regulations, instead of designing detailed rules and control systems, the regulatory authorities prescribe safety goals and permit companies to develop and enforce their own detailed rules. As previously mentioned, this provides more capacity for the authorities to work on other important tasks and at the same time contributes to a heightening of the individual company's sense of responsibility for its own safety and security. When self-regulation is used to assure safety, enterprises are obliged to identify and assess risks and hazards embedded in their operations (Lindøe, Olsen, and Lie, 2006), and internal control gives companies the responsibility to monitor and implement an updated safety management system.

According to Hovden (1998), internal control means both "top down and bottom up" (i.e., top and line management involvement and responsibility combined with participation and industrial democracy). Internal control represents a shift to meta-regulations by society and delegation of direct rule-based control to the industry itself, and each enterprise is free to tailor it to its own needs, routines, organization, and culture. Power (2007) suggested that internal control systems embody both the potential of greater efficiency and coordination on the one hand and greater sensitivity to social responsibility issues on the other. The latter refers to a view of internal control systems as the basis for more substantive improvement of, for example, health, safety, and environment.

Organizations have an incentive to comply with principles of internal control because the regulatory process can focus on desired outcomes rather than regulating detailed processes, with regulatory intervention as a last resort. In cases of breach or dissatisfaction, the regulatory body has options to escalate its enforcement process with more serious consequences for the regulated organization. Some regulatory systems are linked to licensing privileges (including the regulatory system for the Norwegian electric power supply system), where a license to trade or conduct an activity is conditional on compliance with formal or procedural norms, such as having "effective" internal control. The sanction of withdrawing a license is usually a last resort and an outcome of extensive prior negotiation (Power, 2007).

5.4.1.3 Standards

According to Power (2007), institutional capacities to organize in the face of uncertainty have been challenged and threatened by failures, scandals, and disasters. In response, visionary documents and designs in the form of standards and guidelines for individuals and organizations have been produced to maintain perceptions of control and manageability. These recipes and recommendations have constituted a new normativity for risk management. The organization of uncertainty in the form of risk management designs and standards is related to expectations of governance and demands for defendable, auditable processes. The institutional construction of a risk management process is expressed and materialized in standards and guidelines. Standards formalize the fundamental design principles for the organizational self-management of risk and establish baselines against which organizations must evaluate themselves. Technologies are shaped by and embody normative processes, and trade and industrial groups often convene to set standards for a wide range of machines and technical equipment (Scott, 2008).

Along with hierarchies (or formal organizations) and markets, standardization can be seen as one of the primary forms of social coordination, control, and choice. These elements prescribe procedures for human interaction and guide the behavior of various actors. Standardization, along with organizations and markets, is a fundamental societal institution that includes defined patterns of action, rules, and beliefs. On a general and abstract level, standards constitute rules about what those who adopt them should do (Brunsson and Jacobsson, 2000). Applied to the variety of safety issues, the hierarchy of norms can be enforced as laws, regulations, regulatory guidelines, legal standards, and mandatory or voluntary technical (industrial) standards. In a functional regulatory regime, the use of legal, binding norms is minimized, but connected by legal standards to relevant and applicable technical standards (Lindøe and Engen, 2013).

A significant feature of standards and standardization is that expert knowledge is stored in rules and technical solutions, and technical standards have been introduced in more and more areas. A partial explanation is the need for control and supervision, which follows from the reliance on decentralized and deregulated systems. Standardizers have usually been founded with the backing of a state or large companies. However, the mission of these national standards organizations has been to develop standards for aspects of industrial activity which are not subsumed under a formal organization. The vast need for global coordination in the absence of a strong global organization or world state may explain the growing importance of global standardization in recent decades. Standards are explicit and in written form, most are voluntary, and standardizers cannot sanction those who do not comply with their standards. However, some standards become institutionalized in that in practice actors take it for granted that they should be followed (Brunsson and Jacobsson, 2000).

5.5 Cultural-cognitive aspects

Many institutionalists, especially new institutionalists, stress the centrality of cultural-cognitive elements of institutions: the shared conceptions that constitute the nature of social reality and the frames through which meaning is made. As previously mentioned, Scott acknowledged that the cultural-cognitive pillar provides the deeper foundations of institutional forms, i.e., the infrastructure on which not only beliefs, but also norms and rules rest. The concept of risk perception is connected to cognition, mental processes, sensemaking, and culture. Thus, I start this section with a short account of sensemaking theory before describing theories of risk perception, safety culture, management commitment, and awareness.

5.5.1 Sensemaking

According to Weick (2001), new technologies such as complex production systems that use computers (e.g., electric power supply systems) have created unusual problems in sensemaking for managers and operators (employees). Sensemaking comes from preexisting symbols, norms, and social structures that people reproduce and transform rather than create from scratch. Proponents of new institutional organizational theory claim that institutions are both antecedent to and emergent from sensemaking processes. Institutions enter meaning-making processes in three ways: Institutions serve as the building blocks or substance of sensemaking, institutions dynamically guide and edit action formation, and institutions are continually enacted and accomplished in ongoing sensemaking processes (Weber and Glynn, 2006).

According to Weick (2001), organizational members selectively attend to their environments and then, in interaction, make collective sense of what is happening. Weick’s ideas are consistent with ideas of the scholars within organizational institutionalism who emphasize the diffusion of ideas through a process of “translation.” Instead of treating institutionally prescribed structures and practices as “out there” and as adopted more or less “as is,” translation assumes that ideas and practices are interpreted and reformulated during the process of adoption. This approach is faithful to the social constructionist principles of institutional thought. Organizations are not seen as conforming to institutional demands, but as making sense of them, adapting them, enacting them, and working upon them. Thus, the institutional context may be an important part of sensemaking within organizations, and the micro-dynamics of sensemaking offer an opportunity for institutional organizational theory to develop a richer theory of the intersubjective processes of perception, interpretation, and interaction that establish the core of a micro-level understanding of institutionalization (Greenwood et al., 2008).

The use of computer systems involves the self-contained, invisible material process that is actually unfolding, as well as the equally self-contained, equally invisible imagined process that is mentally unfolding in the mind of an individual or a team. There is also continuous intervention improvement and redesign (technological innovations) in computer technologies, which means that the implementation state of development never stops, and these technologies require ongoing structuring and sensemaking if they are to be managed (Weick, 2001). It is difficult to establish a complete system description of these complex systems, and the lack of understanding might lead to “inaccurate” risk perception. Leblebici et al. (1991) noted that new technologies invoke the use of analogies; that is, existing cognitive frameworks are used to make sense of ambiguous or novel events (referred to in Greenwood et al., 2008).

5.5.2 Risk perception

Risk professionals still debate the nature of risks: Are risks social constructions or real phenomena? Do technical risk estimates represent “objective” probabilities of harm or do risks only constitute mental constructions? According to Aven and Renn (2010), it is important to deal with both the “physical” and “social” dimensions of risk and avoid the naive realism of risk as a purely objective category, as well as the relativistic perspective of making all risk judgments subjective reflections. They argued that it is essential to complement data on physical consequences with insights into risk perception when one is dealing with complex and uncertain risk problems. Studies of risk perception have examined the opinions that people express when they are asked to characterize and evaluate hazardous activities and technologies. Perceived risk (i.e., subjective risk judgments or a person’s own estimate of risk) may deviate from "objective" risk. “Objective” risk is the risk that exists independent of an individual’s knowledge and concerns about the source of the risk (Ulleberg and Rundmo, 1996, referred to in Oltedal et al., 2004).

The study of risk perception has a cognitive stance with a focus on perception as mainly a cognitive process. People's risk judgments are related to cognitive processes, for example, how one is able to comprehend the given information (Slovic, Fischoff, and Lichtenstein, 1982). This approach makes up the foundation of the psychometric paradigm in risk perception. According to this paradigm, risk can be understood as a function of general properties of the hazard (risk object) (Sjöberg, 2000). The psychometric model is based on a number of explanatory scales (e.g., new risk versus old risk, involuntary risk versus voluntary risk, dreaded risk, number of people exposed) where the subjects are asked to rate a number of hazards on each of the scales. The cultural theory of risk perception launched by Douglas (1966, 1978) and Douglas and Wildavsky (1982) has also been an important theoretical contribution. According to cultural theory, risk perception is not governed by personality traits, needs, preferences, or properties of the risk objects. It is a socially or culturally constructed phenomenon. What is perceived as dangerous, and how much risk to accept, is a function of one’s cultural adherence and social learning (referred to in Oltedal et al., 2004). Sjöberg (2000), on the other hand, saw attitude as a crucial factor in risk perception, in addition to risk sensitivity and specific fear.

According to Aven and Renn (2010), intuitive risk perception is based on how information about a risk is communicated, the psychological mechanisms for processing uncertainty, and earlier experience of danger. This mental process results in perceived risk, a collection of notions that people form regarding risk sources in relation to the information available to them and their basic common sense (Jaeger et al., 2001, referred to in Aven and Renn, 2010). This thesis will focus on risk perception among managers and employees within organizations (electric power supply network companies); in an organization, risk perceptions may influence risk behavior and hence influence "objective" risk or safety (Rundmo, 1996). Trust is of crucial importance for the understanding of risk perception (Sjöberg, 2000). Trust in an expert, an agency, or a corporation has been assumed to be determined by perceptions of a number of attributes, among them competence and expertise (Peters, Covello, and McCallum, 1997, referred to in Oltedal et al., 2004).

5.5.3 Safety culture

As shown in the previous sections, the concept of risk perception is connected to cognition, mental processes, sensemaking, and culture. According to Windschitl and Wells (1996), uncertainty is a psychological construct that "exists only in the mind; if a person's knowledge was complete, that person would have no uncertainty" (referred to in Sjöberg, Moen, and Rundmo, 2004, p. 7). As mentioned earlier, the cognitive (or cultural) aspects of institutions embody symbols – words, signs, and gestures – as well as cultural rules and frameworks that guide understanding of the nature of reality and the frames through which that meaning is developed (Hoffman, 1999). Geertz (1973) also concluded that culture is most effectively treated as a symbolic system. Symbols are the surface expression of the underlying cultural structure (Oltedal, 2011). According to Scott (1998), the term culture describes an attribute or quality internal to a group, and we can refer to an organizational culture or subculture. In this sense, culture is a fairly stable set of taken-for-granted assumptions, shared beliefs, meanings, and values that form a kind of backdrop for action (p. 132).

Employees' perceptions of organizational support, particularly management's commitment to safety in the organization, are often claimed to be a measure of an organization's safety climate. The terms safety culture and safety climate have often been used interchangeably, although safety culture is considered to be a more complex concept than safety climate, reflecting fundamental values, norms, assumptions, and expectations (Mearns and Flin, 2009, referred to in Skogdalen and Tveiten, 2011). Over time, consensus among industrial psychologists has emerged to differentiate safety climate as the surface features of an organization's safety culture, as discerned from the workforce's comprehension and perceptions at a given point in time. Subcultures possess cultural elements and influence the culture emerging from the interactions of the subcultures within an organization. Different employee groups can exhibit different safety attitudes/climate structures (Skogdalen and Tveiten, 2011).

The concept of safety culture was first used by the International Atomic Energy Agency's (IAEA's) International Nuclear Safety Advisory Group (INSAG), following the Chernobyl accident that occurred in 1986. More recently, several definitions of the safety culture concept have abounded in safety research and organizational literature. There are many different conceptual definitions, but they can, in general, be placed into two broad categories: the socio-anthropological perspective and the organizational psychology perspective. The socio-anthropological perspective suggests that a superficial research model of culture should be avoided so as to build cultural research on a deeper, more complex anthropological model. From an anthropological perspective, appropriate research methods include ethnography and field work, as well as qualitative in-depth studies based on interviews, observations, and/or participation. Within this perspective, culture is described with an emphasis on the organizational member's subjective interpretation and sensemaking (Oltedal, 2011).

From the organizational psychology perspective, one can argue that culture can be described with a limited number of dimensions, usually through large questionnaire surveys. From this perspective, the culture concept is assumed to express itself through an organizational climate, a set of perceptually based psychological attributes. The organizational psychology perspective provides a conceptual bridge among safety culture, safety behavior, and organizational safety management systems, with the aim of controlling, guiding, or directing first-line operators' attitude and behavior toward safe operations (Oltedal, 2011).

From a cultural perspective, safety policies are not important in themselves; the importance stems from how such policies, as symbols, make sense for the organizational members. This understanding of culture establishes a relationship between culture and climate; cultural beliefs and meaning given to organizational factors are reflected in actual behavior (Oltedal, 2011). Contrary to this, Antonsen (2009) questioned the degree to which some of this research fits into the term culture because it has been conceptualized within organizational theory, sociology, and anthropology. Antonsen concluded that the term safety culture should be used only as a conceptual label to denote the relationship between organizational culture and safety. The emphasis should be on organizational culture instead of safety culture, and this would give such studies a firmer theoretical foundation and richer empirical findings.

Guldenmund (2000), on the other hand, pointed out that most characteristics given to culture equally apply to climate, and in recent research it is becoming accepted to view climate as a reflection of an underlying culture. According to Oltedal (2011), organizational culture/climate is an integrated concept subject to change by organizational management practices and structures. One can assume that both organizational cultural and managerial features influence safety, which is defined as safety culture. Organizational safety culture is perceived as a concept with integrated parts from organizational management system practices and organizational culture/climate. The organizational safety culture is assumed to reflect the status of safety in the organization. Organizational safety, or safety culture, can be assessed by using two measurement outcome variables: risk perception and the state of the safety management system.

5.5.4 Management commitment and awareness

ICT safety and security is not purely a technical matter; it is highly dependent on the people and the organization surrounding the ICT system (Line and Tøndel, 2012). According to Reason (1997), commitment is a vital ingredient for managing the safety of an organization. Commitment has two main components: motivation and resources. The motivational issue is related to whether an organization seeks to be the domain model for good safety practices or whether it is simply content to keep one step ahead of the regulators. Top management can come and go, but a good safety culture endures beyond the top management. The second issue concerns the resources allocated to the achievement of safety goals. However, commitment will not suffice unless the organization has a correct awareness – or cognizance – of the dangers that threaten its operations. For cognizant organizations, a lengthy period without a bad accident does not signal the coming of peace. Rather, they see it as a period of heightened danger and so reform and strengthen their defenses accordingly (a common feature of a high reliability organization).

ICT safety and security awareness can be seen as the extent to which organizational members understand the importance of information safety and security, the level of safety and security required by the organization, and their individual safety and security responsibilities and act accordingly (ISF, 2005, referred to in Albrechtsen, 2007). Members of an organization may have inadequate ICT safety and security awareness if they are unfamiliar with possible threats to the systems and how to mitigate them, if they are unaware of the possible consequences of safety and security breaches, or if they see their own work in isolation and are unaware of the implications of their use of ICT systems (Albrechtsen and Hovden, 2009).

6. Research design, research methodology, and methods for data collection

This chapter describes the research design, research methodology, and research methods employed in the thesis. According to Yin (1994), a research design is the logic that links the data to be collected (and the conclusions to be drawn) to the initial questions of a study. The research design guides the researcher in the process of collecting, analyzing, and interpreting data. A methodology is a general approach to studying a research topic; it establishes how one will go about studying any phenomenon (Silverman, 1993). A methodology involves philosophical (i.e., worldview) assumptions that guide the direction of the collection and analysis of data (Creswell, 2011). A method focuses on the collecting and analyzing of data (Silverman, 1993).

According to Creswell (2003), three questions are central to the design of research:

1. What knowledge claims are being made by the researcher (including a theoretical perspective)?
2. What strategies of inquiry will inform the procedures?
3. What methods of data collection and analysis will be used?

These three elements of inquiry combine to form different approaches to research. These approaches are, in turn, translated into processes in the design of research, and using these three elements the researcher can identify a quantitative, qualitative, or mixed-methods approach to inquiry.

Stating a knowledge claim means that researchers start a project with certain assumptions about how they will learn and what they will learn during their inquiry. According to Creswell (2003), these claims are called paradigms, philosophical assumptions, epistemologies and ontologies, and broadly conceived research methodologies. Philosophically, researchers make claims about what knowledge is (ontology), how they know it (epistemology), what values go into it (axiology), how they write about it (rhetoric), and the process for studying it (methodology).

In this research project, the theoretical perspective I have chosen to apply has implications for the research design and methodology. The sociotechnical perspective on risk management, institutional organizational theory, and the chosen definition of institution (Scott’s omnibus conception of institutions) functioned as contextualization for the phenomena studied and as a structure for the thesis. As previously mentioned, modern societies contain many complexes of institutionalized rules and patterns (e.g., products of professional groups, the state, public opinion) and, according to Scott (1998), these are socially constructed realities which provide frameworks for the creation and elaboration of formal organizations. Furthermore, according to the theoretical approach employed in this thesis, technology’s effects on organizations are also socially constructed. These knowledge claims adhere to the perspective of social constructivism. Assumptions made by social constructivism are that meanings are constructed by human beings as they engage with the world they are interpreting. Humans engage with their world and make sense of it based on their historical and social perspective (Creswell, 2003).

However, another position about claims on knowledge is pragmatism. Instead of methods being important, pragmatists view the research problem as being most important, and researchers use all approaches to understand the problem. Pragmatism is not committed to any one system of philosophy and reality. Individual researchers are free to choose the methods, techniques, and procedures of research that best meet their needs and purposes (Creswell, 2003). As mentioned earlier, the use of institutionalism with other theories and topics rather than in isolation is, according to Greenwood et al. (2008), a conspicuous and significant strength. Institutional theory has an important capacity to stimulate contextualization. Institutional theory aids us in contextualizing the phenomena we study, whether that context encompasses regulatory, historical, political, cognitively tacit, or socially embedded settings. Such contextualization (which includes the understanding that knowledge is socially constructed within a broader context) is a distinguishing feature of institutional theory and research. As emphasized in Chapter 5, organizations are penetrated by environments and deeply embedded in institutional contexts. A given organization is supported and constrained by institutional forces. Moreover, a given organization incorporates a multitude of institutionalized features in the form of symbolic systems, relational systems, routines, and artifacts (e.g., technology) within their own boundaries.

I have chosen to use a mixed-methods research approach to achieve a deeper understanding of the organizational environment and all the different factors that may affect the safety and security management of network organizations. Pragmatism opens the door to multiple methods, different worldviews, and different assumptions, as well as different forms of data collection and analysis in the mixed-methods study (Creswell, 2003). Research on risk, safety, and security is in itself multidisciplinary, and multiple methodologies are applied within this research field. According to Mayring et al. (2007, referred to in Creswell, 2011), interdisciplinary research problems call for addressing complex issues using methodologies from both quantitative and qualitative research to bring diverse approaches to studies.

Simply put, quantitative methods are designed to collect numbers and qualitative methods are designed to collect words. In social science, the so-called positivist research methodology uses a set of procedures to define, count, and analyze its variables (quantitative hypothesis testing), and an interpretivist research methodology describes and illuminates the meaningful social world (studying social construction and meanings through qualitative hypothesis generation) (Silverman, 1993). The use of the term qualitative versus quantitative is sometimes discouraged because it creates a binary distinction that does not hold in practice (Creswell, 2011). Many methods can be used in either quantitative or qualitative research studies, including interviews (quantitative surveys to random samples or open-ended questions to small samples) and textual/document analysis (counting in terms of categories or understanding participants' categories). According to Silverman (1993), methods are specific research techniques which take on a specific meaning according to the methodology in which they are used. Writers in the mixed-methods field have tended to dismiss the dichotomy in favor of a continuum for presenting qualitative and quantitative differences (Creswell, 2011).

An enormous array of names and ways exist for conducting mixed-methods research. Some call it multi-methods, but writers in mixed methods are careful to distinguish "multi-method studies" in which multiple types of qualitative *or* quantitative data are collected from "mixed-methods studies" that incorporate collecting *both* qualitative and quantitative data. Creswell and Plano Clark (2007) suggested a parsimonious set of designs:

- Triangulation (or convergent) designs, which involve one phase of qualitative and quantitative data collection gathered concurrently.
- Explanatory or exploratory designs, which require two phases of data collection – quantitative data collection followed sequentially by qualitative data collection (or vice versa).
- Embedded designs, in which one form of data is embedded within another (may be either a single- or a double-phase design with concurrent or sequential approaches).

However, they now acknowledge that these designs are not sufficiently complex to mirror actual practice (Creswell, 2011).

According to Silverman (2006), triangulation involves using data produced by different methods to validate the data. Silverman also used the term combined approach (combining qualitative and quantitative approaches). Combined approaches can strengthen the validity of the study, as some of the findings complement and validate each other. Moreover, a combined approach can also reveal discrepancies between analysis results of data collected using different methods and thus may open new possibilities of interpretation.

Yin (1994) described three types of research design: exploratory, descriptive, and explanatory. The research design for this research project was explorative at the start of the study, and then became more descriptive. The data collection methods applied in this project (i.e., questionnaire survey, interviews, observation studies, document studies) were used for both explorative and descriptive purposes. In addition, the findings were discussed and tentatively explained by use of earlier research studies and theory.

The research design employed in this thesis was partly explorative and involved qualitative data collection followed by quantitative data collection. According to Creswell and Plano Clark (2007), the mixed method's central premise is that the use of quantitative and qualitative approaches, in combination, provides a better understanding of research problems than either approach alone. According to Greene (2007), mixed methods is an orientation toward looking at the social world that actively invites us to participate in dialogue about multiple ways of seeing and hearing, multiple ways of making sense of the social world, and multiple standpoints on what is important and to be valued and cherished (referred to in Creswell, 2011). This way of looking at the social world corresponds well with the institutional organizational perspective.

A quantitative research approach is one in which the investigator primarily uses positivist claims for developing knowledge (e.g., cause and effect thinking, reduction to specific variables and hypotheses and questions, use of measurement and observation), employs strategies of inquiry such as surveys, and collects data on predetermined instruments that yield statistical data. However, when conducting mixed-methods research, one can apply both predetermined and emerging methods, both open- and closed-ended questions, multiple forms of data drawing on all possibilities, and both statistical and text analysis (Creswell, 2003). Qualitative methods can provide a deeper understanding of the studied phenomenon, while quantitative methods simultaneously can show statistical associations and say something about how widespread certain patterns of behavior, attitudes, and perceptions are (Oltedal, 2011). Surveys are a practical way to gather large amounts of information, and they can be useful measurement tools within the field of social science for collecting data on human characteristics, perceptions, attitudes, thoughts, and behavior (Hagen, 2009). In studies of safety culture, risk perception, and attitudes, questionnaire surveys have often been used (see section 5.5.3).

Through the use of the questionnaire survey, I could obtain answers from as many of the chosen types of managers (ICT safety managers/coordinators and contingency planning managers) and employees (ICT staff and process control system operators) as possible. However, I chose to use mixed methods because I also wanted to study other, and perhaps different, views of the challenges for safety and security management of network companies due to increased use of ICT. The regulatory authorities, NVE (which is also responsible for supervision and performing regular inspections to ensure compliance with regulations), might have a different view of the challenges than managers and employees within the network organizations. In addition, documents and personal observations might also tell a different story than responses to survey questions.

Table 1 summarizes the titles of the four articles included in the thesis, the specific challenges for safety and security management of network companies and the research question(s) discussed in each article, the institutional aspect/element that mainly influences the challenges discussed in the articles, and the methods used to collect data for each of the four studies. The data collection methods were used to collect data for the whole research project, and subsequently the data material that gave the best basis for answering each research question was chosen by use of different approaches (e.g., factor analysis, study of previous research literature, qualitative interpretation) to be the data material for the respective study/article. Two of the articles in the thesis discuss challenges that can be influenced by cultural-cognitive elements/aspects of institutions, and emphasis is thus placed on the cultural-cognitive institutional pillar. This is consistent with the previously mentioned acknowledgment that the cultural-cognitive pillar provides the deeper foundations of institutional forms (i.e., the infrastructure on which not only beliefs, but also norms and rules rest). However, it is important to emphasize that the institutional aspects are in fact *analytical* and are intertwined and overlapping in real life.

Table 1. Article titles, challenges studied, research questions, institutional aspects/elements, and data collection methods.

Article title	**Challenge for safety management due to increased use of ICT**	**Research question(s)**	**Institutional aspect**	**Data collection method**
Article 1: Attitudes toward risk regulation – prescriptive or functional regulation?	Attitudes toward risk regulation	What can explain varying attitudes toward the use of functional internal control regulations as the principle for regulating risks?	Regulative aspects	Interviews Observation studies Document studies Questionnaire survey
Article 2: Strengths and weaknesses of technical standards for management of ICT safety and security in electric power supply network companies	Use of technical standards for ICT safety and security	What are strengths and weaknesses of technical standards for management of ICT safety and security?	Normative aspects	Questionnaire survey Interviews Document studies
Article 3: Risk perception regarding the safety and security of ICT systems in electric power supply network companies	Managers' and employees' risk perception regarding the safety and security of ICT systems in electric power supply network companies	What factors can influence the risk perception of users (managers and employees) within electric power supply network companies regarding the risk of malfunctions in or attacks on their ICT systems?	Cultural-cognitive aspects	Interviews Document studies Questionnaire survey
Article 4: Management commitment and awareness creation - ICT safety and security in electric power supply network companies	The degree of management commitment to ICT safety and security within network companies in the electric power supply sector and implementation of awareness creation and training measures for ICT safety and security within these companies	To what degree is the management of network companies in the electric power supply sector committed to the safety and security of their organizations' ICT systems? To what extent are awareness creation and training measures for ICT safety and security implemented within network companies in the electric power supply sector and what type of measures are implemented?	Cultural-cognitive aspects	Questionnaire survey Interviews Observation studies

6.1 Qualitative research methods

As mentioned, the research design employed in this thesis involved qualitative data collection followed by quantitative data collection. The qualitative research methods employed in this thesis were (1) interviews, (2) document studies, and (3) observation studies.

6.1.1 Interviews

To explore my research theme and produce research questions that could be tested by the quantitative questionnaire survey, qualitative data were gathered through two group interviews with representatives from NVE. Furthermore, some results from the interviews were later used to complement the data gathered through the survey.

For this part of the data collection, semi-structured interviews with open-ended questions were used. A semi-structured interview is a verbal interchange where the interviewer attempts to elicit information from another person (or several persons) by asking questions. Although the interviewer prepares a list of predetermined questions (interview guide), the interviews unfold in a conversational manner that offers participants the chance to explore issues they feel are important (Longhurst, 2010). The interviews were performed in collaboration with two master students who were writing their thesis in connection with this research project.

The interviewees were representatives from the contingency planning department in NVE who are responsible for safety, contingency planning, and supervision in the Norwegian electric power supply sector. The first group interview was conducted with three interviewees, and the questions mainly focused on the interviewees' opinion of the Norwegian network companies' risk perception and awareness regarding the risk of electric network failure caused by malfunctions in or attacks on their ICT systems. The second group interview was conducted with two interviewees, and the questions mainly focused on the interviewees' opinion regarding the use of functional internal control regulations for ICT safety and security and their impression of the network companies' attitude toward these regulations.

In addition, a master's thesis was written in connection with this research project, which provided qualitative data from six interviews with representatives from a sample of Norwegian network companies and NVE (Røyksund, 2011). This interview study included questions about risk perception concerning attacks on the network companies' ICT systems (cyber crime) and which ICT safety and security measures were implemented in the organizations. The data results from these interviews were used to supplement the results from my study.

6.1.2 Document studies

Document studies can provide valuable insights into understanding a studied social phenomenon. Document study is an indirect method of data collection that does not require participation of the subjects involved, and by documents I mean any written materials that contain information about the phenomenon I wish to study (Bailey, 1994). I did not perform a document *analysis* where the content of the document was coded into themes and analyzed, but rather a document *study* where I thoroughly read through all the documents and made notes of content that was important in relation to my study.

The documents studied in my research project gave me valuable insight into electric power supply systems and the ICT systems (process control systems/SCADA systems) that run and control them, threats toward these systems, and risk regulations for these systems. Data were collected from a wide array of written documents:

- Norwegian Defense Research Establishment (FFI): "Protection of the Society 3/Measures to Reduce Vulnerabilities in the Electric Power Supply," Final Report BAS3 [“En sårbar kraftforsyning”, Sluttrapport etter BAS3]
- Norwegian Defense Research Establishment (FFI): “Protection of the Society 5/Vulnerability in Critical ICT Systems,” Final Report BAS 5 [“Sårbarhet i kritiske IKT-systemer”, Sluttrapport etter BAS5]
- Report – “Society’s vulnerability,” Vulnerability Commission (NOU 2000:24) [NOU 2000:24 – Sårbarhetsutvalget]
- Report – “Protection of critical infrastructures and critical societal functions in Norway,” Infrastructure Commission (NOU 2006: 6) [NOU 2006:6 – Infrastrukturutvalget]
- White Paper 17 (2001-2002) - Societal Security (Safety). The Road to a Less Vulnerable Society. [St.meld. nr. 17 (2001–2002) - Samfunnssikkerhet. Veien til et mindre sårbart samfunn]
- White Paper 22 (2007-2008) – Societal Security (Safety) [St.meld. nr. 22 (2007–2008) - Samfunnssikkerhet, samvirke og samordning]
- White Paper 29 (2011-2012) – Societal Security (Safety) [St.meld. 29 (2011-2012) – Samfunnssikkerhet]
- Regulations relating to contingency planning in the Norwegian electric power supply system (The contingency planning regulations), 2002 and 2013 [Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (Beredskapsforskriften), 2002 og 2013]
- “Guidelines for the contingency planning regulations in the Norwegian electric power supply system,” NVE, 2003, 2011 and 2013 [“Veiledning til forskrift om beredskap i kraftforsyningen”, NVE , 2003, 2011, 2013]
- “Guideline for risk and vulnerability analysis in the electric power supply system,” NVE and Proactima, 2010 [Veiledning til ROS-analyser for kraftforsyningen, NVE og Proactima , 2010]
- “The Norwegian energy regulator - Annual report,” NVE , 2011 [Årsrapport, NVE, 2011]
- Annual supervision reports, NVE, 2010, 2011, 2012 and 2013 [Årsrapporter for tilsyn, NVE, 2010, 2011, 2012 og 2013]
- Presentations by representatives from NVE at various conferences on ICT safety and security for companies in the Norwegian electric power supply sector (http://www.norsis.no/vedlegg/KraftIS/ and http://www.nve.no/no/Om-NVE/Presentasjoner-fra-NVE-arrangement/)
- “Cyber Security Strategy for Norway”, 2012 [Nasjonal strategi for informasjonssikkerhet, 2012]

- "Action plan for the Cyber Security Strategy," Norway, 2012 [Handlingsplan for Nasjonal strategi for informasjonssikkerhet, 2012]
- "Norwegian Computer Crime and Security Survey," NSR, 2006, 2010, 2012 [Mørketallsundersøkelsen, 2006, 2010, 2012]
- OECD – "Emerging Systemic Risks" (2003), "OECD Studies in Risk Management, Norway – Information Security" (2006), "Innovation in Country Risk Management" (2009), "Future Global Shocks" (2011a), "Reducing Systemic Cybersecurity Risk" (2011b)
- EU – The GRID Consortium, "ICT Vulnerabilities of Power Systems: A Roadmap for Future Research", 2007
- National Institute of Standards and Technology (NIST), "Guide to Industrial Control Systems (ICS) Security," U.S. Department of Commerce, 2011
- FOCUS 2012 and 2013, Annual Assessment by the Norwegian Intelligence Service (NIS), [FOKUS 2012 og 2013, Etterretningstjenestens åpne vurdering]
- Annual Threat Assessment, The Norwegian Police Security Service (PST), 2012 [PSTs årlige trusselvurdering, 2012]
- Newspaper articles – Dagbladet ”No CTRL” [”Null CTRL”], Teknisk Ukeblad, etc.

6.1.3 Observation studies

Observational techniques are methods of collecting data by observing people, most typically in their natural setting. Participant observation is performed by observers who take part in the activities of the people they are studying, and nonparticipant observation is conducted by those who remain as aloof as possible. Observation can be useful when you don't know that much about the subject you are investigating and may also make sense when one wants to understand experience from the point of view of those who are living it or from the context in which it is lived. One of the defining characteristics of observational techniques is their relative unobtrusiveness. However, this unobtrusiveness varies with the role played by the observers and with the degree to which they are open about their research purposes (Adler and Clark, 2014).

Gold's (1958) typology of researcher roles suggests a continuum of possible roles: the complete participant, the participant-as-observer, the observer-as-participant, and the complete observer. Gold's typology also suggests a continuum in the degree to which the researcher is open about his or her research purpose. A complete participant is, or is pretending to be, a genuine participant in the situation he or she observes. A participant-as-observer is primarily a participant, but at the same time admits to an observer status. An observer-as-participant is primarily a self-professed observer, but occasionally participates in the situation. A complete observer is an observer who does not become a part of the situation (Adler and Clark, 2014).

During my research project, observation studies were carried out at two conferences on ICT safety and security for companies within the electric power supply sector, held in Norway in 2011.[17] The participants at both conferences were mainly managers and employees working with ICT safety and security within network companies in Norway, in addition to vendors of process control systems (e.g., SCADA systems) and ICT safety and security solutions for these systems (e.g., ABB and Siemens). The speakers at the conferences included representatives from NVE, NorCERT, Mnemonic AS (one of the largest providers of IT information security services in the Nordic region), Norwegian Centre for Information Security (NorSIS), and ICT safety and security researchers from universities and research institutes. During the observation studies, I observed the types of ICT safety and security issues raised at the conferences, the types of issues on which participants focused, and the types of questions and discussions that came up during the conferences.

In my observation studies, I took on an observer-as-participant role. I listened to the presentations and discussions at the conference and made notes of important issues that were discussed, comments that were made, and arguments that were used, but I did not participate in the discussions. However, during the conferences, I also talked to conference participants and organizers during breaks, during lunches, and during the conference dinners. I discussed the studies I was doing in my PhD project and different issues related to my research purpose and research questions.

6.2 Quantitative research methods

The main data collection method in the thesis was a questionnaire survey which was sent to managers and employees in network companies within the Norwegian electric power supply sector.

6.2.1 Questionnaire development

Abstract constructs cannot be directly observed but are measured through the use of attributes or indicators derived from construct clarification and definition. To operationalize a construct is to define a construct in such a way that it can be measured or identified. Empirical indicators become the items or categories of items on the instrument (Pett, Lackey, and Sullivan, 2003). The starting point when developing a questionnaire and scales is a conceptual definition, which specifies the theoretical basis. When generating the item pool, each item making up a construct should reflect the latent variables underlying the theme (Oltedal, 2011).

I designed the questionnaire for this research project based on a review of previous research literature, document studies of the contingency planning regulations for the Norwegian electric power supply system, and an evaluation of five preexisting questionnaires. The preexisting questionnaires were previously used in studies of offshore (petroleum) safety and ICT safety.[18] As previously mentioned, the questionnaire was designed to be both explorative and descriptive with

[17] Kraft IS (2011) and Forum for informasjonssikkerhet i kraftforsyningen (2011).

[18] The five previously used questionnaires were the “Offshore Safety Questionnaire” (Robert Gordon University, Aberdeen, 1997), Norwegian Petroleum Safety Authorities’ survey “Trends in risk level – Norwegian Shelf” (2007-2008), “Accident prevention – survey for offshore employees” (survey used in PhD project, Centre of Maritime Health and Safety, Syddansk Universitet, Hanna B. Rasmussen, 2008-2012),“The Norwegian Computer Crime and Security Survey” (2010), and questions used in Janne M. Hagen’s study "How do employees comply with security policy? A comparative case study of four organizations under the Norwegian Security Act" in *The Human Factor behind the Security Perimeter. Evaluating the Effectiveness of Organizational Information Security Measures and Employees' Contributions to Security*, Faculty of Mathematics and Natural Sciences, University of Oslo, Oslo, doctoral dissertation, 2009.

regard to possible challenges for safety and security management due to increased use of ICT and, hence, it contained a large number of items.

The questionnaire contained 97 items, divided into 10 sections: background information, knowledge of safety and security, perception of compliance, attitude toward safety, attitude toward regulation, experience of incidents, risk perception, safety and security management, awareness creation and training, and an overall rating of the safety and security level of the organizations' ICT systems. Most of the constructs were measured on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Risk perception was measured on a 6-point Likert scale ranging from 1 (very low risk) to 6 (very high risk), and the overall rating of the safety level of the organizations' ICT systems was measured on a 6-point Likert scale ranging from 1 (very poor) to 6 (very good).

Likert scales are summated rating scales that can be used to measure opinions, beliefs, and attitudes. The scales consist of a set of items that purports to measure a specific construct and are typically summed across items to obtain a single score. An odd number of items allows for the middle scale step to be the neutral, or indifferent, point. Even numbered scale steps force the subject to either agree or disagree to some extent (Pett, Lackey, and Sullivan, 2003). A 6-point scale was chosen for the risk perception scale and the overall rating of the safety level of the organizations' ICT systems to remove the possibility of crossing out the "neutral" middle point. Most of the other scales also included the response alternatives "Don't know" and/or "Not relevant."

The background information section included questions about sex, age, job category (contingency planning manager, ICT safety manager, operator in system control center, employee in ICT staff, "Other"), length of employment (under 1 year, 1-3 years, 3-5 years, 5-10 years, and more than 10 years), company size (more than 100 employees and fewer than 100 employees[19]), company type (corporation, cooperative, partnership, company owned by local authorities, "Other"), type of business activity (transmission/distribution, transmission/distribution and generation/production, transmission/distribution and supply, and transmission/distribution, generation/production, and supply), and classification of process control system/SCADA system (class 1, class 2, class 3, or a combination).

The knowledge of safety and security scale contained five items regarding the respondents' knowledge of ICT safety and security. Examples of items in this scale include "I am familiar with the content of Chapter 6 regarding ICT safety and security in the guidelines for the regulations relating to contingency planning in the Norwegian power supply system," "I am familiar with the content of my organization's information security policy," and "I have access to the information necessary to make decisions regarding ICT safety."

The perception of compliance scale contained 25 items measuring the respondents' perception of compliance with ICT regulations and rules in their organization (not only their own compliance). The scale included items about risk and vulnerability analysis, use of checklists, guidelines, and ICT safety

[19] In this study, I chose to measure the difference between large and small organizations by "more than 100 employees" versus "fewer than 100 employees." Organizational size could also have been measured in different ways (e.g., by the number of customers, by income). This might have affected the results of the statistical analysis.

and security standards, contingency plans, system descriptions, emergency drills, reporting of incidents, antivirus software, and physical safety and security measures for system control centers and servers, among others.

The attitude toward safety and security scale contained nine items measuring the respondents' attitude toward safety and security. Examples of items in this scale include "I think it is important to read the organization's contingency plan, ICT safety policy, and ICT safety instructions to achieve updated knowledge of ICT safety and security," "I can do my job faster if I ignore some of the ICT safety and security rules," and "There is a good attitude toward ICT safety and security in this organization."

The attitude toward regulation scale contained four items regarding the respondents' attitude toward the obligations regarding ICT safety and security within the contingency planning regulations for the Norwegian electric power supply sector. Examples of items in this scale include "I think it's ok that the authorities prescribe the overall safety goals and obligations regarding ICT safety and security and permit the organizations to find and develop their own means to achieve these goals" and "In connection with the introduction of Advanced Metering Infrastructure (AMI) in the Norwegian electric power supply system, I wish that the network companies could receive more detailed guidelines from the authorities."

The experience of incidents section included 13 different incidents to which an organization can be exposed, and the respondents were asked to report the incidents that their organization had experienced. The list of incidents was created on the basis of the contingency planning regulations for the Norwegian electric power supply sector and on questions and results from the Norwegian Computer Crime and Security Survey (2010). The incidents included hacking, information theft, DoS attacks, malware, theft of ICT equipment, blackmail, unauthorized change/deletion of data, pirate copying, loss of personal information, abuse of ICT resources, and ICT system malfunctions caused by technical failure, natural hazards, or human error. The response alternatives for this section were "Yes," "No," and "Don't know."

The risk perception scale contained 21 items addressing the respondent's perception of the risk posed by different threats and vulnerabilities. The set of threats and vulnerabilities was created on the basis of the contingency planning regulations for the Norwegian electric power supply sector and on questions and results from the Norwegian Computer Crime and Security Survey (2010). The listed threats and vulnerabilities included malicious attacks from outside the organization, such as hacking, DoS attacks, malware, information theft, unauthorized change/deletion of data, pirate copying, blackmail, and ICT attacks from terrorists or foreign states, users as a vulnerability due to their lack of skills and knowledge (human error), theft of personal information (phishing), theft of ICT equipment, abuse of ICT resources, ICT malfunctions caused by technical failure or natural hazards, sabotage against power lines or power stations, and ICT attacks from insiders/disgruntled employees.

The safety and security management scale contained five items measuring the management's commitment to ICT safety and security in the network organizations. Examples of items in this scale are "My immediate manager intervenes immediately if the ICT safety and security rules are not followed," "My immediate manager appreciates my pointing out matters of importance to ICT safety and security," and "I would rather not discuss ICT safety and security with my immediate manager."

The section about ICT safety and security awareness and training contained six items regarding the use of different awareness-creating activities in the network organizations. Examples of items include "New employees get thorough training in the organization's ICT safety and security rules (included in the organization's ICT safety and security policy and safety/security instructions)," "ICT safety and security training for managers and employees is implemented when the ICT systems are updated or altered," "In my organization, awareness campaigns about ICT safety and security are held regularly," and "In my organization, e-mails containing information about ICT safety and security are sent out on a regular basis to raise awareness about this issue."

The overall rating of the safety and security level of the organizations' ICT systems contained the question: "All in all, how would you assess the safety and security of the ICT systems used in your organization?" A copy of the questionnaire is provided in Appendix 1.

6.2.2 Web-based questionnaire

The questionnaire survey was developed as a web-based questionnaire using QuestBack Survey (an online survey and feedback platform) and distributed to the respondents by e-mail. The Internet is increasingly seen as offering many advantages over more traditional paper and pencil administration of questionnaires (e.g., reduced cost, ease and speed of administration). Responsibility can be passed to the platform to save the data in a format that may then be imported directly into the software package that is to be used for data analysis (in this case SPSS). Time is saved by not having to split the data manually and the possibility of errors when splitting the data is practically eradicated. A major benefit of web-based questionnaires and surveys is that they do not require the administration of materials in person; thus, the questionnaire administration and recording of responses are self-running. When questionnaires are not administered in person, it is important that the respondents interpret the questions in the manner in which the researcher intended. Respondents to web-based questionnaires do not have someone at hand to check the exact meaning of a sentence (Fox, Murray, and Warm, 2003). I therefore performed a pilot test of the questionnaire before the questionnaire was completed to make sure that the instructions and scale items were clear. The pilot was sent to three respondents: one contingency planning manager, one ICT safety manager, and one system control center operator.

A few minor revisions were made to the questionnaire based on the feedback from the pilot test. The revisions included adding my chosen definition of risk in this research project to the instructions. Risk is a contested term with many different definitions, and clearly stating how I defined the concept of risk made it easier for the respondents to answer the questionnaire. In addition, I added an open-ended question at the end of the questionnaire, where the respondents were given the opportunity to make any comments they might have concerning the issues raised in the questionnaire or about the questionnaire itself. Furthermore, I defined all other relevant concepts in the questionnaire guidelines and explained the purpose of the study. I also added an informative text for each of the scales in the questionnaire. The survey was distributed to respondents in June 2012 and was closed in September 2012. Questionnaire guidelines and information about the aims of the study were included in the e-mail containing the survey, and two e-mail reminders were sent to the respondents before access to the questionnaire was closed.

6.2.3 Survey sample and respondents' demographics

Methods of sampling a population to gain data that are representative of the target population are always a consideration in a research project (Fox, Murray, and Warm, 2003). With the help of sampling, a target population is selected and a target group is invited to answer carefully structured questions (Hagen, 2009). The chosen target population for this research project was managers and employees in Norwegian electric power supply network companies, mainly contingency planning managers, ICT safety and security managers, operators in system control centers, and employees in ICT staff.

The survey was sent to managers in all the 137 network companies that were part of the PSPO. Names and e-mail addresses for ICT safety and security managers and contingency planning managers in all the network companies were provided by NVE. In addition to answering the questionnaire, the managers were asked to provide names and e-mail addresses for employees in their organization's system control centers and ICT staff, as well as any other managers or employees who could be relevant as respondents for this survey. The web-based questionnaire was distributed by e-mail to 334 individuals.

One hundred and three respondents returned the survey questionnaire, for a response rate of 31%. Demographic profiles of the respondents in this research project are shown in Tables 2 through 6.

Table 2. Demographic profiles of the respondents divided by job category.

Job category	**Percentage**	**N**
1 Contingency planning manager	23.3%	24
2 ICT safety and security manager	23.3%	24
3 Operator in system control center	15.5%	16
4 ICT staff	7.8%	8
5 Other	30.1%	31
Total		103

Table 3. Demographic profiles of the respondents divided by company size.

Company size	**Percentage**	**N**
1 More than 100 employees	37.0%	37
2 Less than 100 employees	63.0%	63
-1 Don't know	0.0%	0
Total		100

Table 4. Demographic profiles of the respondents divided by company type.

Company type	**Percentage**	**N**
1 Corporation (AS-ASA)	80.4%	82
2 Cooperative (Andelslag)	2.9%	3
3 Partnership (Ansvarlig selskap)	2.0%	2
4 Company owned by local authorities (Kommunal, fylkeskommunal eller interkommunal bedrift)	6.9%	7
5 Other	7.8%	8
-1 Don't know	0.0%	0
Total		102

Table 5. Demographic profiles of the respondents divided by classification of process control system (SCADA system).

Classification of process control system	**Percentage**	**N**
1 Class 1	40.8%	42
2 Class 2	28.2%	29
3 Class 3	30.1%	31
-1 Don't know	12.6%	13
Total		103

Table 6. Demographic profiles of respondents divided by job category, company size, and gender.

Job category[3]			**Company size**		**Total**
			More than 100 employees	Fewer than 100 employees	
Manager	Gender	Male	19	44	63
		Female	1	1	2
	Total		20	45	65[1]
Employee	Gender	Male	14	15	29
		Female	1	0	1
	Total		15	15	30[1]
Other	Gender	Male	2	3	5
	Total		2	3	5
Total	Gender	Male	35	62	97
		Female[2]	2	1	3
	Total		37	63	100

[1] Three respondents (one manager and two employees) did not answer the item regarding company size.

[2] Only three of the respondents were female and the rest male; however, this corresponds well with the gender distribution of employees in Norwegian network companies.

[3] The categorical variable "Job category" was collapsed into two categories representing managers and employees.

6.2.4 Statistical analysis

The Statistical Package for the Social Sciences (SPSS) v. 18 was used to perform the statistical analysis in the research project. Negatively worded items were reversed, and total scale scores were calculated to provide overall scores for the scales used in the survey. Since it is quite rare to obtain complete data from every case when we do research with human beings, it is important to consider how to deal with missing values in the statistical analyses. In my analyses, I chose to use the "Exclude cases pairwise" option in SPSS, which excludes the cases (respondents) only if they are missing the data required for the specific analysis. These cases were still included in any analyses for which they had the necessary information (Pallant, 2010).

6.2.5 Factor analysis

Factor analysis can be used for assessing construct validity of an instrument for data collection. This type of analysis represents a complex array of structure-analyzing procedures used to identify the interrelationships among a large set of observed variables (items) and, through data reduction, group a smaller set of these variables into dimensions or factors that have common characteristics. A factor is a linear combination or cluster of related observed variables that represents a specific underlying dimension of a construct, which is as distinct as possible from the other factors included in the solution. The factor analysis process generally involves two stages: defining the number of initial factors and rotating the factors to improve interpretation. Exploratory factor analysis (EFA) was chosen to explore the underlying dimensions of the constructs of interest in this research project, and principal component analysis (PCA) was chosen as the factor extraction method (Pett, Lackey, and Sullivan, 2003).

PCA with direct oblimin rotation finally resulted in a two-factor solution, where Factor 1 was named "Risk perception" and Factor 2 was named "Safety and security management, awareness creation, and training." After further analysis, Factor 2 was divided into two smaller factors named "Safety and security management" (Factor A) and "Awareness creation and training" (Factor B). The risk perception scale (Factor 1) was analyzed as data material for article 3, and the safety and security management scale and the awareness creation and training scale (Factor 2) were analyzed as data material for article 4. The four items on the attitude toward regulation scale were also retained as data material for the research project, and descriptive statistics for each item were used for article 1. In addition, the three aforementioned items from the perception of compliance scale were retained (items 3, 7, and 8). Descriptive statistics for each of these three items were used as data material for article 2. Finally, I also decided to keep the data from the knowledge of safety and security scale, which is discussed in article 3. A more thorough description of the factor analysis is provided in Appendix 2.

6.2.6 Correlation

Correlation analysis is used to explore the association between pairs of variables. Correlation provides an indication that there is a relationship between two variables; however, it does not indicate that one variable causes the other. In this research project, correlation analysis (bivariate) was performed to explore the relationships between some of the continuous variables in the studies, i.e., between risk perception and safety and security knowledge (article 3) and between safety and security management (management commitment) and awareness creation and training (article 4). Pearson product-moment correlation coefficients (r) were obtained and interpreted to describe the strength and direction of the linear relationships between the two variables. Pearson correlation coefficients take on values from -1 to +1. A positive correlation indicates that as one variable increases, so does the other, and a negative correlation indicates that as one variable increases, the other decreases (Pallant, 2010).

Finally, the size of the absolute value (r) provides an indication of the strength of the relationship. Various authors have suggested different interpretations of the values between 0 and 1; however, in this research project, I chose to interpret the strength of the correlation according to Cohen's guidelines from 1988: small correlation – r=.10 to .29, medium correlation – r=.30 to .49, and large correlation – r=.50 to 1.0 (Pallant, 2010, p. 134).

6.2.7 Statistical techniques to compare groups

A lot of techniques can be used to test for differences between groups. Parametric techniques make a number of assumptions about the population from which the sample has been drawn and the nature of the data. Non-parametric techniques, on the other hand, do not make the same assumptions and are often seen as more suitable techniques for smaller samples or when the collected data are measured at the ordinal (ranked) level. In this thesis, I chose to use analysis of variance (ANOVA) and t-tests, which are parametric techniques.[20] These techniques indicate whether the difference between the groups is "statistically significant" (i.e., not likely to have occurred by chance) (Pallant, 2010).

Some general assumptions apply to parametric techniques. These techniques assume that the dependent variable is measured at the interval or ratio level (i.e., using a continuous scale) (Pallant, 2010). In this thesis, the dependent variables I tested using these statistical techniques were all continuous variables (i.e., attitude toward regulations, risk perception, safety and security management, awareness creation and training, items regarding the use of standards, guidelines, and checklists for ICT safety and security). These techniques also assume that the scores are obtained using a random sample from the population. However, this is often not the case in real-life research (Pallant, 2010). How the sample for my survey was chosen is described in section 6.2.3.

Another assumption is that the observations that make up the data must be independent from one another (i.e., no observation or measurement is influenced by any other observation or measurement). The respondents in my survey were spread out in many different organizations, and thus I do not think this will be an issue in this research project. For parametric techniques, it is also assumed that the populations from which the samples are taken are normally distributed.[21] In a lot of research (particularly social science research as in this thesis), scores on the dependent variables are not normally distributed. However, according to Pallant (2010), most of the techniques are reasonably "robust" or tolerant of violations of this assumption, and with large enough sample sizes (e.g., 30+), the violation should not cause any major problems. The size of the sample in this survey was 103, and thus I assume that violation of this assumption does not cause a problem for the analysis of my data.

The parametric techniques I have applied in this research project also assume that samples are obtained from populations of equal variances (i.e., the variability of scores for each of the groups is

[20] Non-parametric techniques were tried as well; however, the results of the analysis with both parametric and non-parametric techniques showed similar results.

[21] Normal is used to describe a symmetrical, bell-shaped curve, which has the greatest frequency of scores in the middle with smaller frequencies toward the extremes (Pallant, 2010).

similar). As part of the t-test and ANOVA analyses, SPSS performs Levene’s test for equality of variances. If the significance value obtained is less than .05, it suggests that variances for the two groups are not equal and that the assumption of homogeneity of variance is violated. However, according to Pallant (2010), analysis of variance is reasonably robust to violations of this assumption, provided the size of the groups is reasonably similar. In addition, when you perform t-tests in SPSS, you are provided with two sets of results, for situations where the assumption is not violated and for when it is violated. In this case, one can consult whichever set of results is appropriate for the data.

The purpose of t-tests and ANOVA procedures is to test hypotheses, and in this type of analysis two different errors are possible. It is possible to reject the null hypothesis (the null hypothesis is a hypothesis which the researcher tries to disprove, reject, or nullify) when it is, in fact, true (type 1 error). This occurs when we think there is a difference between our groups, but there actually is not. This possibility can be minimized by selecting an appropriate alpha level (two levels often used are .05 and .01). The second type of error is failing to reject a null hypothesis when it is, in fact, false. This happens when we believe that the groups do not differ when they do. Several factors can influence the power of a test (if the test can correctly identify whether there is a difference between groups) in a given situation, including the alpha level set by the researcher (as mentioned above), sample size, and effect size (Pallant, 2010).

The power of a test depends on the sample size; however, according to Stevens (1996, referred to in Pallant, 2010) “power is not an issue” when the sample size is large (e.g., 100 or more respondents). As mentioned, the sample size of my survey was 103 respondents. Post-hoc comparisons are designed to guard against the possibility of an increased type 1 error. Post-hoc comparisons can be used when conducting a whole set of comparisons, exploring the differences between each of the groups in the study. Analysis of variance does not tell us which group differs from which other group, and one way to find out is to conduct post-hoc tests. An overall F ratio is calculated in SPSS that indicates whether there are any significant differences among the groups in the design. If the overall F is significant, researchers can then go on and perform additional tests to identify where these differences occur. Post-hoc comparisons guard against type 1 errors due to the large number of different comparisons being made. This is done by setting more stringent criteria for significance and, therefore, it is often more difficult to achieve significance. Several post-hoc tests can be used. In this research project, I have chosen to use the post-hoc test Tukey, which is available in SPSS (Pallant, 2010).

Probability values do not indicate the degree to which the variables are associated with one another. Very small differences between groups may become statistically significant (especially in large samples); however, this does not mean that the difference has any practical or theoretical significance. One way to assess the importance of findings is to calculate the “effect size” (strength of association). This is a set of statistics that indicates the relative magnitude of the differences between means, or the amount of the total variance in the dependent variable that is predictable from knowledge of the levels of the independent variable (not just whether the difference could have occurred by chance). Several different effect size statistics exist, and in this research project I have chosen to use partial eta squared effect size statistics (eta squared). Eta squared indicates the proportion of variance of the dependent variable that is explained by the independent variable (values can range from 0 to 1). To interpret the strength of the different effect size statistics, I used the guidelines proposed by Cohen (1988): .01=small effect, .06=moderate effect, .14= large effect (Pallant, 2010).

6.2.7.1 ANOVA

One-way between-groups ANOVA is used to compare the mean scores of several groups (more than two groups). One-way between groups ANOVA is used when you have one independent (grouping variable) with three or more groups and one dependent continuous variable. "One-way" indicates only one independent variable, and "between groups" means that different participants are in each of the groups. An F ratio is calculated, which represents the variance between the groups divided by the variance within the groups. If the F ratio is large, it indicates more variability between the groups (caused by the independent variable) than there is within each group (referred to as the error term). A significant F test will indicate that we can reject the null hypothesis, which states that the population means are equal. If the Sig. value (p value) is less than or equal to .05 (e.g., .03, .001), there is a significant difference somewhere among the mean scores on the dependent variable for the different groups (Pallant, 2010).

One-way between-groups ANOVA with post-hoc tests (i.e., Tukey) were carried out to explore any differences between the mean scores on the main variables in my survey (attitude toward regulation, risk perception, safety and security management (management commitment), and awareness creation and training) for the different company types in the data material (i.e., corporations, cooperatives, partnerships, companies owned by local authorities, and other). The same techniques were used to explore any differences between the different job categories, i.e., contingency planning manager, ICT safety and security manager, operator in system control center, employee in ICT staff, and other.

6.2.7.2 T-tests

After the ANOVA, the categorical variable "job category" was collapsed into two categories representing managers and employees. The category "managers" consisted of contingency planning manager, ICT safety and security manager, and "other leader" and the category "employees" consisted of operator in system control center, employee in ICT staff, and "other employee."

Independent-samples t-tests were then performed to determine whether there were significant differences between the mean scores of managers versus employees and big companies versus small companies on the main variables in this study (i.e., attitude toward regulation, risk perception, safety and security management (management commitment), and awareness creation and training). T-tests were used to compare the scores of managers versus employees, and big companies versus small companies, on the different variables. To find out whether there was a significant difference between my two groups, I referred to the column labeled Sig. (2-tailed), which appears under the section labeled t-test for "Equality of Means" in SPSS. If the value in the column was equal to or less than .05, there was a significant difference in the mean scores on my dependent variable for each of the two groups. If the value was above .05, there was no significant difference between the two groups. SPSS does not provide eta squared values for t-tests; however, effect size was calculated using the information provided in the output (Pallant, 2010).

6.3 Reliability, validity, trustworthiness, and ethical considerations

Reliability, validity, and trustworthiness are important issues related to research findings. Reliability is the extent to which another researcher would find the same answer and describes the consistency or repeatability of the research that has been performed. Validity is based on the positivist paradigm and says something about the confidence or strength of results. Trustworthiness is based on the constructivist paradigm, and important trustworthiness criteria are credibility and transferability (Johnsen, 2012).

6.3.1 Reliability and validity - quantitative research studies

In quantitative studies, researchers advance the relationships among variables and pose this in terms of questions or hypotheses. Being objective is an essential aspect of competent inquiry, and for this reason researchers must examine methods and conclusions for bias. Standards of reliability and validity are important in quantitative research (Creswell, 2003).

According to Yin (1994), reliability means demonstrating that the operations of a study, such as the data collection procedures, can be repeated with the same results. A major benefit of using web-based questionnaires is the reliability of data input. The platform records the data directly, thereby eradicating transcription errors. The cost benefits of this are apparent in terms of the time it takes to input data (Fox, Murray, and Warm, 2003). For my survey, Questback produced an SPSS data sheet that could be imported directly into SPSS for further analysis. Nevertheless, to make sure that there were no mistakes, I thoroughly checked my data set for errors, following the advice of Pallant (2010, pp. 43-49).

Content validity is the degree to which elements of the measurement are relevant to and representative of the underlying concept. Determining whether the scale or item set has good content validity can be accomplished using a number of sources of relevant theory, empirical literature, and expert judgment. As mentioned in section 6.2.1, I designed the questionnaire for this research project based on a theoretical review, document studies of the contingency planning regulations for the Norwegian electric power supply system, and an evaluation of five preexisting questionnaires.

The validity of a scale refers to the degree to which it measures what it is supposed to measure (Pallant, 2010). Construct validity concerns the degree to which inferences can legitimately be made from the operationalized constructs in the questionnaire to the theoretical concepts on which those operationalizations were based (Oltedal, 2011). As previously described in section 6.2.5, factor analysis was used for assessing construct validity of the instrument for data collection (questionnaire survey). The extracted factors are assumed to have good discriminant validity (i.e., the degree to which the items in different subscales measure different rather than the same construct) and convergent validity (i.e., the degree to which the items within a particular subscale measure the same unidimensional construct).

The reliability of a scale indicates how free it is from random error. A frequently used indicator of a scale’s reliability is internal consistency (or convergent validity). As mentioned, internal consistency is the degree to which the items that make up the scale are all measuring the same underlying attribute (i.e., the extent to which the items “hang together”). The most commonly used statistic for measuring internal consistency is Cronbach’s coefficient alpha. This statistic provides an indication of the average correlation among all the items that make up the scale. Values range from 0 to 1, with higher values indicating greater reliability. Nunnally (1978) recommended a minimum level of .7 (referred to in Pallant, 2010). Reliability tests of the scales and factors in my survey indicate that they have good internal consistency. Cronbach's alpha coefficient was .95 for Factor 1 (risk perception) and .90 for Factor 2 (safety and security management, awareness creation, and training). For the two smaller factors, the Cronbach's alpha coefficient was .85 for Factor A (safety and security management) and .84 for Factor B (awareness creation and training). For the knowledge of safety and security scale, Cronbach's alpha was .83.

External validity documents whether the results can be generalized from the research context to a more general setting (i.e., the domain of applicability of the research results) (Johnsen, 2012). My survey sample of 103 respondents can be considered a relatively small sample and may limit the potential for generalizing. Nevertheless, according to Pallant (2010, p. 207), a sample of 100+ respondents can be regarded as a large sample, and the sample size can be seen as adequate for the types of data analyses done in my study (i.e., factor analysis, correlation, t-tests, ANOVA, and descriptive statistics). According to Fricker and Schonlau (2002), response rates for web surveys where no other survey mode is given have tended to range from moderate to poor. Other researchers have also experienced the same response rate problem in studies of information security management. Kotulic and Clark (2004) followed up their small response rate with a study suggesting that the main reasons for non-responses were related to a policy of not sharing information regarding their information security performance, the volume of survey requests received by the organizations, and a desire not to spend valuable time on the particular research project (referred to in Albrechtsen and Hovden, 2009). According to feedback to NVE from some of the network companies, the same seems to apply for the present survey. Managers and employees in the network companies are reluctant to answer questions about ICT safety and security in their organizations. Another factor that may have affected the response rate for my survey was that the questionnaire was sent out during the summer (from June to September) when many of the potential respondents were on vacation. However, due to time pressure, the survey had to be conducted at this time.

In an attempt to raise the response rate, hidden identity for respondents was activated in my electronic survey, and all e-mail addresses were deleted after the survey was closed. When hidden identity is used in surveys, no identifiable information (e.g., browser type and version, Internet IP address, operating system, e-mail address) will be stored with the answer. Because of the policy of not sharing information regarding information security performance, hidden identity was activated to assure the respondents that the information they provided could not in any way be traced back to a specific company or person. In addition, I signed a confidentiality agreement with NVE before I received e-mail addresses for ICT safety and security managers and contingency planning managers in the network companies. In the confidentiality agreement, I agreed not to publish any information or results that could in any way be linked to a specific company or person. The respondents were also given information regarding this confidentiality agreement in the survey invitation e-mail and were informed that they could contact me if they needed a copy of the confidentiality agreement before they agreed to answer the survey. Last, qualitative research data were gathered to support the quantitative results from the survey, which might increase the potential for generalizing.

6.3.2 Trustworthiness - qualitative research methods

As mentioned, trustworthiness is based on the constructivist paradigm, and important trustworthiness criteria are credibility and transferability. Credibility as defined in the constructivist paradigm can be compared to internal validity in the positivist paradigm. When the objective of a study is to establish a causal relationship, internal validity is of particular interest, referring to the confidence placed on the assessed cause-effect relationship. The internal validity of the conclusions reached depends on the reliability and validity of the questionnaire or scales used (Oltedal, 2011). In this research project, I did not use statistical analysis to establish a causal relationship between my variables; however, the reliability and validity of the questionnaire and scales used are discussed in the previous section.

Credibility, on the other hand, demonstrates the match between the constructed realities of stakeholders and the reconstructions as being attributed to the stakeholders (affected actors). Several techniques exist for verifying the credibility of a research study, including member checks (testing hypotheses and interpretations with the stakeholders), prolonged engagement, and peer debriefing with a disinterested peer (Guba and Lincoln, 1989, referred to in Johnsen, 2012). Member checks are based on involvement with key stakeholders in reflections and interpretations. I discussed my research questions and findings with my contact person in NVE several times, and at the end of my research project I presented my findings to the contingency planning department in NVE. I received positive feedback from NVE after my presentation – the representatives from the contingency planning department found my results interesting, and my findings corresponded well with their own impressions and what many of them experienced during inspections at the network companies and at different gatherings with representatives from the network companies.

Prolonged engagement means to participate with the stakeholders over a sufficient period of time to understand the research issues and the industry (sector) setting in depth (Johnsen, 2012). I have worked on this research project for four years and discussed important issues with key stakeholders in different settings during my interviews and observation studies and through my contact with NVE. My document studies also helped me develop a deeper understanding of the research issues and the industry setting. Peer debriefing with a disinterested peer has been done as a natural part of presenting my research results during several national and international research conferences.

Transferability as defined in the constructivist paradigm can be compared to external validity in the positivist paradigm. The generalization of the findings is related to whether the findings can be used in other contexts, that is, whether the findings may be generalized to other people, other places, or other times (Johnsen, 2012). Through my document studies, I found that the challenges and issues discussed in this thesis also exist in other industries and other countries, and a review of previous research literature also showed similar findings from other industrial sectors, such as the oil and gas (petroleum) sector (this is further elaborated in Chapter 8).

6.3.3 Ethical considerations

In some surveys, an important ethical consideration is to maintain the anonymity of respondents. Personal anonymity may be central to gaining reliable information (Fox, Murray, and Warm, 2003). As previously stated, hidden identity for respondents was activated in my electronic survey, all e-mail addresses were deleted after the survey was closed, and I signed a confidentiality agreement with

NVE where I agreed not to publish any information/results that could in any way be linked to a specific company or person.

As mentioned in section 6.1.3., I took on an observer-as-participant role in my observation studies. Many ethical issues are associated with observation, especially related to whether or not the researcher withholds his or her research purpose from those being observed (Adler and Clark, 2014). One conference I observed was open to the public. I talked to the organizers of the conference (representatives from NorSiS) and informed them that I was conducting research at the conference and about the purpose of my research. I also talked to other conference participants about my research study during coffee breaks and dinner. The other conference I observed was not open to the public, but had one day that was open to vendors (suppliers), regulatory authorities, and other relevant actors within the electric power supply sector. I was invited to come this day by the organizers of the conference, Forum for Information Security in the Electric Power Supply, and the conference audience was informed that I was there, that I was a researcher, and what my research project was about.

6.4 Methodological limitations

This section discusses limitations for the thesis with regard to methods and measurements. In statistical analysis, measurement errors threaten the validity of the conclusions about the relationships between the constructs. Method bias has both a systematic and a random component, but the systematic error is in particular considered a major problem. Potential sources of common method biases are produced by a common source or evaluator (e.g., social desirability). For example, respondents might provide socially desirable answers instead of answering truthfully (Oltedal, 2011).

Social desirability occurs when survey respondents seek to present themselves in a positive light and therefore respond to an item according to what they think is the socially correct answer rather than their true answer. Furthermore, on subjective assessments regarding their own company's performance, respondents are often inclined to assess themselves positively. Sometimes, it may also be difficult to answer negatively on questions concerning one's immediate manager (Hagen, Albrechtsen, and Hovden, 2008). A possible remedy for this problem is to use a mixed-methods approach so that results do not rely exclusively on the results of one questionnaire (Spector, 2006, referred to in Oltedal, 2011), which is done in this research project.

Method effects can be caused by an item's characteristics, including complexity, ambiguity, scale format, and negatively worded items (Oltedal, 2011). In this research project, the issue of the accuracy of the gathered data was considered, and attempts were made to gather as truthful responses as possible. When using forced-choice questions, it is inevitable that at least some respondents will not be completely satisfied with the options available. Fox, Murray, and Warm (2003) recommended that researchers consider including a "decline" and "don't know" option in the questionnaire. It can be important to provide the respondents with the option to select a "decline" option, rather than forcing them into responding to all questions. This also allows the distinction to be made between questions where no selection has been made (missing) and those that respondents have read but to which they chose not respond. For this reason, I included a "don't know" and a "not relevant" option in my survey.

Included in the previous guidelines (2003 and 2011) for the contingency planning regulations for the electric power supply sector was also a classified section relating to regulations for ICT safety and security. I did not have access to this classified section for this research project; however, the respondents may have included the requirements in this classified section when they answered some of the questions regarding the use of functional regulations for ICT safety and security. Nevertheless, I do not think that this seriously affected the results of the survey – I still obtained information regarding the respondents' attitude toward the current regulation guidelines, even if I did not have access to the entire content of the guidelines.

7. Research results

This chapter summarizes each of the four articles, including the aim/purpose, applied method, main results, and conclusions. All articles are related to the main research aim in this thesis, which is described in the introduction.

7.1 Summary and results of article 1

Skotnes, R. Ø. and Engen, O. A. (2015), Attitudes toward risk regulation – Prescriptive or functional regulation?, *Safety Science,* Vol. 77, pp. 10–18.

The aim of this article was to address attitudes toward the use of functional versus prescriptive risk regulations. The context for the study was the use of functional internal control regulations for ICT safety and security in network companies within the Norwegian electric power supply sector. As previously mentioned, former research has shown that ambiguity in results of internal control regulations may be explained by organizational size, where large companies may be better suited to implement internal control than smaller companies (Hovden, 1998; Lindøe, 2001). However, the results of my survey suggested that managers and employees in both large and small network companies had diverging views on and varying attitudes toward internal control regulations, depending on the specific question asked.

Hence, the following research question was discussed in the article:

- What can explain varying attitudes toward the use of functional internal control regulations as the principle for regulating risks?

The research question was answered by presenting results from the interviews, observation studies, document studies, and the questionnaire survey. The focus in this article was on the results from the four items regarding attitude toward regulations in the survey. Independent samples t-tests were performed to identify significant differences in the mean values for the respondents. I found no statistically significant differences in the mean scores between managers and employees on the four items. However, I found a statistically significant difference in the mean scores between large and small network companies on item 3; however, the magnitude of the differences in the means was small.[22] Thus, the article focused on descriptive statistics of the whole survey sample. Table 7 shows the distribution of scores on items 1-4 in the survey.

[22] Results of independent samples t-tests - **Item 1:** Managers (N=66, M=3.89, SD=1.07) and employees (N=31, M=3.74, SD=1.06); *t* (95) = .65, *p* = .52, 2-tailed). Large companies (N=37, M=3.89, SD=1.05) and small companies (N=62, M=3.94, SD=1.02; *t* (97) = -.20, *p* = .84, 2-tailed). **Item 2:** Managers (N=66, M=3.06, SD=1.07) and employees (N=31, M=3.39, SD=1.02; *t* (95) = -1.43, *p* =.16, 2-tailed). Large companies (N=36, M=3.22, SD=1.10) and small companies (N=63, M=3.08, SD=1.05; *t* (97) = .64, *p* = .52, 2-tailed). **Item 3:** Managers (N=64, M=2.81, SD=.83) and employees (N=27, M=2.74, SD=.86; *t* (89) = .37, *p* = .71, 2-tailed). Large companies (N=34, M=2.59, SD=.78) and small companies (N=59, M=2.98, SD=.80; *t* (91) = -2.31, *p* = .02, 2-tailed). The magnitude of the differences in the means was small (eta squared = .055). **Item 4:** Managers (N=62, M=3.76, SD=1.06) and employees (N=29, M=3.86, SD= 1.06; *t* (89) = -.43, *p* = .67, 2-tailed). Large companies (N=32, M=3.75, SD=.95) and small companies (N=61, M=3.80, SD=1.12; *t* (91) = -.23, *p* = .82, 2-tailed).

Table 7. Distribution of scores on item 1-4.

	Distribution of scores on items (in percentage)			
	Item 1: *'I think it's ok that the authorities prescribe the overall safety goals and requirements for ICT safety and security and permit the organizations to find and develop their own means to achieve these goals'*	**Item 2:** *'I wish that the authorities would provide us with more detailed guidelines for how we can achieve the goals and requirements for ICT safety and security in the contingency planning regulations'*	**Item 3: '***The requirements and guidelines for ICT safety and security in Chapter 6 of the "Guidelines for the contingency planning regulations for the Norwegian electric power supply" are too detailed'*	**Item 4:** *'In connection with the introduction of Advanced Metering Infrastructure (AMI) in the Norwegian electric power supply system, I wish that the network companies could receive more detailed guidelines from the authorities'*
Strongly disagree	2,9 % (N=3)	2,9 % (N=3)	2,9 % (N=3)	1,0 % (N=1)
Disagree	8,7 % (N=9)	27,2 % (N=28)	29,1 % (N=30)	11,7 % (N=12)
Neither disagree nor agree	17,5 % (N=18)	35,0 % (N=36)	47,6 % (N=49)	23,3 % (N=24)
Agree	37,9 % (N=39)	20,4 % (N=21)	9,7 % (N=10)	28,2 % (N=29)
Strongly agree	32,0 % (N=33)	13,6 % (N=14)	3,9 % (N=4)	29,1 % (N=30)
Not relevant	0,0 % (N=0)	0,0 % (N=0)	1,0 % (N=1)	1,9 % (N=2)
Don't know	1,0 % (N=1)	1,0 % (N=1)	5,8 % (N=6)	4,9 % (N=5)
Total	N=103	N=103	N=103	N=103

The survey suggested that a majority of the respondents had a positive attitude toward functional regulations. At the same time, the respondents had divergent opinions about the need for more detailed guidelines for how to comply with the ICT safety and security goals and requirements in the contingency planning regulations, but very few respondents felt that the requirements and guidelines for ICT safety and security were *too* detailed. On the other hand, a majority of the respondents also answered that they wanted more detailed guidelines concerning the implementation of a new technology (AMI). This confirmed the existence of varying attitudes toward the functional internal control regulations for ICT safety and security in network companies within the Norwegian electric power supply sector. The observation studies showed that some of the network company representatives expressed dissatisfaction with the fact that the requirements for how to implement AMI safely and securely were functional, and they wanted NVE to take more control of the implementation process, instead of just setting the goals and leaving the actual implementation to the companies.

According to my interviews with NVE, there is also a clear need to introduce internal control principles in other areas under its jurisdiction. However, there seems to be a reorientation toward *a combination* of functional and prescriptive regulations within this sector. The Norwegian Energy Act's rules for contingency planning in the electric power supply sector were changed in 2012. In addition, on behalf of the Ministry of Petroleum and Energy, NVE has revised the regulations for contingency planning in the Norwegian electric power supply sector, and new contingency planning regulations and guidelines for these regulations took effect in 2013. Increased vulnerability and threats due to increased use of ICT to monitor, control, and operate power generation plants and power distribution were some of the main reasons for the revisions. In many areas of the regulations, former practice is still followed, but with a clearer specification of the requirements. In some areas, the regulations are tightened through new requirements or a stricter use of existing practice. NVE has tried to make the requirements in the contingency planning regulations clearer and more concrete based on requests from the electric power supply companies.

The article concluded that varying attitudes and conflicting opinions at different times regarding functional regulations can be explained by the complexity and uncertainty of the specific risk problem to be handled, in addition to the size of the company. The more loosely coupled the system to be managed is, and the more controllable and predictable the risk problem is, the greater the request for functional regulations for safety and security will be. Correspondingly, the more tightly coupled the system to be managed is, and the more complex, unpredictable, and uncertain the risk problem is, the greater the request for prescriptive, detailed regulations will be – regardless of whether the company in question is large or small.

7.2 Summary and results of article 2

Skotnes, R. Ø. (2012), Strengths and weaknesses of technical standards for management of ICT safety and security in electric power supply network companies, *Journal of Risk and Governance*, Vol. 3, Iss 2, pp. 119-134.

The aim of this article was to study the use of technical standards for management of ICT safety and security in electric power supply network companies, in addition to discussing the following research question:

- What are strengths and weaknesses of technical standards for management of ICT safety and security?

As mentioned earlier, the consistent application of functional regulations requires a comprehensive and systematic guide (regulatory guidelines) on how the various provisions are to be understood and the appropriate standards that can or should be used to meet the requirements (Lindøe and Engen, 2013). As a means to protect ICT systems from malfunctions and attacks, national and international technical (industrial) standards and public guidelines for ICT safety and security management have been developed to provide a wide array of safety and security measures and activities.

The research question was answered by presenting results from the questionnaire survey, interviews, and document studies. In this article, I chose to focus on the results of three items from the perception of compliance scale: item 8 regarding the use of technical standards, item 7 regarding the use of a guideline for risk and vulnerability analyses, and item 3 regarding the use of checklists.

Standards, guidelines, and checklists are typical tools to use in managing the safety and security in organizations, and it makes sense to compare the use of these different tools. Information about the use of technical standards for ICT safety and security in Norwegian network companies was collected from written documents, including regulations relating to contingency planning in the Norwegian power supply system, guidelines for the contingency planning regulations (NVE, 2013), guidelines for risk and vulnerability analysis (NVE and Proactima, 2010), and presentations by representatives from NVE at different conferences on ICT safety and security for companies in the Norwegian electric power supply sector.[23]

Independent samples t-tests were performed to identify significant differences in the mean values for the respondents. The t-tests found no statistically significant differences in the mean scores between managers and employees or between large companies and small companies on the three items used in the article.[24] Hence, the focus of the article was on descriptive statistics of the whole survey sample. Results from the survey confirmed that very few of the respondents used technical standards when they conducted risk and vulnerability analysis of their ICT systems and developed and implemented their internal ICT safety and security management systems, at least not consistently. Only 17.7% of the respondents answered that they strongly agreed or agreed with item 8 regarding the use of technical standards. A large percentage of the respondents also answered "Neither disagree nor agree" on this item, and many answered "Don't know."

At the same time, the majority of the respondents used NVE's "Guideline for risk and vulnerability analysis in the electric power supply sector"; 68.9% of the respondents answered that they strongly agreed or agreed with this item (item 7), and only 4.9% of the respondents answered that they strongly disagreed or disagreed. However, NVE's guideline for risk and vulnerability analysis does not go specifically into ICT safety and security, even though the methods presented can also be used for ICT systems. Many of the respondents also used checklists when they developed risk and vulnerability analyses for their ICT systems; 45.5% answered that they strongly agreed or agreed with item 3 regarding the use of checklists. However, 33.7% of the respondents also answered "Neither disagree nor agree" on this item, which suggests that they use checklists on some occasions but not on a regular basis. Table 8 presents the distribution of the respondents' scores on the three items used in this article.

[23] Presentations found at http://www.norsis.no/vedlegg/KraftIS/ and http://www.nve.no/no/Om-NVE/Presentasjoner-fra-NVE-arrangement/ (accessed 20 November, 2012).

[24] Results of independent samples t-tests – **Item 8**: Managers (N=51, M=2.92, SD=.94) and employees (N=15, M=3.07, SD=.70); *t* (64) = -.56, *p* = .58, 2-tailed). Large companies (N=23, M=3.04, SD=.64) and small companies (N=45, M=2.96, SD=1.0); *t* (66) = .38, *p* = .70, 2-tailed). **Item 7**: Managers (N=64, M=3.98, SD=.92) and employees (N=24, M=4.04, SD=.81); *t* (86) = -.27, *p* = .79, 2-tailed). Large companies (N=30, M=3.80, SD=.89) and small companies (N=59, M=4.10, SD=.87); *t* (87) = -1.54, *p* = .13, 2-tailed). **Item 3**: Managers (N=62, M=3.56, SD=.92) and employees (N=23, M=3.39, SD=.78); *t* (83) = .80, *p* = .42, 2-tailed). Large companies (N=31, M=3.39, SD=.76) and small companies (N=56, M=3.55, SD=.93); *t* (85) = -.85, *p* = .40, 2-tailed).

Table 8. Distribution of scores on items 3, 7, and 8.

Distribution of scores (in percentage)			
	Item 3: *"In my organization, checklists are always used in the development of risk and vulnerability analyses"*	**Item 7:** *"In my organization, NVE's 'Guideline for risk and vulnerability analysis in the electric power supply sector' is always used in the development of risk and vulnerability analyses"*	**Item 8:** *"In my organization, standards (e.g., ISO/IEC 27001/ISO/IEC 27002/NS-ISO/IEC 17799) are always used in the development of risk and vulnerability analyses, information security policy, and safety/security instructions"*
Strongly disagree	1,0 % (N=1)	1,0 % (N=1)	4,9 % (N=5)
Disagree	8,9 % (N=9)	3,9 % (N=4)	13,7 % (N=14)
Neither disagree nor agree	33,7 % (N=34)	15,5 % (N=16)	32,4 % (N=33)
Agree	35,6 % (N=36)	41,7 % (N=43)	15,7 % (N=16)
Strongly agree	9,9 % (N=10)	27,2 % (N=28)	2,0 % (N=2)
Not relevant	1,0 % (N=1)	1,9 % (N=2)	2,9 % (N=3)
Don't know	9,9 % (N=10)	8,7 % (N=9)	28,4 % (N=29)
Total	N=101	N=103	N=102

A qualitative interview study from 2011 that was conducted in connection with my present study also found that technical standards were rarely used during the development of the electric power supply network companies' ICT risk and vulnerability analysis. Only one of the seven informants in the interview study answered that the company used technical standards as a starting point for development of a risk and vulnerability analysis of its ICT system. Furthermore, the interview study found that most of the companies used checklists to identify objects to be analyzed in the risk and vulnerability analysis (Røyksund, 2011). Last, according to my interviews with NVE, the Directorate's experience is that standards are rarely used by the companies in the Norwegian electric power supply sector.

The article concluded that weaknesses of technical standards for the management of ICT safety and security, because of the complexity of the ICT systems used in the electric power supply sector (process control systems, e.g., SCADA systems), include that they are perceived as too complicated and difficult to follow. Standards are often general and abstract and it can be difficult to do *exactly* what a standard says. Considerable knowledge and technical skill is often required to use the technical standards. In addition, different technical standards are divergent when it comes to their methodology and approach to safety and security for SCADA systems, and this may make it difficult for network companies to choose the right standard. Furthermore, there may be substantial differences between presentation and practice, between formal structure and actual operations, and between what people say and what they do. Standardization might also lead to a loss of local knowledge and system-specific competence, which can be important when facing safety-critical decisions.

Strengths of technical standards for the management of ICT safety and security include that they give updated, international recommendations and advice and provide increased communication, contact, and cooperation between the companies following the standards. SCADA systems are highly complex critical infrastructures that have a direct effect on the physical world and can pose a significant risk to the health and safety of human lives and serious damage to the environment. The complexity of these ICT systems increases the uncertainty, and it is difficult to predict the occurrence of events and their consequences. The use of guidelines and checklists may not be adequate (comprehensive and updated) for developing and implementing safety and security management systems to deal with the fast-paced technological changes and increased connectivity, automation, complexity, and vulnerability of these ICT systems.

7.3 Summary and results of article 3

Skotnes, R. Ø. (2015), Risk perception regarding the safety and security of ICT systems in electric power supply network companies, *Safety Science Monitor,* Vol. 19, Iss 1, article 4.

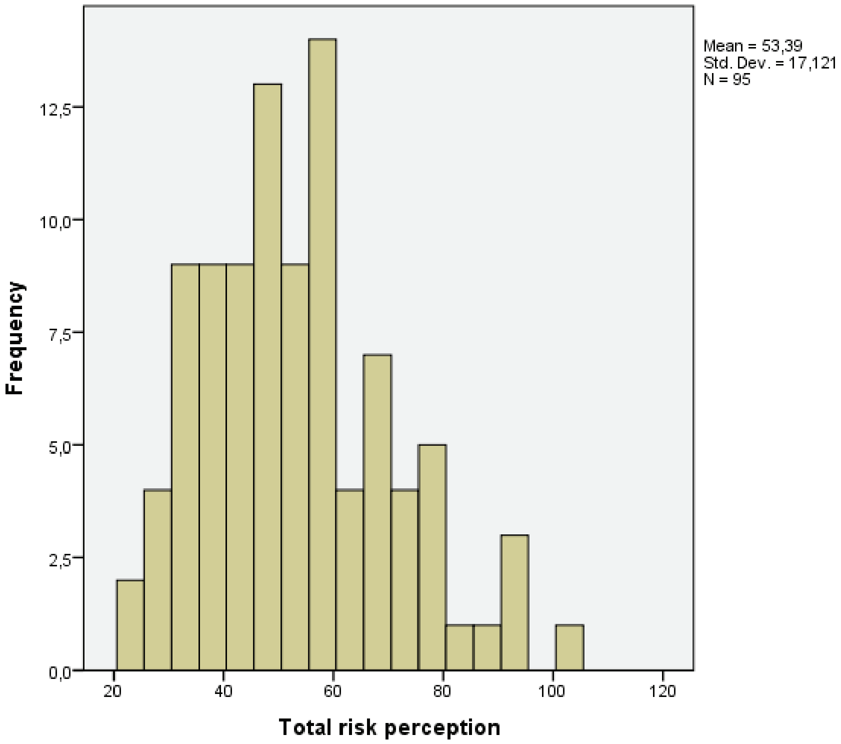
The purpose of this article was to provide insight into risk perception among users (both managers and employees) of ICT systems within electric power supply network companies and to discuss factors that can influence users' risk perception. The following research question was examined in the article:

- What factors can influence the risk perception of users (managers and employees) within electric power supply network companies regarding the risk of malfunctions in or attacks on their ICT systems?

The research question was answered by presenting results from the questionnaire survey, interviews, previous research literature, and document studies. In this article, I chose to focus on the results of the survey items in the risk perception scale, in addition to items regarding knowledge of safety and security, experience of incidents, and overall rating of the safety levels of the organizations' ICT systems.

As described in earlier chapters, the electric power supply system is often seen as the most critical infrastructure in modern society, and a breakdown in the ICT systems used within this industry (process control systems) can seriously compromise the physical grid, which can result in major financial disasters and damage to public safety and health. Hence, ICT safety and security is especially important within this sector, and the vulnerability of these ICT systems is also expected to increase during the next few years due to the implementation of AMI. Therefore, users of ICT systems within electric power supply network companies could be expected to perceive the risk of attacks on or malfunctions in these ICT systems as high. On the contrary, descriptive statistics and a histogram showed that the respondents perceived the risk of a breakdown in their organization's ICT systems caused by malfunctions or attacks as relatively low. The mean value on the total scale score was 53.39, the minimum possible value was 19, and the maximum possible value was 114. The results are shown in Figure 5.

Figure 5. Distribution of scores on the total risk perception scale.



In addition, the qualitative interview study conducted by Røyksund (2011) showed that, despite an increased focus on ICT safety and security within the sector in recent years,[25] representatives from Norwegian electric power supply companies still perceived the risk of an attack on their ICT systems as relatively low.

Furthermore, the survey respondents perceived the overall safety level of the organizations' ICT systems as good, as shown in Table 9.

[25] NVE increased its focus on ICT safety and security after 2006 and has (especially since 2009) been putting more pressure on the electric power supply organizations through heightened regulations and supervision. In addition, in 2009, some of the bigger network companies formed their own Forum for ICT safety in the electric power supply sector (Røyksund, 2011).

Table 9. Distribution of respondents' scores on the question: "All in all, how would you assess the safety of the ICT systems used in your organization?"

	Percentage	**N**
1 Very poor (1)	0.0%	0
2 (2)	0.0%	0
3 (3)	6.9%	7
4 (4)	29.7%	30
5 (5)	56.4%	57
6 Very good (6)	6.9%	7
Total		101

As mentioned, the respondents in my survey were ICT safety and security managers/coordinators, contingency planning managers, operators of process control systems, and ICT personnel. These users work directly with process control systems, ICT issues, and/or safety and security issues within the network companies and can be expected to have more knowledge about ICT systems and/or safety and security than average end-users of traditional computer systems. The respondents generally scored high on items concerning their familiarity with the contingency planning regulations and with the internal safety and security policy and contingency plan in their companies (the knowledge of safety and security scale). However, the interviewees from NVE said they often find during inspections that a number of employees (and possibly also managers) in the network companies have not read the contingency planning regulations and guidelines. The relationship between risk perception and safety and security knowledge was investigated using the Pearson product-moment correlation coefficient, but the analysis showed no statistically significant correlation between the total risk perception scale and the total knowledge of safety and security scale, *r* = .02, *n* = 86, *p* = .83 (two-tailed).

A one-way between-groups ANOVA was conducted to explore differences in risk perception within the network companies (i.e., between the mean scores on the risk perception variable for the different job categories in the data material). The results showed no statistically significant difference at the p < .05 level for the different job categories in the mean scores on the risk perception scale: *F* (7, 87) = 1.3, *p* = .26 (N = 95).

Next, independent-samples t-tests were performed to determine whether significant differences existed among the mean scores of managers versus employees, and of small companies versus large companies, on the risk perception scale. There was no statistically significant difference in scores for managers (*M* = 53.10, *SD* = 16.41) and employees (*M* = 53.17, *SD* = 18.52; *t* (88) = -.019, *p* = .99 (two-tailed), N = 61 for managers, N = 29 for employees). The magnitude of the differences in the means was very small (eta squared = -.0004). Earlier research has shown some differences in risk perception between ICT safety and security managers and other users (Goodhue and Straub, 1991; Albrechtsen, 2007; Albrechtsen and Hovden, 2009). However, because tests did not show any statistically significant difference between managers and employees in their scores on the risk perception scale in my survey, this article examined possible factors that might explain why *the majority* of respondents perceived the risk of attacks on or malfunctions in the network organizations' ICT systems as low.

I did, however, find a statistically significant difference in the mean risk perception scores between managers and employees in small companies (*M* = 48.16, *SD* = 15.61) versus managers and employees in large companies (*M* = 61.85, *SD* = 15.95; *t* (90) = 4.03, *p* = .00 (two-tailed), N = 58 for small companies, and N = 34 for large companies). Managers and employees in large companies perceived the risk of a breakdown in the organization's ICT systems caused by malfunctions or attacks as higher than the managers and employees in the smaller organizations. The magnitude of the differences in the means was large (eta squared = .15).

The respondents in my survey were also asked if their organizations had experienced different safety and security incidents. On some of the incidents (e.g., malware attacks, malfunctioning in the ICT systems caused by human error), a majority of the respondents answered that their organizations had experienced such incidents, but many of the respondents still rated these types of incidents at the low end of the risk perception scale. Interviews with representatives from NVE revealed that the regulatory authorities consider most of the network companies to have adequate day-to-day operational safety and security, but think they should perform better when it comes to planning for extraordinary incidents with potentially large consequences.

According to results from my interviews and observation studies, in addition to the qualitative interview study by Røyksund (2011), two different subcultures can be said to exist in the network companies, depending on whether the people operating the SCADA systems have an education in ICT or a background from the electricity industry. According to NVE, the network companies focus on the possibilities that the SCADA systems provide (i.e., access to more information and the possibilities of operating more electrical plants in a simpler way), but there is not as much focus on, or awareness of, the risk of "unwanted" access to these systems, protection against malicious software, and similar concerns. During inspections, NVE often discovers access points in the SCADA systems that the companies haven't considered, especially concerning remote access, supplier access, external DVDs, and USB sticks.

The article concluded that company size, awareness regarding ICT safety and security, and earlier experience of danger are factors that can influence the risk perception of ICT system users within companies. The article also concluded that knowledge of safety and security may affect risk perception, even though I did not find any statistical correlation between these two dimensions in the analysis of my survey results. System complexities, which can be seen as a natural source of threats against process control systems, can also affect the risk perception of the companies' managers and employees. Process control networks are often more complex than traditional ICT networks and require a different level of expertise. Increased cognitive demands, increased electronic complexity, and dense organizational interdependence over large areas often lead to an increase in incidences of unexpected outcomes that produce unexpected ramifications. Furthermore, a lack of communication between subcultures with different focus points and mindsets within the companies was found to influence the risk perception of users of ICT systems, in addition to a certain "taken for grantedness" regarding many issues surrounding ICT safety and security. Too much trust in the expertise of system vendors can also lead to a lack of focus on the safety and security of network companies' ICT systems and thus influence users' risk perception.

7.4 Summary and results of article 4

Skotnes, R. Ø., (2015), Management commitment and awareness creation – ICT safety and security in electric power supply network companies, *Information & Computer Security*, Vol. 23, Iss 3, pp. 302 – 316.

The aim of this article was to study the degree of management commitment to ICT safety and security within network companies in the electric power supply sector, implementation of awareness creation and training measures for ICT safety and security within these companies, and the relationship between these two variables.

The article follows up on previous research which has shown a positive relationship between management commitment to ICT safety and security and implementation of awareness creation and training measures. The following research questions were addressed:

- To what degree is the management of network companies in the electric power supply sector committed to the safety and security of their organizations' ICT systems?
- To what extent are awareness creation and training measures for ICT safety and security implemented within network companies in the electric power supply sector, and what type of measures are implemented?

The research questions were answered by presenting results from the questionnaire survey, interviews, and observation studies. In this article, I chose to focus on the survey results of the items in the safety and security management scale (management commitment) and the awareness creation and training scale.

The mean value on the total scale score for the safety and security management scale was 18.83, the minimum possible value was 5, and the maximum possible value was 25. This means that the respondents agreed with most statements. The results are shown in Figure 6.

Figure 6. Total scores on the safety and security management scale (calculated by adding the scores from the 5 items that make up the scale).

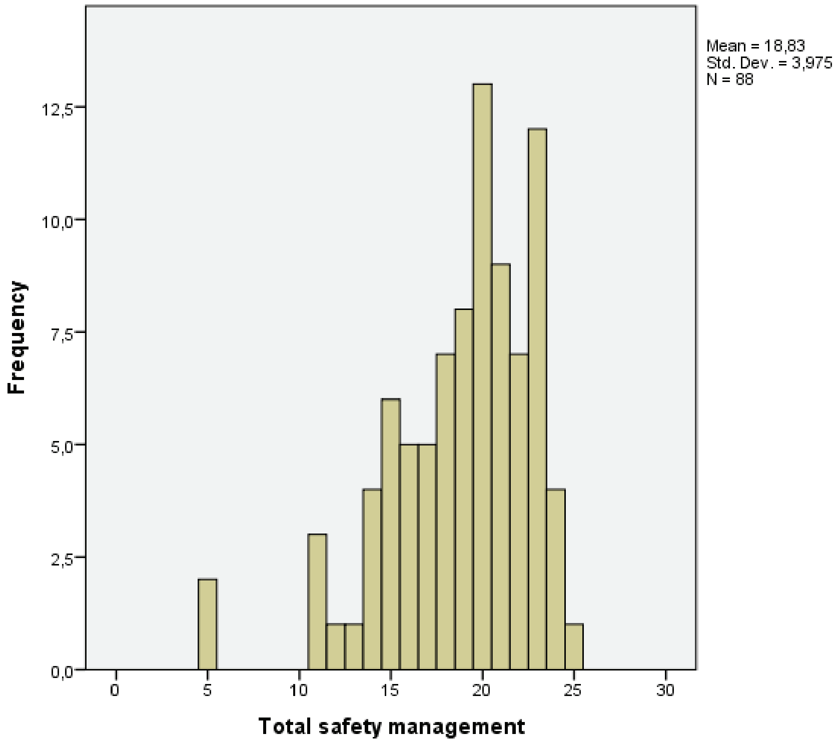


Table 10 presents the distribution of the respondents' scores on the individual items of the awareness creation and training scale.

Table 10. Distribution of scores on items 1-6 within the awareness creation and training scale.

	Distribution of scores on items (in percentage)					
	Item 1: *"New employees receive thorough training in the organization's ICT safety and security rules (included in the organization's ICT safety and security policy and safety and security instructions)"*	**Item 2:** *"Training sessions in ICT safety and security for managers and employees are conducted whenever the ICT systems are updated or altered"*	**Item 3:** *"Awareness campaigns about ICT safety and security are often[1] held in my organization"*	**Item 4:** *"In my organization e-mails containing information about ICT safety and security are often distributed to raise employee awareness"*	**Item 5:** *"In my organization formal face-to-face presentations of information about ICT safety and security are often held to raise employee awareness"*	**Item 6:** *"In my organization informational videos on ICT safety and security are often shown to raise employee awareness"*
Strongly disagree	3,9 % (N=4)	4,9 % (N=5)	4,9 % (N=5)	7,8 % (N=8)	12,7 % (N=13)	23,3 % (N=24)
Disagree	9,7% (N=10)	16,7% (N=17)	27,2 % (N=28)	23,5 % (=24)	42,2 % (N=43)	53,4 % (N=55)
Neither disagree nor agree	26,2 % (N=27)	43,1 % (N=44)	35,0 % (N=36)	35,3 % (N=36)	33,3 % (N=34)	18,4 % (N=19)
Agree	46,6 % (N=48)	28,4 % (N=29)	27,2 % (N=28)	25,5 % (N=26)	9,8 % (N=10)	3,9 % (N=4)
Strongly agree	10,7 % (N=11)	3,9 % (N=4)	4,9 % (N=5)	6,9 % (N=7)	1,0 % (N=1)	0,0 % (N=0)
Not relevant	0 % (N=0)	1,0 % (N=1)	0,0 % (N=0)	1,0% (N=1)	1,0% (N=1)	1,0 % (N=1)
Don't know	2,9 % (N=3)	2,0 % (N=2)	1,0 % (N=1)	0,0 % (N=0)	0,0 % (N=0)	0,0 % (N=0)
Total	103	102	103	102	102	103

[1] In the awareness creation and training scale, the word "often" was defined as "at least once a year." The respondents were informed of this in the scale's text information.

The distribution of the respondents' scores on the individual items of the awareness creation and training scale suggested that the majority of the network companies had implemented training in ICT safety and security for new employees. Some network companies had implemented training sessions in ICT safety and security whenever their ICT systems were updated and altered; however, a large percentage of the respondents answered "Neither disagree nor agree" (43.1%) on this item. The use of awareness campaigns and distribution of e-mails containing information about ICT safety and security seemed to vary considerably between the companies; 54.9% answered negatively[26] on the item regarding use of face-to-face presentations of information about ICT safety and security and 76.7% answered negatively on the item regarding use of informational videos on ICT safety and security.

The relationship between management commitment to ICT safety and security (as measured by the total safety and security management scale) and implementation of awareness creation and training measures (as measured by the total awareness creation and training scale) in the network companies was investigated using the Pearson product-moment correlation coefficient. The correlation analysis revealed a large positive correlation between the two variables "management commitment" and "awareness creation and training," r = .641, n = 81.[27] There was a strong, positive relationship[28] between the variables, and high levels of management commitment were associated with high levels of awareness creation and training.

The article concluded that results from the survey showed a strong relationship between management commitment to ICT safety and security, and the implementation of awareness creation and training measures for ICT safety and security in the network companies. These findings corresponded well with results from former studies (Johnson, 2006; Hagen, Albrechtsen, and Hovden, 2008; Hagen and Albrechtsen, 2009a). The survey data also showed that the majority of respondents viewed management commitment to ICT safety and security in their organization as high. However, contrary to this, results from the interviews and observation studies indicated that it is easier to get the network companies to implement technological and technical-administrative measures than to achieve management commitment to and create awareness of ICT safety and security within the companies.

Furthermore, the results from the survey suggested that the majority of the network companies had implemented training in ICT safety and security for new employees. Some network companies had also implemented training sessions whenever their ICT systems were updated and altered; however, my results indicated that these types of training sessions were not conducted on a regular basis. The use of awareness campaigns and distribution of e-mails containing information about ICT safety and security seemed to vary a lot between the companies. Interactive face-to-face presentations of information about ICT safety and security and informational videos on ICT safety and security did not seem to be used as measures to raise employee awareness within most of the network companies.

[26] "Strongly disagree" and "Disagree."

[27] Correlation was significant at the 0.01 level (2-tailed).

[28] The strength of the correlation is interpreted according to Cohen's guidelines from 1988: small correlation – r=.10 to .29, medium correlation – r=.30 to .49, large correlation – r=.50 to 1.0 (Pallant, 2010, p. 134).

7.5 Summary of research results

The main conclusions drawn from the research indicate that:

1) Varying attitudes and conflicting opinions at different times regarding functional risk regulations can be explained by the complexity and uncertainty of the specific risk problem to be handled, as well as the size of the company.
2) Weaknesses in technical standards include that they can be perceived as too general, complicated, and difficult to follow. Different technical standards also have varying methodologies and approaches when it comes to the complex ICT systems used in the electric power supply sector, which can make it difficult to choose between them. In addition, many Norwegian network companies have not seen the benefits of being certified for compliance with technical standards because the national regulations specify the requirements with which they must comply to protect their ICT systems. Strengths of technical standards for management of ICT safety and security are that they give updated, international recommendations and advice and are said to provide increased communication, contact, and cooperation between companies following the standards. Furthermore, the use of guidelines and checklists may not be adequate to deal with these highly complex ICT systems and fast-paced technological changes.
3) Company size, knowledge and awareness regarding ICT safety and security, and earlier experience of danger are factors that can influence the risk perception of ICT system users within companies. System complexities can also affect the risk perception of the companies' managers and employees. Furthermore, a lack of communication between subcultures with different focus points and mindsets within the companies was found to influence the risk perception of users of ICT systems, in addition to a certain "taken for grantedness" regarding many issues surrounding ICT safety and security. Too much trust in the expertise of their system vendors (suppliers) can also lead to a lack of focus on the safety and security of network companies' ICT systems and thus influence users' risk perception.
4) Consistent with previous research, a statistically significant correlation between management commitment to ICT safety and security and implementation of awareness creation and training measures was found. The majority of survey respondents viewed the degree of management commitment to ICT safety and security within their own organization as high, even though qualitative studies showed contradictory results. The network companies had implemented awareness creation and training measures to a varying degree. However, interactive awareness measures were used to a lesser extent than formal one-way communication methods.

8. Discussion – challenges for safety and security management

This chapter presents a discussion of the research results from the articles included in the thesis. The discussion is related to the thesis' main research aim and the research questions, which were presented in the introduction and in descriptions of the four articles.

8.1 Regulative aspects – prescriptive or functional regulations?

According to Scheytt et al. (2006), regulation is central to any discussion of the relationship between organizations and the management of risk. Risk regulation has a constitutive role in shaping internal organizational practices, a process in which management and self-regulation are difficult to distinguish. A well-known challenge, which appears to be distinct with regard to the regulations for ICT safety and security in the Norwegian electric power supply system, is finding the right balance between command and control risk regulations with detailed and prescriptive rules versus performance- and risk-based regulation with functional rules (self-regulation).

The rapid development in ICT has made traditional methods of command and control regulation by government less than adequate in coping with modern risks, and the introduction of internal control has been an attempt to develop new approaches and means to cope with new challenges of misfits between technology and regulation (Hovden, 1998). In the Norwegian electric power supply sector, principles of internal control were introduced in the area of contingency planning in 2002. The internal control system can be a demanding and comprehensive system for the authorities to keep up-to-date. They need a lot of knowledge and expertise to monitor whether companies comply with the functional regulations and must keep pace with technological developments and new knowledge. However, the advantage of using the principles of internal control is that the scope and form of the internal control system can vary with a company's size, complexity, domain, and risk scenario, and this allows each company to adjust the system to its own needs, routines, organization, and culture. The function-based character of the regulatory regime creates a large degree of autonomy in how employers and companies design the safety practices they think are appropriate. Such autonomy can be advantageous for employers in several ways, including financially. It has an intrinsic value for the employer side because employers can determine the means by themselves and not be overruled by the authorities (Bang and Thuestad, 2014).

Detailed and prescriptive rules, on the other hand, provide no incentives for companies to engage in innovative practices and bind them to the established technology and organizational solutions. The more prescriptive rules and technical standards the regulator takes as legally binding, the more responsibility and the greater "burden of proof" they impose on themselves. Explicit and detailed requirements are certainly highly predictable and easily interpreted, but they may soon stiffen in technologies from the past. It is difficult to see how safety-critical issues related to management, organization, and technology can be improved by the authorities' use of additional or more detailed rules (Bieder and Bourier, 2013).

My study on attitudes toward risk regulations in the Norwegian electric power supply network companies found that generally the companies wanted functional internal control risk regulations with more freedom of choice, but in specific situations involving specific risk problems (e.g., the implementation of AMI) they asked for more detailed rules and wanted NVE to tell them exactly what to do. According to the interviewees from NVE, attitudes toward functional internal control regulations in the network companies also vary depending on with whom one speaks. Top management may be interested in having functional regulations, but middle management and the employees working with the actual implementation of the internal control system might want more concrete and detailed regulations. The findings in this thesis correspond well with results from the previously mentioned interview study in the Norwegian petroleum industry (Engen et al., 2013).

According to my interviewees from NVE, the introduction of internal control regulations has actually led to a *lesser* focus on contingency planning in the network companies. Many of the companies feel pressured from all sides and have not established enough internal resources to keep the focus on contingency planning. Nevertheless, because of the large differences among the network companies, NVE still sees a clear need to introduce internal control principles also in other areas under its jurisdiction. However, as shown in Chapter 7, a reorientation toward *a combination* of functional and prescriptive regulations within this sector is occurring.

Even if the ICT safety and security requirements are the most detailed of the internal control regulations for contingency planning in the Norwegian electric power supply sector, many network companies still wanted more detailed rules and guidance from the authorities in this area. Functional internal control regulations for ICT safety and security can pose a specific challenge for the safety and security managers in electric power supply network companies because of the complexity of the ICT systems. It is difficult to establish a complete system description of these complex systems (Rundmo, 1996), which can make it difficult to identify successful attacks and their consequences and develop comprehensive defenses for all the relevant threats. The scale and complexity of the AMI and smart grid, along with the increased connectivity and automation, make risk regulation of this area particularly challenging. These high complexity systems have tight coupling of their components and processes. The fast-paced technological changes, the invisibility of the material processes, the lack of oversight, and the problems in sensemaking contribute to a feeling of uncertainty, uncontrollability, and unpredictability regarding the risk problems connected to these ICT systems. Most of the network companies lack expert knowledge in this area, which increases the need for more detailed prescriptive regulations.

The pros and cons of rule compliance versus risk management is continuously debated (Hopkins, 2011) and, according to Lindøe and Engen (2013), defining how the roles in safety and security management should be distributed between the state and industry is among the most complex questions regarding risk regulation. The complexity of the ICT systems (process control systems), the complexity of the interdependencies between critical infrastructure, and the complexity of the risk problems add to this question.

8.2 Normative aspects – strengths and weaknesses of technical standards for IT safety and security

Risk regulation regimes contain many more organizational actors than dedicated regulatory agencies. As previously mentioned, some researchers within organizational institutionalism have focused on the emergence of "soft" regulations, and the institutional change of interest is the displacement of coercive, state-level regulations by more voluntary regulations such as standards, rankings, and accreditations. These softer regulatory structures are developed and applied by non-governmental agencies and elicit compliance because they provide legitimacy (Greenwood et al., 2008). Emphasis within the normative pillar is on normative rules that introduce a prescriptive, evaluative, and obligatory dimension into social life. Normative systems include both values and norms. Values are conceptions of the preferred or the desirable, together with the construction of standards to which existing structures or behaviors can be compared and assessed. Norms specify how things should be done; they define legitimate means to pursue valued ends (Scott, 2008).

A multiplicity of organizations has been created at “the world level” to provide coordination and direction for risk management (Scheytt et al., 2006), including international standards organizations such as ISO, IEC, and the Committee of Sponsoring Organizations of the Treadway Committee (COSO). Variants of generic risk management create isomorphic pressures on organizations to conform to these models and to apply them. Risk management knowledge is formed and disseminated through the interplay among various types of “carriers,” (e.g., business schools, management scholars, practicing organizations, media, consultants), through the interaction of these groups, risk management has become an established body of knowledge and a formalized organizational and management practice. The carriers all add to an amplified supply of models for organizations, and they all establish a conceptual framework to which organizations need to relate to be legitimate. A “good” organization is now one which manages risk in accordance with established frameworks; organizations that value their reputation must adopt legitimate practices (Scheytt et al., 2006).

Organizations are often advised to use international standard ISO/IEC27001:2005 (formal requirements for information security management systems) when they develop and implement their ICT safety and security management system, with the support of ISO 27002 (code of practice for information security management). The ISO / IEC 27000 family is a series of information security standards developed and published by the ISO and the IEC. These standards provide a globally recognized framework for best practice information security management. For example, the Norwegian public sector is required to have an internal control system for ICT safety and security based on recognized technical standards for ICT safety and security management systems. The Agency for Public Management and eGovernment (Difi) recommends that governmental bodies use ISO/IEC 27001. In 2013, Difi, on behalf of the public sector, signed a framework agreement on the accessibility of these technical standards for management of ICT safety and security.

Results from my survey confirmed that very few of the respondents used technical standards for ICT safety and security, and my interviews with NVE also showed that the Directorate’s experience is that standards are rarely used by the companies in the Norwegian electric power supply sector. According to a representative from NVE, this does not necessarily imply that the companies within the sector do not have a methodical approach to ICT safety and security, only that the companies have not seen the benefits of being certified for compliance with technical standards because it is the contingency planning regulations that specify the requirements with which they must comply to protect their SCADA systems.

Several different technical standards for ICT safety and security were previously mentioned in NVE’s guidelines for the contingency planning regulations, including ISO 27001, ISO 27002, Standard of Good Practice from Information Security Forum (ISF), and Control Objectives for Information and Related Technology (COBIT). These standards were mentioned in the guidelines as possible tools/methods that organizations can use to develop and establish a safety and security management system and as a starting point for their risk and vulnerability analysis process.[29] In presentations[30] held at conferences on ICT safety and security for companies within the electric power supply sector, representatives from NVE also advised the network companies to use international and national technical standards for ICT safety and security.

However, both the contingency planning regulations and the regulatory guidelines have recently been revised, and in the new guidelines from 2013 the technical standards for ICT safety and security are no longer mentioned. Instead, the regulatory guidelines are now extended from 168 to 310 pages, and the guidelines for ICT safety and security are extended from one to two chapters (one regarding information safety and security (§6) and one regarding safety and security for process control systems (§7)) containing more detailed process descriptions.

A follow-up question regarding the missing references to technical standards in the new guidelines was posed to one of our former interviewees from the contingency planning department in NVE. The answer was that the references to technical standards for ICT safety and security did not become a part of the new guidelines for the contingency planning regulations because of an error, but the references are planned to be reintroduced in the next version of the guidelines. Nevertheless, several of the requirements in NVE's guidelines are similar to the requirements in ISO 27001, and NVE has also included parts of NIST 800-82, "Guide to Industrial Control Systems (ICS) Security," in the guidelines.

Because of the complexity of ICT systems, the technical standards for ICT safety and security may also be perceived as too complicated and difficult to follow; it is easier just to cross off items on a checklist. Standards are often general and abstract and it can be difficult to do *exactly* what a standard says (Brunsson and Jacobsson, 2000). On the other hand, the complexity of the ICT systems can also be why it is necessary to use the technical standards instead of simple checklists when developing a risk and vulnerability analysis and establishing internal safety and security management systems. If the technical standards are not implemented, it may be more difficult for the companies to try to anticipate and plan for extraordinary incidents with potentially devastating consequences. With regard to updating, ISO 27001 has a website called "Wotsnew"[31] which is updated frequently, often several times a month, reflecting the work going on behind the scenes to develop and maintain the ISO27k standards. Users of the standard are encouraged to "revisit periodically or check the history of changes below to avoid missing out on anything important."

There are many different types of process control systems with varying levels of potential risk and impact, which means that there are also many different methods and techniques for securing these systems (Stouffer, Falco, and Scarfone, 2011). The advantage of using functional internal control regulations is that the scope and form of the internal control system can vary with a company's size, complexity, domain, and risk scenario, and this allows each company to adjust the system to its own needs, routines, organization, and culture (Hovden, 1998). Standardizers (e.g., national standards organizations), on the other hand, argue that standards facilitate communication, contact, and cooperation over large areas (Brunsson and Jacobsson, 2000). However, according to NVE, different

[29] NVE's guidelines from 2003 and 2011.

[30] One example is a presentation by senior advisor Øystein Korum from the contingency planning department in NVE, at Kraft IS, an ICT safety and security conference held by NVE and NorSIS, Nov. 30-Dec. 1, 2010. http://www.norsis.no/vedlegg/KraftIS/Beredskapsforskriften_og_IKT-sikkerhet.pdf (accessed 16 May 2013).

[31] http://www.iso27001security.com/html/wotsnew.html.

technical standards are divergent when it comes to methodology and approach to safety and security for SCADA systems; for example, NIST (guide to process control systems security) and NERC CIP (critical infrastructure protection) have a very specific approach, while ISO, the Information Technology Infrastructure Library (ITIL), and COBIT have a more general approach because they cover a broad spectrum of systems, including SCADA systems. This can make it difficult for the network companies to choose the right standard and will necessitate NVE expanding on the different approaches in the guidelines to aid companies in choosing the right one.

According to Power (2007), institutional capacities to organize in the face of uncertainty have been challenged and threatened by failures, scandals, and disasters, and in response visionary documents and designs in the form of standards and guidelines for individuals and organizations have been produced so as to maintain perceptions of control and manageability. The organization of uncertainty in the form of safety and security management designs and standards is related to expectations of governance and demands for defendable, auditable processes. However, many laws, regulations, and standards are sufficiently controversial or ambiguous that they do not provide clear prescriptions for conduct. In such cases, laws, regulations, and standards are better conceived as occasions for sensemaking and collective interpretation, relying more on cognitive and normative than coercive elements for its effects. Thus, institutions supported by one institutional pillar may, as time passes and circumstances change, be sustained by different pillars (Scott, 2008).

8.3 Cultural-cognitive aspects – risk perception

Humans are influenced by their surroundings, and the environment affects cognition as well as behavior and individual decisions. The perceived risk concerns how an individual understands and experiences a phenomenon (Oltedal et al., 2004). The concept of risk perception is connected to cognition, mental processes, sensemaking, and culture. Uncertainty is a psychological construct, and people's risk judgments are related to cognitive processes, including how one comprehends information (Slovic, Fischoff, and Lichtenstein, 1982). Risk related to ICT systems is one of today's produced uncertainties contributing to Beck's (1992) characteristics of a risk society (referred to in Albrechtsen, 2007).

As shown in Chapter 7, the results from my survey of managers and employees in Norwegian network companies showed that most of the respondents perceived the risk of attacks on or malfunctions in the network organizations' ICT systems as relatively low. The managers and employees in the network companies are closest to their ICT systems (including SCADA systems) and have system knowledge. Hence, one might ask why their judgment of the risk should be disregarded. However, as described in Chapter 2, numerous research reports and newspaper articles have shown that this is a real risk, and many examples of incidents exist worldwide. In light of this, I discuss factors that might explain the differences in risk perception.

8.3.1 Factors that can influence risk perceptions

Previous studies have found that company size can influence risk perception within companies (Eakin, 1992; Hasle and Limborg, 2006; Hagen, Sivertsen, and Rong, 2008), and the analysis of my survey results also showed a statistically significant difference in the mean risk perception scores between managers and employees in small companies versus managers and employees in large companies.

An organization’s technology can be used to assess what type of work is performed by the organization and organizational size measures how much of that work the organization carries on (i.e., the scale on which the work is conducted). Most studies of the relationship between organizational size and structure have used the number of participants (usually employees) as an indicator of size. This measure can reflect both the capacity of the organization to perform work, as well as the current scale of actual performance (Scott, 1998). Most of the network companies in the Norwegian electric power supply sector have fewer than 100 employees and can be considered small organizations according to the measurement of organizational size chosen in this study. The introduction of ICT systems to monitor, control, and operate power generation plants and power distribution first led to a downsizing of employees within the electric power supply companies in favor of ICT systems. However, at the same time, the deregulation of the electric power supply sector and the introduction of market principles have led to a centralization of the sector due to company mergers and acquisitions.

As previously mentioned, twenty-three of the network companies are organized in large corporate groups with several subsidiaries or daughter companies. In these companies, some of the employees in the corporate group might perform work for the network companies, even if they are registered as employees in other companies within the group. Some of the large companies have even organized system control centers in separate companies. In large corporate groups, the basic ICT functions are often managed by corporate IT departments, and these departments may be a bit too removed from the different problem areas that are regulated in the contingency planning regulations.

The smallest companies are often dominated by a combined owner-manager, who is very often the sole person responsible for all or most activities not directly related to production. The main focus for the owner-manager is the survival of the company and for natural reasons safety and security will often be a minor focus due to limited resources in terms of money, personnel, and knowledge (Eakin, 1992; Hasle and Limborg, 2006). These small organizations may also have only limited contact with regulatory authorities, and owner-managers will sometimes accuse the regulatory bureaucracy of having a choking effect on small companies (Power, 2007), a notion that was confirmed by our survey based on comments from some of the respondents. All network companies in Norway are obligated to appoint an ICT safety and security manager/coordinator, but in the smaller companies the ICT safety and security managers do not usually work full time in that position. Because of limited resources, many of the smaller network companies cannot hire their own ICT staff and instead choose to outsource this function to other companies (Hagen, 2009).

The big network companies have larger process control systems (SCADA systems) and system control centers and distribute electrical power to more customers (e.g., critical infrastructures such as transport, finance, and telecommunication, hospitals, and other organizations, as well as individual households) than the smaller network companies. Hence, an attack on the large network companies’ ICT systems can have more serious consequences for societal safety. Most of the large SCADA systems in the big network companies are subject to stricter obligations in the contingency planning regulations than the smaller SCADA systems, and large companies often have a separate IT department with significant expertise in ICT. Knowledge and expertise in ICT might lead to a more accurate perception of the risks from threats to the companies’ ICT systems. However, another department may run the SCADA systems on a daily basis and departments may not always communicate well on these issues. In addition to having a separate corporate IT department, outsourcing of basic ICT functions to external companies is also increasingly common. Many of the local companies in the corporate group may know little about the potential threats to their ICT systems, and the IT department might not have a complete overview of what the consequences of a security breach may be in the different application areas. Large companies are also often less transparent than smaller companies due to larger and more complex systems, and this can make it easier for insiders to engage in crime and not be detected (Hagen, Sivertsen, and Rong, 2008).

Regulation introduces obligations which can be a financial burden for smaller companies. The governmental inspectors can impose sanctions on the organizations if they commit serious infringements of the legislation, most often in the form of monetary fines (the sanction of withdrawing the license is usually the last resort). The threat of having such costs imposed can be considered a potential burden for the organization (Hasle and Limborg, 2006). According to my interviews with NVE, inspectors also have the impression that small organizations find it difficult to keep up with obligations regarding ICT safety and security.

Technically, risks are becoming increasingly integrated and interconnected. However, at the organizational level, the organizations that are responsible for dealing with these risks are becoming increasingly fragmented, which might influence users' risk perception. Seen from a safety and reliability perspective, this paradox involves a major challenge when it comes to identifying and mitigating cross-sectorial risks. According to Almklov, Antonsen, and Fenstad (2012), NPM-inspired ways of organizing infrastructure production generate organizational weaknesses that can influence the reliability of critical infrastructures. NPM has led to variants of functional splitting along the value chain. Consequently, more organizations are involved in the infrastructure production. Several Norwegian network companies are split into one network company (the actual concessionaire) and internal suppliers. For instance, one internal supplier handles the planning functions and much of the follow-up of fitting contractors. Another supplier runs the control central. Though belonging to the same corporation, these companies are regarded as suppliers to the network company and sell services to the network company and each other according to formalized contracts.

Thus, one integrated utility is split into a network of cooperating businesses coordinated by contracts and business relationships. Though this kind of reorganization can have many advantages, including in terms of reliability, it also introduces new organizational complexity. One effect of a modularized system is that informal organizational structures are weakened and communication patterns and cooperation modes are standardized. The personal networks across functions are also weakened as they belong to different organizations. In the older integrated companies, personal networks facilitated smooth operations and information flow that fostered many of the typical characteristics of a robust organization. In general, modularization and related developments increase the organizational distance between personnel with practical knowledge of the system and those with a systematic overview (Almklov, Antonsen, and Fenstad, 2012).

A problem related to organizational fragmentation is that several network companies have chosen to outsource their operational work. This means that the fitters now belong to other companies competing for operation and emergency preparedness for different sectors of the grid and for specific "packages" of maintenance work. In cases where operational work is outsourced, it is important for competition for contracts to be fair and transparent. In this respect, personnel networks across functions may be problematic and may even be actively discouraged. However, this weakens the personal networks across functions, even though good relationships and dialogue between planners (with system knowledge) and doers (with practical knowledge) are particularly potent sources of robustness and risk sensitivity (Almklov, Antonsen, and Fenstad, 2012). In Norway, NVE has tried to fix the growing problem of lack of competent personnel by introducing a new requirement in the contingency planning regulations for the electric power supply sector. Since 2013, all network companies have been required to have competent personnel on their permanent staff. However, representatives from the industry are skeptical of these requirements and want to have them removed. These representatives do not want requirements for how many employees are needed to serve different functions or restrictions on the companies' outsourcing of services, but rather they want to replace these requirements with more general quality and safety requirements.

A common concern when NPM is introduced in critical infrastructure sectors is that the drive for effectiveness may lead to cheap solutions and reduce technical and organizational redundancy. However, NPM can also introduce issues of coordinating redundancy. According to Almklov, Antonsen, and Fenstad (2012), an interesting case observed by NVE was that the overall redundancy of fitters to handle emergencies in the industry had been reduced and that several network companies had contracts with the same contractors. Thus, while the emergency response capacity was very good for typical incidents, and more effective than before, there was less slack in the industry as a whole to tackle extraordinary incidents. If several network companies needed assistance, the extra personnel could be contractually obliged to be in several places at the same time and thus a false redundancy is created.

Results of the Norwegian Computer Crime Survey (2012) suggested that managers outsource not only functions but also the responsibility for ICT safety and security. Only half of the enterprises in the computer crime survey answered that they had allocated internal resources with ICT knowledge to follow up on the contracts with and deliveries from their vendors and subcontractors. According to the interviewees from NVE, representatives from ABB and Siemens (the two main vendors (suppliers) of process control systems/SCADA systems in Norway) have claimed that if the network companies utilized more of the safety mechanisms that are already available in the systems, the overall safety and security would be increased. NVE suggests that this reflects a certain naiveté or gullibility about ICT risk, safety, and security in the sector. Many of the network companies have a lot of trust in the expertise of their system vendors, believe that the vendors will create safe solutions, and take for granted that some type of technical applications can manage all problems, and this might also influence their risk perception. The system owners (network companies) are responsible for the safety and security of their own ICT systems, and it might be necessary for the network companies to tell their vendors to provide more safety and security solutions for these systems.

Earlier studies have shown that having had an accident or having experienced an attack can influence the current perception of risk. As described in Chapters 6 and 7, the respondents in my survey were asked if their organizations had experienced different safety and security incidents. For some of the incidents (e.g., malware attacks, malfunctioning in the ICT systems caused by human error), a majority of the respondents answered that their organizations had experienced such incidents, but many still rated these types of incidents at the low end of the risk perception scale. Indeed, one respondent wrote on the questionnaire: "We constantly experience attempts to hack into our ICT systems, but I have only answered based on the attempts that succeeded." This might indicate that even though the network companies *do* experience attempts to break into their ICT systems, they do not perceive these attempts as a high risk because so far most attempts have failed. According to the interviewees from NVE, managers and employees in many of the network companies find it difficult to prepare for something that *might* happen, but hasn't happened yet.

Perceptions can be the result of incomplete or faulty knowledge (Okrent and Pidgeon, 1998). As described in Chapter 7, the respondents in my survey generally scored high on items concerning their familiarity with the contingency planning regulations and with the internal safety and security policy and contingency plan in their companies (the knowledge of safety and security scale). However, I found no correlation between knowledge of safety and security and risk perception, and the interviewees from NVE said they often find during inspections that a number of employees (and possibly also managers) in the network companies have not read the contingency planning regulations and guidelines.

Another factor that might influence risk perception is that many issues surrounding ICT safety and security seem to be taken for granted within Norwegian network companies. The smaller network companies often take for granted that they are unimportant and not a target of potential attack and that the potential consequences of an attack on small companies' ICT systems are not as significant as on a large organization's systems. However, with the introduction of AMI and the smart grid, the potential consequences are likely to increase in seriousness. My interviewees from NVE said they expect several of the smaller network companies to have to team up and join resources to implement and manage the AMI, and this might greatly increase the consequences of malfunctions in or attacks on their ICT systems. According to Hagen, Sivertsen, and Rong (2008), both small and large enterprises may evaluate (or perceive) the risk of malfunctions in or attacks on their ICT systems as too low to put much effort into user education.

Many network companies also seem to take for granted that the system vendors (suppliers) will make safe solutions and that some type of technical applications embedded in the systems can manage all possible problems. Furthermore, employees can unintentionally misuse software and e-mail and import infected information, and they can disclose confidential or sensitive information unintentionally. Employees can also intentionally misuse ICT resources and disclose information (Hagen, 2009). The consequences of insider attacks can be worse than the consequences of external attacks (Johnson, 2006; Hagen, 2009). However, according to NVE, a high threshold for acknowledging this kind of risk exists in the network companies. It might be taken for granted that "this does not happen in our company," which can affect managers' and employees' risk perception.

As mentioned in Chapter 7, two different subcultures exist in the network companies, depending on whether the people operating the SCADA systems have an education in ICT or a background from the electricity industry. In addition to these two different subcultures – information technology and automation technology – representatives from the contingency planning section in NVE suggested that other subcultures also exist (e.g., employees with backgrounds in telemetrics). The different group cultures result in different focus points and mindsets; the groups have different ways of thinking and draw on different scripts and frames when they make sense of the technology. For example, people who have training in electrical engineering generally focus on keeping the systems running without interruption, and they may be less focused on installing security measures and spending time to apply software patches. Follow-up on specific tasks, such as network configuration and control of firewalls, can often be seen as a “necessary evil” that system users relate to as only an annoying delay in their work. As mentioned in Chapter 3, this type of separation of the workforce into subcultures has also been reported in studies from the offshore oil and gas industry (Mearns, Flin, and O’Connor, 2001).

A lack of safety and security awareness by users has often been cited as the top obstacle for effective ICT safety and security (Goodhue and Straub, 1991; Johnson, 2006; Hagen, 2009; Albrechtsen and Hovden, 2009), and lack of awareness might also affect users’ risk perception. According to the Norwegian National Strategy for Information Security of 2012, the owners of critical infrastructure in many cases have limited knowledge and awareness of vulnerabilities, interdependencies of critical infrastructures, and what the individual enterprise must do to protect the infrastructure. If a low level of risk perception regarding the safety and security of the ICT systems in the electric power supply sector can lead to a lack of compliance with the requirements of ICT regulations, the network organizations can fail in their attempt to develop broad and comprehensive defenses for all the relevant threats and to identify successful attacks and their consequences. Thus, risk perception can be a challenge for the safety and security management of electric power supply network companies.

8.4 Cultural-cognitive aspects - management commitment, awareness creation, and training

ICT safety and security law in Norway places responsibility for ICT safety and security on the management and boards of directors of companies. The contingency planning regulations for the Norwegian electric power supply sector also emphasize that contingency planning (which includes ICT safety and security) is the responsibility of the top managers in the organization, and the authorities expect the top management to convey the importance of and follow up on safety and security within their organization. If the management is engaged, it will be aware of the need for information security measures to comply with the laws and assure that security measures are implemented (Hagen and Albrechtsen, 2009a). However, according to the interviewees from NVE, the network companies focus on the possibilities that the SCADA systems provide (i.e., access to more information and the possibilities of operating more electrical plants in a simpler way), but there is not as much focus on, or awareness of, the risk of “unwanted” access to these systems, protection against malicious software, and similar issues.

According to Hagen and Albrechtsen’s (2009a) study, a larger number of electric power supply companies reported incidents typically caused by insiders (e.g., abuse of ICT systems, unintentional use violating security) than financial companies. As previously said, the interviewees from NVE had the impression that there exists a high threshold for acknowledging the risk of insider incidents in the network companies. The companies might take for granted that “this does not happen in our company,” which can affect their awareness.

One of the findings in article 4 was that it is easier to get the network companies to implement technological and technical-administrative measures than to achieve management commitment to and create awareness about ICT safety and security within the companies. As previously mentioned, a possible explanation for this may be that when formal management systems (i.e., policies, procedures, and tools) are in place, these measures may be taken for granted and accepted as contributors to an adequate security level. However, contrary to the results from my interviews and observation studies, the majority of respondents in my survey viewed management commitment to ICT safety and security in their organization as high. One possible explanation for this discrepancy may be that on subjective assessments regarding their own company's performance respondents are often inclined to assess themselves positively. Sometimes, it may also be difficult to answer negatively on questions concerning one's immediate manager (Hagen, Albrechtsen, and Hovden, 2008).

My survey found results similar to Albrechtsen and Hovden's (2009) study of measures that were used by managers to influence user behavior and awareness; 54.9% of the respondents answered negatively ("Strongly disagree" or "Disagree") on the statement, "In my organization, formal face-to-face presentations of information about ICT safety and security are often held to raise employee awareness," and only 10.8% of the respondents answered positively ("Strongly agree" or "Agree"), while 33.3% answered "Neither disagree nor agree." According to Albrechtsen and Hovden, the problem with formal one-way communication measures for creating safety and security awareness was that users often lacked the motivation and awareness to obtain the knowledge in this information, in addition to being bombarded with other types of information.

Previous research has suggested employee participation, practical learning through interaction, role-playing exercises, and e-learning as good techniques to achieve information security awareness among users of ICT systems (Albrechtsen and Hovden, 2009; Thomson and von Solms, 1998; Hagen and Albrechtsen, 2009b). However, these types of awareness creating and training measures are often resource demanding because they must be repeated to be effective. Removing employees from their work during presentations, meetings, and training sessions can also reduce the production capacity of the company. This may be why these types of measures are used to a lesser extent than formal one-way measures, even though studies have shown that they are considered better and more effective for raising awareness about ICT safety and security (Hagen, Albrechtsen, and Hovden, 2008; Albrechtsen and Hovden, 2009). This type of trade-off is well known in the safety research domain. Reason (1997) described how trade-offs are made at an organizational level, and safety margins are eroded due to an emphasis on efficiency rather than safety (Albrechtsen and Hovden, 2009).

The Norwegian petroleum industry uses process control systems (SCADA systems) which are similar to the technology used in the electric power supply industry. According to Johnsen (2012), the integration of technologies, distribution of information, and collaboration in teams create new vulnerabilities, new complexities, and new uncertainties in the systems used to control operations, just as in the electric power supply industry. Johnsen found an absence of systematic awareness training related to ICT/SCADA security, which would affect anticipation and attention and might reduce the resilience of the system. According to Jaatun et al. (2009), the petroleum industry still does not consider information security to be a matter of sufficient importance. One consequence of this is that incidents are treated in an ad hoc manner. The results from my survey in the electric power supply sector are similar to Johnsen's and Jaatun et al.'s findings and suggest a lack of awareness of ICT safety and security and that use of awareness creation and training measures for ICT safety and security varies a lot among the survey respondents' network companies.

The Cyber Security Strategy for Norway of 2012 concluded that the lack of awareness concerning ICT safety and security constitutes a high and increasing risk. The complexity of the process control systems (SCADA systems), together with an increase in the number of attacks on ICT systems, demands a large effort to create awareness of the threats, provide information about safety and security measures, and influence positive attitudes. Thus, the lack of both management commitment and awareness creation and training for ICT safety and security present challenges for the safety and security management of electric power supply network companies.

8.5 Theoretical limitations - rational versus institutional?

In this thesis, I have chosen to apply a sociotechnical perspective and institutional organizational theory (or organizational institutionalism) as a theoretical framework, which emphasizes that organizations are open systems, strongly influenced by their environments. Organizations are embedded in society and affected by institutions, ideas, rules, and legitimate patterns of action that are generally taken for granted. Attention is directed toward forces that lie beyond the organizational boundary in the realm of social processes (Brunsson and Jacobsson, 2000; DiMaggio and Powell, 1983, 1991; Hoffman, 1999). Modern societies contain many complexes of institutionalized rules and patterns (e.g., products of professional groups, the state, public opinion), and these socially constructed realities provide frameworks for the creation and elaboration of formal organizations (Scott, 1998).

Furthermore, according to the theoretical approach employed in this thesis, technology's effects on organizations are socially constructed. Artifacts are created by human ingenuity to assist in the performance of various tasks. The most important characteristic of artifacts is that they embody both technical and symbolic elements (Suchman, 2003, referred to in Scott, 2008), and users draw on familiar schemas and frames to make sense of a new technology. The formal organization can also be considered an institution with accompanying rules and instructions for its incorporation and employment in a social setting. Institutions are taken for granted in that they are both treated as relative fixtures in a social environment and accounted for as functional elements of that environment (Jepperson, 1991).

However, this thesis discusses safety and security management of organizations where organizations implement different preventive measures based on the results of risk and vulnerability analyses (Hagen, Albrechtsen, and Hovden, 2008) and, according to Antonsen et al. (2012), the philosophy of safety management represents a highly rationalist account of management and organization. Among other things, the philosophy emphasizes the standardization of work methods, the separation of planning and execution, and the use of scientific methods and statistics to detect flaws in a system.

From a rational system perspective, organizations are instruments designed to attain specific predetermined goals with maximum efficiency. The organizational structure is viewed as a means, an instrument that can be modified as necessary to improve performance. Theorists utilizing this perspective focus on the normative structure of organizations, that is, the specificity of goals and the formalization of rules and roles (Scott, 1998). One basic assumption of safety management is that safety should be a management responsibility. Management systems are created, aiming to control an organization's operational performance (Antonsen et al., 2012). Johnson (2006) argued that the top management must be committed to ICT safety and security through its activities and through a dedicated budget. An organization's safety and security policy should contain a letter of commitment from the top management showing commitment to ICT safety and security within the organization and assign the responsibilities of each member of the organization, particularly line management, top management, and safety and security professionals. This can again imply an instrumental organizational perspective, where actors are rational and have oversight over all alternatives and where leaders can plan ahead and influence how the organization works by introducing new measures.

However, according to Scheytt et al. (2006), it is well known to management scholars that decision capacity within organizations is limited, yet managerial legal discourses often ascribe to such imperfect management capacity "full" accountability for adverse outcomes. The concept of bounded rationality emphasizes that it is impossible for individuals to be informed about *all* available decision alternatives, and individual choice takes place in an environment of "givens" (i.e., premises that are accepted by the subject as bases for his or her choice), and behavior is adaptive only within the limits set by these givens. By providing integrated subgoals, stable expectations, required information, necessary facilities, routine performance programs, and in general a set of constraints within which required decisions can be made, organizations supply these givens to individual participants (Simon, 1976, referred to in Scott, 1998).

However, according to cultural-cognitive theorists, underlying all decisions and choices are socially constructed models, assumptions, and schemas. All decisions are admixtures of rational calculations and non-rational premises. Institutions provide guidelines and resources for taking action, as well as prohibitions and constraints on action (Scott, 2008). According to Hagen (2009), an effective security culture that includes consistent, appropriate attention to employee security awareness, training, and education is essential to effective information security. Documents are often seen as important because they form the basis for other measures (Albrechtsen and Hovden, 2009); however, procedures must actually be followed to be effective and can be taken for granted (Hagen, 2009). In addition, as previously stated, many laws, regulations, and standards are better conceived as an occasion for sensemaking and collective interpretation.

As mentioned in Chapter 4, research on safety has evolved from being dominated by a formal rational perspective through a bounded rational perspective to a cultural open perspective where social and cultural factors are increasingly important for the understanding and analysis of safety. At the same time, safety research has evolved from a primary focus on the rational actor model (focus on the individual) to a focus on the social and cultural context (focus on the organization) where safety culture and safety climate have received more attention (Dyreborg, 2006).

According to the subset of theorists endorsing a cultural-cognitive perspective, the very concept of an organization as a special-purpose, instrumental entity is a product of institutional processes – constitutive processes that define the capacities of collective actors, both generally and as specialized subtypes (Scott, 2008). As previously mentioned, proponents of new institutional organizational theory also claim that institutions are both antecedent to and emergent from sensemaking processes. Institutions enter meaning-making processes in three ways: Institutions serve as the building blocks or substance of sensemaking, institutions dynamically guide and edit action formation, and institutions are continually enacted and accomplished in ongoing sensemaking processes (Weber and Glynn, 2006). Last, according to Scheytt et al. (2006), scholarly and practical reflections on organizations and the management of risk are necessarily multi-disciplinary and need to recognize the ongoing social construction of risk knowledge.

9. Contributions of the study and concluding remarks

In this chapter, I start by discussing the contributions of the thesis. Then I provide recommendations and suggestions for measures to reduce the complex challenges for safety and security management of network companies and improve the safety and security of their ICT systems, based on the findings and theoretical discussions in this thesis. Finally, I suggest topics for further research.

This thesis highlights important challenges for safety and security management of network companies that result from the increased use of ICT to monitor, control, and operate electric power distribution. The study has elaborated on previous research on the use of functional internal control risk regulations and added new knowledge about the challenges for regulating (and managing) risks in complex ICT systems operating critical infrastructures. The introduction of new technologies leads to complex risks which in turn lead to varying attitudes to regulation of these risks, depending on the degree of complexity and uncertainty of the specific risk problem. Finding the right balance between different principles for controlling risks is especially challenging with regard to complex technological risk problems.

Another finding is that very few Norwegian network companies use technical standards for ICT safety and security. This result also confirmed assumptions held by representatives from the contingency planning department in NVE, as well as results from a previous interview study (Røyksund, 2011). The findings from my study indicate that technical standards for managing ICT safety and security should be evaluated and further developed if they are to become more applicable for process control systems (SCADA systems) running critical infrastructures. An interesting finding in this thesis is also that the risk of attacks on or malfunctions in their ICT systems appear to be perceived as low among my survey respondents in Norwegian network companies. In addition, I found that among my respondents *both* managers and employees perceive the risk as low, contrary to findings in some other studies, including Albrechtsen and Hovden (2009), who found a "digital divide" between information security managers and users of ICT systems.

Furthermore, I have elaborated on previous research on the importance of management commitment and awareness creation and training with regard to ICT safety and security. I have confirmed results from previous studies in other sectors and found a statistically significant correlation between management commitment to ICT safety and security and implementation of awareness creation and training measures in the companies. However, regarding the question of management commitment, I found a discrepancy between the results of my interviews and observation studies and the results from the survey. According to my interviews with NVE and the results of my observation studies, it is easier to get the network companies to implement technological and technical-administrative measures than to achieve management commitment to and create awareness about ICT safety and security within the companies. However, the majority of respondents in my survey viewed management commitment to ICT safety and security in their organization as high. Another important finding is that the use of awareness creation and training measures for ICT safety and security vary a lot between the network companies.

The thesis also highlights that one main factor influences all the different challenges I have studied, namely, complexity. The environmental contexts in which organizations exist are constantly changing, and at an increasing rate. These changes lead to increasing complexity, especially with the impact of fast-paced technological change. According to Scheytt et al. (2006), information overload, bounded rationality, and the complex nature of possible threats are aspects that add to the intricacy of risk management practices.

The theoretical framework for the thesis (i.e., the sociotechnical perspective and institutional organizational theory) has helped to contextualize the studied phenomena, highlight aspects and elements that are important to consider in relation to safety and security (or risk) management, and show that many different factors can lead to challenges for safety and security management at every level of the sociotechnical system. The thesis illustrates why it is important to consider human, technological, *and* organizational factors, as well as the dynamic interaction between these factors. It is especially important to consider cultural-cognitive factors and be aware how these elements affect safety and security management. Institutional organizational theory contributes to illustrate that there is no clear distinction between organizations and their environments and that many socially constructed and institutionalized aspects can influence organizations and create important challenges. Regulative (regulations), normative (technical standards), and cultural-cognitive (sensemaking, risk perception, commitment, and awareness) processes are connected in complex and changing mixtures, and these processes shape organizational structures and activities. The use of institutional organizational theory also sheds light on the important fact that many issues related to safety and security are taken for granted.

According to Almklov, Antonsen, and Fenstad (2012), critical infrastructures are *systems taken for granted*. Critical infrastructures are themselves often built on the expectation of the functioning of other infrastructures. This goes for the technical infrastructure itself (e.g., water pumps that depend on electricity), but equally important is the operational context around it (e.g., ICT-based maps, global positioning systems (GPS) and mobile networks in emergency handling, dependence on transport to get critical spare components). The tendency to take infrastructures for granted may be a problem when analyzing risk because it may challenge the imagination to really understand how they are interconnected in different situations. Dependencies do not follow institutional or organizational boundaries, so when analyzing and managing risk, several actors should be involved in this imaginative work.

The results of the current study are especially relevant for regulators, top managers, and safety and security managers/coordinators in the Norwegian electric power supply sector. However, the challenges discussed in this thesis are likely also relevant for similar electric power supply sectors in other countries, as well as other companies that operate critical national infrastructure with similar ICT systems (process control systems/SCADA systems). It is important for companies and the regulatory authorities to be aware of these challenges, which should be considered when risk regulations and safety and security management systems are developed, implemented, and adapted. In the next section, I suggest several recommendations for measures that can reduce the challenges for safety and security management of network companies and improve the safety and security of their ICT systems.

9.2 Recommendations and suggestions

- Detailed regulatory requirements may hinder natural development which takes into account new technologies and operational patterns; such requirements can be difficult to update fast enough. A combination of functional and prescriptive regulations may be more convenient, and the new contingency planning regulations for the Norwegian electric power supply sector from 2012 (including the new guidelines from 2013) are a step in this direction.
- However, when implementing new complex technology, more detailed guidelines, in addition to more monitoring and support, are necessary.
- Technical standards for ICT safety and security are often too general and complex, which can also lead to unnecessary additional costs and reduced efficiency (a lot of time and expertise is needed to use them). It can also be difficult to choose an appropriate standard for process control systems (SCADA systems). However, some technical standards provide frequently updated international recommendations and advice. Technical standards for managing ICT safety and security need to be evaluated and further developed if they are to become more applicable for process control systems (SCADA systems) running critical infrastructures. According to Nicholson et al. (2012), any upcoming standards should address shortcomings in current SCADA system architectures, administrative policies, and platform security mechanisms, and it is important for both vendors and end-users to comply with these standards.
- With a poor understanding of risk, the quality of the preventive safety and security work will not be satisfactory. Human factors such as a basic understanding of risk, knowledge, expertise, determination, and attitudes must be in place for organizational and technical aspects of the safety and security work to function as intended.
- The different subcultures within the network companies should learn to communicate better with regard to ICT safety and security. In the oil and gas industry, Johnsen (2012) found that key mitigating factors for similar challenges were a focus on common meeting arenas, increased training and awareness, cooperation, and the establishment of common goals and common risk perceptions (common mental models) among the relevant groups.
- Instead of trusting in the expertise of their system vendors (suppliers) and counting on the vendors to create safe solutions, the SCADA system owners (network companies) need to become more vocal in demanding secure products from their vendors.
- There is a general need for increased awareness of the uncertainty and complexity of the ICT systems used in the electric power supply, as well as an increased focus on ICT safety and security among managers and employees in both large and small network companies. This is particularly relevant today because of the implementation of AMI and the smart grid.
- The top management must demonstrate its commitment to ICT safety and security through its activities and through a dedicated budget.

- The lack of awareness of a danger might lead to weak vigilance by users and a greater potential for abuse. Interactive face-to-face presentations of information about ICT safety and security can be a useful measure to raise awareness among managers and employees in the network companies, as can involving the employees in the development of ICT safety and security measures.

- Role playing exercises and e-learning can also be useful measures to improve knowledge and awareness of how to act safely and securely, which in turn can affect managers' and employees' risk perception.

- With infrequent incidents, the risk of inaction may seem small and owners need appropriate motivation. Hildick-Smith (2005) suggested that this could come from a government-funded awareness blitz. Experts could debunk naive assumptions, instill some fear, and provide stepped guidance documents with common language.

9.3 Future research

An interesting topic for future research is a closer examination of the internal control systems in the network companies. The regulations require the companies to have internal ICT safety and security management systems, but it would be interesting to find out more about how the network companies actually comply with the regulations. Many of the respondents in my survey answered "don't know" on questions regarding perception of compliance, which made it difficult to perform analyses of the data material (e.g., correlation) because there were too many missing values. Moreover, the use of hidden identity in the survey made it difficult to conduct a missing data analysis to obtain information about the respondents who answered "don't know" in this survey. However, that so many respondents answered "don't know" on these items can be seen as an interesting finding in itself, and it may point to a lack of knowledge and awareness of the ICT safety and security requirements in the regulations and thus a lack of compliance with these regulations.

Many of the deviations from the contingency planning regulations that NVE noted during inspections relate to incomplete or inadequate risk and vulnerability analysis and contingency plans. According to NVE's annual supervision reports in recent years, many companies lack a systematic approach to safety, security, and contingency planning. Another interesting path for further research is a more thorough study of the network companies' risk and vulnerability analyses and contingency plans related to ICT safety and security in their SCADA systems, including how often they are updated and how they are actually used in the safety and security management of the companies.

According to discrepancies in the results of my study, further research on management commitment to ICT safety and security in the network companies is needed, including examination of the role top management plays in the safety and security management of these companies. Further exploration of the use of ICT safety and security awareness creation and training measures involving employee participation and practical learning through interaction (e.g., e-learning, role-playing exercises) might also be an interesting topic for further research.

10. References

Adler, E. and Clark, R. (2014), *An Invitation to Social research – How it's done* 5th edition, Cengage Learning, Stamford, USA.

Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26, pp. 276-289.

Albrechtsen E., and Hovden, J. (2007), "Industrial safety management and information security management: risk characteristics and management approaches", in Aven, T. and Vinnem, J.E. (Eds.) *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference 2007* (Esrel 2007), Taylor & Francis, London, pp. 2333-40.

Albrechtsen, E., and Hovden J. (2009), "The information security digital divide between information security managers and users", *Computers & Security,* Vol. 28 No. 4, pp. 76-90.

Albrechtsen, E., and Hagen, J. M. (2009), "Information security measures influencing user performance", in Martorell et al. (Eds.), *Proceedings of Safety, Reliability and Risk Analysis: Theory, Methods and Applications,* Taylor & Francis Group, London, pp. 2649-2656.

Almklov, P., Antonsen, S. and Fenstad, J. (2012), "Organizational Challenges Regarding Risk Management in Critical Infrastructures", in Hokstad P., Utne I. B., and Vatn J. (Eds.), *Risk and Interdependencies in Critical Infrastructures: A guideline for analysis,* Springer-Verlag, London, pp. 211-225.

Andersson H. (2011), "Perception of Own Death Risk: An Assessment of Road-Traffic Mortality Risk", *Risk Analysis*, Vol. 31 No. 7, pp. 1069-1082.

Ansell, C., Boin, A., and Keller, A. (2010), "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System, *Journal of Contingencies and Crisis Management,* Vol. 18 No. 4, pp. 196-207

Antonsen, S. (2009), *Safety Culture: Theory, Method and Improvement,* Ashgate.

Antonsen, S., Almklov, P., Fenstad, J., and Nybø, A. (2010), "Reliability Consequences of Liberalization in the Electricity Sector: Existing Research and Remaining Questions"*, Journal of Contingencies and Crisis Management*, Vol. 18 No. 4, pp. 208-219.

Antonsen, S., Skarholt, K., and Ringstad, A. J. (2012), «The role of standardization in safety management – A case study of a major oil & gas company», *Safety Science,* Vol. 50, pp. 2001-2009.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H. and Sandve, K. (2004), *Samfunnssikkerhet [Societal Safety],* Universitetsforlaget, Oslo.

Aven, T. (2007), "A unified framework for risk and vulnerability analysis covering both safety and security"*, Reliability Engineering and System Safety,* Vol. 92, pp. 745-754.

Aven, T. (2014), "What is Safety Science?", *Safety Science,* Vol. 67, pp. 15-20.

References

Aven, T., and Renn, O. (2010), Risk *Management and Governance: Concepts, Guidelines and Application*, Springer, Heidelberg, Dordrecht, London, New York.

Bailey, K. D. (1994), *Methods of Social Research* 4th edition, The Free Press, New York, Ontario.

Baldwin, R., Cave, M., and Lodge, M. (2012), *Understanding Regulation – Theory, Strategy and Practice,* 2nd edition, Oxford University Press.

Bang, P., and Thuestad, O. (2014), “Governmental enforced self regulation. The Norwegian case”, in Lindøe P. H., Baram, M., and Renn, O. (Eds.), *Risk governance of offshore oil and gas operations*, Cambridge University Press, New York, pp. 243-273.

Baumeister, T. (2010), “Literature Review on Smart Grid Cyber Security”, Collaborative Software Development Laboratory, Department of Information and Computer Sciences, University of Hawai‘I, Honolulu, HI.

Beck, U. (1992), *Risk Society – Towards a New Modernity*, Sage, London.

Berger, P. L. and Luckmann, T. (1966), *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, Anchor Books, New York.

Besnard, D., and Arief, B. (2004), “Computer security impaired by legitimate users”, *Computers & Security*, Vol. 23, pp. 253-264.

Bieder, C. and Bourier, M. (2013), *Trapping Safety into Rules. How Desirable or Avoidable is Proceduralization?,* Ashgate, London.

Boin, A. and McConnel, A. (2007), “Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience”, *Journal of Contingencies and Crisis Management,* Vol. 15 No. 1, pp. 50-59.

Brooks, B. (2005), “Not drowning, waving! Safety management and occupational culture in an Australian commercial fishing port”, *Safety Science*, 43, pp.795-814.

Brunsson, N., and Jacobsson, B. (2000), *A world of standards*, Oxford University Press Inc., New York.

Cristensen, T., Lægreid, P. and Rykkja, L. H. (2012), “How to cope with a terrorist attack? – A challenge for the political and administrative leadership”, COCOPS Working Paper No. 6, European Commission, Seventh Framework Programme.

Cooper, M. D. (2000), “Towards a Model of Safety Culture”*, Safety Science*, Vol 36, pp. 111-136.

Creswell, J. W. (2003), *Research design – Qualitative, Quantitative, and Mixed Methods Approaches* 2nd edition, Sage publications, Thousand Oaks, London, New Dehli.

Creswell, J. W. (2011), “Controversies in mixed methods research”, in Denzin, N. K., and Lincoln, Y. S. (Eds.), *The SAFE handbook of qualitative research* 4th edition, Sage, Thousand Oaks, pp. 269-284.

Creswell, J. W., and Plano Clark, V. L. (2007), *Designing and conducting mixed methods research,* Sage, Thousand Oaks.

References

Dagbladet (2013), http://www.dagbladet.no/nullctrl/ (accessed 30 December 2013).

DiMaggio, P. J. and Powell, W. W. (1983), "The iron cage revisited" institutional isomorphism and collective rationality in organizational fields", *American Sociological Review*, Vol. 48, pp. 147-60.

DiMaggio, P. J. and Powell, W. W. (1991), “Institutional Isomorphism and Collective Rationality”, in Powell, W. W. and DiMaggio, P. J. (Eds.), *The New Institutionalism in Organizational Analysis*, The University of Chicago Press, Chicago and London.

Dobbin, F. (1994), “Cultural models of organization: The social construction of rational organizing principles”, *The sociology of culture*, pp. 117-142.

Dyreborg, J. (2006), «Mellem papiret & virkeligheden – Institusjonalisering af sikkerhed i byggebransjen» [Between paper and reality – institutionalisation of work safety in the Construction industry], Ph.d. avhandling, Institut for Miljø, Teknologi og Samfund, Roskilde Universitetscenter & Arbeidsmiljøinstituttet.

Eakin, J. (1992), “Leaving it up to the workers: sociological perspective on the management of health and safety in small workplaces”, *International Journal of Health Services*, Vol. 22 No. 4, pp. 689-704.

Engen, O. A., and Olsen, O. E. (2010), “Small steps toward big accidents”, in Bris, Guedes Soares and Martorell (Eds), *Reliability, Risk and Safety: Theory and Applications,* Taylor & Francis Group, London.

Engen, O. A., Hagen, J., Kringen, J., Kaasen, K., Lindøe, P. H., Selnes, P. O., and Vinnem, J. E. (2013), Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet [The Norwegian safety regime for the petroleum industry], Report, 27 August.

Eriksson, K. and McConnell, A. (2011), “Contingency planning for crisis management: Recipe for success or political fantasy?, *Policy and Society,* Vol. 30, pp. 89-99.

Eriksson, G., Svensson, O., and Eriksson, L. (2013), “The time-saving bias: judgements, cognition and perception”, *Judgement and decision making*, Vol. 8 No. 4, pp. 492-497.

FACTS (2013), “Energy and Water Resources in Norway”, Norwegian Ministry of Petroleum and Energy.

Flin, R., A. O’Dea, and S. Yule (2002), “Leadership Behaviours for Maximizing Safety”, SPE International Conference on Health, Safety and Environment in Oil and Gas Exploration and production, The Society of Petroleum Engineers, Kuala Lumpur, March 20-22.

Fosso, O. B., Molinas, M., Sand, K., and Coldevin, G. H. (2014), “Moving Towards the Smart Grid: The Norwegian Case”, The 2014 International Power Electronics Conference.

Fox, J., Murray, C. and Warm, A. (2003), “Conducting research using web-based questionnaires: practical, methodological, and ethical considerations”, *Int. J. Social Research Methodology,* Vol. 6 No. 2, pp. 167-180.

Fricker, R. D., and Schonlau, M. (2002), “Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature”, *Field Methods,* Vol. 14 No. 4, pp. 347-367.

Fridheim, H., Hagen, J. and Henriksen, S. (2001), ”En sårbar kraftforsyning – Sluttrapport etter BAS3” [A vulnerable electric power supply – Final report from BAS3], FFI/RAPPORT-2001/02381.

Fridheim, H. and J. Hagen (2007), «Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport» [Protection of the society 5: Vulnerability in critical ICT systems – final report], FFI-rapport 2007/01204.

Gilad, S. (2010), “It Runs in the Family: Meta-Regulation and its Siblings”, *Regulation & Governance,* Vol. 4, pp. 485-506.

Gold, R. (1958), "Roles in sociological field observation", *Social Forces*, Vol. 36, pp. 217-213.

Goodhue, D. L., and Straub, D. W. (1991), “Security concerns of system users – A study of perceptions of the adequacy of security”, *Information &Management*, Vol. 20, pp. 13-27.

Greenwood, R., Oliver, C., Suddaby, R., and Sahlin, K. (2008), *The SAGE Handbook of Organizational Institutionalism,* SAGE.

Guldenmund, F. W. (2000), “The nature of safety culture: A review of theory and research”, *Safety Science*, Vol. 34 No. 1-3, pp. 215-257.

Guldenmund, F. W. (2007), *The use of questionnaires in safety culture research – an evaluation.* Safety Science, Vol 45, pp. 723-743.

Hagen, J. M., Albrechtsen, E., and Hovden, J. (2008), “Implementation and effectiveness of organizational information security measures”, *Information Management & Computer Security,* Vol. 16 No. 4, pp. 377-397.

Hagen J. M. (2009), “The Human Factor behind the Security Perimeter – Evaluating the effectiveness of organizational information security measures and employees' contributions to security”, PhD Thesis no. 2009:874, Series of dissertations submitted to the Faculty of Mathematics and Natural Sciences, University of Oslo.

Hagen, J. M., and Albrechtsen, E. (2009a), “Regulation of information security and the impact on top management commitment: A comparative study of the energy supply sector and the finance sector”, in Martorell et al. (Eds.), *Proceedings of Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Taylor & Francis Group, London, pp. 407-413.

Hagen, J. M., and Albrechtsen, E. (2009b), “Effects on employees’ information security abilities by e-learning”, *Information Management & Computer Security,* Vol. 17 No. 5, pp. 388-407.

Hagen, J., Fridheim, H. and Nystuen, K. O. (2005), “New Challenges for Emergency Preparedness in the Information Society”, *Telektronikk* 1, pp. 48-54.

Hagen, J. M., Sivertsen, T. K., and Rong, C. (2008), “Protection against unauthorized access and computer crime in Norwegian enterprises”, *Journal of Computer Security*, Vol. 16, pp. 341-366.

Hagen, J. M. (2011), http://www.ffi.no/no/Aktuelle-tema/Sider/Doktorgrad-ominformasjonssikkerhet.aspx (accessed 4 October 2013).

References

Hair, J. F. (1998), *Multivariate data analysis*, Prentice Hall, New Jersey.

Hansen, L., and Nissenbaum, H. (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly,* Vol. 53, pp. 1155–1175.

Hasle, P., and Limborg, H. J. (2006), A review of the literature on preventive occupational health and safety activities in small enterprises, *Industrial Health,* Vol. 44 No. 1, pp. 6-12.

Hildick-Smith, A. (2005), "Security for Critical Infrastructure SCADA Systems", SANS Institute.

Hoffman, A. J. (1999), "Institutional Evolution and Change: Environmentalism and the US Chemical Industry", *Academy of Management Journal*, Vol. 42 No. 4, pp. 351-371.

Hokstad, P., Utne, I. B. and Vatn, J. (2012), "Risk and Vulnerability Analysis of Critical Infrastructures", in Hokstad P., Utne I. B., and Vatn J. (Eds.), *Risk and Interdependencies in Critical Infrastructures: A guideline for analysis,* Springer-Verlag, London, pp. 23-34.

Hollnagel, E., Pariès, J., Woods, D. D., and Wreathhall, J. (2010), *Resilience Engineering in Practice: A Guidebook,* Ashgate Studies in resilience Engineering.

Hood, C., Rothstein, H., and Baldwin, R. (2001), *The Government of Risk: Understanding Risk Regulation regimes,* Oxford University Press.

Hopkins, A. (2011), "Risk-management and rule-compliance: Decision-making in hazardous industries", *Safety Science,* Vol. 49, pp. 110-120.

Hopkins, A. (2014), "Issues in Safety Science", *Safety Science,* Vol 67, pp. 6-14.

Hovden, J. (1998), "The Ambiguity of Contents and Results in the Norwegian Internal Control of Safety, Health and Environment Reform", *Reliability Engineering and System Safety,* Vol. 60, pp. 133-141.

Hughes, T. P. (1992), "The Evolution of Large Technological Systems", in Bijker, Pinch and Hughes (Eds), *Social Construction of Technological Systems*, MIT.

IRGC (2010), "The Emergence of Risks: Contributing Factors", International Risk Governance Council, Geneva.

Jaatun, M.G., Albrechtsen, E., Line, M.B., Tøndel, I.A., and Longva, O.H. (2009), "A Framework for Incident Response Management in the Petroleum Industry", *International Journal of Critical Infrastructure Protection*, Vol. 2, No. 1, pp. 26-37.

Jepperson, R. L. (1991), "Institutions, Institutional Effects, and Institutionalism"*,* in Powell, W. W. and DiMaggio, P. J. (Eds), *The New Institutionalism in Organizational Analysis,* The University of Chicago Press, Chicago and London.

Johnsen, S. O. (2012), "An Investigation of Resilience in Complex Socio-Technical Systems to Improve Safety and Continuity in Integrated Operations", Thesis for the degree of Philosophiae Doctor, NTNU.

Johnson, E. C. (2006), “Awareness training, security awareness: switch to a better programme”, *Network Security*, Vol. 2, pp. 15-18.

Johnson, C. W. (2014), “Anti-social networking: crowdsourcing and the cyber defence of national critical infrastructures”, *Ergonomics*, Vol. 57 No. 3, pp. 419-433.

Juhl, K. (2009), “Problem of Ethnic Politics and Trust: The Missing Persons Institute of Bosnia-Herzegovina”, *Genocide Studies and Prevention,* Vol. 4, No. 2, pp. 239-270.

KAEC (2014), Kentucky Association of Electric Cooperatives, Inc., http://www.kaec.org/energy/article1.htm (accessed 19 December 2014)

Kahneman D, Tversky A. On the Reality of Cognitive Illusions. Psychological Review 1996; 103(3):582-591.

Kraemer, S., Carayon, P., and Clem, J. (2009), “Human and organizational factors in computer and information security: Pathways to vulnerabilities”, *Computer Security,* Vol. 28, pp. 509-520.

Kundur, D., Feng, X., Liu, S., Zountos, T., and Butler-Purry, K. L. (2010), “Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid”, Texas A&M University: Department of Electrical and Engineering.

Lango, P., Lægreid, P. and Rykkja, L. H. (2011), “Organizing for Internal Security and Safety in Norway”, in Nota, G., *Risk Management Trends*, INTECH, pp. 167-189.

Leonardi, P. M., and Barley, S. R. (2010), "What's Under Construction Here? Social Action, Materiality, and Power in Constructivist Studies of Technology and Organizing", *Academy of Management Annals,* Vol. 4, pp. 1–51.

Leveson, N. (2004), “A New Accident Model for Engineering Safer Systems”, *Safety Science,* Vol. 42 No. 4, pp. 237-270.

Leveson, N., Dulac, N., Marais, K. and Carroll, J. (2009), “Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems”, *Organization Studies*, Vol. 30 No. 2-3, pp. 227-249.

Lindøe, P.H. (2001), “Integrating Occupational Health, Environment and Safety Management with Management Systems. An Easy Match for Bigger Enterprises and a Mismatch for the Smaller Ones?”, Paper presented at the 6th European International Industrial Relation Congress, Oslo, June 25-26.

Lindøe, P. H., Baram, M., and Renn, O. (2014), *Risk Governance of Offshore Oil and Gas Operations*. Cambridge University Press, New York.

Lindøe, P. H., and Engen, O. A. (2013), “Offshore Safety Regimes - A Contested Terrain”, in Nordquist, M. H., Moore, J. N., Chircop, A., and Long, R. (Eds), *The Regulation of Continental Shelf Development. Rethinking International Standards*, Martinus Nijhoff Publishers, Leiden, Boston, pp. 195-212.

Lindøe, P. H., Olsen, O. E., and Lie, T. (2006), “Systematic Occupational Health and Safety Management in Complex Industrial Settings”, *Applied Ergonomics* (CD-ROM), 6. ISSN 0003-6870.

Line, M. B., and Tøndel, I. A. (2012), “Information and Communication Technology: Enabling and Challenging Critical Infrastructure”, in Hokstad, P., Utne, I. B., Vatn, J. (Eds), *Risk and Interdependencies in Critical Infrastructures: A guideline for analysis*, Springer-Verlag, London, pp. 147-225.

Longhurst, R. (2010), “Semi-structured Interviews and Focus Groups”, in Clifford N., French S., and Valentine, G., *Key methods in Geography* 2nd Edition, Sage Publications, Thousand Oaks.

Lægreid, P. and Rykkja, L. H. (2013), “Coordination practice: Coordinating for internal security and safety in Norway”, COCOPS, European Commission, Seventh Framework Programme.

Mearns, K., Flin R., Fleming, M., Gordon, R. (1997), “Human and Organizational Factors in Offshore Safety”, Health and Safety Executive – Offshore Technology Report, HSE Books.

Mearns, K., Flin, R. and O’Connor, P. (2001), “Sharing “worlds of risk”; improving communication with crew resource management”, *Journal of Risk Research*, Vol. 4 No. 4, pp. 377-392.

Nicholson, A., Webber, S., Dyer S., Patel, T. and Janicke, H. (2012), “SCADA security in the light of Cyber-Warfare”, *Computers and Security,* Vol. 31, pp. 418-436.

NIS (2013), “FOCUS 2013 - Annual Assessment by the Norwegian Intelligence Service”, http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/0886-FOCUS-english-2013.pdf (accessed 10 June 2014).

NordForsk (2013), “Societal Security in the Nordic Countries”, Policy Paper 1-2013.

NSM (2011), “ICT risk scenario – A strategic challenge”, https://www.nsm.stat.no/Engelsk-start-side/News-publications/news/ICT-risk-scenario-A-strategic-challenge/ (accessed 10 June 2014).

NSR (2012), “Norwegian Computer Crime and Security Survey” [Mørketallsundersøkelsen], http://www.nsr-org.no/moerketall/ (accessed 10 June 2014).

NSR (2014), “The Norwegian Business and Industry Security Council (NSR)”, http://www.nsr-org.no/summary-in-english/the-norwegian-business-and-industry-security-council-nsr-article346-172.html (accessed 10 June 2014).

NVE and Proactima (2010), «Veiledning i risiko- og sårbarhetsanalyser for kraftforsyning» [Guideline for risk and vulnerability analysis for the electric power supply], Veileder nr: 2-2010.

NVE (2013), «Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften)» [Guideline for contingency planning regulations], Veileder nr: 1-2013.

NVE (2014a), “About NVE – Acts and regulations”, http://www.nve.no/en/About-NVE/Acts-and-regulations/ (accessed 10 June 2014).

NVE (2014b), “Licensing”, http://www.nve.no/en/Licensing/Introduction-to-licensing/ (accessed 10 June 2014).

OECD (2003), “Emerging risks in the 21st century”, OECD Publications, Paris.

OECD (2006), “Studies in Risk Management, Norway – Information Security”, OECD Publications, Paris.

OECD (2009), “Innovation in Country Risk Management”, OECD Publications, Paris.

OEDC (2011a), “Future Global Shocks - improving risk governance”, OECD Publications, Paris.

OECD (2011b), “Reducing Systemic Cybersecurity Risk”, OECD Publications, Paris.

Okrent, D. and Pidgeon, N.F. (Eds) (1998), “Risk assessment versus risk perception”, special volume of *Reliability Engineering and System Safety*, Vol. 59, pp. 1-159.

Olsen, O.E., Kruke, B. I., and Hovden, J. (2007), “Societal safety: Concept, borders and dilemmas”, *Journal of contingencies and Crisis Management,* Vol 15 No. 2, pp. 69-79.

Oltedal, S., Moen, B. E., Klempe, H., and Rundmo, T. (2004), “Explaining risk perception – An evaluation of cultural theory”, Rotunde publications no. 85.

Oltedal, H. A. (2011), “Safety culture and safety management within the Norwegian-controlled shipping industry – State of art, interrelationships, and influencing factors”, PhD Thesis UiS no. 137 – October 2011, Faculty of Social Sciences.

Open Security Alliance (2014), “Cyber War”, http://opensecurityalliance.org/OSA/cyber-war/ (accessed 6 June 2014).

Orlikowski, W. J., and Barley, S. R. (2001), “Technology and Institutions: What can research on information technology and research on organisations learn from each other?”, *MIS Quarterly,* Vol. 25 No. 2, pp. 145-165.

Pallant, J. (2010), *SPSS Survival Manual – A step by step guide to data analysis using SPSS* 4th ed., Open University Press, Berkshire, New York.

Patel, S. C. and Sanyal, P. (2008), “Securing SCADA systems”*, Information Management & Computer Security*, Vol. 16 No. 4, pp. 398-414.

Perrow, C. (1984), *Normal Accidents: Living with High-Risk Technologies,* Princeton University Press, New Jersey.

Pett, M. A., Lackey, N. R. and Sullivan, J. J. (2003), *Making sense of factor analysis – The use of factor analysis for instrument development in Health care research*, Sage publications, Thousand Oaks, London, New Delhi.

Piètre-Cambacédès, L., and C. Chaudet (2010), “The SEMA Referential Framework: Avoiding Ambiguities in the Terms ‘Security’ and ‘Safety’”*, International Journal of Critical Infrastructure Protection,* Vol. 3, pp. 55-66.

Power, M. (2007), *Organized Uncertainty: Designing a World of Risk Management,* Oxford University Press, Oxford.

PST (2012), “Annual threat assessment”, http://www.pst.no/media/utgivelser/annual-threat-assessment-2012/ (accessed 10 June 2014).

Rasmussen, J. (1997), "Risk management in a dynamic society: A modelling problem", *Safety Science*, Vol. 27, pp. 183-213.

Reason, J. (1997), *Managing the Risks of Organizational Accidents,* Ashgate Publishing Limited, Aldershot.

Reiman, T. and Rollenhagen, C. (2011), "Human and organizational biases affecting the management of safety", *Reliability Engineering & System Safety*, Vol. 96, 1263-1274.

Regjeringen (2012a), "Cyber Security Strategy for Norway" [Nasjonal strategi for informasjonssikkerhet], *http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf* (accessed 10 January 2013).

Regjeringen (2012b), "Cyber Security Strategy for Norway - Action Plan" [Nasjonal strategi for informasjonssikkerhet – Handlingsplan], *http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf* (accessed 10 January 2013).

Renn, O. (2008*), Risk governance: Coping with uncertainty in a complex world*, Earthscan, London.

Renn, O. (2014), "A Generic Model for Risk Governance – Concept and Application to Technological Installations", in Lindøe, P. H., Baram, M., and Renn, O. (Eds), *Risk Governance of Offshore Oil and Gas Operations,* Cambridge University Press, New York, pp. 9-33.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001), "Identifying, understanding, and analyzing critical infrastructure interdependencies", *IEEE Control Systems Magazine*, Vol. 21, pp. 11-25.

Roberts, K. H., and Grabowski, M. (1996), "Organizations, Technology, and Structuring", in Clegg, S. R., Hardy, C., and Nord, W. R., Sage, pp. 409-423.

Rodal, S. K. (2001), "Sårbarhet i kraftforsyningens drifts- og styringssystemer" [Vulnerabilities in the information systems of the electric power supply], FFI report no. 04278; 2001.

Roe, E. and Schulman, P. R. (2008), *High Reliability Management*, Stanford University Press.

Rundmo, T. (1996), "Associations between risk perceptions and safety", *Safety Science,* Vol. 24 No. 3, pp. 197-209.

Rykkja, L. H., Fimreite, A. L., and Lægreid, P. (2011), "Attitudes towards Anti-terror Measures: The Role of Trust, Political Orientation and Civil Liberties Support", *Critical Studies of Terrorism*, Vol. 4 No. 2, pp. 219-237.

Røyksund, M. (2011), «Informasjonssikkerhet i kraftforsyningen» [Information Security in the electric power supply], Master thesis in societal safety, University of Stavanger.

Sarewitz, D., Pielke, R. J., and Keykhah, M. (2003), "Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective", *Risk Analysis,* Vol. 23 No. 4, pp. 805-810.

Scheytt, T., Soin, K., Sahlin-Andersson, K. and Power M. (2006), "Special Research Symposium: Organizations and the Management of Risk. Introduction: organizations, Risk and Regulations", *Journal of Mangement Studies*, Vol. 43 No. 6, p. 1331 - 1337.

Scott, W. R. (1995), *Institutions and Organizations. Ideas, Interests and Identities,* Sage.

Scott, W. R. (1998), *Organizations: Rational, Natural and Open Systems*, 4th ed., Prentice Hall, Englewood, Cliffs, NJ.

Scott, W. R. (2008), *Institutions and Organizations: Ideas and Interest,* 3rd ed. SAGE Publications.

Short J. L., and Toffel, M. W. (2010), "Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment", *Administrative Science Quarterly,* Vol. 55, pp. 361-396.

Silverman, D. (1993), *Interpreting Qualitative Data. Methods for Analysing Talk, Text and Interaction* 1st edition, Sage publications, London.

Silverman, D. (2006), *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction* 3rd edition, Sage publications, London.

Sinclair, D. (1997), "Self-Regulation Versus Command and Control? Beyond False Dichotomies", *Law & Policy*, Vol. 19 No. 4, 529–559.

Siponen, M., and Oinas-Kukkonen, H. (2007), "A Review of Information Security Issues and Respective Research Contributions", *SIGMIS Database*, Vol. 38 No. 1, pp. 60-80.

Sivertsen, T. K. (2007), «Risikoanalyse av samfunnskritiske IKT-systemer – Teknologiske erfaringer» [Risk analysis of critical information systems – Technological experiences], FFI/Rapport – 2007/00910.

Sjöberg, L. (2000), "Factors in Risk Perception", *Risk Analysis,* Vol. 20 No. 1, pp. 1-11.

Sjöberg L., Moen, B-E., and Rundmo, T. (2004), "Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research", Rotunde, No. 84.

Skogdalen, J.E. and Tveiten, C. (2011), Safety perceptions and comprehensions among offshore installation managers on the Norwegian Continental Shelf, Working on Safety, Røros, Norway, 2010.

Slovic, P., Fischoff, B., and Lichtenstein, S. (1982), "Why Study Risk Perception?", *Risk Analysis*, Vol. 2 No. 2, pp. 83-93.

Slovic, P. et al. (2000), *The perception of risk,* Earthscan Publications Ltd., London.

Smart grid (2014), "Advanced Metering Infrastructure and Customer Systems", https://www.smartgrid.gov/recovery_act/deployment_status/ami_and_customer_systems (accessed 5 June 2014).

Stouffer, K., Falco, J., and Scarfone, K. (2011), "Guide to industrial control systems (ICS) security – Recommendations of the National Institute of Standards and Technology", U.S. Department of Commerce, Special Publication 800-82.

Svensson, O. (2008), "Decisions among time saving options: When intuition is strong and wrong", *Acta Psychologica*, Vol. 127, pp. 501-509.

Swanson, M., Bowen, P., Philips, A. W., Gallup, D. and Lynes, D. (2010), “Contingency Planning Guide for Federal Information Systems”, NIST Special Publication 800-34 Rev. 1.

Tabachnick, B. G. and Fidell, L. S. (2007), *Using multivariate statistics* 5th ed., Pearson Education, Boston.

TBSMUN (2014), “Cyberwarfare”, TBS Model United Nations, Disarmament and International Security (DISEC).

Teknisk Ukeblad (2012), ”Sikkerhet i kraftnettet– Kraftsystemet må ikke bli lavterskeltilbud for terrorister” [Security in the power grid – The electric power supply system must not become a low-treshold service for terrorists], http://www.tu.no/energi/2012/12/14/-kraftsystemet-ma-ikke-bli-lavterskel-tilbud-for-terrorister (accessed 17 December 2012).

The GRID Consortium (2007), “ICT Vulnerabilities of Power Systems: A Roadmap for Future Research”, European Commission, Joint Research Centre, Institute for Protection and Security of the Citizen.

Thomson M. E., von Solms R. (1998), “Information security awareness: educating your users effectively”, *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

Tversky, A., Kahneman, D. (2000), “Advances in Prospect Theory – Cumulative Representation of Uncertainty”, in *Choices, Values and Frames*, Kahneman, D. and Tversky, A., (Eds), Cambridge University Press, Cambridge, United Kingdom, pp. 44-65.

Utne, I. B., Hassel, H. and Johansson, J. (2012), “A Brief Overview of Some Methods and Approaches for Investigating Interdependencies in Critical Infrastructures”, in Hokstad P., Utne I. B., and Vatn J. (Eds), Risk and Interdependencies in Critical Infrastructures: A guideline for analysis, Springer-Verlag, London, pp. 1-11.

Vatn, J., Hokstad, P. and Utne, I. B. (2012), “Defining Concepts and Categorizing Interdependencies”, in Hokstad P., Utne I. B., and Vatn J. (Eds), *Risk and Interdependencies in Critical Infrastructures: A guideline for analysis*, Springer-Verlag, London, pp. 13-22.

Weber, K. and M. A. Glynn (2006), “Making Sense with Institutions: Context, Thought and Action in Karl Weick’s Theory”*, Organization Studies,* Vol. 27 No. 11, pp. 1639-1660.

Weick, K. E. (2001), *Making Sense of the Organization*, Blackwell Business, Oxford.

Westrum, R. (1992), “Cultures with requisite imagination”, in Wise, J., D. Hopkin and P. Stager (Eds), *Verificaton and Validation of Complex Systems: Human Factors Issues,* Springer-Verlag, Berlin, pp. 401-16.

Westrum, R. (2004), “A typology of organizational cultures”, *Qual Saf Health Care*, Vol. 13 (Suppl II), pp. ii22-ii27.

White Paper 17 (2001-02), “Societal Safety” (Norway).

References

Yin, R. K. (1994), *Case Study Research. Design and Methods* 2nd edition, Sage publications, Thousand Oaks, London, New Delhi.

Part II

List of articles

Article 1

Skotnes, R. Ø. and Engen, O. A. (2015), Attitudes toward risk regulation – Prescriptive or functional regulation?, *Safety Science,* Vol. 77, pp. 10–18.

Article 2

Skotnes, R. Ø. (2012), Strengths and weaknesses of technical standards for management of ICT safety and security in electric power supply network companies, *Journal of Risk and Governance*, Vol. 3, Iss 2, pp. 119-134.

Article 3

Skotnes, R. Ø. (2015), Risk perception regarding the safety and security of ICT systems in electric power supply network companies, *Safety Science Monitor,* Vol. 19, Iss 1, article 4.

Article 4

Skotnes, R. Ø., (2015), Management commitment and awareness creation – ICT safety and security in electric power supply network companies, *Information & Computer Security*, Vol. 23, Iss 3, pp. 302 – 316.

Article 1

Safety Science 77 (2015) 10–18

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Attitudes toward risk regulation – Prescriptive or functional regulation?

Ruth Østgaard Skotnes *, Ole Andreas Engen

Center for Risk Management and Societal Safety (SEROS), Department of Media, Culture, and Social Sciences, University of Stavanger, 4036 Stavanger, Norway

ARTICLE INFO

Article history:
Received 14 October 2014
Received in revised form 27 January 2015
Accepted 13 March 2015
Available online 1 April 2015

Keywords:
Attitudes
Risk regulation
Functional
Prescriptive
ICT

ABSTRACT

This article addresses attitudes toward the use of functional versus prescriptive risk regulations. The context for the study is the use of functional internal control regulations for information and communication technology (ICT) safety and security in network companies within the Norwegian electric power supply sector. The rapid development in ICT has made traditional methods of command and control (prescriptive) regulation by government less adequate in coping with modern risks, and the introduction of internal control has been an attempt to develop new approaches and means to cope with new challenges of misfits between technology and regulation (Hovden, 1998). The article concludes that the degree of complexity, uncertainty and uncontrollability of a specific risk problem experienced by different actors, can explain varying attitudes toward the use of functional regulations for controlling risks.

1. Introduction

Information and communication technology (ICT) is increasingly becoming a part of all critical infrastructures (Line and Tøndel, 2012), and ICT is now used to monitor, control and operate power generation plants and power distribution within electric power supply systems (Patel and Sanyal, 2008). The recent trends are toward more general-purpose solutions, software, and using the Internet for communication related to operation and management of remote processes and production systems. This increases efficiency and cooperation, saves time, and reduces costs. However, this also makes formerly isolated ICT systems vulnerable to a set of threats and risks they have not been exposed to before (Line and Tøndel, 2012). Process control systems, e.g. supervisory control and data acquisition systems (SCADA systems) , and other ICT systems used within electric power supply systems, are vulnerable to a multitude of physical, electromagnetic, and logical threats, both natural and man-made (Rodal, 2001).

Vulnerability of ICT systems within electric power supply systems is also expected to increase during the next few years. Advanced Metering Infrastructure (AMI) and, later on the Smart Grid, are now being introduced in electric power systems in the Western world. The electric Smart Grid promises increased capacity, reliability, and efficiency through the marriage of cyber technology and the existing electricity network. However, the scale and complexity of the smart grid, along with its increased connectivity and automation, make the task of cyber protection particularly challenging (Kundur et al., 2010).

During the past decades there has been a marked change in the way risk, safety, and security legislation is framed in many industrialized countries. The trend has moved toward functional rules that emphasize the required outcomes of safety and security management, allowing considerable freedom on the part of the organizations to identify the means by which these ends will be achieved (Reason, 1997). The context for this study is regulations for ICT safety and security in network (transmission and distribution) companies within the Norwegian electric power supply sector. The current study is part of a larger research project which focuses on challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector. Based on a literature review, document studies of the contingency planning regulations for the Norwegian electric power supply system, and an evaluation of pre-existing questionnaires regarding similar issues, we chose to explore several different dimensions in the research project, i.e. knowledge of safety and security, perception of compliance, attitude toward safety and security, attitude toward regulation, experience of incidents, risk perception, safety and security management (management commitment), and awareness creation and training. The aim of the current article is to discuss possible explanations for varying attitudes toward the use of functional internal control regulations as the principle for regulating risks.

In the Norwegian electric power supply sector principles of internal control were introduced in the area of contingency

* Corresponding author at: SEROS, Department of Media, Culture and Social Sciences, University of Stavanger, Kristine Bonneviesvei 15, 4036 Stavanger, Norway. Tel.: +47 51 83 15 13; fax: +47 51 83 15 50.
E-mail addresses: ruth.skotnes@uis.no (R.Ø. Skotnes), ole.a.engen@uis.no (O.A. Engen).

http://dx.doi.org/10.1016/j.ssci.2015.03.008
0925-7535/© 2015 Elsevier Ltd. All rights reserved.

planning in 2002, and one of the areas regulated by internal control is ICT safety and security. Instead of designing detailed rules and control systems, the authorities prescribe safety and security goals and permit the companies to develop and enforce their own detailed rules. This provides more capacity for the authorities to work on other important tasks, and is at the same time meant to contribute to a heightening of the individual company's sense of responsibility for their own safety and security (Ot.prp. nr. 56 (2000–2001)).

Previous research has shown that ambiguity of results of internal control regulations may be explained by organizational size, where large companies have been seen as better suited to implement internal control than smaller companies (Hovden, 1998; Lindøe, 2001). However, results of a survey we conducted among managers and employees in Norwegian network companies in 2012 revealed no statistically significant differences between large and small network companies regarding their attitude toward the internal control regulations for ICT safety and security. Managers and employees in both large and small network companies had diverging views on and varying attitudes toward internal control regulations, depending on the specific question that was asked.

Hence, the following research question is discussed in the article:

– What can explain varying attitudes toward the use of functional internal control regulations as the principle for regulating risks?

The article is organized as follows: First, we give a brief overview of the regulatory context for this study and the complexity of ICT systems. Second, we present our theoretical perspectives followed by presentations of method and data analysis. In the theory section we argue for a distinction between safety and security, introduce the principles of internal control and function based regulatory systems, and conclude why an analysis of complex technologies and functional risk regulations is required. In the section concerning material and methods we present the mixed method applied in this study and give an overview of the interviews, observation studies, document studies, and questionnaire survey. The results and discussion are divided in two sections where the first aims to present different viewpoints concerning function based regulation among the groups of actors, and the second discusses reasons for these viewpoints and whether the findings express challenges for safety and security management in the electric power supply sector as such.

1.1. Regulatory context for the study

In Norway, internal control principles for controlling safety were introduced in the offshore oil industry in the 1980s, and have since then spread to many other sectors. In 1992, the principles of internal control were introduced for all onshore activities, and the internal control regulation was again revised in 1997. The Norwegian Water Resources and Energy Directorate (NVE) has the legislative power to issue regulations for companies within the electric power supply sector, is responsible for supervision, and perform regular inspections to ensure compliance with regulations. Risk management is required by law, in the Internal Control Regulation from 1997.[1] For the electric power supply sector the requirement for risk management is further reinforced through several different regulations. Contingency planning is regulated by the Energy Act,[2] the Energy Act Regulations,[3] and the Contingency Planning Regulations.[4] ICT safety and security is regulated by The Norwegian Security Act,[5] and is further reinforced through Sections 6 and 7 in the contingency planning regulations. In addition, NVE develop regulatory guidelines for the contingency planning regulations. The guidelines are to be continually developed and quality assured based on feedback from the electric power supply companies.

1.2. Complexities of ICT systems

Technology has an ever-changing nature, and current technologies (e.g. ICT systems) in many cases strain and stretch old models of technology and organizations (Roberts and Grabowski, 1996). The use of computer systems involves the self-contained, invisible material process that is actually unfolding, as well as the equally self-contained, equally invisible imagined process that is mentally unfolding in the mind of an individual or a team. Both managers and operators (employees) experience increasing cognitive demands for inference, integration, problem solving, and mental mapping to understand what is going on out of sight. There is also continuous intervention improvement and redesign (technological innovations) in computer technologies, which means that the implementation state of development never stops, and these technologies require ongoing structuring and sensemaking if they are to be managed (Weick, 2001). Increased cognitive demands, increased electronic complexity, and dense organizational interdependence over large areas, often lead to an increase in incidences of unexpected outcomes that produce unexpected ramifications (Roberts and Grabowski, 1996).

The main problem is that it will be impossible to predict the widespread impacts should one system component fail. Systems can be described by their complexity, and by the tight coupling of their components and processes. Most societal services and critical infrastructure will adhere to Perrow's (1984) description of complexity and tight couplings, and this is especially true for critical ICT systems (Hagen et al., 2005). New technologies, such as complex production systems that use computers, have created unusual problems in sensemaking for managers and employees (Weick, 2001). According to Leveson (2004), technology today (especially digital technology) is changing faster than engineering techniques to cope with the new technology is being created. Lessons learned over centuries about designing to prevent accidents may be lost or become ineffective when older technologies are replaced with new ones. The time to market for new products has significantly decreased, and carefully testing systems and designs to understand all the potential behaviors and risks before commercial and scientific use is often no longer possible. Interactive complexity is increasing in the systems we are building, and we are designing systems with potential interactions among the components that cannot be thoroughly planned, understood, anticipated, or guarded against. Thus the degree of uncertainty is also high (Aven and Renn, 2010).

2. Theory

In the area of risk research, it is traditional to distinguish between the terms safety and security, and the meaning of the terms can vary considerably from one context to another. According to Piètre-Cambacédès and Chaudet (2010), two relevant and representative distinctions can be identified (the SEMA referential framework). The first is the system versus environment

[1] January 1, 1997: Regulation concerning Systematic Health, Environment and Safety Activities at Enterprises (Internal Control Regulation).

[2] Act No. 50 of 29 June 1990.

[3] REG. No. 1990 of 7 December 1990.

[4] Reg. No. 1157 of 7 December 2012: Regulations relating to contingency planning in the power supply system.

[5] Act No. 10 of 20 March 1998: Regulations relating to Protective Security Services.

distinction, where security is concerned with the risks originating from the environment and potentially affecting the system, whereas safety deals with the risks arising from the system and potentially affecting the environment. The second is the malicious versus accidental distinction, where security typically addresses malicious (intentional) risks, while safety addresses purely accidental (unintentional) risks (p. 59). With regards to ICT systems, both safety and security issues are important. ICT systems are vulnerable to both attacks and accidents (e.g. technical malfunctions), and risks that may arise both within the organizations and in the organizations' environment.

Modes of risk (or safety and security) regulation can be seen as a discussion of the pros and cons of rule-compliance versus risk management (Hopkins, 2011), with a distinction between 'hard regulation' based on 'command and control' with prescriptive rules, and 'soft regulation' with concepts coined as 'self-regulation' (Sinclair, 1997; Short and Toffel, 2010), 'meta-regulation' (Gilad, 2010), etc. An important question is whether these modes of regulation represent a dichotomy or whether they are complementary as presented in Fig. 1. Our argument follows Sinclair (1997), stating that the dichotomy is false. Different countries often have different regulatory regimes; many factors in each country influence regulation itself and what is given attention by the regime (Lindøe et al., 2013). In practice, risk regulation regimes will combine responsibilities and roles in a public–private partnership with a top-down approach with legal binding norms, and a bottom-up approach with industrial (technical) standards and 'best practice'. The use of legal standards becomes a 'linking pin' that brings the two approaches together as indicated in the right part of Fig. 1.

Function based regulation needs some form of discretionary criteria that are considered as legal standards and provide some special interpretation challenges. The term 'legal standard' refers to words or phrases in a law claim that stipulates a scale or norm beyond the law, i.e. a particular practice, widespread attitudes in the community or other conditions that change with time. While these phenomena change over time, the contents of the law do not. The use of legal standards aims to achieve an appropriate regulation of complex fields in constant development. It can also be seen as an expression of respect for the importance of expert knowledge to ensure the safety and quality in key areas of society. Legal standards probably safeguard the goal of safety and quality better than if they had been fully formulated in laws and regulations. The underlying measure of the legal standards is based on an understanding of the issues, terminology and solutions that are understood in the professional and scientific community. Through stakeholder involvement in the process of developing these norms, the use of legal standards may enjoy greater legitimacy than rules based on legal terminology and legal text.

A consistent application of a function based regulation requires a comprehensive and systematic review on how the various provisions are to be understood and how the appropriate standards should be used to meet the requirements. Procedures must provide relationships between laws and regulations and technical/professional standards to comply in accordance with the laws and predictability in relation to regulators' evaluations. For the regulatory authorities and inspectors this can be a demanding and comprehensive system to keep up to date, and it requires that the standards keep pace with developments and new knowledge. Comprehensive guidelines may also be an excuse for companies for not taking responsibility in monitoring and implementing new recognized expertise and scientific knowledge.

2.1. Internal control regulations

When self-regulation is used to assure safety, enterprises are obliged to identify and assess risks and hazards embedded in their operations (Lindøe et al., 2006). Internal control gives companies a personal responsibility to monitor and implement an updated safety management system. The term 'safety management system' (or 'risk management system') can be used to describe all measures that are implemented to achieve, maintain and develop a level of safety in accordance with defined safety goals.

According to Power (2007), internal control systems embody both the potential of greater efficiency and coordination on the one hand, and of greater sensitivity to social responsibility issues on the other. The latter refers to a view of internal control systems as the basis for more substantive improvement of, for example, health, safety and environment. Organizations have an incentive for compliance with principles of internal control, because the regulatory process can focus on desired outcomes rather than regulating detailed processes, with regulatory intervention as a last resort. In cases of breach or dissatisfaction, the regulatory body has options to escalate its enforcement process with more serious consequences for the regulated organization. Some regulatory systems are linked to licensing privileges (including the regulatory system for the Norwegian electric power supply system), where a license to trade or conduct an activity is conditional on compliance with formal or procedural norms; such as having 'effective' internal control. The sanction of withdrawing a license is usually a last resort and an outcome of extensive prior negotiation (Power, 2007).

The rapid development in ICT has made traditional methods of command and control regulation by government less than adequate in coping with modern risks, and the introduction of internal control has been an attempt to develop new approaches and means to cope with new challenges of misfits between technology and regulation (Hovden, 1998). Detailed and prescriptive rules provide no incentives for enterprises to engage in innovative practice, and bind them to the established technology and organizational solutions. The more prescriptive rules and technical standards the regulator takes as legally binding, the more responsibility and greater 'burden of proof' are imposed on themselves. Explicit and detailed requirements are certainly highly predictable and easily interpreted, but they soon may stiffen in technologies from the past. It is difficult to see how safety critical issues related to management, organization and technology can be improved by the authorities using additional or more detailed rules (Bieder and Bourier, 2013).

The internal control system can be equally demanding and comprehensive system to keep up to date for the authorities. They need a lot of knowledge and expertise to monitor that companies comply with the functional regulations, and have to keep pace with technological developments and new knowledge. However, the advantage of using principles of internal control is that the scope and form of the internal control system can vary with a company's size, complexity, domain, and risk scenario, and this allows each company to adjust it to their own needs, routines, organization, and culture. The function based character of the regulatory regime creates a large degree of autonomy for how employers and companies can design the technology and safety and security practices they think are appropriate. Such autonomy can be advantageous for employers in several ways, also financially. It has not least an intrinsic value for the employer side because they can decide the choice of means by themselves instead of being overruled by the authorities (Bang and Thuestad, 2014).

3. Material and methods

As mentioned in the introduction, the aim of this study was to discuss possible explanations for varying attitudes toward the use of functional internal control regulations as the principle for regulating risks. To fulfill this aim a mixed-method approach was used,

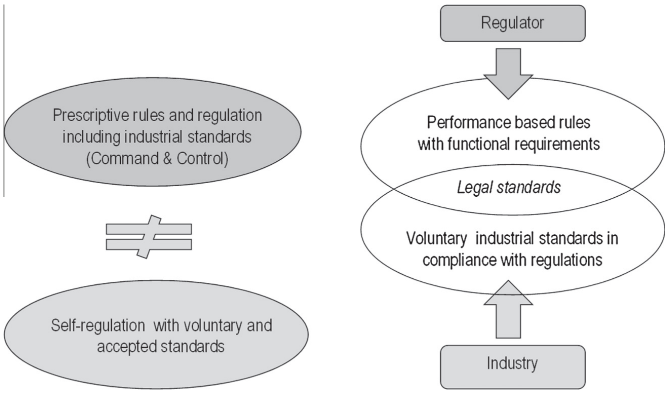

Prescriptive rules and regulation including industrial standards (Command & Control)
≠
Self-regulation with voluntary and accepted standards
Regulator
Performance based rules with functional requirements
Legal standards
Voluntary industrial standards in compliance with regulations
Industry

Fig. 1. Two modes of risk regulations.

including both qualitative and quantitative research methods. The research methodology was based on interviews, observation studies, document studies, and a survey among managers and employees in network companies within the Norwegian electric power supply sector. A combined approach can strengthen the validity of the study, as some of the findings can complement and validate each other (Silverman, 2006). Moreover, a combined approach can also show discrepancies between analysis results of data collected using different methods, as in the current study, and may thus open for new possibilities of interpretation.

3.1. Interviews, observation studies, and document studies

Qualitative data was gathered through two group interviews with representatives from NVE. These interviews were performed at the beginning of the research project which this study is a part of, to explore our research theme and produce research questions that could be tested by the quantitative survey. Furthermore, some of the results from the interviews are also provided in this article to complement the data gathered through the survey.

Semi-structured interviews with open ended questions were used. The interviewees were representatives from the contingency planning department in NVE, who are responsible for safety, contingency planning, and supervision and inspection in the Norwegian electric power supply sector. The first interview was done with three interviewees, and the questions mainly focused on the interviewees' opinion of the Norwegian network companies' risk perception and awareness regarding the risk of electric network failure caused by malfunctions in or attacks on their ICT systems. The second interview was done with two interviewees, and the questions mainly focused on the interviewees' opinion regarding the use of functional internal control regulations for ICT safety and security, and their impression of the network companies' attitude toward these regulations.

Observation studies were carried out at two conferences on ICT safety and security for companies within the electric power supply sector. During the observation studies we observed the types of ICT safety and security issues raised at the conferences, the type of issues participants focused on, and the types of questions and discussions that came up during the conferences. Both the interviews and observation studies were conducted in 2011. In addition, information about the internal control regulations for ICT safety and security in Norwegian network companies was collected from written documents, e.g. regulations relating to contingency planning in the Norwegian power supply system, and guidelines for the contingency planning regulations.

3.2. Questionnaire development and survey sample

A questionnaire was designed for the research project which this study is a part of. As previously mentioned, this design was based on a literature review, document studies of the contingency planning regulations for the Norwegian electric power supply system, and an evaluation of 5 pre-existing questionnaires. The pre-existing questionnaires were used in studies of offshore (petroleum) safety and ICT safety and security, i.e. 'Offshore Safety Questionnaire' (Mearns et al., 1997), Norwegian Petroleum Safety Authorities' survey 'Trends in risk level – Norwegian Shelf' from 2007–2008, 'Accident prevention – survey for offshore employees' (survey used in PhD project, Centre of Maritime Health and Safety, University of Southern Denmark, H. B. Rasmussen, 2008–2012), 'The Norwegian Computer Crime and Security Survey' from 2010, and questions used in Janne M. Hagen's study 'How do employees comply with security policy? A comparative case study of four organizations under the Norwegian Security Act' (Hagen, 2009).

A web-based questionnaire was developed using QuestBack Survey, and distributed to the respondents by e-mail. Web-based surveys can eliminate some of the more labor-intensive fielding tasks, such as survey package preparation and mailing, and the subsequent data entry. In web surveys the respondents' answers can be directly downloaded into a database, avoiding transcription errors (Fricker and Schonlau, 2002). Before distributing the survey, we performed a pilot-test of the questionnaire to ensure that the instructions and scale items were clear. We sent the pilot to three respondents; one contingency planning manager, one ICT safety and security manager, and one system control center operator, and the questionnaire was adjusted according to feedback. The survey was distributed to respondents in June 2012, and was closed in September 2012. We sent two e-mail reminders to each respondent during the time the survey was open.

The survey was sent to managers in all the 137 network companies that were part of the Power Supply Preparedness Organisation (PSPO), 334 individuals in total. The PSPO prepares, establishes, and maintains a structure to efficiently handle extraordinary situations in the power supply system. In 2012, the PSPO included 197 organizations, and 137 of these could be classified as network companies (numbers were provided by NVE). The questionnaire contained ten sections – background information, knowledge of safety and security, perception of compliance, attitude toward safety and security, attitude toward regulation, experience of incidents, risk perception, safety and security management, awareness creation and training, and overall rating of the safety and security level of the organizations' ICT systems. The focus in this article is on results from 4 items regarding attitude toward regulations, which are shown in Table 3 Items on the scale were measured on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

One hundred and three respondents returned the survey questionnaire, for a response rate of 31%. NVE provided the names and e-mail addresses of ICT safety and security managers/coordinators and contingency planning managers in the network companies, and the managers were asked to provide names and e-mail addresses for employees in the organizations' system control centers and ICT staff. The Statistical Package of the Social Sciences (SPSS) v. 18 was used to perform all analyses. The categorical variable 'job category' was collapsed into two categories representing managers and employees. The category 'managers' consisted of contingency planning manager, ICT safety and security manager, and 'other leader', and the category 'employees' consisted of: operator in system control center, employee in ICT staff, and 'other employee'.

Table 1 shows the demographical distribution of the respondents. 66 respondents were managers, and 32 were employees (5 respondents did not specify their job category). Only 3 of the respondents were female and the rest male, however this corresponds well with the gender distribution of employees in Norwegian network companies. 63 respondents worked in small network companies with less than 100 employees, and 37 respondents worked in large network companies with more than 100 employees (3 respondents did not answer the item regarding company size). Based on the use of hidden identity in the electronic survey we lack information regarding how many of the 137 network companies the respondents actually represented. However, 29 respondents were ICT safety and security managers (information security managers), 11 from large companies and 18 from smaller companies. Due to the fact that each company only has one ICT safety and security manager, at least 29 companies are represented in the data material and most likely more.

A survey sample of 103 respondents can be considered a relatively small sample, and may limit the potential for generalizing. Nevertheless, according to Pallant (2010, p. 207) a sample of 100+ respondents can be regarded as a large sample, and the sample size can be seen as adequate for the types of data analyses done in our study. According to Fricker and Schonlau (2002), response rates for web surveys where no other survey mode is given have tended to range from moderate to poor. Other researchers have also experienced the same response rate problem in studies of information security management. Kotulic and Clark (2004, referred to in Albrechtsen and Hovden (2009)) followed up their small response rate with a study suggesting that the main reasons for non-responses were related to a policy of not sharing information regarding their information security performance, the volume of survey requests received by the organizations, and a desire not to spend valuable time on the particular research project.

In an attempt to raise the response rate, hidden identity for respondents was activated in our electronic survey, and all e-mail addresses were deleted after the survey was closed. When hidden identity is used in surveys, no identifiable information (e.g. browser type and version, Internet IP address, operating system, or e-mail address) will be stored with the answer. Because of the policy of not sharing information regarding information security performance, hidden identity was activated to assure the respondents that the information they provided could not be traced back to themselves or their company. In addition, we signed a confidentiality agreement with NVE before we received e-mail addresses for ICT safety and security managers and contingency planning managers in the network companies. In the confidentiality agreement we agreed that we would not publish any information or results that could in any way be linked to a specific company or person. The respondents were also given information of this confidentiality agreement in the survey invitation e-mail, and were informed that they could contact us if they needed a copy of the confidentiality agreement before they agreed to answer the survey. Lastly, qualitative research data were gathered through interviews, observation studies and document studies to support the quantitative results from the survey.

Table 1
Demographic profiles of respondents.

Job categories			Company size		Total
			More than 100 employees	Fewer than 100 employees	
Manager	Gender	Male	19	44	63
		Female	1	1	2
	Total		20	45	65[a]
Employee	Gender	Male	14	15	29
		Female	1	0	1
	Total		15	15	30[a]
Other	Gender	Male	2	3	5
	Total		2	3	5
Total	Gender	Male	35	62	97
		Female	2	1	3
	Total		37	63	100

[a] Three respondents (1 manager and 2 employees) did not answer the item regarding company size. Thus, the numbers in this table are not completely consistent with the numbers in Section 4.1.

4. Results

4.1. Results from interviews, observation studies and document studies

According to our interviewees from NVE, the introduction of internal control regulation has actually led to a *lesser* focus on contingency planning in the organizations. Many of the companies feel pressured from all sides, and have not been able to establish enough internal resources to keep the focus on contingency planning. The results from our interviews also suggested that the larger network companies generally have been most interested in having functional rather than detailed prescriptive rules. On the other hand, several small companies are also asking for less detailed ICT safety and security rules and requirements. These smaller companies may now have acquired more expertise on safety and security management since the internal control regulations were introduced.

According to NVE, the network companies express divergent views at different times regarding the question about functional versus prescriptive rules and requirements. On a general basis the network companies want functional internal control risk regulations with more freedom of choice, but in specific situations involving specific risk problems (e.g. the implementation of Advanced Metering Infrastructure (AMI)) they ask for more detailed rules and want NVE to tell them exactly what to do. According to our interviewees from NVE, the attitudes toward functional internal control regulations in the network companies can also vary depending on who you are talking to. The top management may be interested in having functional regulations, but the middle-management and employees working with the actual implementation of the internal control system might want more concrete and detailed regulations. However, NVE sees a clear need for the introduction of internal control principles also in other areas under their jurisdiction.

During observation studies at ICT safety and security conferences within the electric power supply sector, we observed several representatives from network companies questioning the authorities regarding the implementation of AMI. The network company representatives asked whether the authorities would give them more concrete requirements for how to implement AMI besides recommendations, e.g. technical demands, demands regarding choice of suppliers, etc. The answer from NVE's representative was that the requirements in the regulations are mainly functional, and it is up to the individual network companies to identify the means by which these ends will be achieved. NVE did, however, strongly recommend that all decisions regarding how to implement AMI should be based on a thorough risk assessment of all possible vulnerabilities and threats to the ICT systems' safety and security. Some of the network company representatives expressed dissatisfaction with this answer, and wanted NVE to take more control of the implementation process, instead of just setting the goals and leaving the actual implementation to the companies.

4.2. Data analysis and results of survey

Independent samples *t*-tests were performed in order to identify significant differences in the mean values for the respondents. We found no statistically significant differences in the mean scores between managers and employees on the 4 items regarding attitude toward functional internal control regulations for ICT safety and security in the survey. We found a statistically significant difference in the mean scores between large and small network companies on item 3, however the magnitude of the differences in the means were small. Hence, in the present article the focus will be on descriptive statistics of the whole survey sample. Table 2 shows the results of the independent samples *t*-tests.

4.2.1. Descriptive statistics

Table 3 shows the distribution of scores on items 1–4 in the survey. The distribution of scores on item 1 regarding the use of functional regulations shows that around 70% of the respondents were positive to functional regulations ('Agree' and 'Strongly agree'). On item 2 regarding the need for more detailed guidelines the highest percentage of the respondents answered 'Neither disagree nor disagree' (35%), which is the neutral middle point. 30, 1% answered negatively on this item ('Strongly disagree' and 'Disagree'), and 34% answered positively ('Strongly agree' and 'Agree'). On item 3 regarding the guidelines being too detailed, 32% of the respondents did not think that the requirements and guidelines for ICT safety and security in chapter 6 of the guidelines for the contingency planning regulations were too detailed ('Strongly disagree' and 'Disagree'). Only 13, 6% of the respondents agreed with the item, and found the requirements and guidelines too detailed. On the other hand, 47, 6% of the respondents answered that they neither disagreed nor agreed with the item, and 5, 8% answered 'Don't know'. On item 4 regarding the desire for more detailed guidelines in connection to the introduction of AMI, 57% of the respondents were positive ('Strongly agree' and 'Agree') to more detailed guidelines from the authorities for the introduction of AMI, while only 12, 7% were negative ('Strongly disagree' and 'Disagree'). 23, 3% neither disagreed nor agreed to this item.

The survey among managers and employees in Norwegian network companies suggested that a majority of the respondents had a positive attitude toward functional regulations. At the same time the respondents had divergent opinions about the need for more detailed guidelines for how to comply with the ICT safety and security goals and requirements in the

Table 2
Results of independent samples *t*-tests.

	Managers	Employees	*t*	*P*	Large companies	Small companies	*t*	*p*
Item 1	*N* = 66, *M* = 3.89, SD = 1.07	*N* = 31, *M* = 3.74, SD = 1.06	*t* (95) = .65	*p* = .52 (2-tailed)	*N* = 37, *M* = 3.89, SD = 1.05	*N* = 62, *M* = 3.94, SD = 1.02	*t* (97) = –.20	*p* = .84, (2-tailed)
Item 2	*N* = 66, *M* = 3.06, SD = 1.07	*N* = 31, *M* = 3.39, SD = 1.02	*t* (95) = –1.43	*p* = .16 (2-tailed)	*N* = 36, *M* = 3.22, SD = 1.10	*N* = 63, *M* = 3.08, SD = 1.05	*t* (97) = .64	*p* = .52 (2-tailed)
Item 3	*N* = 64, *M* = 2.81, SD = .83	*N* = 27, *M* = 2.74, SD = .86	*t* (89) = .37	*p* = .71 (2-tailed)	*N* = 34, *M* = 2.59, SD = .78	*N* = 59, *M* = 2.98, SD = .80	*t* (91) = –2.31[1]	*p* = .02 (2-tailed)
Item 4	*N* = 62, *M* = 3.76, SD = 1.06	*N* = 29, *M* = 3.86, SD = 1.06	*t* (89) = –.43	*p* = .67 (2-tailed)	*N* = 32, *M* = 3.75, SD = .95	*N* = 61, *M* = 3.80, SD = 1.12	*t* (91) = –.23	*p* = .82 (2-tailed)

[1] The magnitude of the differences in the means was small (eta squared = .055).

Table 3
Distribution of scores on item 1–4.

	Distribution of scores on items (in percentage)			
	Item 1: *"I think it's ok that the authorities prescribe the overall safety goals and requirements for ICT safety and security, and permit the organizations to find and develop their own means to achieve these goals"*	Item 2: *"I wish that the authorities would provide us with more detailed guidelines for how we can achieve the goals and requirements for ICT safety and security in the contingency planning regulations"*	Item 3: *"The requirements and guidelines for ICT safety and security in Chapter 6 of the 'Guidelines for the contingency planning regulations for the Norwegian electric power supply' are too detailed"*	Item 4: *"In connection to the introduction of Advanced Metering Infrastructure (AMI) in the Norwegian electric power supply system, I wish that the network companies could receive more detailed guidelines from the authorities"*
Strongly disagree	2.9% (*N* = 3)	2.9% (*N* = 3)	2.9% (*N* = 3)	1.0% (*N* = 1)
Disagree	8.7% (*N* = 9)	27.2% (*N* = 28)	29.1% (*N* = 30)	11.7% (*N* = 12)
Neither disagree nor agree	17.5% (*N* = 18)	35.0% (*N* = 36)	47.6% (*N* = 49)	23.3% (*N* = 24)
Agree	37.9% (*N* = 39)	20.4% (*N* = 21)	9.7% (*N* = 10)	28.2% (*N* = 29)
Strongly agree	32.0% (*N* = 33)	13.6% (*N* = 14)	3.9% (*N* = 4)	29.1% (*N* = 30)
Not relevant	0.0% (*N* = 0)	0.0% (*N* = 0)	1.0% (*N* = 1)	1.9% (*N* = 2)
Don't know	1.0% (*N* = 1)	1.0% (*N* = 1)	5.8% (*N* = 6)	4.9% (*N* = 5)
Total	*N* = 103	*N* = 103	*N* = 103	*N* = 103

contingency planning regulations, but very few respondents felt that the requirements and guidelines for ICT safety and security were *too* detailed. On the other hand, a majority of the respondents also answered that they wanted more detailed guidelines concerning the implementation of a new technology (Advanced Metering Infrastructure). This confirms the existence of varying attitudes toward the functional internal control regulations for ICT safety and security in network companies within the Norwegian electric power supply sector.

5. Discussion

The pros and cons of rule-compliance versus risk management is continuously debated (Hopkins, 2011), and defining how the roles in safety and security management should be distributed between the state and the industry is one of the most complex questions regarding risk regulation (Lindøe and Engen, 2013).

In Norway, internal control principles (enforced self-regulation and functional requirements) for controlling risk were, as previously mentioned, introduced in the offshore oil (petroleum) industry in the 1980s. The regulatory system for this industry builds on a diversified mixture of legal and industrial norms and standards (Lindøe, 2010). In 2013, an expert group (appointed by the government) reviewed the regulatory strategy and the Health, Safety and Environment (HSE) regulations for the Norwegian petroleum sector through an extensive interview-study with relevant organizations and agencies. According to the expert group's report, all the interview-groups were positive to the regulatory regime; the risk-based regulations with functional requirements were regarded as well-functioning, with an ability to get a complicated industry to comply with the goal of safe and efficient operation. Functional regulations are intended to be flexible in relation to introduction of new technology, new organizational forms, routines, and practices, and thus ensuring continuous learning. However, these regulations leave a lot of room for interpretations, which for some companies can lead to uncertainty as to what is appropriate and correct (Engen et al., 2013).

The guidelines to the risk regulations in the Norwegian Petroleum industry refer to recognized technical (industrial) standards as a way to fulfill the functional requirements. However, with a steadily growing number of technical standards considerable knowledge and technical skill is required to be able to use them. Renewing these standards also requires a lot of resources, and several of the interview-groups in the petroleum sector study found the regulatory regime to be too complicated, with overlapping of standards in some areas. Furthermore, the respondents all agreed that increasing complexity within the sector had major implications for the risk regulation. Some of the respondents pointed out that the flexibility of the functional internal control regulations may be misused to choose only minimum solutions during less prosperous times, and thus not facilitating any development. On the other hand, to meet the requirements in the functional regulations other companies develop rigid internal systems with routines and procedures which can exceed the functional requirements and thus lead to reduced flexibility (Engen et al., 2013).

Results from our interviews suggested that the introduction of internal control has lead to a lesser focus on safety, security and contingency planning in the Norwegian network companies. Earlier research has shown that small companies with limited resources have often had more problems with their internal control implementation due to a lack of clear and detailed guidelines on how to do it, while larger and more proactive companies with competence and resources have found it easier to tailor an effective safety and security management system. Large companies with a bureaucratic form, clear lines of authority, and expertise on safety and security management, may be better suited for the implementation of internal control systems. The reason for the revision of the internal control regulation in Norway in 1997 was to take into account the special problems of small and medium sized enterprises by a simplification of the requirements (Hovden, 1998; Lindøe, 2001). Even so, the results of our survey did not show significant differences in attitudes toward the functional internal control regulations for ICT safety and security between small and large network companies within the Norwegian electric network sector.

The findings from our interviews and observation studies correspond well with results from the previously mentioned interview-study in the Norwegian petroleum industry. The relationship between functional and prescriptive risk regulations is an area of conflict between the different actors within this industry as well. The industry in general considers the functional regulations as well-functioning and wants as few detailed requirements as possible. However, contrary to this, the labor unions and the government want to increase the amount of minimum requirements. New companies within the industry are also requesting more guidance and detailed requirements from the authorities (Engen et al., 2013).

The Norwegian electric power supply sector consists of companies with different organizational forms, functions, tasks, size, and goals, and it can be difficult to issue detailed regulations that would apply to all companies. The advantage of using principles of internal control is that the scope and form of the internal control system can vary with a company's size, complexity, domain, and risk scenario, and this allows each company to adjust it to their own needs, routines, organization, and culture (Hovden, 1998).

Even though NVE sees a clear need for the introduction of internal control principles also in other areas under their jurisdiction, there seem to be a reorientation toward *a combination* of functional and prescriptive regulations within this sector. The Norwegian Energy Act's rules for contingency planning in the electric power supply sector were changed in 2012. In addition, on behalf of the Ministry of Petroleum and Energy, NVE has revised the regulations for contingency planning in the Norwegian electric power supply sector, and new contingency planning regulations and guidelines for these regulations have taken effect from 2013. Increased vulnerability and threats due to increased use of ICT to monitor, control, and operate power generation plants and power distribution is one of the main reasons for the revisions. In many areas of the regulations former practice is still followed, but with a clearer specification of the requirements. In some areas the regulations are tightened through new requirements, or a stricter use of the existing practice. NVE has tried to make the requirements in the contingency planning regulations clearer and more concrete based on requests from the electric power supply companies.

Internal control regulations regarding ICT safety and security can pose a specific challenge for the safety and security managers in electric power supply network companies because of the complexity of the ICT systems. It is difficult to establish a complete system description of these complex systems (Rundmo, 1996), which can make it hard to identify successful attacks and their consequences and develop comprehensive defenses for all the relevant threats. The scale and complexity of the AMI and Smart Grid, along with its increased connectivity and automation, will make risk regulation of this area particularly challenging. These high complexity systems have tight coupling of their components and processes. The fast paced technological change, the invisibility of the material processes, the lack of overview, and the problems in sensemaking, contribute to a sense of uncertainty, uncontrollability, and unpredictability regarding the risk problems connected to these ICT systems. Most of the network companies lack expert knowledge in this area, which increases the need for more detailed prescriptive regulations.

6. Conclusion

As previously stated, a function based regulatory risk regime creates a large degree of autonomy for how companies can design the safety and security practices they think are appropriate, and it is difficult to see how safety critical issues related to management, organization and technology can be improved by using additional or more detailed rules by the authorities. Even so, the results of interviews, observation studies, and a survey among managers and employees in Norwegian network companies, confirmed that there exists varying attitudes and divergent opinions at different times regarding the question about functional versus prescriptive risk regulation. The respondents generally have a positive attitude toward functional regulations for ICT safety and security, however, at the same time a majority of the respondents have also answered that they want more detailed guidelines for the current implementation of a new complex technology (Advanced Metering Infrastructure). This may be caused by the increased electronic complexity, increased cognitive demands, fast paced technological change, and problems in sensemaking that these new technologies have created for both managers and employees.

Thus, varying attitudes and divergent opinions at different times toward the use of functional risk regulations can be explained by the degree of complexity and uncertainty of a specific risk problem experienced by different actors. The more loosely coupled the system to be managed is, and the more controllable and predictable the risk problem is perceived to be, the greater the request for functional risk regulations will be. And correspondingly, the more tightly coupled the system to be managed is, and the more complex, unpredictable, and uncertain the risk problem is perceived to be, the greater the request for prescriptive, detailed regulations will be – regardless of whether the company in question is large or small.

References

Albrechtsen, E., Hovden, J., 2009. The information security digital divide between information security managers and users. Comput. Secur. 28, 476–490.

Aven, T., Renn, O., 2010. Risk Management and Governance: Concepts, Guidelines and Application. Springer, Heidelberg, Dordrecht, London, New York.

Bang, P., Thuestad, O., 2014. Governmental enforced self regulation. The Norwegian case. In: Lindøe, P.H., Baram, M., Renn, O. (Eds.), Risk Governance of Offshore Oil and Gas Operations. Cambridge University Press, New York.

Bieder, C., Bourier, M., 2013. Trapping Safety into Rules. How Desirable or Avoidable is Proceduralization? Ashgate, London.

Engen, O.A., Hagen, J., Kringen, J., 2013. Tilsynsstrategi og HMS-regelverk i norsk petroleumsvirksomhet [The Norwegian Safety Regime for the Petroleum Industry]. Report, 27 August.

Fricker, R.D., Schonlau, M., 2002. Advantages and disadvantages of internet research surveys: evidence from literature. Field Methods 14 (4), 347–367.

Gilad, S., 2010. It runs in the family: meta-regulation and its siblings. Regul. Govern. 4, 485–506.

Hagen, J., 2009. The Human Factor Behind the Security Perimeter. Evaluating the Effectiveness of Organizational Information Security Measures and Employees' Contributions to Security. Ph.D. Diss., University of Oslo.

Hagen, J., Fridheim, H., Nystuen, K.O., 2005. New challenges for emergency preparedness in the information society. Telektronikk 1, 48–54.

Hopkins, A., 2011. Risk-management and rule-compliance: decision-making in hazardous industries. Saf. Sci. 49, 110–120.

Hovden, J., 1998. The ambiguity of contents and results in the Norwegian internal control of safety, health and environment reform. Reliab. Eng. Syst. Saf. 60, 133–141.

Kundur, D., Feng, X., Liu, S., Zountos, T., Butler-Purry, K.L., 2010. Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. Texas A&M University: Department of Electrical and Engineering.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42 (4), 237–270.

Lindøe, P.H., 2001. Integrating occupational health, environment and safety management with management systems. An easy match for bigger enterprises and a mismatch for the smaller ones? Paper presented at the 6th European International Industrial Relation Congress, Oslo, June 25–26.

Lindøe, P.H., 2010. Complex roles and mixed norms – a dilemma for safety inspections? Paper presented at the Working on Safety (WOS) 5th International Conference, Røros, September 7–10.

Lindøe, P.H., Engen, O.A., 2013. Offshore safety regimes – a contested Terrain. In: Nordquist, M.H., Moore, J.N., Chircop, A., Long, R. (Eds.), The Regulation of Continental Shelf Development. Rethinking International Standards. Martinus Nijhoff Publishers, Leiden, Boston, pp. 195–212.

Lindøe, P.H., Olsen, O.E., Lie, T., 2006. Systematic Occupational Health and Safety Management in Complex Industrial Settings. Applied Ergonomics (CD-ROM): 6. ISSN 0003-6870.

Lindøe, P.H., Baram, M., Renn, O., 2013. Risk Governance of Offshore Oil and Gas Operations. Cambridge University Press, New York.

Line, M.B., Tøndel, I.A., 2012. Information and communication technology: enabling and challenging critical infrastructure. In: Hokstad, P., Utne, I.B., Vatn, J. (Eds.), Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis. Springer-Verlag, London, pp. 147–225.

Mearns, K., Flin R., Fleming, M., Gordon, R., 1997. Human and Organizational Factors in Offshore Safety. Health and Safety Executive – Offshore Technology Report. HSE Books.

Ot.prp. nr. 56, 2000–2001. Olje- og energidepartementet [Ministry of Petroleum and Energy]. Ot. prp. nr. 56 (2000–2001): Om lov om endringer i lov 29. juni nr. 50 om produksjon, omforming, overføring, omsetning og fordeling av energi m.m. (energiloven) [Energy Act].

Pallant, J., 2010. SPSS Survival Manual – A Step by Step Guide to Data Analysis using SPSS, fourth ed. Open University Press, Berkshire, New York.

Patel, S.C., Sanyal, P., 2008. Securing SCADA systems. Inform. Manage. Comput. Secur. 16 (4), 398–414.

Perrow, C., 1984. Normal Accidents: Living with High-Risk Technologies. Princeton University Press, Princeton, New Jersey.

Piètre-Cambacédès, L., Chaudet, C., 2010. The SEMA referential framework: avoiding ambiguities in the terms 'Security' and 'Safety'. Int. J. Crit. Infrastruct. Prot. 3, 55–66.

Power, M., 2007. Organized Uncertainty: Designing a World of Risk Management. Oxford University Press, Oxford.

Reason, J., 1997. Managing the Risks of Organizational Accidents. Ashgate Publishing Limited, Aldershot.

Roberts, K.H., Grabowski, M., 1996. Organizations, technology, and structuring. In: Clegg, S.R., Hardy, C., Nord, W.R. (Eds.), Handbook of Organization Studies. Sage, pp. 409–423.

Rodal, S.K., 2001. Sårbarhet i kraftforsyningens drifts- og styringssystemer [Vulnerability in the Electric Power Supply Sector's Process Control Systems]. FFI Report No. 04278; 2001.

Rundmo, T., 1996. Associations between risk perceptions and safety. Saf. Sci. 24 (3), 197–209.

Short, J.L., Toffel, M.W., 2010. Making self-regulation more than merely symbolic: the critical role of the legal environment. Adm. Sci. Quart. 55, 361–396.

Silverman, D., 2006. Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction, third ed. Sage publications, London.

Sinclair, D., 1997. Self-regulation versus command and control? Beyond false dichotomies. Law Policy 19 (4), 529–559.

Weick, K.E., 2001. Making Sense of the Organization. Blackwell Business, Oxford.

Article 2

Article 3

SAFETY SCIENCE Monitor

Issue 1 2015 VOL 19

Article 4

RISK PERCEPTION REGARDING THE SAFETY AND SECURITY OF ICT SYSTEMS IN ELECTRIC POWER SUPPLY NETWORK COMPANIES

RUTH ØSTGAARD SKOTNES

Center for Risk Management and Societal Safety, Department of Media, Culture and Social Sciences, University of Stavanger, 4036 Stavanger, Norway. E-mail address: ruth.skotnes@uis.no. Tel.: +47 51 83 15 13.

ABSTRACT

The purpose of this article is to provide insight into risk perception among users (both managers and employees) of information and communication technology (ICT) systems within electric power supply network companies, and discuss factors that can influence users' risk perception. The electric power supply system is the most critical infrastructure in modern society, and a breakdown in the ICT systems used within this industry (process control systems) can seriously compromise the physical grid which can result in major financial disasters and damage to public safety and health. Process control systems are vulnerable to a multitude of threats, both natural and man-made, and the vulnerability of these ICT systems is also expected to increase during the next few years due to the implementation of new technology. It could therefore be expected that users of ICT systems within network companies would perceive the risk of attacks on or malfunctions in these ICT systems as high. On the contrary, results from a survey sent to 137 Norwegian network companies showed that the respondents perceived this risk as relatively low. Previous research has found that company size, knowledge and awareness of ICT safety and security, and earlier experience of danger, are factors that can influence risk perception within companies. In this article we also suggest that complexities of the ICT systems and a lack of communication between subcultures with different focus points and mindsets within the companies, can explain why users perceive the risk of attacks on or malfunctions in these ICT systems as low. In addition, many issues surrounding ICT safety and security seem to be taken for granted within Norwegian network companies, and many companies trust that the system suppliers will make safe technological solutions that can take care of all problems.

Keywords: Risk perception, ICT safety and security, critical infrastructures, electric power supply, network companies, ICT systems, users

1. INTRODUCTION

Perceived risk, i.e. subjective risk judgments, can be influenced by several factors, and may deviate from "objective" risk. According to Rundmo (1996), biased perception of risk can cause misjudgments of potentially-hazardous risk sources. In a report from the project "Emerging systemic risks in the 21st Century", OECD (Organization for Economic Co-ordination and Development) points to risk perception itself as one factor that can delay or exaggerate precautionary measures (OECD, 2003).

The following research question is examined in the article:

What factors can influence the risk perception of users (managers and employees) within electric power supply network companies regarding the risk of malfunctions in or attacks on their ICT systems?

The research question is answered by presenting results from previous research literature and document studies, results from a survey sent to 137 network companies in Norway, and results from interviews with representatives from the contingency planning department of the Norwegian Water Resources and Energy Directorate (NVE).

ICT has increasingly become a part of all critical infrastructures[i] (Line and Tøndel, 2012), and is used to monitor, control and operate power generation plants and power distribution within electric power supply systems. The electric power supply can be seen as the most critical infrastructure in modern society (Hagen and Albrechtsen, 2009), and a prolonged interruption of the electric power supply may have consequences for many critical societal functions caused by interdependencies between infrastructures. A breakdown in the ICT systems (i.e. process control systems) used within the electric power supply sector can seriously compromise the physical grid, which can result in major financial disasters and damage to public safety and health (Patel and Sanyal, 2008). It could therefore be expected that users of ICT systems within electric power supply network companies would perceive the risk of attacks on or malfunctions in these ICT systems as high.

On the contrary, results from our survey of managers and employees in Norwegian network companies showed that most of the respondents perceived the risk of attacks on or malfunctions in the network organizations' ICT systems as relatively low. Interviews with representatives from NVE also revealed that the regulatory authorities consider most of the network companies to have adequate day-to-day operational safety and security[ii], but think they should perform better when it comes to planning for extraordinary incidents with potentially large consequences. In addition, a qualitative interview study done by Røyksund (2011) showed that, despite an increased focus on ICT safety and security within the sector during recent years[iii], representatives from Norwegian electric power supply companies still perceived the risk of an attack on their ICT systems as relatively low.

The respondents in our survey were ICT safety and security managers, contingency planning managers, operators of process control systems, and ICT personnel. These users work directly with process control systems, ICT issues, and/or safety and security issues within the network companies, and can be expected to have more knowledge about ICT systems and/or safety and security than average end-users of traditional computer systems.

The rest of the article is structured in the following way. The article starts with a presentation of some results from literature and document studies of threats to and vulnerabilities in the electric power supply's ICT systems, and users' view on ICT safety and security. In section 2 theoretical foundations for the study are presented, section 3 presents the data material and methods used in the study, and data analysis and results of the survey are presented in section 4. In section 5 results from the survey, document studies and interviews are interwoven in the discussion, and in section 6 our main findings are summarized in the conclusion.

1.1 Threats to and vulnerabilities in the electric power supply's ICT systems

According to our studies of previous research literature and document studies, process control systems, e.g. supervisory control and data acquisition systems (SCADA systems)[iv], are vulnerable to a multitude of threats, both natural and man-made (Stouffer, Falco and Scarfone, 2011; Rodal, 2001; Hagen, 2009; Line and Tøndel, 2012). The application of ICT systems contributes to increase power system vulnerabilities, in a worldwide scenario where malicious threats against large and complex infrastructures are increasing (The Grid Consortium, 2007). In the past, process control systems were completely isolated from the outside world, but because of market demands there are now logical links between the process control systems and other networks (administrative systems and the internet). In addition, reductions in staff and expertise within the network companies as a result of restructuring and deregulation of the sector since the 1990s have led to increasing dependence on external competence. Work by external suppliers may often be carried out online, and this increases the need to tie all the different participants of the electric power supply together in a massive ICT network. Since logical connections exist between the different ICT systems, skilled hackers may be able to penetrate defenses (Hagen et al., 2005).

Over the last decades, a shift from proprietary hardware to standardized and less expensive operating systems and security products, with commonly known vulnerabilities, has also dramatically increased the number of systems subject to attack (OECD, 2006). According to the U.S. National Institute of Standards and Technology (NIST), electric power is often thought to be one of the most prevalent sources of disruptions of interdependent critical infrastructures. Threats to industrial (process) control systems can come from numerous sources, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders, and natural sources such as system complexities, human errors and accidents, equipment failures and natural disasters (Stouffer, Falco and Scarfone, 2011). The ICT industry itself has started to address many of these security concerns. Soon after a vulnerability is identified, software producers often develop a corrective "patch", that they make available free of charge. However, ICT administrators often find it difficult to keep up to date with corrective patches, and the time lag between the moment a vulnerability is announced (and a patch made available) and the moment hackers start to exploit it is also shrinking (OECD, 2006).

A report from 2012 on terror towards the U.S. electrical grid, concluded that a few, well-informed persons may be able to blackout large areas over a long period of time, with devastating and life-threatening consequences. According to NVE, this threat is just as great for Norway as for the U.S. (Teknisk Ukeblad, 2012). Results from the national “Norwegian Computer Crime and Security Survey” from 2012, showed an increasing gap between threats and safety and security measures in Norwegian organizations, at the same time as ICT dependence is increasing (Næringslivets sikkerhetsråd, 2012). In December 2012, the Norwegian government also launched its “National Strategy for Information Security” (Regjeringen, 2012a). According to the action plan that accompanied this national strategy, the Norwegian authorities’ annual threat assessments ascertained that threats related to ICT based espionage and sabotage have increased in recent years, and we must now expect sophisticated attacks aimed at critical societal information, including ICT systems that operates industrial processes and critical infrastructure (Regjeringen, 2012b).

In 2013, the Norwegian newspaper Dagbladet published a series of articles called “Null CTRL” [“No CTRL”]. The newspaper articles have studied online devices in Norway, and have revealed how a lack of computer security can affect us all at home, at work, and in public spaces. The newspaper has so far alerted the authorities and network owners and/or providers of over 2500 Norwegian control systems (used in e.g. the armed forces, and health, oil, and transport sectors) that are connected to the internet with little or no protection. NVE was interviewed in connection to the article series, and warned that the vulnerability of ICT systems used in electric power supply systems is expected to increase during the next few years (Dagbladet, 2013). Advanced Metering Infrastructure (AMI) and, later on the Smart Grid, are now being introduced in the Norwegian electric power system, as in other Western countries. Smart Grids introduce ICT components into the power distribution grid (e.g. sensors for monitoring and control, smart meters, and two-way communication). Smart Grids connect power plants and system control centers with all households, businesses, and buildings all over the country, as well as abroad (Line and Tøndel, 2012). The electric Smart Grid promises increased capacity, reliability and efficiency through the marriage of cyber technology and the existing electricity network. On the other hand, the scale and complexity of the electric smart grid, along with its increased connectivity and automation, make the task of cyber protection particularly challenging (Kundur et al., 2010).

2. THEORY

2.1 Users’ view on ICT safety and security

According to Dhillon and Backhouse (2000), the role, responsibility and integrity of users are important principles of information security management. A user can be characterized as a person with legitimate access to the organization’s information (and communication) systems (referred to in Albrechtsen, 2007), e.g. end-users, security officers, managers, designers (Besnard and Arief, 2004). Users are said to play an important role in the information security performance of organizations by their security awareness and cautious behavior (Albrechtsen, 2007). Goodhue and Straub (1991) studied the level of security concern among ICT system users, and focused on user’s perceptions about the security of their systems. Previous studies had found that neither end-users nor information security staff believed that there were persuasive reasons to be concerned about security. This lack of concern was found to be alarming in the face of mounting empirical evidence that a significant number of security breaches did occur. A lack of awareness of the danger might lead to weak vigilance by users and a greater potential for abuse.

According to Albrechtsen (2007), a user’s view on information security is created by several interlocking organizational, technological and individual factors. The context of a user’s work may create information security trade-offs, e.g. individuals tend to put emphasis on efficient and least-effort work instead of loss prevention. Social norms and interactions at the work place influence individual understanding of information security, and the quality of information security management also affects users’ awareness, motivation and behavior in some way. Technological information security solutions influence users, and individual factors such as motivation, knowledge, attitudes, values and behavior also influence individual views on information security. Last, but not least, how people perceive risk is a part of the explanation for users’ view on information security, which is the focus of our present study.

2.2 Risk perception

According to Aven and Renn (2010), it is essential to complement data on physical consequences with insights into risk perception when one is dealing with complex and uncertain risk problems. Studies of risk perception examine the opinions that people express when they are asked to characterize and evaluate hazardous activities and technologies. Perceived risk, i.e. subjective risk judgments or a person’s own estimate of risk, may deviate from "objective" risk. “Objective” risk is the risk that exists independent of an individual’s knowledge and worries of the source of the risk (Ulleberg and Rundmo, 1996, referred to in Oltedal et al., 2004). According to Andersson (2011), individuals will be able to make well-informed decisions and expose themselves to an optimal risk level if they have accurate perceptions of risk (i.e. knowledge about the true levels of risk they face. To some extent perceived risk can be a reflection of "objective" (real) risk, especially when risks are well-known (Sjöberg, 2000). Humans are influenced by their surroundings, and the environment affects cognition as well as behavior and individual decisions. The perceived risk concerns how an individual understands and experiences the phenomenon (Oltedal et al., 2004).

Several factors have been found to influence risk perception. Heuristics, probability judgment biases, and frequent media exposure has been said to influence the level of perceived risk (Sjöberg, 2000). Tversky and Kahneman (1974) introduced a program of research on judgment under uncertainty which has come to be known as the heuristics and biases approach. They suggested that intuitive predictions and judgments often are mediated by a small number of distinctive mental operations, called judgmental heuristics. These heuristics are often useful, but they sometimes lead to characteristic errors or biases (referred to in Kahneman and Tversky, 1996). Kahneman and Tversky (1979), criticized expected utility theory as a descriptive model of decision making under risk, and developed an alternative model, called prospect theory. When faced with a complex problem, people employ a variety of heuristic procedures in order to simplify the representation and the valuation of prospects (Tversky and Kahneman, 2000). Examples of perceptual biases can be biases in people's judgments of time saved by increasing the speed of an activity (Svensson, 2008). Time gain is one of the motivators for drivers to speed up, and in turn speeding increases the risk of having an accident (Eriksson, Svensson and Eriksson, 2013). According to Sjöberg (2000), the risk target is of paramount importance in risk studies; people do not make the same estimate when they rate the risk to themselves, to their family, or to people in general. Risk denial is an important feature, and this phenomenon has been related to what has been called unrealistic optimism. People tend to estimate the general risks to be larger than the personal ones. Familiarity with the source of danger, control over the situation, and the dramatic character of the events can also influence risk perception (Oltedal et al., 2004).

Thus, the study of risk perception has a cognitive stance with focus upon perception as mainly a cognitive process. People's risk judgments are related to cognitive processes, e.g. how one is able to comprehend the given information (Slovic, Fischoff and Lichtenstein, 1982). This approach makes up the foundation of the psychometric paradigm in risk perception. According to this paradigm risk can be understood as a function of general properties of the hazard (risk object) (Sjöberg, 2000). The psychometric model is based on a number of explanatory scales (e.g. new risk versus old risk, involuntary risk versus voluntary risk, dreaded risk, number of people exposed, etc.) where the subjects are asked to rate a number of hazards on each of the scales. The cultural theory of risk perception launched by Douglas (1966, 1978) and Douglas and Wildavsky (1982), has also been an important theoretical contribution. According to cultural theory risk perception is not governed by personality traits, needs, preferences, or properties of the risk objects. It is a socially, or culturally, constructed phenomenon. What is perceived as dangerous, and how much risk to accept, is a function of one's cultural adherence and social learning (referred to in Oltedal et al., 2004). Sjöberg (2000) on the other hand, rather sees attitude as a crucial factor in risk perception, in addition to risk sensitivity and specific fear.

According to Aven and Renn (2010), intuitive risk perception is based on how information about a risk is communicated, the psychological mechanisms for processing uncertainty, and earlier experience of danger. This mental process results in perceived risk - a collection of notions that people form regarding risk sources, relative to the information available to them and their basic common sense (Jaeger et al., 2001, referred to in Aven and Renn, 2010). The present article will focus on risk perception among managers and employees within organizations (electric power supply network companies), and in an organization risk perceptions may influence risk behavior and hence influence "objective" risk or safety (Rundmo, 1996). Trust is often held to be of crucial importance for the understanding of risk perception (Sjöberg, 2001). Trust in an expert, an agency, or a corporation has been assumed to be determined by perceptions of a number of attributes, among them competence and expertise (Peters, Covello & McCallum, 1997, referred to in Oltedal, 2004). For network companies trust in suppliers of ICT systems may be a factor that can influence their risk perception regarding the safety and security of these systems.

2.3 Complexities of ICT systems

According to Aven and Renn (2010), the degree of complexity and uncertainty are two of the aspects that can be used to distinguish between different types of risk problems (situations). Here complexity refers to the difficulty of identifying causal links between a multitude of potential causal agents and specific effects, and uncertainty refers to the difficulty of predicting the occurrence of events and their consequences. Large interconnected infrastructures are characterized by high complexity, and ICT is both a critical infrastructure in itself, and at the same time an important component of other critical infrastructures, which further increases the complexity (Line and Tøndel, 2012).

Perrow (1984) claimed that failures may be inevitable as systems grow increasingly complex. The main problem is that it will be impossible to predict the widespread impacts should one system component fail. Systems can be described by their complexity, and by the tight coupling of their components and processes. Most societal services and critical infrastructure will adhere to Perrow's description of complexity and tight couplings, and this is especially true for critical ICT systems (Hagen et al., 2005). According to Weick (2001) new technologies, such as complex production systems that use computers, have created unusual problems in sensemaking for managers and operators (employees). The use of computer systems involves the self-contained, invisible material process that is actually unfolding, as well as the equally self-contained, equally invisible imagined process that is mentally unfolding in the mind of an individual or a team. There is also continuous intervention improvement and redesign (technological innovations) in computer technologies, which means that the implementation state of development never stops, and these technologies require ongoing structuring and sensemaking if they are to be managed (Weick, 2001).

Increased cognitive demands, increased electronic complexity, and dense organizational interdependence over large areas, often lead to an increase in incidences of unexpected outcomes that produce unexpected ramifications (Roberts and Grabowski, 1996). According to Leveson (2004), technology today (especially digital technology) is changing faster than engineering techniques to cope with the new technology is being created. Interactive complexity is increasing in the systems we are building, and we are designing systems with potential interactions among the components that cannot be thoroughly planned, understood, anticipated, or guarded against. Thus the degree of uncertainty is also high. Risk related to ICT systems is one of today's produced uncertainties contributing to Beck's (1992) characteristic of a risk society. This shows that macro-sociological factors can be important factors for understanding risk perception and behavior (referred to in Albrechtsen, 2007).

3. MATERIAL AND METHODS

A multi-method approach was used in this study, including both qualitative and quantitative methods. Qualitative data were gathered through document studies and interviews. In addition, statistical data were collected through a survey among managers and employees in network companies within the Norwegian electric power supply sector. The combined approach can strengthen the validity of the study, as some of the findings complement and validate each other (Silverman, 2006).

3.1 Document studies

Data regarding vulnerability, safety and security of ICT systems used within the electric power supply sector were collected from guidelines for the regulations relating to contingency planning in the Norwegian power supply system from 2003, 2011 and 2013, and annual supervision reports from NVE. In addition, other strategies and reports regarding ICT safety and security were studied (from the U.S., Europe and Norway), e.g. NIST's "Guide to Industrial Control Systems (ICS) Security" from 2011, the GRID Consortium's "ICT Vulnerabilities of Power Systems: A Roadmap for Future Research" from 2007, OECD's (Organization for economic coordination and development) study "OECD Studies in Risk Management, Norway – Information Security; 2006", reports from the "Norwegian Computer Crime and Security Survey" from 2006, 2010 and 2012, the Norwegian "National Strategy for Information Security" from 2012 and the action plan that accompanied this national strategy. A selection of newspaper articles on the same topic in Norwegian newspapers were studied as well.

3.2 Interviews

To explore our research theme, produce research questions that could be tested by the quantitative survey, and to compliment the data gathered through the survey, qualitative data was gathered through two group interviews with representatives from NVE.

Semi-structured interviews with open ended questions were used. The interviewees were representatives from the contingency planning department in NVE, who are responsible for safety and security, contingency planning, and supervision in the Norwegian electric power supply sector. The first interview were done with three interviewees, and the questions mainly focused on the interviewees' opinion of the Norwegian network companies' risk perception and awareness regarding the risk of electric network failure caused by malfunctions in or attacks on their ICT systems. The second interview were done with two interviewees, and the questions mainly focused on the interviewees' opinion regarding the use of functional internal control regulations for ICT safety and security, and their impression of the network companies' attitude towards these regulations.

3.3 Survey

A questionnaire was designed for a research project which this study is a part of, based on a theoretical review, document studies of the contingency planning regulations for the Norwegian electric power supply system, and an evaluation of 5 pre-existing questionnaires. The pre-existing questionnaires were previously used in studies of offshore (petroleum) safety and ICT-safety[v]. A web-based questionnaire was developed using

QuestBack Survey, and distributed to the respondents by e-mail[vi]. Web-based surveys can eliminate some of the more labor-intensive fielding tasks, such as survey package preparation and mailing, and the subsequent data entry. In web surveys the respondents' answers can be directly downloaded into a database, avoiding transcription errors (Fricker and Schonlau, 2002).

The survey was sent to managers and employees in all the 137 network companies that are part of the PSPO[vii], 334 individuals in total[viii]. The questionnaire contained ten sections - background information, knowledge of safety and security, perception of compliance, attitude towards safety and security, attitude towards regulation, experience of incidents, risk perception, safety and security management, awareness creation and training, and overall rating of the safety levels of the organizations' ICT systems. In this article we have chosen to focus on the results of the items in the risk perception scale, in addition to items regarding knowledge of safety and security, experience of incidents, and overall rating of the safety levels of the organizations' ICT systems.

The risk perception scale contained 19 items addressing the respondents' perception of the risk posed by different threats and vulnerabilities. We created the set of threats and vulnerabilities on the basis of the contingency planning regulations for the Norwegian electric power supply sector and questions and results from the "Norwegian Computer Crime and Security Survey" (2010). The listed threats and vulnerabilities included malicious attacks from outside the organization (e.g. hacking, denial-of-service attacks (DoS attacks), malware, ICT attacks from terrorists or foreign states); users as a vulnerability due to their lack of skills and knowledge (human error); theft of personal information (phishing); ICT malfunctions caused by technical failure or natural hazards; sabotage against power lines or power stations; and ICT attacks from insiders/disgruntled employees. Items on the risk perception scale were measured on a 6-point Likert scale ranging from 1 (very low risk) to 6 (very high risk).

The knowledge of safety and security scale contained 5 items regarding the respondents' knowledge of ICT safety and security. Examples of items in this scale were: *"I am familiar with the content of chapter 6 regarding ICT safety and security in the guidelines for the regulations relating to contingency planning in the Norwegian power supply system", "I am familiar with the content of my organization's information security policy",* and *"I have access to the information necessary to make decisions regarding ICT safety".* Items on the knowledge of safety and security scale were measured on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The experience of incidents section included 13 different incidents that an organization can be exposed to, and the respondents were asked to report the incidents that their organization had experienced. The overall rating of the safety and security level of the organizations' ICT systems contained the question: "All in all, how would you assess the safety and security of the ICT systems used in your organization?" (measured on a 6-point Likert scale ranging from 1 (very poor) to 6 (very good)).

One hundred and three respondents returned the survey questionnaire, for a response rate of 31%. NVE provided the names and e-mail addresses of ICT safety and security managers/coordinators and contingency planning managers in the network companies, and the managers were asked to provide names and e-mail addresses for employees in the organizations' system control centers and ICT staff. A survey sample of 103 respondents can be considered a relatively small sample, and may limit the potential for generalizing. According to Fricker and Schonlau (2002), response rates for web surveys where no other survey mode is given have tended to range from moderate to poor. Other researchers have also experienced the same response rate problem in studies of information security management. Kotulic and Clark (2004) followed up their small response rate with a study suggesting that the main reasons for non-responses were related to a policy of not sharing information regarding their information security performance, the volume of survey requests received by the organizations, and a desire not to spend valuable time on the particular research project (referred to in Albrechtsen and Hovden, 2009). In an attempt to raise the response rate, hidden identity for respondents was activated in our electronic survey, and all e-mail addresses were deleted after the survey was closed.

On the other hand, according to Pallant (2010) a sample of 100+ respondents can be regarded as a large sample (p. 135), and the sample size can be seen as adequate for the types of data analyses done in our study. In addition, qualitative research data were gathered through interviews and document studies to support the quantitative results from the survey, which might increase the potential for generalizing.

4. ANALYSIS AND RESULTS OF SURVEY DATA

The Statistical Package for the Social Sciences (SPSS) v. 18 was used to perform the analyses, which included descriptive statistics, tests of variance (ANOVA) and t-tests. A total scale score was calculated to give an overall score for the scales used in the survey. A reliability test of the total scale scores indicate that the scales used in this study had good internal consistency; Cronbach's alpha was .95 for the risk perception scale and .83 for the knowledge of safety and security scale.

4.1 Descriptive statistics

Table 1 shows the demographical distribution of the respondents. 66 respondents were managers, and 32 were employees (5 respondents did not specify their job category). Only 3 of the respondents were female, and the rest male. 63 respondents worked in small network companies with less than 100 employees, and 37 respondents worked in large network companies with more than 100 employees (3 respondents did not answer the item regarding company size). Based on the use of hidden identity in the electronic survey we lack information regarding how many of the 137 network companies the respondents actually represented. However, 29 respondents were ICT safety and security managers (information security managers), 11 from large companies and 18 from smaller companies. Due to the fact that each company only has one ICT safety and security manager, at least 29 companies are represented in the data material and most likely more.

Table 1. Demographic profiles of respondents.

Job categories			Company size		
			More than 100 employees	Fewer than 100 employees	Total
Manager	Gender	Male	19	44	63
		Female	1	1	2
	Total		20	45	65[1]
Employee	Gender	Male	14	15	29
		Female	1	0	1
	Total		15	15	30[1]
Other	Gender	Male	2	3	5
	Total		2	3	5
Total	Gender	Male	35	62	97
		Female	2	1	3
	Total		37	63	100

[1] Three respondents (1 manager and 2 employees) did not answer the item regarding company size. Thus, the numbers in Table 1 are not completely consistent with the numbers in Section 4.1.

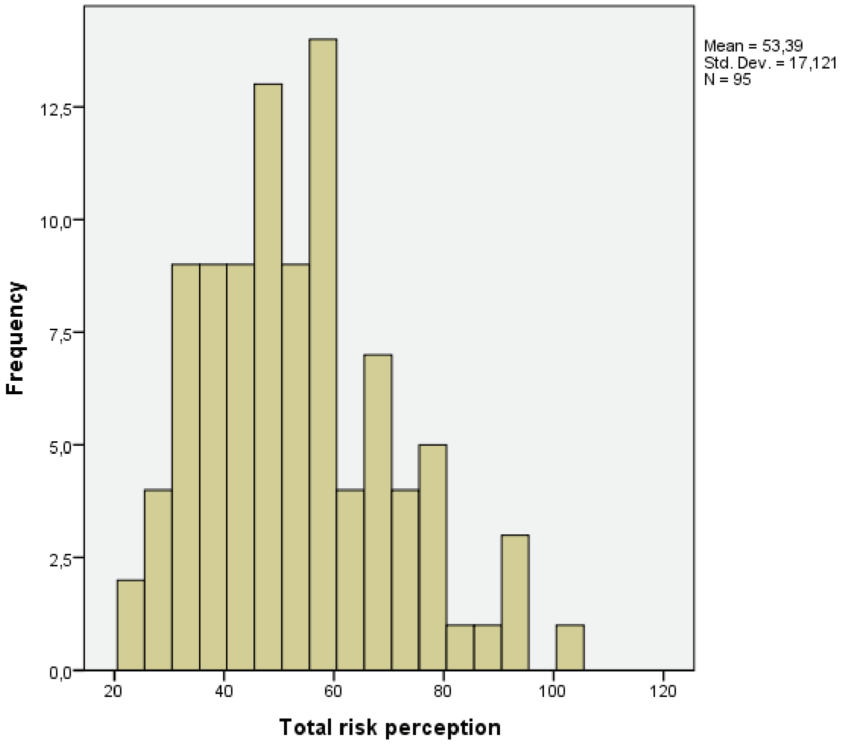
The respondents perceived the overall safety level of the organizations' ICT systems as good, as shown in Table 2.

Table 2. Distribution of respondents' scores on the question: "All in all, how would you assess the safety of the ICT systems used in your organization?"

	Percent	N
1 Very poor (1)	0,0 %	0
2 (2)	0,0 %	0
3 (3)	6,9 %	7
4 (4)	29,7 %	30
5 (5)	56,4 %	57
6 Very good (6)	6,9 %	7
Total		101

In addition, descriptive statistics and histogram show that the respondents perceived the risk of a breakdown in their organization's ICT systems caused by malfunctions or attacks as relatively low. The mean value on the total scale score was 53.39, the minimum possible value was 19, and the maximum possible value was 114. The results are shown in Fig. 1.

Figure 1 – Distribution of scores on the total risk perception scale.



4.2 Correlation, analysis of variance (ANOVA) and t-tests

The relationship between risk perception and safety and security knowledge was investigated using Pearson product-moment correlation coefficient. The analysis showed no statistically significant correlation between the total risk perception scale and the total knowledge of safety and security scale, *r* = .02, *n* = 86, *p* = .83 (two-tailed).

We conducted a one-way between-groups ANOVA to explore differences in risk perception within the network companies (i.e. between the mean scores on the risk perception variable for the different job categories in the data material). The results showed no statistically significant difference at the p < .05 level for the different job categories in the mean scores on the risk perception scale: *F* (7, 87) = 1.3, *p* = .26 (N = 95).

Next, the categorical variable "job category" was collapsed into two categories representing managers and employees. The category "managers" consisted of contingency planning manager, ICT safety manager, and "other leader", and the category "employees" consisted of: operator in system control center, employee in ICT staff, and "other employee". Independent-samples t-tests were performed to determine whether significant differences existed among the mean scores of different groups on the risk perception scale. There was no statistically significant difference in scores for managers (*M* = 53.10, *SD* = 16.41) and employees (*M* = 53.17, *SD* = 18.52; *t* (88) = -.019, *p* = .99 (two-tailed), N = 61 for managers, N = 29 for employees). The magnitude of the differences in the means was very small (eta squared = -.0004).

However, a statistically significant difference was found in the mean risk perception scores between managers and employees in small companies (*M* = 48.16, *SD* = 15.61) versus managers and employees in large companies (*M* = 61.85, *SD* = 15.95; *t* (90) = 4.03, *p* = .00 (two-tailed), N = 58 for small companies, and N = 34 for large companies). Managers and employees in large companies perceived the risk of a breakdown in the organization's ICT systems caused by malfunctions or attacks as higher than the managers and employees in the smaller organizations. The magnitude of the differences in the means was large (eta squared = .15).

5. DISCUSSION

Results from our studies of previous research literature and documents, suggested that process control systems are vulnerable to a multitude of threats, both natural and man-made, and the vulnerability of these ICT systems is also expected to increase during the next few years due to the implementation of new technology. Contrary to this, the results from our survey among users of ICT systems within Norwegian electric power supply network companies showed that both managers and employees perceived the overall safety levels of the network companies' ICT systems as good, and at the same time they also perceived the risk of the threats to ICT systems listed in the risk perception scale as relatively low.

Former research has shown some differences in risk perception between ICT safety and security managers and other users. Goodhue and Straub (1991) found that information security managers showed more concern for the security of their company's ICT system than general managers, as might be expected. According to Albrechtsen (2007), the individual's and the security management's perception of risk can differ, and individuals might not see the range of consequences in the same manner as the security management in an organization does. A later study done by Albrechtsen and Hovden (2009), found that information security managers evaluated the risk level of some threats/vulnerabilities to be lower than did the end-users (e.g. incautious use of the internet, spam mail, and hacking). On the other hand, security managers also ranked the risk level of a few threats as significantly higher than did end-users (e.g. IT-related human error, and social engineering attempts).

However, tests of variance (ANOVA) showed no statistically significant difference between the mean scores on the risk perception scale between the different job categories in our survey, and t-tests did not show any statistically significant difference between managers (including ICT safety and security managers) and employees in their scores on the risk perception scale. ICT safety managers have a particular responsibility for ICT safety and security, and can be considered experts in this field based on their knowledge (Albrechtsen and Hovden, 2009). Even so, as previously mentioned, the users studied in our survey work directly with process control systems, ICT issues, and/or safety and security issues within the network companies, and can be expected to have more knowledge about ICT systems and/or safety and security than average end-users of traditional computer systems. Hence, this article examines possible factors that may explain why *the majority* of respondents in our survey perceived the risk of attacks on or malfunctions in the network organizations' ICT systems as low.

Former research has found that a company's size is a significant factor for whether or not a company has implemented a proper security policy, and the analysis of our survey results also showed a statistically significant difference in the mean risk perception scores between managers and employees in small companies versus managers and employees in large companies. Managers and employees in large companies perceived the risk of a breakdown in their organization's ICT systems caused by malfunctions or attacks as higher than the managers and employees in the smaller organizations. Hagen, Sivertsen and Rong, (2008), present a selection of findings from the "Norwegian Computer Crime and Security Survey" from 2006. According to their study, smaller businesses are less likely to have extensive security arrangements in place. Some of the constraints of small businesses are that they generally do not have the diverse ICT staff typical of larger companies, and many managers in small businesses also have little understanding of information security threats and risks. Smaller enterprises may, however, be exposed to several kinds of computer crime incidents due to weaknesses in access control measures and data protection.

The smallest companies are often dominated by a combined owner-manager, who is very often the sole person responsible for all or most activities not directly related to production. The main focus for the owner-manager is the survival of the company and for natural reasons safety and security will often be a minor focus due to limited resources in terms of money, personnel, and knowledge (Eakin, 1992; Hasle and Limborg, 2006). These small organizations may also have only limited contact with the regulatory authorities, and owner-managers will sometimes accuse the regulatory bureaucracy of having a choking effect on small companies (Power, 2007), a notion that was confirmed by our survey based on comments from some of the respondents. All network companies in Norway are obligated to appoint an ICT safety and security manager, but in the smaller companies the ICT safety and security managers do not usually work full time in that position. Because of limited resources, many of the smaller network companies cannot hire their own ICT staff and instead choose to outsource this function to other companies (Hagen, 2009).

The big network companies have larger process control systems (SCADA systems) and system control centers, and distributes electrical power to more customers (e.g. critical infrastructures such as transport, finance, and telecommunication, hospitals, and other organizations, as well as individual households) than the smaller network companies. Hence, an attack on the large network companies' ICT systems can have more serious consequences for societal safety. Most of the large SCADA systems in the big network companies are subject to stricter obligations in the contingency planning regulations than the smaller SCADA systems, and large companies often have a separate information technology (IT) department with significant expertise in ICT. Knowledge and expertise in ICT might lead to a more accurate perception of the risks from threats to the companies' ICT systems. However, another department may run the SCADA systems on a daily basis and departments may not always communicate well on these issues. In addition to having a separate corporate IT department, outsourcing of basic ICT functions to external companies is also increasingly common. Many of the local companies in the corporate group may know little about the potential threats to their ICT systems, and the IT department might not have a complete overview of what the consequences of a security breach may be in the different application areas. Large companies are also often less transparent than smaller companies, due to larger and more complex systems, and this can make it easier for insiders to engage in crime and not be detected (Hagen, Sivertsen and Rong, 2008).

How a security incident is handled can depend on how serious the security violation is perceived to be (Hagen, 2009). According to Hagen (2009), the way employees *interpret* (make sense of) a security situation depends on the extent of their security knowledge. Perceptions can be the result of incomplete or faulty knowledge (Okrent and Pidgeon, 1998). In our survey, the respondents generally scored high on items concerning their familiarity with the contingency planning regulations and with the internal safety and security policy and contingency plan in their companies (the knowledge of safety and security scale). However, we found no correlation between knowledge of safety and security and risk perception in our survey. Furthermore, our interviewees from NVE said they often find during inspections that a number of employees (and possibly also managers) in the network companies have not read the contingency planning regulations and guidelines. According to Besnard and Arief (2004), humans may be biased at perceiving *actual* levels of risk, and rarely have an exhaustive knowledge of the systems they interact with.

A lack of safety and security awareness by users has often been cited as the top obstacle for effective ICT safety and security (Goodhue and Straub, 1991; Johnson, 2006; Hagen, 2009; Albrechtsen and Hovden, 2009). According to Albrechtsen and Hovden (2009), members of an organization can have inadequate ICT safety and security awareness if they are unfamiliar with possible threats to the systems and how to mitigate them, if they are unaware of the possible consequences of safety and security breaches, if they see their own work in isolation and are unaware of the implications of their use of ICT systems. According to the Norwegian "National Strategy for Information Security" of 2012, the owners of critical infrastructure in many cases have limited knowledge and awareness about vulnerabilities, the interdependencies of critical infrastructures, and what the individual enterprise must do to protect the infrastructure.

No earlier experience of danger can also affect the risk perception of users of ICT systems within companies. According to Flin et al. (1996), there is a relationship between risk perception and accident involvement, and having had an accident or having experienced an attack can influence the current perception of risk. In a study of fishermen's risk perception (subjective assessments of risks), Brooks (2005) found that they did not consider it necessary to conduct emergency procedures (e.g. capsize, abandon ship), and that this may be related to the absence of capsizes in recent times. According to Goodhue and Straub (1991), it often takes a major loss from computer abuse to initiate or reinforce security management. The respondents in our survey were asked if their organizations had experienced different safety and security incidents. On some of the incidents (e.g. malware attacks, and malfunctioning in the ICT systems caused by human error), a majority of the respondents answered that their organizations had experienced such incidents, but many of the respondents still rated these types of incidents at the low end of the risk perception scale. Indeed, one respondent wrote as a comment on the questionnaire: "We constantly experience attempts to hack into our ICT systems, but I have only answered based on the attempts that succeeded". This might indicate that even though the network companies *do* experience attempts to break into their ICT systems, they do not perceive these attempts as a high risk, because so far most of the attempts have failed. According to our interviewees from NVE, managers and employees in many of the network companies find it difficult to prepare for something that *might* happen, but hasn't happened yet.

NIST have developed a guide to process control systems security, and one of the threats to process control systems listed in this guide is complexities. Process control networks are often more complex than traditional ICT networks, and requires a different level of expertise (e.g. control networks are often managed by control engineers, not ICT personnel). Process control systems can have very complex interactions with physical processes, and consequences in the process control system domain can manifest in physical events (Stouffer, Falco and Scarfone, 2011). It is difficult to establish a complete system description of these complex systems, and the lack of understanding might lead to a biased perception of risk and result in misjudgments about potentially-hazardous risk sources (Rundmo, 1996).

As previously mentioned, another factor that may influence users risk perception is the amount of communication between IT departments and system control centers. According to results from our interviews and observation studies, in addition to the qualitative interview study done by Røyksund (2011), two different subcultures can be said to exist in the network companies, depending on whether the people operating the SCADA systems have an education in ICT or a background from the electricity industry. These two different group cultures result in different focus points and mindsets; they have different ways of thinking and draw on different scripts and frames when they make sense of the technology. People who have training in electrical engineering generally focus on keeping the systems running without interruption, and they may be less focused on installing security measures and spending time to apply software patches. Follow-up of specific tasks, such as network configuration and control of firewalls, can often be seen as a "necessary evil" that users of the system do not relate to as anything but an annoying delay in their work.

Many issues surrounding ICT safety and security also seem to be taken for granted within Norwegian network companies. The smaller network companies often take for granted that they are unimportant and not a target of potential attack, and that the potential consequences of an attack on small companies' ICT systems are not as significant as on a large organization's systems. However, with the introduction of AMI and the smart grid, the potential consequences are likely to increase in seriousness. Our interviewees from NVE said they expect several of the smaller network companies to have to team up and join resources to be able to implement and run the AMI, and this can greatly increase the consequences of malfunctions in or attacks on their ICT systems. According to Hagen, Sivertsen and Rong (2008), both small and large enterprises may evaluate (or perceive) the risk of malfunctions in or attacks on their ICT systems as too small to put much effort into user education.

According to our interviewees from NVE, they find a certain naiveté or gullibility about ICT risk, safety and security in the sector; many of the network companies have a lot of trust in the expertise of their system suppliers, believe that the suppliers will make safe solutions, and take for granted that some type of technical applications can take care of all problems. The system owners (network companies) are responsible for the safety and security of their own ICT systems, and it might be necessary for the network companies to tell their suppliers to provide more safety and security solutions for these systems. According to NVE, the network companies focus on the possibilities that the SCADA systems provide (i.e., access to more information and the possibilities of operating more electrical plants in a simpler way), but there is not as much focus on, or awareness of, the risk of "unwanted" access to these systems, protection against malicious software, and similar concerns. During inspections, NVE often discover access-points in the SCADA systems that the companies haven't considered, especially concerning remote access, supplier access, external DVDs and USB sticks. Furthermore, the consequences of insider attacks can be worse than the consequences of external attacks (Johnson, 2006; Hagen, 2009). However, according to NVE, a high threshold for acknowledging this kind of risk exists in the network companies. It might be taken for granted that "this does not happen in our company" which can affect managers' and employees' risk perception.

6. CONCLUSIONS

The results from our survey among users of ICT systems (process control systems) within Norwegian electric power supply network companies showed that both managers and employees perceived the overall safety level of their ICT systems as good, and at the same time perceived the risk of attacks on or malfunctions in their ICT systems as relatively low. Our results correspond well with results from a former interview study done by Røyksund (2011), as well as with results from our interviews with representatives from the Norwegian Water Resources and Energy Directorate (NVE). The impression is that the risk of attacks on or malfunctions in their ICT systems is not perceived as high within a lot of the Norwegian network companies.

We found, in accordance with previous research, that company size, knowledge and awareness regarding ICT safety and security, and earlier experience of danger are factors that can influence the risk perception of ICT system users within companies. System complexities, which can be seen as a natural source of threats against process control systems, can also affect the risk perception of the companies' managers and employees. Process control networks are often more complex than traditional ICT networks, and requires a different level of expertise. Increased cognitive demands, increased electronic complexity, and dense organizational interdependence over large areas often lead to an increase in incidences of unexpected outcomes that produce unexpected ramifications. Furthermore, a lack of communication between subcultures with different focus points and mindsets within the companies was found to influence the risk perception of users of ICT systems, in addition to a certain "taken for grantedness" regarding many issues surrounding ICT safety and security. Too much trust in the expertise of their system suppliers can also lead to a lack of focus on the safety and security of network companies' ICT systems and thus influence users risk perception.

REFERENCES

Albrechtsen E. A qualitative study of users' view on information security. Computers &Security 2007;26:276-289.

Albrechtsen E, Hovden, J. The information security digital divide between information security managers and users. Computers & Security 2009; 28:476-490.

Andersson H. Perception of Own Death Risk: An Assessment of Road-Traffic Mortality Risk. Risk Analysis 2011;31(7):1069-1082.

Aven T, Renn O. Risk Management and Governance - Concepts, Guidelines and Application. Heidelberg, Dordrecht, London, New York: Springer; 2010.

Besnard D, Arief B. Computer security impaired by legitimate users. Computers & Security 2004;23:253-264.

Brooks B. Not drowning, waving! Safety management and occupational culture in an Australian commercial fishing port. Safety Science 2005;43:795-814.

Dagbladet, 2013. http://www.dagbladet.no/nullctrl/ (accessed 30 December 2013).

Eakin J. Leaving it up to the workers: sociological perspective on the management of health and safety in small workplaces. International Journal of Health Services 1992;22(4):689-704.

Eriksson G, Svensson O, Eriksson L. The time-saving bias: judgements, cognition and perception. Judgement and decision making 2013;8(4);492-497.

Flin R, Mearns K, Fleming M, Gordon R. Risk Perception and Safety in the Offshore Oil and Gas Industry. HSE Books: Health and Safety Executive – Offshore Technology Report; 1996.

Fricker RD, Schonlau M. Advantages and Disadvantages of Internet Research Surveys: Evidence from literature. *Field Methods* 2002;14(4):347-367.

Goodhue DL, Straub DW. Security concerns of system users – A study of perceptions of the adequacy of security. Information &Management 1991;20:13-27.

Hagen JM, Fridheim H, Nystuen KO. New challenges for emergency preparedness in the information society. Telektronikk 2005;1:48-54.

Hagen JM, Sivertsen TK, Rong C. Protection against unauthorized access and computer crime in Norwegian enterprises. Journal of Computer Security 2008;16:341-366.

Hagen JM. The Human Factor behind the Security Perimeter. Evaluating the Effectiveness of Organizational Information Security Measures and Employees' Contributions to Security. PhD dissertation, University of Oslo; 2009.

Hagen, JM, Albrechtsen E. Regulation of information security and the impact on top management commitment: A comparative study of the energy supply sector and the finance sector. In: Martorell et al., editors. Proceedings of Safety, Reliability and Risk Analysis: Theory, Methods and Applications. London: Taylor & Francis Group; 2009. p. 407-413.

Hasle P, Limborg HJ. A review of the literature on preventive occupational health and safety activities in small enterprises. Industrial Health 2006;44(1):6-12.

Johnson EC. Awareness training, security awareness: switch to a better programme. Network Security 2006;2:15-18.

Kahneman D, Tversky A. On the Reality of Cognitive Illusions. Psychological Review 1996;103(3):582-591.

Kundur D, Feng X, Liu S, Zountos T, Butler-Purry KL. Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid. Texas A&M University: Department of Electrical and Engineering; 2010.

Leveson N. A New Accident Model for Engineering Safer Systems. Safety Science 2004;42(4):237-270.

Line MB, Tøndel IA. Information and Communication Technology: Enabling and Challenging Critical Infrastructure. In: Hokstad P, Utne IB, Vatn J, editors. Risk and Interdependencies in Critical Infrastructures: A guideline for analysis. London: Springer-Verlag; 2012. p. 147-225.

NVE (2012). Annual report 2011 – The Norwegian Energy regulator. http://webby.nve.no/publikasjoner/rapport/2012/rapport2012_19.pdf (accessed 20 November 2012).

Næringslivets sikkerhetsråd (2012). Mørketallsundersøkelsen – informasjonssikkerhet og datasikkerhet. http://www.nsrorg.no/getfile.php/Dokumenter/NSR%20publikasjoner/Mørketallsundersøkelsen/moerketall_2012.pdf (accessed 17 December 2012).

OECD (Organization for Economic Co-ordination and Development). Emerging Systemic Risks in the 21st Century: An Agenda for Action; 2003.

OECD (Organization for Economic Co-ordination and Development). OECD Studies in Risk Management, Norway – Information Security; 2006.

Okrent D, Pidgeon N. Risk perception versus risk analysis. Reliability Engineering and System Safety 1998;59:1-4.

Olsen OE, Kruke BI, Hovden J. Societal Safety: Concept, Borders and Dilemmas. Journal of Contingencies and Crisis Management 2007;15(2):69-79.

Oltedal S, Moen BE, Klempe H, Rundmo T. Explaining risk perception – An evaluation of cultural theory. Rotunde publications no. 85; 2004.

Pallant J. SPSS Survival Manual – A step by step guide to data analysis using SPSS, 4th ed. Berkshire, New York: Open University Press; 2010.

Patel SC, Sanyal P. Securing SCADA systems. Information Management & Computer Security 2008;16(4):398-414.

Perrow C. Normal Accidents – Living with High-Risk Technologies. Princeton, New Jersey: Princeton University Press; 1984.

Piètre-Cambacédès L, Chaudet C. The SEMA referential framework: Avoiding ambiguities in the terms '"security" and "safety". International Journal of Critical Infrastructure Protection 2010;3:55-66.

Power M. Organized Uncertainty: Designing a World of Risk Management. Oxford: Oxford University Press; 2007.

Regjeringen (2012a). Nasjonal strategi for informasjonssikkerhet. *http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf* (accessed 10 January 2013).

Regjeringen (2012b). Nasjonal strategi for informasjonssikkerhet – Handlingsplan. *http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf* (accessed 10 January 2013).

Roberts KH, Grabowski M. Organizations, Technology, and Structuring. Handbook of Organization Studies, edited by SR Clegg, C Hardy, and WR Nord, 1996;409-423. Sage.

Rodal SK. Sårbarhet i kraftforsyningens drifts- og styringssystemer. FFI report no. 04278; 2001.

Rundmo T. Associations between risk perceptions and safety. Safety Science 1996;24(3):197-209.

Røyksund M. Informasjonssikkerhet i kraftforsyningen. Master thesis in societal safety, University of Stavanger; 2011.

Silverman D. Interpreting qualitative data: methods for analysing talk, text and interaction. London: Sage; 2006.

Sjøberg L. Factors in Risk Perception. Risk Analysis 2000;20(1):1-11.

Slovic P, Fischoff B, Lichtenstein S. Why Study Risk Perception? Risk Analysis 1982;2(2):83-93.

Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security – Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce. Special Publication 800-82. 2011.

Svensson O. Decisions among time saving options: When intuition is strong and wrong. Acta Psychologica 2008;127:501-509.

Teknisk Ukeblad (2012). Sikkerhet i kraftnettet– Kraftsystemet må ikke bli lavterskeltilbud for terrorister. http://www.tu.no/energi/2012/12/14/-kraftsystemet-ma-ikke-bli-lavterskel-tilbud-for-terrorister (accessed 17 December 2012).

The Grid Consortium. ICT Vulnerabilities of Power Systems: A Roadmap for Future Research. European Commission, Joint Research Centre, Institute for Protection and Security of the Citizen; 2007.

Tversky A, Kahneman D. Advances in Prospect Theory – Cumulative Representation of Uncertainty. Choices, Values and Frames, edited by D Kahneman and A Tversky, 2000,44-65. Cambridge, United Kingdom: Cambridge University Press.

Weick KE. Making Sense of the Organization. Oxford: Blackwell Business; 2001.

NOTES

[i] An infrastructure is critical if its failure would lead to unacceptable human or economic consequences, and would impact societies' capabilities of rescue, response and recovery. This links the notion of critical infrastructures closely to the concept of societal safety. Societal safety can be defined as "society's ability to maintain critical social functions, to protect the life and health of the citizens and to meet the citizens' basic requirements in a variety of stress situations" (Olsen et al. 2007,71)

[ii] In the area of risk research, it is traditional to distinguish between the terms safety and security, and the meaning of the terms can vary considerably from one context to another. According to Piètre-Cambacédès and Chaudet (2010), two relevant and representative distinctions can be identified (the SEMA referential framework). The first is the system vs. environment distinction, where security is concerned with the risks originating from the environment and potentially affecting the system, whereas safety deals with the risks arising from the system and potentially affecting the environment. The second is the malicious vs. accidental distinction, where security typically addresses malicious (intentional) risks, while safety addresses purely accidental (unintentional) risks (p. 59).

[iii] NVE increased its focus on ICT safety and security after 2006, and has (especially since 2009) been putting more pressure on the electric power supply organizations, through heightened regulations and supervision. In addition, in 2009, some of the bigger network companies formed their own Forum for ICT-safety in the electric power supply sector (Røyksund, 2011).

[iv] SCADA systems help control and monitor utilities by gathering field data from sensors and instruments located at remote sites, transmitting and displaying these data at a central site, and enabling engineers to send control commands to the field instruments (Patel and Sanyal, 2008:398). SCADA systems are also called "industrial control systems" or "process control systems".

[v] The five previously used questionnaires were: Offshore Safety Questionnaire (The Robert Gordon University, Aberdeen, 1997), Norwegian Petroleum Safety Authorities' survey "Trends in risk level – Norwegian Shelf" (2007-2008), "Accident prevention – survey for offshore employees" (survey used in PhD project, Centre of Maritime Health and Safety, Syddansk Universitet, Hanna B. Rasmussen, 2008-2012),"The Norwegian Computer Crime and Security Survey" (2010), and questions used in Janne M. Hagen's study "How do employees comply with security policy? A comparative case study of four organizations under the Norwegian Security Act" (Hagen 2009).

[vi] Before distributing the survey, we performed a pilot-test of the questionnaire to ensure that the instructions and scale items were clear. We sent the pilot to three respondents; one contingency planning manager, one ICT safety

and security manager, and one system control center operator, and the questionnaire was adjusted according to feedback.

[vii] The Power Supply Preparedness Organization (PSPO) prepares, establishes, and maintains a structure to efficiently handle extraordinary situations in the power supply system. In 2012, the PSPO included 197 organizations, and 137 of these can be classified as network companies (numbers were provided by NVE).

[viii] The survey was distributed to respondents in June 2012, and was closed in September 2012.

Article 4

Management commitment and awareness creation - ICT safety and security in electric power supply network companies

Ruth Østgaard Skotnes*, Center for Risk Management and Societal Safety, Department of Media, Culture and Social Sciences, University of Stavanger, Stavanger, Norway*

Abstract

Purpose - The aim of this article is to follow up on previous research by studying the degree of management commitment to information and communication technology (ICT) safety and security within network companies in the electric power supply sector, implementation of awareness creation and training measures for ICT safety and security within these companies, and the relationship between these two variables.

Design/methodology/approach – Data were mainly collected through a survey among users of ICT systems in network companies within the Norwegian electric power supply sector. In addition, qualitative data were gathered through interviews with representatives from the regulatory authorities, and observation studies were conducted at ICT safety and security conferences.

Findings – In accordance with previous research, our survey data showed a statistically significant correlation between management commitment to ICT safety and security and implementation of awareness creation and training measures. The majority of survey respondents viewed the degree of management commitment to ICT safety and security within their own organization as high, even though qualitative studies showed contradictory results. The network companies had implemented awareness creation and training measures to a varying degree. However, interactive awareness measures were used to a lesser extent than formal one-way communication methods.

Originality/value - The article provides insight into management commitment to and implementation of awareness creation and training measures for ICT safety and security within network companies.

Keywords - ICT, safety, security, management commitment, awareness creation, training, electric power supply

Article Classification – Research paper

1. Introduction

Previous research has advocated the need for more training, awareness creation, and management commitment regarding ICT safety and security[1] (Johnson, 2006; Hagen, Albrechtsen and Hovden 2008; Hagen, 2009; Hagen and Albrechtsen, 2009a). Studies of safety have suggested that management involvement is important for the safety work within companies. If the management is engaged it will be aware of the need for information security measures to comply with the laws, and assure that safety and security measures are implemented. The success of safety and security management systems is often said to be dependent on the commitment of all staff, and all members must be aware of their responsibility for safety and security. Otherwise, the safety and security mechanisms can be bypassed or diminished by employees.

This article follows up on previous research which has shown a positive relationship between management commitment to ICT safety and security and implementation of awareness creation and training measures. The following research questions are addressed:

- To what degree is the management of network companies in the electric power supply sector committed to the safety and security of their organizations' ICT systems?
- To what extent are awareness creation and training measures for ICT safety and security implemented within network companies in the electric power supply sector, and what type of measures are implemented?

ICT has increasingly become a part of all critical infrastructures[2] (Line and Tøndel, 2012), and is used to monitor, control and operate power generation plants and power distribution within electric power supply systems. A breakdown in these ICT systems (process control systems) can seriously compromise the physical grid, which can result in major financial disasters and damage to public safety and health (Patel and Sanyal, 2008). The electric power supply is the most critical infrastructure in modern society (Hagen and Albrechtsen, 2009a), and a prolonged interruption of the electric power supply may have consequences for many critical societal functions caused by the interdependencies between infrastructures.

Process control systems, e.g. supervisory control and data acquisition systems (SCADA systems)[3], and other ICT systems used within the electric power supply system, are vulnerable to a multitude of threats, both natural and man-made (Rodal, 2001). Connecting the ICT systems to the Internet has increased the risk for system breakdowns and serious failures (Hagen and Albrechtsen, 2009a), and has made the formerly isolated ICT systems vulnerable to a set of threats and risks they have not been exposed to before (Line and Tøndel, 2012). Vulnerability of ICT systems in the electric power supply system is also expected to increase during the next years. Advanced Metering Infrastructure (AMI) and, later on the Smart Grid, are now being introduced in the electric power systems of the Western countries. The electric Smart Grid promises increased capacity, reliability and efficiency through the marriage of cyber technology and the existing electricity network. However, the scale and complexity of the smart grid, along with its increased connectivity and automation, make the task of cyber protection particularly challenging (Kundur et al., 2010).

The research questions are answered by presenting results from a survey sent to 137 network companies in Norway, supplemented by results from interviews with representatives from the Norwegian Water Resources and Energy Directorate (NVE) and observation studies. The next section introduces the theoretical foundations for the study. Section 3 presents the data material and methods used in the study, and data analysis and results of the survey are presented in section 4. In section 5 results from the survey, interviews, and observation studies are interwoven in the discussion, and finally section 6 contains the conclusion.

2. Theory

2.1 ICT safety and security measures

ICT safety and security measures include both technological and organizational measures. Technological measures can consist of personal passwords, redundancy of critical systems, intruder detection systems, anti-virus software, and firewalls. Hagen, Albrechtsen and Hovden (2008) have categorized organizational measures into four main groups: security policy, procedures and control, administrative tools and methods (e.g. risk analysis, audits, incident reporting systems), and organizational and individual awareness creation and maintenance. The first three groups of organizational safety and security measures can also be described as technical-administrative measures. The forth group of organizational measures consists of training/education, awareness campaigns, user participation, top management's engagement and involvement of all parts of the organization in learning processes from incidents. In this study we have chosen to focus on management's engagement/commitment (both top management and middle-management), and training/education and awareness campaigns.

According to Hagen, Albrechtsen and Hovden's (2008) survey among information security professionals in Norway, awareness-creation measures were assessed to be very effective compared to the basic, formal security systems, however awareness-creation measures were also the least implemented. Information security management has traditionally emphasized formal management approaches, and formal measures are also less resource demanding than awareness-creation measures. When formal management systems (i.e. policies, procedures, and tools) are in place, these measures may be taken for granted and accepted as contributors to an adequate security level.

2.2 Management commitment

According to Rasmussen (1997), management's commitment to safety and security has appeared to be a major problem, and has lead to the relating efforts of society to control management incentives by safety and security regulation. Research on safety climate has also indicated that the safety levels of organizations are influenced by managers' attitudes towards safety, and the perceived priority given to safety training (Antonsen, 2009). Hagen (2009) defines information security as essentially a management responsibility. Information security should be embedded in all management processes, and include incident reporting and organizational learning. According to Johnson (2006), organizational policies and user guidelines require the commitment of top level managers, and should be directly linked to the company's business strategies. The top management must be committed to ICT safety and security through its activities and through a dedicated budget. In addition, an organization's safety and security policy should contain a letter of commitment from the top management showing commitment to ICT safety and security within the organization, and assign responsibilities of each member of the organization, particularly line management, top management and safety and security professionals.

2.3 Awareness creation and training

Formal technical-administrative measures and documented systems, e.g. safety and security policies, guidelines and instructions, can be taken for granted, and often few users[4] have actually read the documents. Nevertheless, documents are often seen as important because they form the basis for other measures (Albrechtsen and Hovden, 2009). But when technological and administrative measures are in place, "softer" resources can be used to modify performance. Influencing individuals' knowledge, attitudes, and behavior must be regarded as important means that are complementary to formal technical-administrative measures (Hagen, 2009). As Siponen (2000) puts it: "(…) security people want end-users to internalize and follow given guidelines (…) rather than to be aware of them but for some reason or other fail to apply them in reality" (p. 36).

ICT safety and security awareness can be seen as the extent to which organizational members understand the importance of information safety and security, the level of safety and security required by the organization and their individual safety and security responsibilities, and act accordingly (ISF, 2005, referred to in Albrechtsen, 2006). Members of an organization can have inadequate ICT safety and security awareness if they are unfamiliar with possible threats to the systems and how to mitigate them, if they are unaware of the possible consequences of safety and security breaches, if they see their own work in isolation and are unaware of the implications of their use of ICT systems (Albrechtsen and Hovden, 2009). A lack of safety and security awareness by users has been cited as the top obstacle for effective ICT safety and security. If people (management and employees) do not handle and protect ICT systems in a safe and secure manner, even the best technologies will be ineffective. Previous research has suggested that the impact of ICT safety and security breaches coming from people inside an organization is bigger than all other sources combined (Johnson, 2006; Hagen, 2009).

According to Albrechtsen and Hovden (2009), users often assume that the responsibility for ICT safety and security rests with the technology and with the ICT safety and security managers and they do not realize the benefits of ICT safety and security measures. In addition, users often trade off ICT safety and security against efficiency and functionality, which can be caused by efficiency demands, emphasis on minimum-effort work, and poor quality of ICT safety and security training and education resulting in insufficient skills and knowledge. For employees, the responsibility for acting in a manner that is safe and secure for the organization comes on top of other demands they are faced with in their everyday work.

3. Material and methods

The research methodology in this study was mainly based on a survey; statistical data were collected from users of ICT systems (managers and employees) in network companies within the Norwegian electric power supply sector. In addition, qualitative data were gathered through in depth qualitative interviews and observation studies. A combined approach can strengthen the validity of the study, as some of the findings can complement and validate each other (Silverman, 2006). However, as in this study, a combined approach can also show discrepancies between analysis results of data collected using different methods, and may thus open for new possibilities of interpretation.

3.1 Survey

A web-based questionnaire was developed using QuestBack Survey, and distributed to the respondents by e-mail[5]. The survey was sent to managers and employees in the 137 network companies that are part of the PSPO[6], 334 individuals in total[7]. The questionnaire contained ten sections - background information, knowledge of safety and security, perception of compliance, attitude towards safety and security, attitude towards regulation, experience of incidents, risk perception, safety and security management, awareness creation and training, and overall rating of the safety and security levels of the organizations' ICT systems. In this article we have chosen to focus on the results of the items in the safety and security management scale (management commitment) and the awareness creation and training scale. Items on the scales were measured on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

The safety and security management scale contained 5 items measuring the management's commitment to ICT safety and security in the network organizations. The items in this scale were: *"My immediate manager intervenes immediately if the ICT safety and security rules are not followed", "My immediate manager checks from time to time whether we are actually working safely and securely", "My immediate manager is involved in the organization's ICT safety and security work", "My immediate manager appreciates my pointing out matters of importance to ICT safety and security",* and *"I would rather not discuss ICT safety and security with my immediate manager".* Managers (ICT safety and security managers/coordinators and contingency planning managers) and employees (operators in system control centers and ICT staff) responded to the same items, hence we received information about the commitment of both top-management and middle-management in the network organization. The awareness creation and training scale contained 6 items related to the use of different awareness-creating and training measures in the network organizations (the individual items are shown in section 4.1).

One hundred and three respondents returned the survey questionnaire, for a response rate of 31%. NVE provided the names and e-mail addresses of ICT safety and security managers/coordinators and contingency planning managers in the network companies, and the managers were asked to provide names and e-mail addresses for employees in the organizations' system control centers and ICT staff. A survey sample of 103 respondents can be considered a relatively small sample, and may limit the potential for generalizing. According to Fricker and Sconlau (2002), response rates for web surveys where no other survey mode is given have tended to range from moderate to poor. Other researchers have also experienced the same response rate problem in studies of information security management. The main reasons for non-responses has been related to a policy of not sharing information regarding their information security performance, the volume of survey requests received by the organizations, and a desire not to spend valuable time on the particular research project (Albrechtsen and Hovden, 2009). In an attempt to raise the response rate, hidden identity for respondents was activated in our electronic survey, and all e-mail addresses were deleted after the survey was closed.

On the other hand, according to Pallant (2010) a sample of 100+ respondents can be regarded as a large sample (p. 135), and the sample size can be seen as adequate for the types of data analyzes done in our study. In addition, qualitative research data were gathered to support the quantitative results from the survey, which might increase the potential for generalizing.

3.2 Interviews and observation studies

To explore our research theme, produce research questions that could be tested by the quantitative survey, and to complement the data gathered through the survey, qualitative data was gathered through two group interviews with representatives from NVE. To complement the data from the survey and inform our study, observation studies were also carried out at two conferences on ICT safety and security within the electric power supply industry.

Semi-structured interviews with open ended questions were used. The interviewees were representatives from the contingency planning department in NVE, who are responsible for safety, contingency planning, and supervision in the Norwegian electric power supply sector. The first interview was done with three interviewees, and the questions mainly focused on the interviewees' opinion of the Norwegian network companies' risk perception and awareness regarding the risk of electric network failure caused by malfunctions in or attacks on their ICT systems. The second interview was done with two interviewees, and the questions mainly focused on the interviewees' opinion regarding the use of functional internal control regulations for ICT safety and security, and their impression of the network companies' attitudes towards these regulations.

The two conferences on ICT safety and security within the electric power supply industry were held in Norway in 2011. The participants at both conferences were mainly managers and employees working with ICT safety and security within network companies in Norway, in addition to suppliers of industrial control systems (e.g. SCADA-systems) and ICT safety and security solutions for these systems. The speakers at the conferences included representatives from NVE, NorCERT (the Norwegian Computer Emergency Response Team), Mnemonic AS (one of the largest providers of IT information security services in the Nordic region), NorSIS (Norwegian Centre for Information Security), and ICT safety and security researchers from universities and research institutes. During the observation studies we observed the types of ICT safety and security issues raised at the conferences, the types of issues participants focused on, and the types of questions and discussions that came up during the conferences.

4. Data analysis and results of survey

The Statistical Package for the Social Sciences (SPSS) v. 18 was used to perform the analyses, which included descriptive statistics and correlation. Negatively worded items were reversed, and total scale scores were calculated to give an overall score for the two scales used in the survey. A reliability test of the total scale scores indicated that the scales used in this study had good internal consistency; Cronbach's alpha was .85 for the safety and security management scale and .84 for the awareness creation and training scale.

4.1 Descriptive statistics

Table 1 shows the demographical distribution of the respondents. 66 respondents were managers, and 32 were employees (5 respondents did not specify their job category). Only 3 of the respondents were female, and the rest male. 63 respondents worked in small network companies with less than 100 employees, and 37 respondents worked in large network companies with more than 100 employees (3 respondents did not answer the item regarding company size). Based on the use of hidden identity in the electronic survey we lack information regarding how many of the 137 network companies the respondents actually represented. However, 29 respondents were ICT safety and security managers (information security managers), 11 from large companies and 18 from smaller companies. Due to the fact that each company only has one ICT safety and security manager, at least 29 companies are represented in the data material and most likely more.

Table 1. Demographic profiles of respondents.

Job categories			Company size		Total
			More than 100 employees	Fewer than 100 employees	
Manager	Gender	Male	19	44	63
		Female	1	1	2
	Total		20	45	65[1]
Employee	Gender	Male	14	15	29
		Female	1	0	1
	Total		15	15	30[1]
Other	Gender	Male	2	3	5
	Total		2	3	5
Total	Gender	Male	35	62	97
		Female	2	1	3
	Total		37	63	100

[1] Three respondents (1 manager and 2 employees) did not answer the item regarding company size. Thus, the numbers in Table 1 are not completely consistent with the numbers in Section 4.1.

The mean value on the total scale score for the safety and security management scale was 18.83, the minimum possible value was 5, and the maximum possible value was 25. This means that the respondents agreed to most statements, and the majority of respondents viewed management commitment to ICT safety and security in their organization as high. The results are shown in Fig. 1.

Figure 1. Total scores on the safety and security management scale (calculated by adding up the scores from the 5 items that make up the scale).

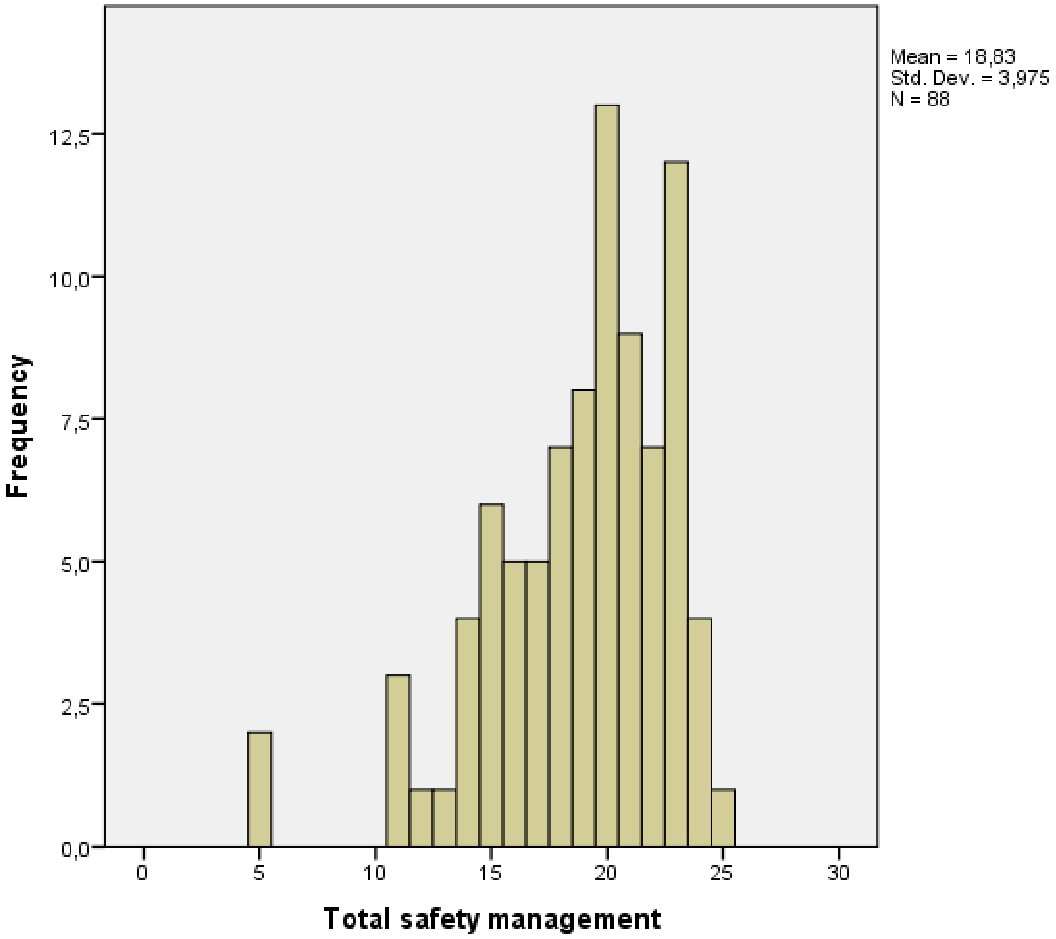


Table 2 presents the distribution of the respondents' scores on the individual items of the awareness creation and training scale.

Table 2. Distribution of scores on item 1-6 within the awareness creation and training scale.

	Distribution of scores on items (in percentage)					
	Item 1: *"New employees receive thorough training in the organization's ICT safety and security rules (included in the organization's ICT safety and security policy and safety and security instructions)"*	**Item 2:** *"Training sessions in ICT safety and security for managers and employees are conducted whenever the ICT systems are updated or altered"*	**Item 3:** *"Awareness campaigns about ICT safety and security are often[1] held in my organization"*	**Item 4:** *"In my organization e-mails containing information about ICT safety and security are often distributed to raise employee awareness"*	**Item 5:** *"In my organization formal face-to-face presentations of information about ICT safety and security are often held to raise employee awareness"*	**Item 6:** *"In my organization informational videos on ICT safety and security are often showed to raise employee awareness"*
Strongly disagree	3.9 % (N=4)	4.9 % (N=5)	4.9 % (N=5)	7.8 % (N=8)	12.7 % (N=13)	23.3 % (N=24)
Dis-agree	9.7% (N=10)	16.7% (N=17)	27.2 % (N=28)	23.5 % (=24)	42.2 % (N=43)	53.4 % (N=55)
Neither disagree nor agree	26.2 % (N=27)	43.1 % (N=44)	35.0 % (N=36)	35.3 % (N=36)	33.3 % (N=34)	18.4 % (N=19)
Agree	46.6 % (N=48)	28.4 % (N=29)	27.2 % (N=28)	25.5 % (N=26)	9.8 % (N=10)	3.9 % (N=4)
Strongly agree	10.7 % (N=11)	3.9 % (N=4)	4.9 % (N=5)	6.9 % (N=7)	1.0 % (N=1)	0.0 % (N=0)
Not relevant	0 % (N=0)	1.0 % (N=1)	0.0 % (N=0)	1.0% (N=1)	1.0% (N=1)	1.0 % (N=1)
Don't know	2.9 % (N=3)	2.0 % (N=2)	1.0 % (N=1)	0.0 % (N=0)	0.0 % (N=0)	0.0 % (N=0)
Total	103	102	103	102	102	103

[1] In the awareness creation and training scale the word "often" was defined as "at least once a year". The respondents were informed of this in the scale's text information.

The distribution of the respondents' scores on the individual items of the awareness creation and training scale suggested that the majority of the network companies had implemented training in ICT safety and security for new employees. Some network companies had implemented training sessions in ICT safety and security whenever their ICT systems were updated and altered, however a large percentage of the respondents answered "Neither disagree nor agree" (43.1 %) on this item. The use of awareness campaigns and distribution of e-mails containing information about ICT safety and security seemed to vary a lot between the companies. 54.9% answered negatively[8] on the item regarding use of face-to-face presentations of information about ICT safety and security, and 76.7% answered negatively on the item regarding use of informational videos on ICT safety and security.

4.2 Correlation

The relationship between management commitment to ICT safety and security (as measured by the total safety and security management scale) and implementation of awareness creation and training measures (as measured by the total awareness creation and training scale) in the network companies was investigated using Pearson product-moment correlation coefficient. Before this statistical analysis could be performed on the data set, the total scale scores for the two scales needed to be calculated by adding up the scores from the items that made up each scale (Pallant, 2010). The correlation analysis revealed a large positive correlation between the two variables "management commitment" and "awareness creation and training", r = .641, n = 81[9]. There was a strong, positive relationship[10] between the variables, and high levels of management commitment were associated with high levels of awareness creation and training.

5. Discussion

The "Cyber Security Strategy for Norway" (Regjeringen, 2012) from 2012, concluded that the lack of awareness concerning ICT safety and security constitutes a high and increasing risk. In many cases, the owners of critical infrastructure have limited knowledge and awareness about vulnerabilities, the interdependencies of critical infrastructures, and what the individual enterprise must do to protect the infrastructure. The complexity of the process control systems, together with an increase in the number of attacks on ICT systems, demands a large effort to create awareness of the threats, to provide information about safety and security measures, and to influence positive attitudes.

Studies of safety have suggested that management involvement is important for the safety work within companies. ICT safety and security law in Norway places responsibility for ICT safety and security on the management and the boards. The contingency planning regulations for the Norwegian electric power supply sector also emphasize that contingency planning (which includes ICT safety and security) is the responsibility of the top managers in the organizations, and the authorities expect the top management to convey the importance of and follow up on safety and security within their organization. If the management is engaged it will be aware of the need for information security measures to comply with the laws, and assure that security measures are implemented (Hagen and Albrechtsen, 2009a).

The results from our survey showed a strong relationship between management commitment to ICT safety and security, and the implementation of awareness creation and training measures for ICT safety and security in the network companies. High levels of management commitment were associated with high levels of awareness creation and training. These findings correspond well with results from former studies (Johnson, 2006; Hagen, Albrechtsen, and Hovden, 2008; Hagen and Albrechtsen, 2009a).

According to Hagen and Albrechtsen's (2009a) comparative study of regulation of information security and the impact on top management commitment in the electric power supply sector versus the finance sector in Norway, a larger number of electric power supply companies reported incidents typically caused by insiders (e.g. abuse of ICT systems, unintentional use violating security, etc.) compared with financial companies. The researchers found that higher organizational security awareness corresponded with less exposure to insider threats. The results of the study also showed that high management engagement corresponded with a high degree of adopted security measures and a lower degree of insider incidents. According to our interviews with representatives from NVE, a high threshold for acknowledging the risk of insider incidents exists in the network companies. The companies might take for granted that "this does not happen in our company" which can affect their awareness.

During our observation studies at an ICT safety and security conference for companies within the Norwegian electric power supply sector in 2011, we observed a representative from one of the network companies asking the representative from NorCERT if the ICT systems in the Norwegian electric power supply sector were considered a high target for cyber attacks. The representative from NorCERT answered that the Norwegian Police Security Service (PST) did not assign a high threat level to the possibility of cyber attacks on Norwegian ICT systems, but they had observed an increasing amount of internet espionage. According to several of the participants at the conference it was hard to get money for ICT safety and security measures from the top management when the authorities did not consider the threat level as high.

On the other hand, our observation studies were carried out in 2011, and according to PST's annual threat assessment for 2012, there *is* a danger that foreign intelligence services' computer and internet based intelligence activity could more severely affect Norwegian intelligence targets. A report from 2012 on terror towards the U.S. electrical grid, concluded that a few, well-informed persons may be able to blackout large areas over a long period of time, with devastating and life-threatening consequences. According to NVE, this threat is just as great for Norway as for the U.S. (Teknisk Ukeblad, 2012). And according to The Norwegian Intelligence Service's (Etterretningstjenesten) open security threat assessment from February 2013 (FOCUS 2013), cyber terror is now one of the main threats to national security. As previously mentioned, there are also large ICT safety and security challenges related to the implementation of AMI.

According to our interviewees from NVE, they had the impression that it was easier to get the network companies to implement technological and technical-administrative measures, than to achieve management commitment to and create awareness about ICT safety and security within the companies. As previously mentioned, a possible explanation for this may be that when formal management systems (i.e. policies, procedures, and tools) are in place, these measures may be taken for granted and accepted as contributors to an adequate security level. However, contrary to the results from our interviews and observation studies, the majority of respondents in our survey viewed management commitment to ICT safety and security in their organization as high. One possible explanation for this discrepancy may be that on subjective assessments regarding their own company's performance, respondents are often inclined to assess themselves positively. Sometimes it may also be difficult to answer negatively on questions concerning one's immediate manager (Hagen, Albrechtsen and Hovden, 2008).

Of the awareness creation and training measures listed in our survey, the most implemented was training in ICT safety and security for new employees. Some network companies had also implemented training sessions in ICT safety and security whenever their ICT systems were updated and altered, however a large percentage of the respondents answered "Neither disagree nor agree" on this item which might indicate that these types of training sessions were not conducted on a regular basis.

According to Albrechtsen and Hovden (2009), both the ICT safety and security managers and end-users of ICT systems that were interviewed in their study agreed that end-users often do not have the knowledge and skills needed for safe and secure behavior. Both groups believed this shortcoming to be the result of insufficient training. Users of ICT systems often do not realize the benefits of information security, and consider practicality and efficiency as far more important for their work. Both the interviewed managers and end-users also agreed that the best measures to raise awareness about ICT safety and security were interactive, face-to-face measures, e.g. personal meetings or presentations. However, this type of measure was also among the least frequently used approaches by the companies in the study. Formal one-way communication methods, such as information material and electronic information (e.g. screen savers, e-mail messages, and leaflets) were extensively used because these measures are simple and cheap. The problem with these types of measures was that users often lacked the motivation and awareness to obtain the knowledge in this information, in addition to being bombarded with other types of information.

Similar results were found in our survey. 54.9% of the respondents answered negatively ("Strongly disagree" or "Disagree") on the statement: *"In my organization formal face-to-face presentations of information about ICT safety and security are often held to raise employee awareness"*, only 10.8 % of the respondents answered positively ("Strongly agree" or "Agree"), and 33.3 % answered "Neither disagree nor agree"[11].

According to Albrechtsen and Hagen (2009), employee participation is valuable for measures influencing user performance as well as for other parts of information security management. Practical learning (through interaction), rather than formal education, is likely to be the most effective way to improve knowledge on how to act safely and securely. Thomson and von Solms (1998) argued that social psychological principles needed to be introduced to improve the effectiveness of security awareness programs. The use of role playing exercises and the use of examples related to the employee's own work situation were suggested as good techniques to achieve information security awareness among users of ICT systems. Use of e-learning can be another way to strengthen individual security awareness and behavior. A study by Hagen and Albrechtsen (2009b) discusses the effects of a computer-based security training program (using e-learning software) which was introduced in a multinational commercial organization in 2008. The study documented significant improvements in information security knowledge, awareness and behavior of the employees that participated in the training program.

However, these types of awareness creating and training measures are often resource demanding because they must be repeated to be effective. Removing employees from their work during presentations, meetings, and training sessions, can also reduce the production capacity of the company. This may be a reason for why these types of measures are used to a lesser extent than formal one-way measures, even though studies have shown that they are considered better and more effective for raising awareness about ICT safety and security (Hagen, Albrechtsen and Hovden, 2008; Albrechtsen and Hovden, 2009).

6. Conclusion

The results from our survey among managers and employees in Norwegian electric power supply network companies showed a strong relationship between management commitment to and the implementation of awareness creation and training measures for ICT safety and security in the companies. High levels of management commitment were associated with high levels of awareness creation and training. These findings correspond well with results from former studies (Johnson, 2006; Hagen, Albrechtsen, and Hovden, 2008; Hagen and Albrechtsen, 2009a).

The survey data showed that the majority of respondents viewed management commitment to ICT safety and security in their organization as high. However, contrary to this, results from our interviews with representatives from the authorities and observation studies at ICT safety and security conferences indicated that it is easier to get the network companies to implement technological and technical-administrative measures, than to achieve management commitment to and create awareness about ICT safety and security within the companies.

Furthermore, the results from our survey suggested that the majority of the network companies had implemented training in ICT safety and security for new employees. Some network companies had also implemented training sessions whenever their ICT systems were updated and altered, however our results indicated that these types of training sessions were not conducted on a regular basis. The use of awareness campaigns and distribution of e-mails containing information about ICT safety and security seemed to vary a lot between the companies. Interactive face-to-face presentations of information about ICT safety and security did not seem to be used as a measure to raise employee awareness within most of the network companies, even though former research has found that interactive measures are often viewed as the best measures to raise awareness about ICT safety and security (Hagen, Albrechtsen and Hovden, 2008; Albrechtsen and Hovden, 2009). Other measures involving employee participation and practical learning through interaction, e.g. e-learning or role-playing exercises, have also been shown to improve knowledge and awareness about how to act safely and securely. Our current survey did not include items regarding the use of these types of measures within the Norwegian network companies, however this would be an interesting topic for further research.

References

Albrechtsen E. (2006),“A qualitative study of users’ view on information security”, *Computers & Security,* Vol. 26, pp. 276-289.

Albrechtsen E., and Hovden J. (2009), “The information security digital divide between information security managers and users”. *Computers & Security,* Vol. 28, No. 4, pp. 76-490.

Albrechtsen E., and Hagen J. M. (2009), “Information security measures influencing user performance”, in Martorell et al. (Eds.), Proceedings of Safety, Reliability and Risk Analysis: Theory, Methods and Applications. Taylor & Francis Group, London, pp. 2649-2656.

Antonsen, S. (2009), *Safety Culture: Theory, Method and Improvement.* Ashgate Publishing Limited, London.

Besnard D., and Arief B. (2004),“Computer security impaired by legitimate users”. *Computers & Security*, Vol. 23, pp. 253-264.

FOCUS (2013), “Annual Assessment by the Norwegian Intelligence Service”, available at: http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/0886-FOCUS-english-2013.pdf (accessed 15 August 2013).

Fricker R. D., and Schonlau M. (2002), “Advantages and Disadvantages of Internet Research Surveys: Evidence from literature”, *Field Methods*, Vol. 14, No. 4, pp. 347-367.

Hagen J. M., Albrechtsen E., and Hovden J. (2008),“Implementation and effectiveness of organizational information security measures”, *Information Management & Computer Security,* Vol. 16, No. 4, pp. 377-397.

Hagen J. M. (2009), “The Human Factor behind the Security Perimeter – Evaluating the effectiveness of organizational information security measures and employees' contributions to security”, PhD Thesis no. 2009:874, Series of dissertations submitted to the Faculty of Mathematics and Natural Sciences, University of Oslo.

Hagen, J. M., and Albrechtsen E. (2009a), “Regulation of information security and the impact on top management commitment: A comparative study of the energy supply sector and the finance sector”, in Martorell et al. (Eds.), Proceedings of Safety, Reliability and Risk Analysis: Theory, Methods and Applications. Taylor & Francis Group, London, pp. 407-413.

Hagen, J. M., and Albrechtsen E. (2009b), “Effects on employees’ information security abilities by e-learning”, *Information Management & Computer Security,* Vol. 17 No. 5, pp. 388-407.

Johnson E. C. (2006), “Awareness training, security awareness: switch to a better programme”, *Network Security*, Vol. 2, pp. 15-18.

Kundur D., Feng X., Liu S., Zountos T., and Butler-Purry K. L. (2010), “Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid”. Texas A&M University: Department of Electrical and Engineering.

Line M. B., and Tøndel I. A. (2012), “Information and Communication Technology: Enabling and Challenging Critical Infrastructure”, in Hokstad P., Utne I. B., and Vatn J. (Eds.), *Risk and Interdependencies in Critical Infrastructures: A guideline for analysis.* Springer-Verlag, London, pp. 147-225.

Olsen O. E., Kruke B. I., and Hovden J. (2007), “Societal Safety: Concept, Borders and Dilemmas”, *Journal of Contingencies and Crisis Management*, Vol. 15, No. 2, pp. 69-79.

Pallant J. (2010), *SPSS Survival Manual – A step by step guide to data analysis using SPSS, 4th ed.,* Open University Press, Berkshire, New York.

Patel S. C., and Sanyal P. (2008), “Securing SCADA systems”, *Information Management & Computer Security*, Vol. 16, No. 4, pp. 398-414.

Piètre-Cambacédès L., and Chaudet C. (2010), “The SEMA referential framework: Avoiding ambiguities in the terms ”security” and “safety””, *International Journal of Critical Infrastructure Protection,* Vol. 3, pp. 55-66.

Rasmussen J. (1997), “Risk Management in a Dynamic Society: A Modelling Problem”, *Safety Science*, Vol. 27, No. 2-3, pp. 183-213.

Regjeringen (2012). Cyber Security Strategy for Norway [Nasjonal strategi for informasjonssikkerhet]. *http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf* (accessed 10 January 2013).

Rodal S. K. (2001), ”Sårbarhet i kraftforsyningens drifts- og styringssystemer” [Vulnerabilites in the information systems of the electric power supply], FFI report no. 04278., available at: http://rapporter.ffi.no/rapporter/2001/04278.pdf (accessed 20 November 2012).

Silverman D. (2006), *Interpreting qualitative data: methods for analyzing talk, text and interaction*, Sage, London.

Siponen M. (2000), “A conceptual foundation for organizational information security awareness”, *Information Management and Computer Security,* Vol. 8, No. 1, pp. 31-41.

Teknisk Ukeblad (2012),”Sikkerhet i kraftnettet– Kraftsystemet må ikke bli lavterskeltilbud for terrorister” [Safety and security in the power grid – The electric power supply system must not become a low threshold service for terrorists], available at: http://www.tu.no/energi/2012/12/14/-kraftsystemet-ma-ikke-bli-lavterskel-tilbud-for-terrorister (accessed 17 December 2012).

Thomson M. E., von Solms R. (1998), “Information security awareness: educating your users effectively”, *Information Management & Computer Security*, Vol. 6, No. 4, pp. 167-173.

Notes

[1] A number of different terms are commonly used when discussing ICT safety and security and threats to ICT systems: information security, IT safety and security, computer safety, computer crime, data safety, cyber safety, cyber threats, cyber crime, cyber terror, logical threats, etc. In this article we mainly use the term ICT

safety and security, but different terms will be used when referencing to other research studies. In the area of risk research, it is traditional to distinguish between the terms safety and security, and the meaning of the terms can vary considerably from one context to another. According to Piètre-Cambacédès and Chaudet (2010), two relevant and representative distinctions can be identified (the SEMA referential framework). The first is the system vs. environment distinction, where security is concerned with the risks originating from the environment and potentially affecting the system, whereas safety deals with the risks arising from the system and potentially affecting the environment. The second is the malicious vs. accidental distinction, where security typically addresses malicious (intentional) risks, while safety addresses purely accidental (unintentional) risks (p. 59).

[2] An infrastructure is critical if its failure would lead to unacceptable human or economic consequences, and would impact societies' capabilities of rescue, response and recovery. This links the notion of critical infrastructures closely to the concept of societal safety. Societal safety can be defined as "society's ability to maintain critical social functions, to protect the life and health of the citizens and to meet the citizens' basic requirements in a variety of stress situations" (Olsen et al. 2007,71)

[3] SCADA systems help control and monitor utilities by gathering field data from sensors and instruments located at remote sites, transmitting and displaying these data at a central site, and enabling engineers to send control commands to the field instruments (Patel and Sanyal, 2008:398).

[4] A user can be characterized as a person with legitimate access to the organization's information (and communication) systems (Albrechtsen, 2006), e.g. end-users, security officers, managers, designers (Besnard and Arief, 2004).

[5] Before distributing the survey, we performed a pilot-test of the questionnaire to ensure that the instructions and scale items were clear. We sent the pilot to three respondents; one contingency planning manager, one ICT safety and security manager, and one system control centre operator, and the questionnaire was adjusted according to feedback.

[6] The Power Supply Preparedness Organisation (PSPO) prepares, establishes, and maintains a structure to efficiently handle extraordinary situations in the power supply system. In 2012, the PSPO included 197 organisations, and 137 of these can be classified as network companies (numbers were provided by NVE).

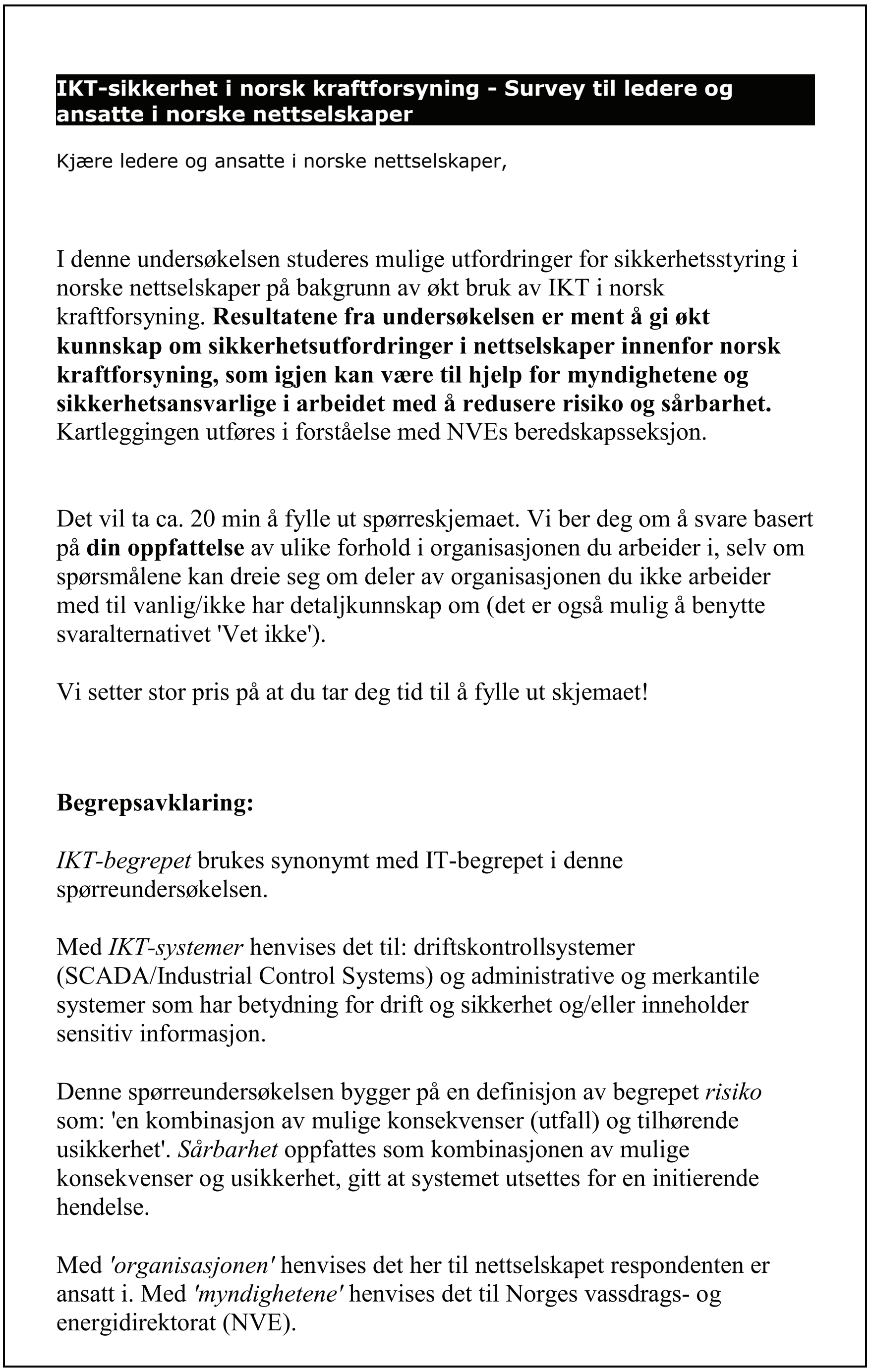
[7] The survey was distributed to respondents in June 2012, and closed in September 2012.

[8] "Strongly disagree" and "Disagree".

[9] Correlation was significant at the 0.01 level (2-tailed).

[10] The strength of the correlation is interpreted according to Cohen's guidelines from 1988: small correlation – r=.10 to .29, medium correlation – r=.30 to .49, large correlation – r=.50 to 1.0 (Pallant, 2010:134).

[11] N=102.



IKT-sikkerhet i norsk kraftforsyning - Survey til ledere og ansatte i norske nettselskaper

Kjære ledere og ansatte i norske nettselskaper,

I denne undersøkelsen studeres mulige utfordringer for sikkerhetsstyring i norske nettselskaper på bakgrunn av økt bruk av IKT i norsk kraftforsyning. **Resultatene fra undersøkelsen er ment å gi økt kunnskap om sikkerhetsutfordringer i nettselskaper innenfor norsk kraftforsyning, som igjen kan være til hjelp for myndighetene og sikkerhetsansvarlige i arbeidet med å redusere risiko og sårbarhet.** Kartleggingen utføres i forståelse med NVEs beredskapsseksjon.

Det vil ta ca. 20 min å fylle ut spørreskjemaet. Vi ber deg om å svare basert på **din oppfattelse** av ulike forhold i organisasjonen du arbeider i, selv om spørsmålene kan dreie seg om deler av organisasjonen du ikke arbeider med til vanlig/ikke har detaljkunnskap om (det er også mulig å benytte svaralternativet 'Vet ikke').

Vi setter stor pris på at du tar deg tid til å fylle ut skjemaet!

Begrepsavklaring:

IKT-begrepet brukes synonymt med IT-begrepet i denne spørreundersøkelsen.

Med *IKT-systemer* henvises det til: driftskontrollsystemer (SCADA/Industrial Control Systems) og administrative og merkantile systemer som har betydning for drift og sikkerhet og/eller inneholder sensitiv informasjon.

Denne spørreundersøkelsen bygger på en definisjon av begrepet *risiko* som: 'en kombinasjon av mulige konsekvenser (utfall) og tilhørende usikkerhet'. *Sårbarhet* oppfattes som kombinasjonen av mulige konsekvenser og usikkerhet, gitt at systemet utsettes for en initierende hendelse.

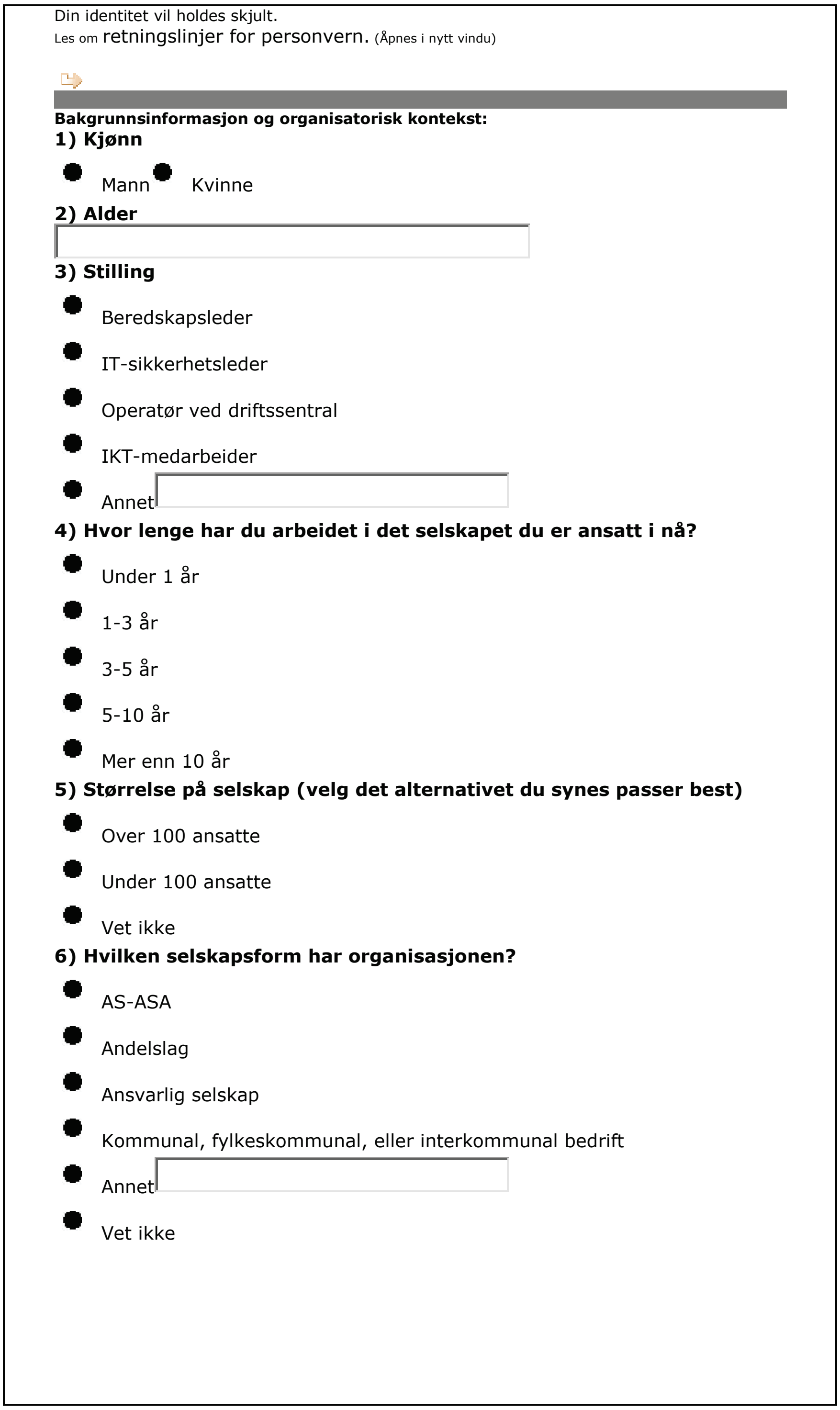
Med *'organisasjonen'* henvises det her til nettselskapet respondenten er ansatt i. Med *'myndighetene'* henvises det til Norges vassdrags- og energidirektorat (NVE).

Risiko- og sårbarhetsanalyser (ROS-analyser): I Beredskapsforskriften kreves det at alle organisasjoner som inngår i Kraftforsyningens Beredskapsorganisasjon (KBO) skal ha oppdaterte ROS-analyser for å identifisere organisasjonens risikopotensiale og de tiltak som effektivt oppfyller kravene i forskriften. Det anbefales å gjennomføre ROS-analyser for overordnet nivå, detaljerte analyser for avgrensede deler av organisasjonen, og mer detaljerte analyser på komponentnivå.

Beredskapsplan: I følge Beredskapsforskriften skal alle organisasjoner som inngår i KBO ha en oppdatert og funksjonell beredskapsplan. Beredskapsplanen skal blant annet omfatte forberedelser og tiltak det kan bli nødvendig å iverksette ved ulykker, skader, rasjonering og andre ekstraordinære situasjoner som kan påvirke kraftforsyningens drift og sikkerhet.

Informasjonssikkerhetspolicy (sikkerhetspolicy): En informasjonssikkerhetspolicy skal uttrykke ledelsens intensjoner og mål for IKT-sikkerhetsarbeidet. Den skal beskrive mål, hovedprinsipper, ansvar og roller i forbindelse med organisasjonens arbeid med IKT-sikkerhet.

Sikkerhetsinstruks: I følge beredskapsforskriften bør organisasjonene utarbeide en sikkerhetsinstruks for IKT-sikkerhet. Dette skal være en instruks for håndtering og beskyttelse av viktig og sensitiv informasjon, samt viktige informasjonssystemer, både teknisk og administrativt. Sikkerhetsinstruksen bør være et resultat av tiltak som er identifiserte i den løpende helhetlige vurderingen av IKT-sikkerheten i organisasjonen.



Din identitet vil holdes skjult.

Les om retningslinjer for personvern. (Åpnes i nytt vindu)

Bakgrunnsinformasjon og organisatorisk kontekst:

1) Kjønn

● Mann ● Kvinne

2) Alder

3) Stilling

● Beredskapsleder

● IT-sikkerhetsleder

● Operatør ved driftssentral

● IKT-medarbeider

● Annet

4) Hvor lenge har du arbeidet i det selskapet du er ansatt i nå?

● Under 1 år

● 1-3 år

● 3-5 år

● 5-10 år

● Mer enn 10 år

5) Størrelse på selskap (velg det alternativet du synes passer best)

● Over 100 ansatte

● Under 100 ansatte

● Vet ikke

6) Hvilken selskapsform har organisasjonen?

● AS-ASA

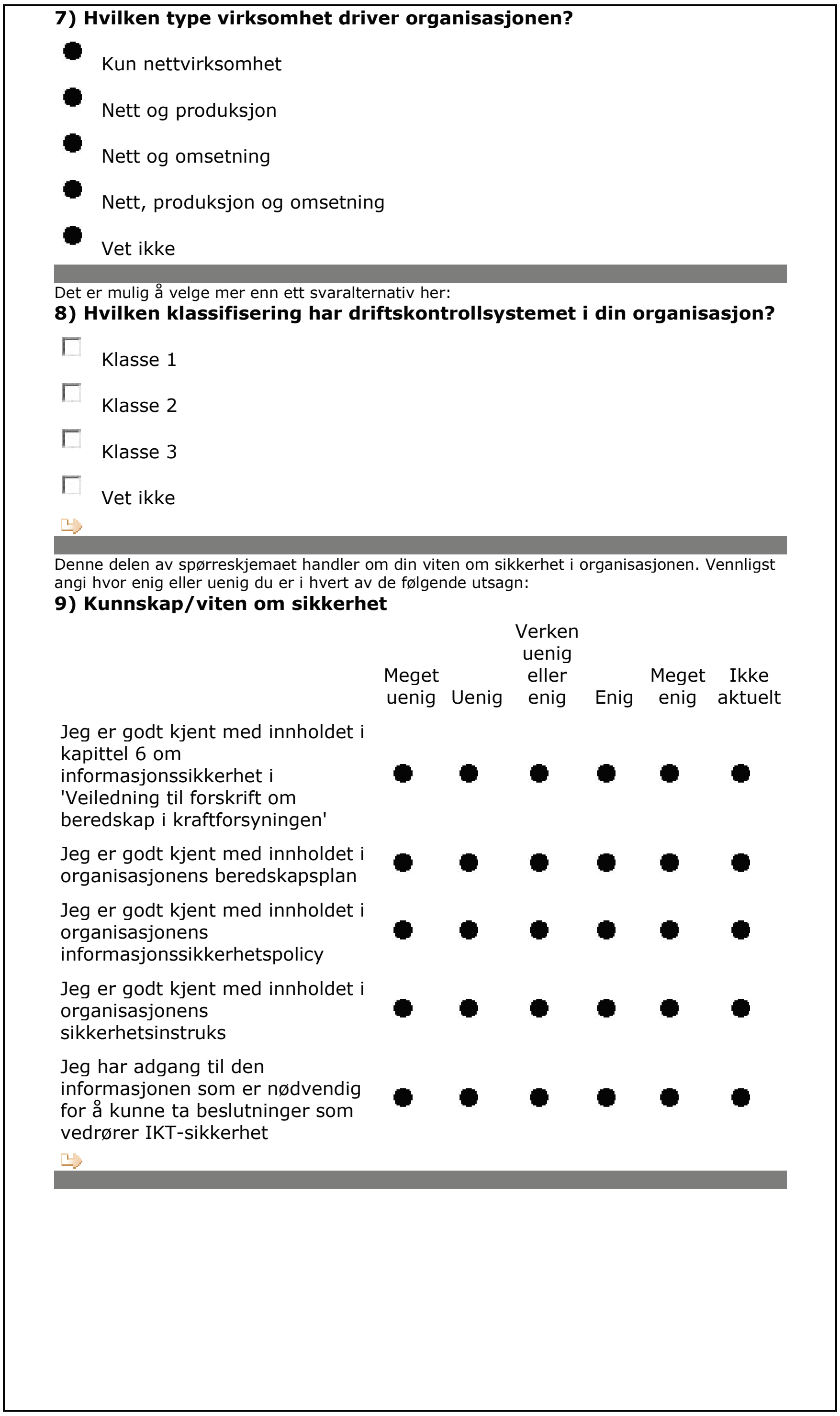
● Andelslag

● Ansvarlig selskap

● Kommunal, fylkeskommunal, eller interkommunal bedrift

● Annet

● Vet ikke



7) Hvilken type virksomhet driver organisasjonen?

● Kun nettvirksomhet

● Nett og produksjon

● Nett og omsetning

● Nett, produksjon og omsetning

● Vet ikke

Det er mulig å velge mer enn ett svaralternativ her:

8) Hvilken klassifisering har driftskontrollsystemet i din organisasjon?

□ Klasse 1

□ Klasse 2

□ Klasse 3

□ Vet ikke

Denne delen av spørreskjemaet handler om din viten om sikkerhet i organisasjonen. Vennligst angi hvor enig eller uenig du er i hvert av de følgende utsagn:

9) Kunnskap/viten om sikkerhet

	Meget uenig	Uenig	Verken uenig eller enig	Enig	Meget enig	Ikke aktuelt
Jeg er godt kjent med innholdet i kapittel 6 om informasjonssikkerhet i 'Veiledning til forskrift om beredskap i kraftforsyningen'	●	●	●	●	●	●
Jeg er godt kjent med innholdet i organisasjonens beredskapsplan	●	●	●	●	●	●
Jeg er godt kjent med innholdet i organisasjonens informasjonssikkerhetspolicy	●	●	●	●	●	●
Jeg er godt kjent med innholdet i organisasjonens sikkerhetsinstruks	●	●	●	●	●	●
Jeg har adgang til den informasjonen som er nødvendig for å kunne ta beslutninger som vedrører IKT-sikkerhet	●	●	●	●	●	●

Denne delen av spørreskjemaet handler om din oppfattelse av etterlevelse i din organisasjon, når det gjelder krav i Beredskapsforskriften, og organisasjonens interne beredskapsplan, informasjonssikkerhetspolicy og sikkerhetsinstruks for IKT-sikkerhet. Vi ber deg her om å vennligst angi hvor enig eller uenig du er i hvert av de følgende utsagn (NB! I de fleste utsagnene er ordet 'alltid' benyttet for at du skal ta stilling til i hvilken grad dette stemmer i din organisasjon. Hvis noe for eksempel gjøres ofte, men ikke alltid, kan man svare 'Enig' i stedet for 'Meget enig'):

10) Oppfattelse av etterlevelse

	Meget uenig	Uenig	Verken uenig eller enig	Enig	Meget enig	Ikke aktuelt	Vet ikke
I min organisasjon er IKT-sikkerhet et viktig tema i ROS-analysene	●	●	●	●	●	●	●
I min organisasjon utarbeides det alltid ROS-analyser for alle nivå i organisasjonen	●	●	●	●	●	●	●
I min organisasjon benyttes alltid sjekklister ved utarbeidelse av ROS-analysene	●	●	●	●	●	●	●
I min organisasjon oppdateres ROS-analysene ved alle endringer (systemmessige og organisatoriske endringer, eksternt og internt)	●	●	●	●	●	●	●
I min organisasjon oppdateres alltid ROS-analysene ved oppdatering av programvare, maskinvare og arkitekturløsninger	●	●	●	●	●	●	●
I min organisasjon oppdateres alltid ROS-analysene når organisasjonen får kjennskap til mulige nye trusler mot IKT-sikkerheten	●	●	●	●	●	●	●
I min organisasjon benyttes alltid NVEs 'Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen' ved utarbeidelsen av ROS-analysene	●	●	●	●	●	●	●
I min organisasjon benyttes alltid standarder (som ISO 27001/ISO 27002/NS-ISO/IEC 17799) ved utarbeidelse av blant annet ROS-analyser, informasjonssikkerhetspolicy og sikkerhetsinstruks	●	●	●	●	●	●	●
	●	●	●	●	●	●	●

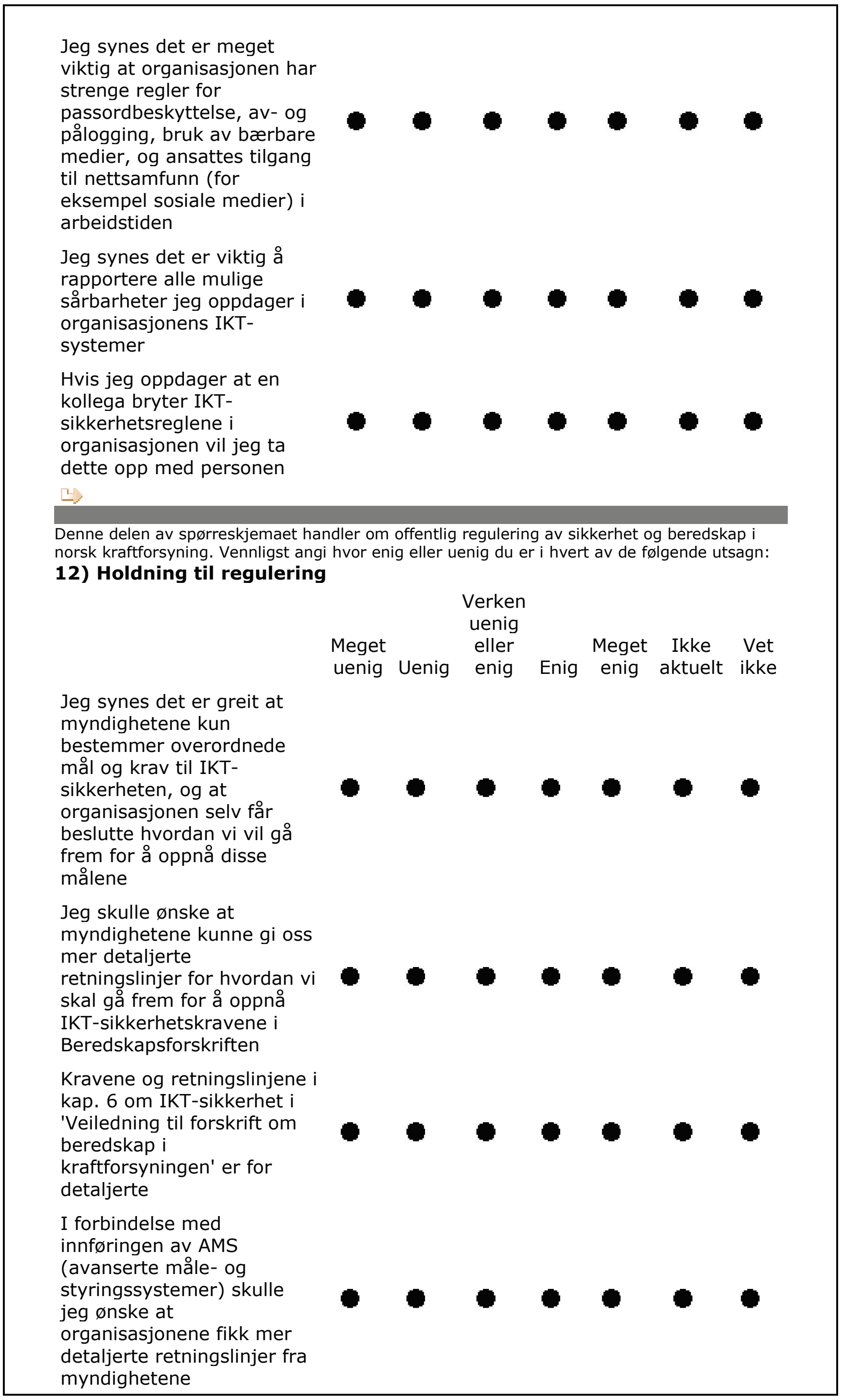
I min organisasjon er beredskap i forbindelse med IKT-sikkerhet en viktig del av beredskapsplanen							
I min organisasjon har vi alltid tilgjengelig en oppdatert systembeskrivelse av driftskontrollsystemet	●	●	●	●	●	●	●
I min organisasjon blir det sett på som viktig å teste IKT-sikkerheten gjennom beredskapsøvelser	●	●	●	●	●	●	●
Når organisasjonens beredskapsplan har vært i bruk, enten gjennom øvelser eller reelle hendelser, blir planen alltid evaluert	●	●	●	●	●	●	●
Evalueringer av beredskapsplanen blir alltid benyttet som utgangspunkt for oppdateringer av organisasjonens ROS-analyser	●	●	●	●	●	●	●
Det er lett å ta kontakt med IT-sikkerhetslederen hvis man har spørsmål eller informasjon vedrørende IKT-sikkerheten i organisasjonen	●	●	●	●	●	●	●
I min organisasjon er det enkelt å rapportere hendelser knyttet til IKT-sikkerheten, og brudd på denne, til overordnede ledd i organisasjonen	●	●	●	●	●	●	●
Rapportering av hendelseer knyttet til IKT-sikkerheten, og brudd på denne, blir alltid fulgt opp av ledelsen i organisasjonen	●	●	●	●	●	●	●
Alle ansatte informeres om innholdet i organisasjonens informasjonssikkerhetspolicy	●	●	●	●	●	●	●
I min organisasjon er sikkerhetsinstruksen tilgjengelig for alle ansatte	●	●	●	●	●	●	●
I min organisasjon er det kun autorisert personell som har tilgang til rom som inneholder driftssentral med tilhørende utrustning	●	●	●	●	●	●	●
I min organisasjon er det alltid oppdaterte autorisasjonslister for	●	●	●	●	●	●	●

brukere av organisasjonens IKT-systemer							
I min organisasjon er driftskontrollsystemet totalt atskilt fra andre systemer (det administrative systemet, internett, osv.)	●	●	●	●	●	●	●
I min organisasjon inngås det alltid sikkerhetsavtaler med leverandører	●	●	●	●	●	●	●
I min organisasjon føres det alltid logg over eksterne forbindelser til driftskontrollsystemet, og andre relevante aktiviteter	●	●	●	●	●	●	●
I min organisasjon blir det sett på som viktig å alltid ha oppdatert anti-virus programvare	●	●	●	●	●	●	●
I min organisasjon blir det sett på som viktig å alltid ha oppdaterte operativsystem	●	●	●	●	●	●	●

Denne delen av spørreskjemaet handler om holdning til sikkerhet. Vennligst angi hvor enig eller uenig du er i hvert av de følgende utsagn:

11) Holdning til sikkerhet

	Meget uenig	Uenig	Verken uenig eller enig	Enig	Meget enig	Ikke aktuelt	Vet ikke
Jeg utfører mitt arbeid bedre hvis jeg ignorerer noen IKT-sikkerhetsregler (i informasjonssikkerhetspolicy og sikkerhetsinstruks)	●	●	●	●	●	●	●
Det er viktig å lese organisasjonens beredskapsplan, IKT-sikkerhetspolicy, og sikkerhetsinstruks for å ha oppdatert kunnskap om IKT-sikkerhet	●	●	●	●	●	●	●
Jeg kan utføre arbeidet fortere hvis jeg ignorerer noen IKT-sikkerhetsregler	●	●	●	●	●	●	●
Det er en god holdning til IKT-sikkerhet i denne organisasjonen	●	●	●	●	●	●	●
I praksis går hensynet til produksjon foran hensynet til IKT-sikkerhet i denne organisasjonen	●	●	●	●	●	●	●
Jeg har et personlig ansvar overfor IKT-sikkerheten i organisasjonen	●	●	●	●	●	●	●



Jeg synes det er meget viktig at organisasjonen har strenge regler for passordbeskyttelse, av- og pålogging, bruk av bærbare medier, og ansattes tilgang til nettsamfunn (for eksempel sosiale medier) i arbeidstiden	●	●	●	●	●	●	●
Jeg synes det er viktig å rapportere alle mulige sårbarheter jeg oppdager i organisasjonens IKT-systemer	●	●	●	●	●	●	●
Hvis jeg oppdager at en kollega bryter IKT-sikkerhetsreglene i organisasjonen vil jeg ta dette opp med personen	●	●	●	●	●	●	●

Denne delen av spørreskjemaet handler om offentlig regulering av sikkerhet og beredskap i norsk kraftforsyning. Vennligst angi hvor enig eller uenig du er i hvert av de følgende utsagn:

12) Holdning til regulering

	Meget uenig	Uenig	Verken uenig eller enig	Enig	Meget enig	Ikke aktuelt	Vet ikke
Jeg synes det er greit at myndighetene kun bestemmer overordnede mål og krav til IKT-sikkerheten, og at organisasjonen selv får beslutte hvordan vi vil gå frem for å oppnå disse målene	●	●	●	●	●	●	●
Jeg skulle ønske at myndighetene kunne gi oss mer detaljerte retningslinjer for hvordan vi skal gå frem for å oppnå IKT-sikkerhetskravene i Beredskapsforskriften	●	●	●	●	●	●	●
Kravene og retningslinjene i kap. 6 om IKT-sikkerhet i 'Veiledning til forskrift om beredskap i kraftforsyningen' er for detaljerte	●	●	●	●	●	●	●
I forbindelse med innføringen av AMS (avanserte måle- og styringssystemer) skulle jeg ønske at organisasjonene fikk mer detaljerte retningslinjer fra myndighetene	●	●	●	●	●	●	●

Hvilken type hendelser har organisasjonen vært utsatt for? Sett kryss:

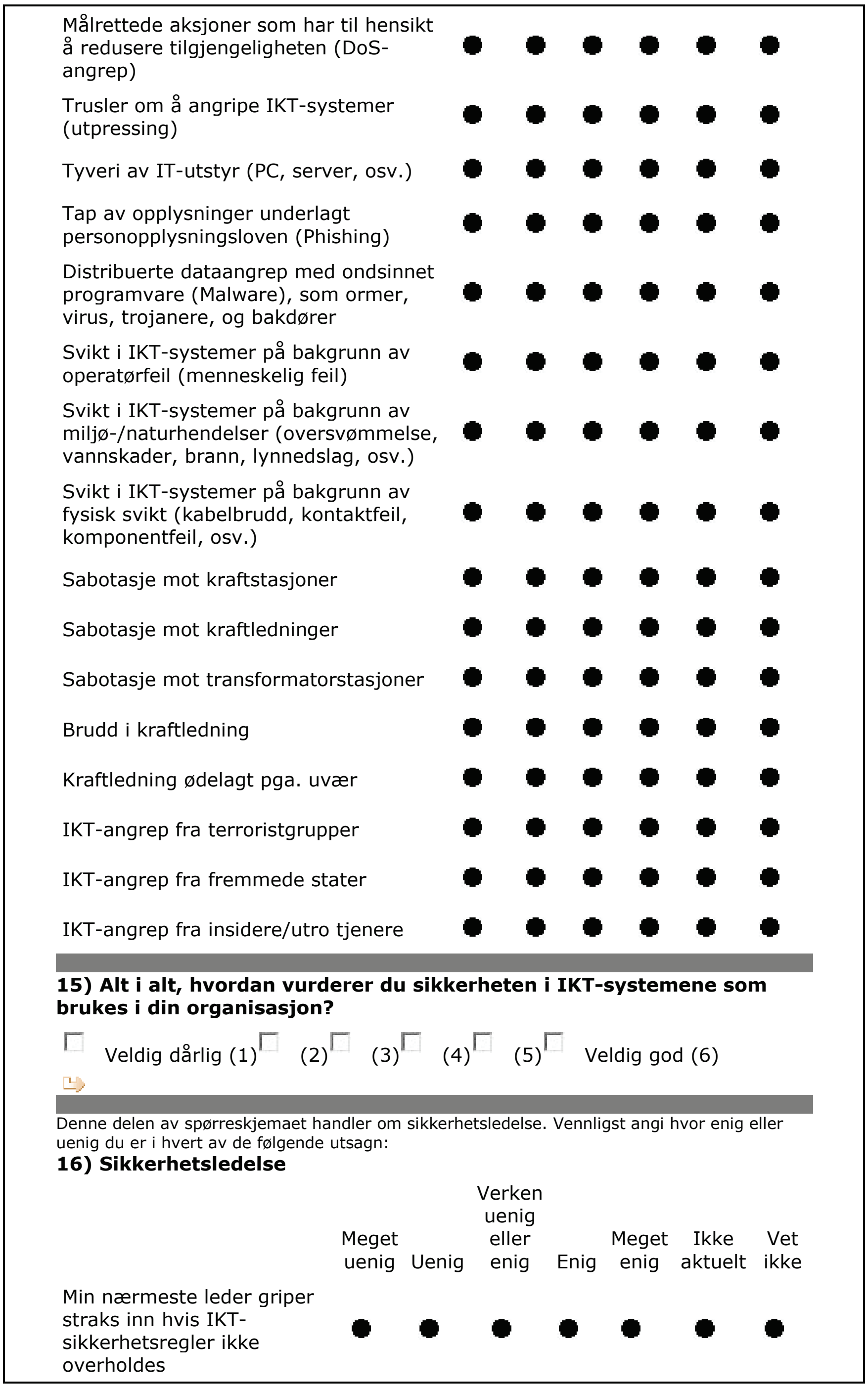
13) Hendelser

	Ja	Nei	Vet ikke
Målrettede datainnbrudd (hacking)	●	●	●
Tyveri av informasjon (industriell spionasje, stjeling av passord, osv.)	●	●	●
Uautorisert endring/sletting av data	●	●	●
Misbruk av IKT-ressurser (PC/nett/server)	●	●	●
Spredning av ulovlig/opphavsrettslig beskyttet materiale (piratkopiering)	●	●	●
Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)	●	●	●
Trusler om å angripe IKT-systemer (utpressing)	●	●	●
Tyveri av IT-utstyr (PC, server, osv.)	●	●	●
Tap av opplysninger underlagt personopplysningsloven	●	●	●
Distribuerte dataangrep med ondsinnet programvare (Malware), som ormer, virus, trojanere, og bakdører	●	●	●
Svikt i IKT-systemer på bakgrunn av operatørfeil (menneskelig feil)	●	●	●
Svikt i IKT-systemer på bakgrunn av miljø-/naturhendelser (oversvømmelse, vannskader, brann, lynnedslag, osv.)	●	●	●
Svikt i IKT-systemer på bakgrunn av fysisk svikt (kabelbrudd, kontaktfeil, komponentfeil, osv.)	●	●	●

Nedenfor er det angitt noen fare- og ulykkeskategorier som kan oppstå i organisasjonen. Markér vennligst hvor stor risiko du mener de forskjellige kategoriene kan utgjøre for organisasjonen. Vi er her interessert i din personlige vurdering. Kryss av én boks for hver situasjon:

14) Risikooppfattelse/-persepsjon

	Meget liten risiko (1)	(2)	(3)	(4)	(5)	Meget stor risiko (6)
Målrettede datainnbrudd (hacking)	●	●	●	●	●	●
Tyveri av informasjon (industriell spionasje, stjeling av passord, osv.)	●	●	●	●	●	●
Uautorisert endring/sletting av data	●	●	●	●	●	●
Misbruk av IKT-ressurser (PC/nett/server)	●	●	●	●	●	●
Spredning av ulovlig/opphavsrettslig beskyttet materiale piratkopiering)	●	●	●	●	●	●



Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)	●	●	●	●	●	●
Trusler om å angripe IKT-systemer (utpressing)	●	●	●	●	●	●
Tyveri av IT-utstyr (PC, server, osv.)	●	●	●	●	●	●
Tap av opplysninger underlagt personopplysningsloven (Phishing)	●	●	●	●	●	●
Distribuerte dataangrep med ondsinnet programvare (Malware), som ormer, virus, trojanere, og bakdører	●	●	●	●	●	●
Svikt i IKT-systemer på bakgrunn av operatørfeil (menneskelig feil)	●	●	●	●	●	●
Svikt i IKT-systemer på bakgrunn av miljø-/naturhendelser (oversvømmelse, vannskader, brann, lynnedslag, osv.)	●	●	●	●	●	●
Svikt i IKT-systemer på bakgrunn av fysisk svikt (kabelbrudd, kontaktfeil, komponentfeil, osv.)	●	●	●	●	●	●
Sabotasje mot kraftstasjoner	●	●	●	●	●	●
Sabotasje mot kraftledninger	●	●	●	●	●	●
Sabotasje mot transformatorstasjoner	●	●	●	●	●	●
Brudd i kraftledning	●	●	●	●	●	●
Kraftledning ødelagt pga. uvær	●	●	●	●	●	●
IKT-angrep fra terroristgrupper	●	●	●	●	●	●
IKT-angrep fra fremmede stater	●	●	●	●	●	●
IKT-angrep fra insidere/utro tjenere	●	●	●	●	●	●

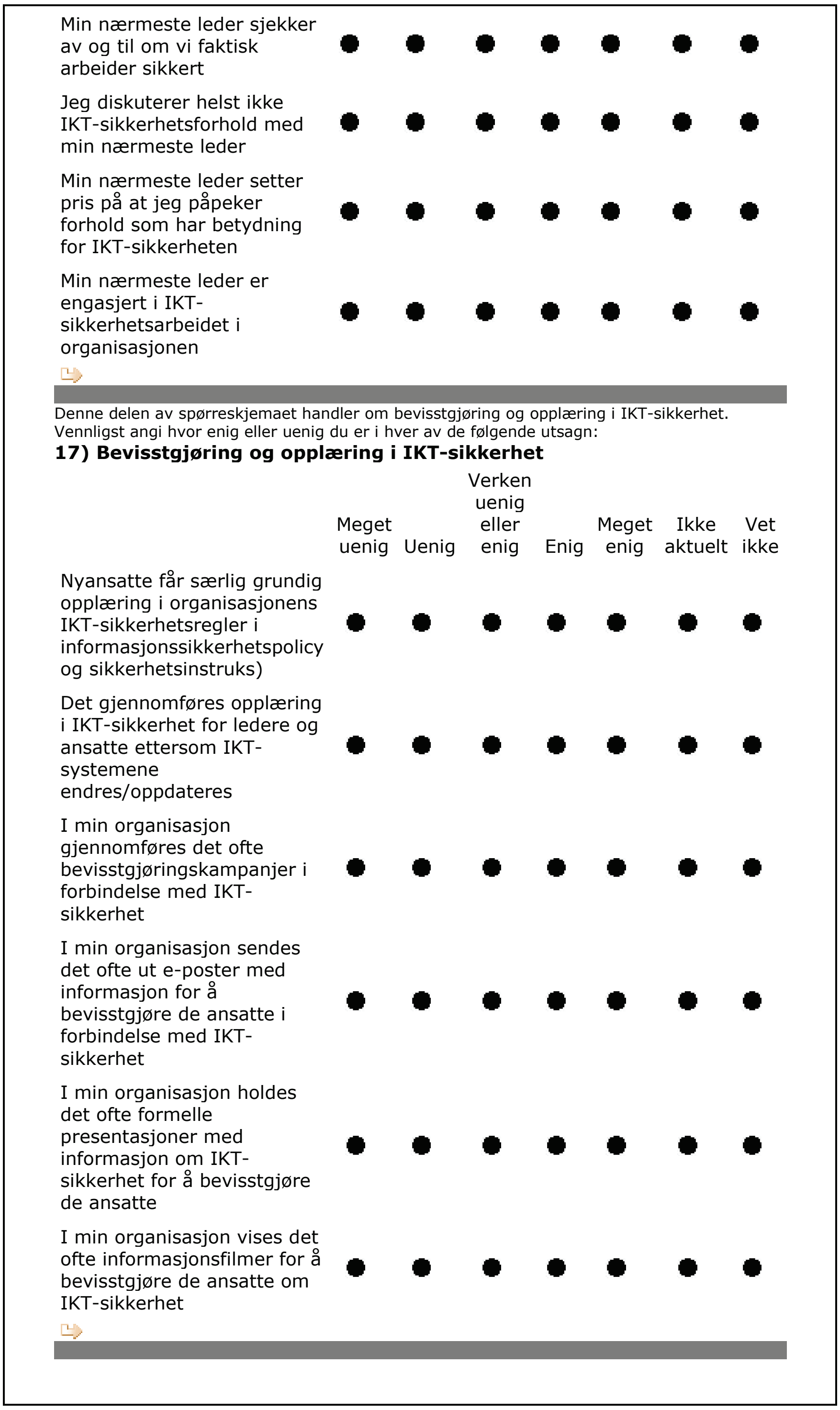
15) Alt i alt, hvordan vurderer du sikkerheten i IKT-systemene som brukes i din organisasjon?

□ Veldig dårlig (1)□ (2)□ (3)□ (4)□ (5)□ Veldig god (6)

Denne delen av spørreskjemaet handler om sikkerhetsledelse. Vennligst angi hvor enig eller uenig du er i hvert av de følgende utsagn:

16) Sikkerhetsledelse

	Meget uenig	Uenig	Verken uenig eller enig	Enig	Meget enig	Ikke aktuelt	Vet ikke
Min nærmeste leder griper straks inn hvis IKT-sikkerhetsregler ikke overholdes	●	●	●	●	●	●	●

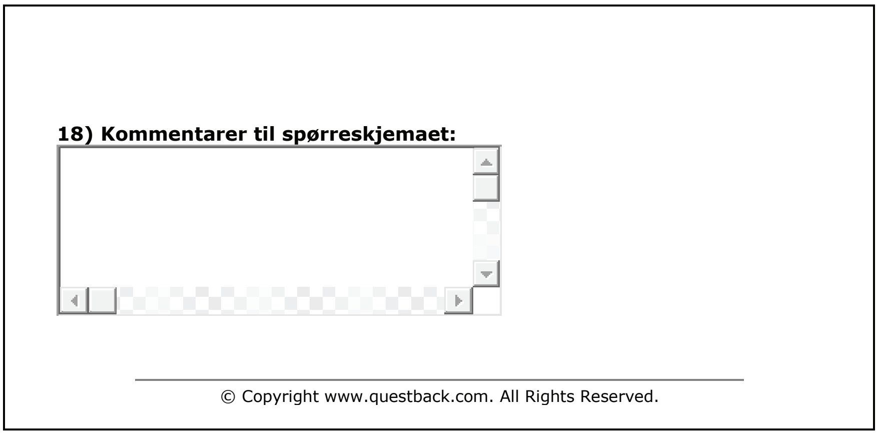


Min nærmeste leder sjekker av og til om vi faktisk arbeider sikkert	●	●	●	●	●	●	●
Jeg diskuterer helst ikke IKT-sikkerhetsforhold med min nærmeste leder	●	●	●	●	●	●	●
Min nærmeste leder setter pris på at jeg påpeker forhold som har betydning for IKT-sikkerheten	●	●	●	●	●	●	●
Min nærmeste leder er engasjert i IKT-sikkerhetsarbeidet i organisasjonen	●	●	●	●	●	●	●

Denne delen av spørreskjemaet handler om bevisstgjøring og opplæring i IKT-sikkerhet. Vennligst angi hvor enig eller uenig du er i hver av de følgende utsagn:

17) Bevisstgjøring og opplæring i IKT-sikkerhet

	Meget uenig	Uenig	Verken uenig eller enig	Enig	Meget enig	Ikke aktuelt	Vet ikke
Nyansatte får særlig grundig opplæring i organisasjonens IKT-sikkerhetsregler i informasjonssikkerhetspolicy og sikkerhetsinstruks)	●	●	●	●	●	●	●
Det gjennomføres opplæring i IKT-sikkerhet for ledere og ansatte ettersom IKT-systemene endres/oppdateres	●	●	●	●	●	●	●
I min organisasjon gjennomføres det ofte bevisstgjøringskampanjer i forbindelse med IKT-sikkerhet	●	●	●	●	●	●	●
I min organisasjon sendes det ofte ut e-poster med informasjon for å bevisstgjøre de ansatte i forbindelse med IKT-sikkerhet	●	●	●	●	●	●	●
I min organisasjon holdes det ofte formelle presentasjoner med informasjon om IKT-sikkerhet for å bevisstgjøre de ansatte	●	●	●	●	●	●	●
I min organisasjon vises det ofte informasjonsfilmer for å bevisstgjøre de ansatte om IKT-sikkerhet	●	●	●	●	●	●	●



18) Kommentarer til spørreskjemaet:

Appendix 2: Factor analysis

Factor analysis

In this appendix, I provide a thorough description of the factor analysis used for assessing the construct validity of the questionnaire survey, which guided the selection of the specific challenges that came to be the focus of this thesis.

As mentioned earlier in the thesis, exploratory factor analysis (EFA) was chosen to examine the underlying dimensions of the constructs of interest in this research project. EFA is used when the researcher does not know how many factors are necessary to explain the interrelationships among a set of characteristics, indicators, or items. A basic assumption of EFA is that within a collection of observed variables there exists a set of underlying factors, smaller in number than the observed variables, that can explain the interrelationships among those variables (Pett, Lackey, and Sullivan, 2003).

Two main issues must be considered in determining whether a particular data set is suitable for factor analysis: sample size and the strength of the relationships among the items. There is little agreement among authors concerning how large a sample should be; however, the recommendation is generally to have a large sample. Some suggest having at least 300 cases for factor analysis (Tabachnick and Fidell, 2007), while others say the sample size should be 100 or larger (Hair, 1998; Oltedal, 2011). It is also important to determine whether there are sufficient numbers of significant correlations among the items in the questionnaire to justify undertaking a factor analysis. If the correlations among the items are not significant, it will not be possible to obtain a parsimonious set of factors that represent the items in the proposed scale. Several tests can be undertaken by computer to ascertain whether it would be judicious to proceed with factor analysis. In this project, I used Bartlett's test of sphericity and the Kaiser-Meyer-Olkin test (Pett, Lackey, and Sullivan, 2003).

Principal component analysis (PCA) was chosen as the factor extraction method in this research project. PCA is commonly used by researchers interested in scale development and evaluation (Pallant, 2010). The goal of PCA is to arrive at a succinct set of uncorrelated components that extract variance in descending order and summarize the data set. PCA is especially useful when the researcher wants to summarize the relationships among a large number of variables with a smaller number of components, which is relevant for this project. Rotation was used to improve the meaningfulness and interpretation of the generated factors. Factor rotation is the process of turning the reference axes of the factors about their own origin to achieve a simple structure and theoretically more meaningful factor solution. In this research project, both varimax rotation (orthogonal) and direct oblimin rotation (oblique) were used to rotate the factors, and the type of rotation that found the simplest factor solution for the items was chosen (Pett, Lackey, and Sullivan, 2003).

PCA with both direct oblimin and varimax rotation was carried out to explore the underlying factor structure of the scales used in the survey. Factors were extracted based on the following analytical criteria: (1) pairwise deletion (excluding cases if they were missing the data required for the specific analysis), (2) eigenvalue greater than 1.0, (3) factor loading of more than .4, and (4) inspection of the screeplot (Pett, Lackey, and Sullivan, 2003). A scale reliability test was then performed for the chosen factors to check the new scale's internal consistency (i.e., whether all the items measured the same underlying construct). Cronbach's alpha coefficient is one of the most commonly used indicators of internal consistency, and ideally the Cronbach's alpha coefficient of a scale should be above .7 (Pallant, 2010).

PCA typically requires that the variables being examined be based on similar units of measurement. In this research project, the variables examined by factor analysis were the items from the knowledge of safety and security scale, the perception of compliance scale, the attitude toward safety and security scale, the attitude toward regulation scale, the risk perception scale, the safety and security management scale, and the awareness creation and training scale. As previously mentioned, all the items were measured on similar Likert scales. The items on the risk perception scale were measured on a scale from 1 to 6, and the rest of the items were measured on a scale from 1 to 5. This means that each item in the scales shares a similar or standardized scale of measurement (Pett, Lackey, and Sullivan, 2003).

The first attempt to perform PCA with all the chosen items did not show any results because the resulting matrix was not a positive definite. This was probably due to pairwise deletion of missing values. The perception of compliance scale had a lot of missing data, and many of the respondents answered "don't know" on the questions concerning the organizations' compliance with ICT safety and security regulations and rules. In addition, self-report surveys might not be the best method for measuring concepts like compliance with rules and regulations. The respondents might give socially desirable answers instead of answering truthfully. Social desirability occurs when survey respondents seek to present themselves in a positive light and therefore respond to an item according to what they think is the socially correct answer rather than their true answer. This can distort the data and affect the validity of the instrument (Pett, Lackey, and Sullivan, 2003). In this research project, the respondents were asked to answer according to their perception of compliance in the organization as a whole, and not their own compliance with rules and regulations. Nevertheless, the respondents might also have given a socially desirable answer on behalf of their organization.

Compliance with ICT safety and security rules and regulations may also be measured more objectively (e.g., by on-site inspections and revisions). Because the items on the perception of compliance scale did not load on any specific factors, a lot of data were missing, and to manage the problem with social desirability, I decided to remove most of the items on the scale from the factor analysis. Qualitative data from document studies of NVE's supervision reports and interviews with representatives from the contingency planning department in NVE were used instead. Three items from the perception of compliance scale were retained for subsequent factor analyses: item 3 regarding the use of checklists when preparing risk and vulnerability analysis, item 7 regarding the use of NVE's guideline when preparing risk and vulnerability analysis, and item 8 regarding the use of standards when preparing risk and vulnerability analysis, information safety/security policy, and safety/security instructions. These items were retained as data material for article 2.

After removing all the items from the perception of compliance scale, the suitability of the data for factor analysis was assessed. The sample size was 103, which by some is considered too small. However, inspection of the correlation matrix from the initial factor analysis of all the chosen items revealed the presence of many coefficients of .3 and above, the Kaiser-Meyer-Olkin value was .614, exceeding the recommended value of .6, and Bartlett's test of sphericity reached statistical significance (.000), supporting the factorability of the correlation matrix (Pallant, 2010). These results are shown in Table 11.

Table 11 - KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		,614
Bartlett's Test of Sphericity	Approx. Chi-Square	3316,637
	df	1225
	Sig.	,000

Several factor analyses with different numbers of specific factors were undertaken to determine the number of factors that represented the dimensions of the constructs being measured. By examining the results of extracting different numbers of factors, it is easier to arrive at that parsimonious set of factors that makes the most intuitive sense given the problem area (Pett, Lackey, and Sullivan, 2003).

One approach to determining the number of initial factors is to select only factors with an eigenvalue greater than 1.00. This means that these factors account for more than their share of the total variance in the items (the Kaiser-Guttman rule). Another approach for determining the number of factors is the cumulative percentage of variance extracted by successive factors. However, there are no definitive guidelines for what the threshold for maximum variance extracted should be. According to some authors, the first few components should extract a sizable percentage of the total variance (50% or more) or there is little to be gained from the application of PCA. A third method, called the scree plot, is to plot the extracted factors against their eigenvalues in descending order of magnitude to identify distinct breaks in the slope of the plot. It is necessary to use subjective judgment to determine where the discontinuity of eigenvalues occurs, and one often needs to examine the loadings of items on the factors to determine which solution makes the most theoretical and intuitive sense. One way to make it easier to discern the patterns of high and low loadings is to suppress absolute values less than .4. This does not delete any of the item-to-factor correlations, but the loadings that remain in view are strong (Pett, Lackey, and Sullivan, 2003).

The items on the knowledge of safety and security scale and the attitude toward safety and security scale did not load on any specific factors/components. A source of confusion is often the distinction made between perceptions and attitudes. Perceptions are regarded as descriptive and referring to external objects, whereas attitudes are considered personal evaluations of the same objects (Guldenmund, 2007). However, according to Guldenmund (2007), perceptions are infused with the attitudes that underlie them in that perceptions are not mere descriptions, but rather evaluations of what people see around them and, consequently, perceptions reflect attitudes. The main focus in this research project (in article 3) is on risk perception. Therefore, I decided to remove the items on the knowledge of safety and security scale and the attitude toward safety and security scale from the factor analysis and concentrate on using the data from the risk perception scale.

Most of the items on the risk perception scale loaded substantially on one component. However, two items from the scale did not load as strongly on the same component. These items were item 17 (the risk of a fracture in a power line) and item 18 (the risk of a power line being destroyed by bad weather). The Cronbach's alpha coefficient for the total risk perception scale was .95 and removing these two items did not change the value of the coefficient alpha. The two items' contribution to the overall instrument was of little importance; hence, I decided to delete these two items from the risk perception scale.

A new PCA was performed after removing all the items on the knowledge of safety and security scale and the attitude toward safety and security scale, in addition to items 17 and 18 on the risk perception scale. The three items that I chose to retain from the perception of compliance scale were also added to the analysis (items 3, 7, and 8). The Kaiser-Meyer-Olkin value now increased to .690, and Bartlett's test of sphericity still reached statistical significance (.000). These results are shown in Table 12.

Table 12 - KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,690
Bartlett's Test of Sphericity	Approx. Chi-Square	1642,317
	df	666
	Sig.	,000

The PCA revealed the presence of eight components with eigenvalues exceeding 1. However, this survey contained a large number of items, which led to a large number of eigenvalues that met the criterion. An inspection of the scree plot revealed a break after the third component. However, all the retained items on the risk perception scale loaded strongly (above .4) on one component, and all the items on the safety and security management scale and the awareness creation and training scale loaded strongly on another component. The two-component solution explained a total of 43.1% of the variance, with Factor 1 contributing 27.4% and Factor 2 contributing 15.7%. According to Pett, Lackey, and Sullivan (2003), the decision regarding how many factors to extract should not be based solely on statistical criteria; it should also make theoretical sense. The ultimate criteria for determining the number of factors are factor interpretability and usefulness. The four items on the attitude toward regulation scale and the three items from the perception of compliance scale did not load strongly on any specific components. Thus, it made more theoretical sense to choose a two-factor solution.

Based on this reasoning, I removed the four items on the attitude toward regulation scale and the three items from the perception of compliance scale and performed a new PCA with the remaining items (the items from the risk perception scale minus items 17 and 18, the items on the safety and security management scale, and the items from the awareness creation and training scale). The Kaiser-Meyer-Olkin value now increased to .813 (Table 13).

Table 13 - KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,813
Bartlett's Test of Sphericity	Approx. Chi-Square	2155,927
	df	435
	Sig.	,000

I chose a two-factor solution and rotated this using both direct oblimin and varimax rotation. A simple two-factor solution for the items was found using direct oblimin rotation. This two-component solution explained a total of 51.5% of the variance, with Factor 1 contributing 33.5% and Factor 2 contributing 18%. The rotated solution showed a simple structure, with both components showing a number of strong loadings and all variables loading substantially on only one component (Pallant, 2010). All the chosen items from the risk perception scale loaded on Factor 1, and all the items on the safety and security management scale and the awareness creation and training scale loaded on Factor 2. There was a very weak negative correlation between the two factors (r = -.09). I named Factor 1 "Risk perception" and Factor 2 "Safety and security management, awareness creation, and training."

Using factor analysis, factors can be refined through successive factoring of a set of items within a single factor (Pett, Lackey, and Sullivan, 2003). The items that loaded on Factor 2 originally came from two different scales (i.e., the safety and security management scale and awareness creation and training scale). Based on this, I chose to factor analyze Factor 2 a second time to determine whether the items represent a single factor or several smaller factors. The Kaiser-Meyer-Olkin value was now .885, and Bartlett's test of sphericity reached statistical significance (.000), supporting the factorability of the correlation matrix (Pallant, 2010). Again I chose a two-factor solution, and a simple solution for the items was found using direct oblimin rotation. This two-component solution explained a total of 62.6% of the variance, with Factor A contributing 49.5% and Factor B contributing 13.1%.

The rotated solution showed a relatively simple structure, with both components showing a number of strong loadings. All the items from the safety and security management scale loaded on Factor A, and all the items from the awareness creation and training scale loaded on Factor B. Some items had strong loadings on both the components. However, these items were placed with the factor on which they had the highest loading, which was also the factor with which the items were most closely related conceptually (Pett, Lackey, and Sullivan, 2003). Based on these results, Factor 2 was divided into two smaller factors called "Safety and security management" and "Awareness creation and training." There was a medium positive correlation between these two factors (r = .46).

As described earlier in the thesis, PCA with direct oblimin rotation finally resulted in a two-factor solution, where Factor 1 was named "Risk perception" and Factor 2 was named "Safety and security management, awareness creation, and training." After further analysis, Factor 2 was divided into two smaller factors named "Safety and security management" (Factor A) and "Awareness creation and training" (Factor B). The risk perception scale (Factor 1) was analyzed as data material for article 3, and the safety and security management scale and the awareness creation and training scale (Factor 2) were analyzed as data material for article 4. The four items on the attitude toward regulation scale were still retained as data material for the research project, and descriptive statistics for each item were used in article 1. In addition, the three aforementioned items from the perception of compliance scale were retained (items 3, 7, and 8). Descriptive statistics for each of these three items were used as data material for article 2. Finally, I also decided to keep the data from the knowledge of safety and security scale, which is discussed in article 3.