SAFETY SCIENCE Monitor

Issue 1 2015

Article 4

VOL 19

# 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.

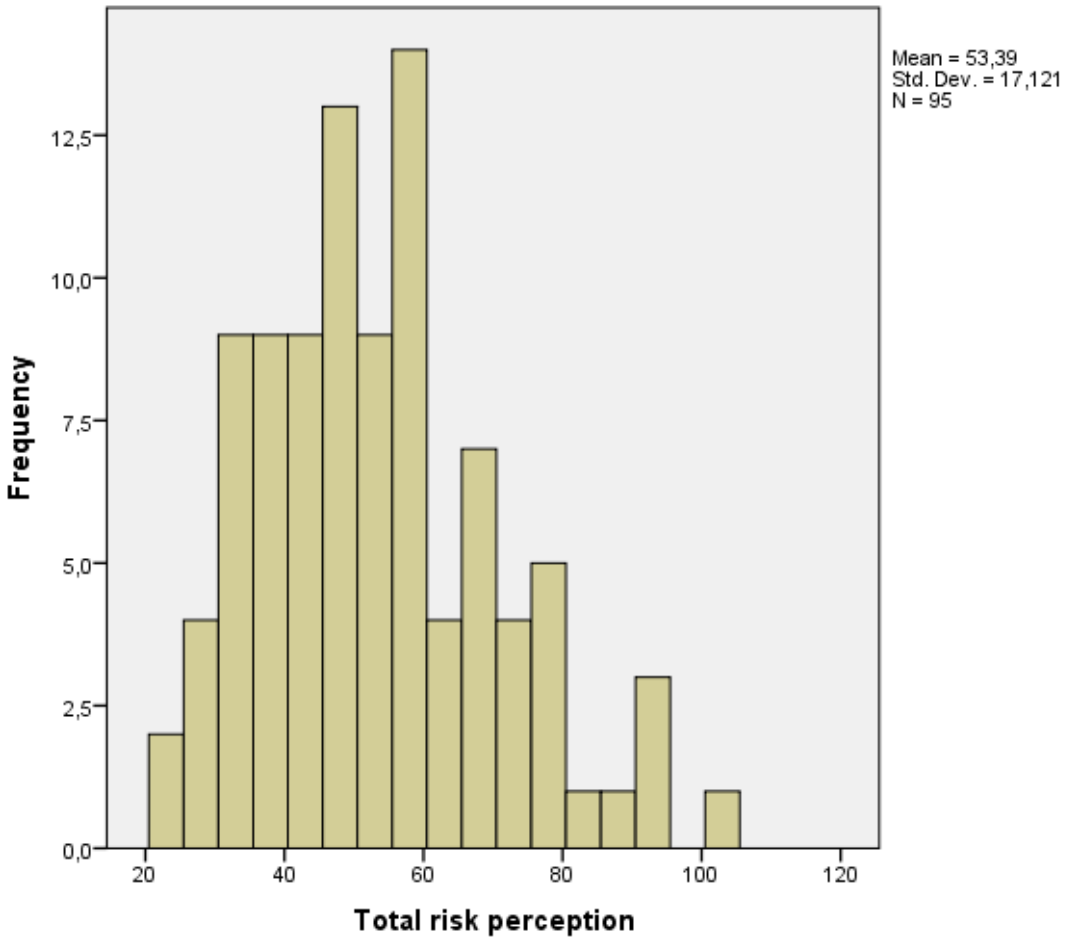
The respondents perceived the overall safety level of the organizations' ICT systems as good, as shown in Table 2.

**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.