Division of Cyber Safety and Security Responsibilities Between Control System Owners and Suppliers

Ruth Skotnes

Chapter 8

DIVISION OF CYBER SAFETY AND SECURITY RESPONSIBILITIES BETWEEN CONTROL SYSTEM OWNERS AND SUPPLIERS

Ruth Skotnes

Abstract The chapter discusses the important issue of responsibility for information and communications technology (ICT) – or cyber – safety and security for industrial control systems and the challenges involved in dividing the responsibility between industrial control system owners and suppliers in the Norwegian electric power supply industry. Industrial control system owners are increasingly adopting information and communications technologies to enhance business system connectivity and remote access. This integration offers new capabilities, but it reduces the isolation of industrial control systems from the outside world, creating greater security needs. The results of observation studies indicate that Norwegian power network companies and industrial control system suppliers have contributed to the creation of a culture that does not focus on information and communications systems safety and security. The increased use of standards and guidelines can help improve cooperation between industrial control system owners and suppliers. Norwegian industrial control system owners should also implement a culture change in their organizations and should attempt to influence the safety and security culture of their suppliers. Power network companies need to place information and communications systems safety and security on par with operational priorities and they need to become more vocal in demanding secure products from their suppliers.

Keywords: Power networks, Norway, industrial control systems, owners, suppliers

1. Introduction

Industrial control systems (ICSs) are vital to the operation of critical infrastructure assets that are increasingly interconnected and mutually depen-

dent. Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs) and other systems such as programmable logic controllers (PLCs) and human-machine interfaces (HMIs) [14]. Industrial control systems are deployed worldwide and are traditionally used by utilities and industries in areas such as electric power supply, oil and natural gas, railroads, water and wastewater. These systems support many aspects of modern life and are vital to societal wellbeing and the functioning of the economy [16].

Historically, industrial control systems have had little resemblance to traditional information and communications technology (ICT) – or cyber – systems in that they were isolated systems running proprietary control protocols using specialized hardware and software. However, according to Leith and Piper [14], industrial control systems are increasingly adopting information and communications technologies to support corporate system connectivity and remote access. Manufacturers, vendors and suppliers of industrial control systems (collectively referred to as "suppliers" in this work) are designing and implementing industrial control systems using commodity hardware, software, network devices and protocols; hence, they increasingly resemble traditional information and communications systems. This integration supports new business and operational capabilities, but it reduces the isolation of industrial control systems from the outside world, creating a greater need for security.

According to the U.S. Industrial Control Systems Emergency Response Team (ICS-CERT), infrastructure assets that use industrial control systems have become high-profile targets and are recording increasing numbers of cyber vulnerabilities and incidents [22]. Byres [4] has stated that shifts in technology have greatly increased the complexity and interconnectedness of control systems. As a result, industrial control systems now have many of the same vulnerabilities that have long plagued enterprise networks. In addition, devices in industrial control networks are being subjected to new threats that they were not designed to handle. All these conditions have led to significant increases in the numbers of industrial plant disruptions and shutdowns due to cyber security problems.

This chapter focuses on the Norwegian electric power supply sector. Electric power supply is the basic infrastructure for all kinds of production and services and is highly dependent on computers and communications [15]. Since the early 1990s, the energy sectors in European countries have undergone considerable institutional restructuring, where large state-owned monopolies have been transformed to multiple, smaller independent entities [3]. Emerging control systems that make intensive use of information and communications technologies have greatly assisted in dealing with the multiple independent entities, open access and progressive integration of electricity markets, and the intensification of cross-border trade. However, the full application of these technologies demands a new approach to system design and operation, and their integration in existing control infrastructures and practices has been very challenging [26].

This research focuses on two key questions:

- How is the responsibility for information and communications systems safety and security shared between the owners and suppliers of industrial control systems in the Norwegian electric power supply sector and how do they follow up on this responsibility?

- How should owners and suppliers of industrial control systems share the responsibility for information and communications systems safety and security in order to reduce the potential risks and threats to these systems?

These research questions are primarily answered via observation studies and interviews, in addition to results from an item in a survey sent to 137 power network companies in Norway. The primary contribution of this research is its exposition of the important issue of responsibility for information and communications systems safety and security for industrial control systems, and the challenges involved in dividing the responsibility between industrial control system owners and suppliers in the Norwegian electric power supply industry.

This chapter uses the term "information and communications systems safety and security" to cover the terms information security, cyber security, data security, information technology security, information and communications technology security and data security, among others. Following the 2015 Official Norwegian Report NOU 2015:13 on digital vulnerabilities in society [7], information and communications systems security is considered to be synonymous with cyber security. However, the term "safety" is added to emphasize that industrial control systems have very complex interactions with physical processes and consequences in the industrial control system domain can manifest in harmful physical events [27].

2. Background

Critical infrastructure is a term used by governments to describe assets that are essential to the functioning of a society and its economy. Since the word infrastructure refers to physical assets (e.g., complex technological systems), other terms are often introduced to focus on what is to be achieved. An important term is society-critical functions, which are essential to ensuring the basic needs of society. The basic needs include food, water, heating and cooling, and safety and security. The society-critical functions depend on infrastructure components. The basic infrastructure components include electric power grids, information and communications networks, water and sewage networks, roads, railroads and harbors [28].

Information and communications technology is increasingly becoming a part of all critical infrastructure assets. According to the European Union Agency for Network and Information Security (ENISA), information and communications systems can be viewed as critical infrastructures in themselves, where critical information infrastructure protection (CIIP) is an essential part of comprehensive critical infrastructure protection (CIP) efforts [2].

The increasing complexity of modern industrial control systems introduces several vulnerabilities and attack vectors, including indirect access through corporate networks or directly via the Internet, virtual private networks (VPNs), wireless networks and dial-up modems [14]. According to Leith and Piper [14], threats to industrial control systems come from numerous sources, including adversarial sources such as hostile governments, terrorist groups, industrial spies, disgruntled employees, malicious intruders and hacktivists, and from natural sources such as system complexity, human errors and accidents, equipment failures and natural disasters.

According to Knowles et al. [13], the default perspective for industrial control system stakeholders has been to view security as a low priority goal while relying on "security through obscurity" (i.e., using secrecy in an attempt to ensure security). However, Byres [4] has noted that the discovery of Stuxnet in 2010 was a wake-up call for many operators of industrial control systems. Another wake-up call came in December 2015, when, what is believed to be, the first cyber attack on a power grid caused a black-out for hundreds of thousands of people in Ukraine. The power outage was initiated by destructive malware called BlackEnergy that compromised computers and wiped out sensitive control systems in portions of the Ukrainian power grid [21].

Industrial control systems are used to operate geographically-dispersed assets such as electric power grids that are often scattered over thousands of square kilometers. SCADA systems and distributed control systems are often networked together, as in the case of electric power control centers and electric power generation facilities [27]. The integration of information and communications technologies with industrial control systems used for electric power supply has increased the vulnerabilities, especially due to the introduction of advanced metering infrastructures (AMIs) and smart grids. An advanced metering infrastructure is an integrated system of smart meters, communications networks and data management systems that enable two-way communications between utilities and end users. Smart grids connect power plants and system control centers with households, businesses and buildings over large regions (states, countries and groups of countries). These technological developments increase system connectivity and criticality [27], but also make previously-isolated industrial control systems vulnerable to new threats and risks [15].

In 2015, the Centre for the Protection of National Infrastructure (CPNI) in the United Kingdom published the Security for Industrial Control Systems (SICS) Framework, which provides organizations with best practices for securing industrial control systems. The framework consists of a Good Practice Guide Framework Overview [6], which describes eight core elements at a high level. This research focuses on one of the elements, namely, managing third-party risks.

The CPNI's Good Practice Guide, Manage Third-Party Risks [5] states that the security of an organization's industrial control systems can be put at significant risk by third parties (e.g., suppliers, support organizations and other entities in the value chain) and, therefore, warrants considerable attention. Ac-

cording to the guide, third parties are often considered a weak link and must, therefore, be engaged as a part of an industrial control systems security program at the earliest stage.

In the past, industrial control systems were often bespoke systems that were developed in-house; now, most systems are configured by third-party integrators and suppliers. Consequently, third-party products and services are present in almost all industrial control systems, bringing with them a number of associated risks. One might assume that industrial control system suppliers would be very security conscious. However, according to Leith and Piper [14], this is often not the case, as evidenced by suppliers who have delivered systems with dial-up modems to provide remote access and ostensibly "ease the burdens of maintenance" for field support personnel. Leith and Piper state that, in many instances, cyber security controls are not enabled by end users for reasons of convenience. In other cases, remote administrative-level access to industrial control systems is provided to support staff via an unlisted telephone number in combination with an access control password. According to CPNI's Good Practice Guide [5], seemingly innocuous systems that provide technical support can have significant direct or indirect impacts on critical systems.

3. Norwegian Electric Power Supply Sector

The Norwegian electric power grid depends almost entirely (98%–99%) on hydropower generation. The Norwegian grid is divided into a transmission (main) grid, regional grid and distribution grid. The transmission grid comprises the highways of the power system that link producers and consumers across the country; the transmission grid also includes international interconnections. The regional grid links the transmission and distribution grids. The distribution grid comprises the local grids that supply power to end users such as households, services and industry. Minor consumers are connected to the distribution grid while major consumers, such as power-intensive industries, are directly connected to the regional or transmission grids [19].

The regulation of safety and security in the Norwegian electric power supply system is based on functional regulation (enforced self-regulation), where internal control is essential. Safety and security management (or risk management) is required by the Internal Control Regulation Act of 1997 (Regulation Concerning Systematic Health, Environment and Safety Activities at Enterprises). Internal control gives companies the responsibility to implement updated safety management systems. In the case of the electric power supply sector, the requirement for safety and security management is further reinforced by several regulations [18]. All power network companies are required to appoint an information and communications technology safety and security manager (or coordinator), and are required to perform risk and vulnerability analyses of their industrial control systems [20].

The regulatory authority, the Norwegian Water Resources and Energy Directorate (NVE), has developed a guideline for contingency planning to assist companies in complying with the internal control requirement. The power net-

work companies are responsible for ensuring that their information and communications system suppliers protect sensitive information (belonging to power companies) and are also responsible for instituting safety and security agreements with the suppliers of their industrial control systems. Routines and procedures describing how changes are controlled must be described in the internal control system and stipulated in the agreements with suppliers. The regulations require power network companies to have specific procedures for remote access to their industrial control systems (by their employees and suppliers). The power network companies are also required to keep logs of external accesses to their industrial control systems and all other relevant activities. The Norwegian Water Resources and Energy Directorate also recommends that power network companies cooperate with their suppliers, especially when incorporating new technologies in their industrial control systems (e.g., advanced metering infrastructures) [20].

Norwegian enterprises (including power network companies) are often advised to use the ISO/IEC27001:2005 Standard (Formal Requirements for Information Security Management Systems) when they develop and implement their information and communications safety and security management systems (with the support of ISO/IEC 27002 (Code of Practice for Information Security Management)). The ISO/IEC 27000 series of information security standards was developed by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). According to the European Union Agency for Network and Information Security [2], ISO/IEC 27002 is the most widely-used standard by industrial control system operators, including the control-system-specific standards.

However, results from a previous study [23] have shown that very few power network companies in Norway actually use the technical standards. The study results implied that Norwegian power network companies do not see the benefits of being certified for compliance with technical standards, because Norwegian contingency planning regulations specify the requirements for protecting their integrated information/communications and industrial control systems. On the other hand, several requirements described in the Norwegian Water Resources and Energy Directorate guidelines for contingency planning are similar to the requirements in ISO/IEC 27001 and 27002, and the Norwegian Water Resources and Energy Directorate has also included parts of NIST 800-82 [27] in its guidelines. The NIST 800-82 document, which covers industrial control systems security, was developed by the National Institute of Standards and Technology (NIST), a U.S. Department of Commerce agency.

4. Materials and Methods

The research methodology involved a mixed-methods approach. It was mainly based on qualitative data collected via observation studies and group interviews. Results from an item in a survey of managers and employees at Norwegian power network companies were also added to complement the qualitative data.

4.1 Observation Studies

Observation studies were conducted at two information and communications technology safety and security conferences for electric power supply companies that were held in Norway in 2011. The conference participants were mainly managers and employees working in the area of information and communications technology safety and security at Norwegian power network companies or suppliers of industrial control systems and information and communications technology safety and security solutions for these systems. The conference speakers included representatives from the Norwegian Water Resources and Energy Directorate and system suppliers, in addition to information and communications technology safety and security experts from universities and research institutes. The types of safety and security issues raised at the conferences, the types of issues focused on by participants and the types of questions and discussions that came up during the conferences were observed.

An observer-as-participant role was employed in the observation studies [1]. A researcher listened to the conference presentations and discussions and made notes of the important issues discussed, comments and arguments, but did not participate in any material manner. However, the conference participants were made aware that a researcher was present, and the researcher was introduced by the conference organizers at the start of each conference.

The data gathered during the observation studies was recorded in field notes. Field notes are written records of observed proceedings that also contain the researcher's impressions, reactions and hypotheses about what occurred. The data from the observation studies are presented in this chapter in the form of a narrative that describes the observations in detail and includes information on the researcher's reactions and interpretations.

4.2 Interviews

Qualitative data was gathered via two group interviews with representatives from the Norwegian Water Resources and Energy Directorate. Semi-structured interviews with open-ended questions were used. The interviewees were from the contingency planning department and were responsible for safety and security, contingency planning, and supervision and inspection of the Norwegian electric power supply sector. The first set of interviews involved three interviewees and the questions mainly focused on the interviewees' opinions of the risk perceptions of Norwegian power network companies and their awareness regarding the risk of failure caused by malfunctions in or attacks on their control systems. The second set of interviews involved two interviewees and the questions mainly focused on the interviewees' opinions of the use of functional internal control regulations for information and communications systems safety and security and their impressions of the attitudes of power network companies toward the applicable regulations.

4.3 Questionnaire Survey

The research study was part of a Ph.D. dissertation project that examined the challenges in safety and security management at power network companies due to the increased use of information and communications technologies in the electric power supply sector. A questionnaire survey was developed for the larger research project and a web-based questionnaire was sent to 334 managers or employees at 137 Norwegian power network companies. In all, 103 respondents returned the survey questionnaire, corresponding to a response rate of 31%.

One survey item focused on the division of responsibility of information and communications systems safety and security between the power network companies and their suppliers. The item stated: "In my organization, we always sign safety and security agreements with the suppliers of our ICT and ICS/SCADA systems" (Item 22). The respondents were asked to rate the degree to which they agreed with this statement. The responses were measured on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Interested readers are referred to [24, 25] for a detailed description of the survey.

5. Results and Discussion

The first research question posed in the study was:

- How is the responsibility for information and communications systems safety and security shared between the owners and suppliers of industrial control systems in the Norwegian electric power supply sector and how do they follow up on this responsibility?

The Official Norwegian Report (NOU 2015:13) submitted in November 2015 by the Committee on Digital Vulnerabilities in Society [7] found that digital vulnerabilities in interconnected systems cut across different sectors and industries through the supplier industry. Large international companies supply industrial control systems to industries around the globe, including Norwegian enterprises. The same types of vulnerabilities recur in products used in the various industries. Large industrial control systems often have components from several suppliers. According to the NOU 2015:13 Report, increased complexity and demands for reliability have made power network companies very dependent on their suppliers for maintenance and repairs through remote access. In recent years, the Norwegian Water Resources and Energy Directorate has prioritized the oversight and inspection of industrial control systems at Norwegian power companies due to increased vulnerabilities. Inspections often reveal inadequacies in the documentation of the connections between industrial control systems and other company networks. The Norwegian Water Resources and Energy Directorate has also found that there is insufficient documentation of the agreements and guidelines for remote access to industrial control systems.

Interviews with personnel from the Norwegian Water Resources and Energy Directorate revealed that many power network companies greatly trust the expertise of their suppliers and take for granted that the suppliers will develop safe technological solutions. Most of the infringements of safety and security regulations identified by the Norwegian Water Resources and Energy Directorate relate to industrial control systems and incomplete or inadequate risk and vulnerability analyses and contingency plans. The Norwegian Water Resources and Energy Directorate often discovers undocumented access points to industrial control systems, most of them involving remote access, supplier access and USB drives. According to the Norwegian Water Resources and Energy Directorate, many power network companies appear to have too much faith in the safety and security of their control systems and the gap between requirements and compliance is, in many instances, too great. Moreover, according to the interviews with Norwegian Water Resources and Energy Directorate personnel, some industrial control system suppliers have stated that, if power network companies were to engage the safety and security mechanisms already available in their industrial control systems, then the overall safety and security would be increased.

During the observation studies at one of the conferences, a representative from a Norwegian industrial control systems supplier stated that the owners are responsible for the safety and security of their systems and that the suppliers are only responsible for the safety and security of their products. The main reason is that the products were developed based on safety and security standards, mainly the NERC CIP and/or BDEW Standards. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) set of eleven reliability standards constitutes a framework for identifying and protecting bulk electrical systems [13]. The BDEW Standard, defined by the German Association of Energy and Water Industries, provides general guidelines for the planning and operation of generating plants connected to medium voltage distribution systems.

According to the representative from the supplier, the levels of safety and security of industrial control systems should be described in the customers' specifications of their systems. At the same time, owners should be careful not to provide too many details about how the safety and security of their systems are ensured. Also, the suppliers deliver products that their customers request and it would be difficult for them to deliver a standard level of safety and security due to differences in the customers' systems.

The representative also stated that industrial control systems usually incorporate products from multiple suppliers; thus, the focus on securing control systems should, to a larger degree, involve securing the entire information and communications infrastructure. In his opinion, safety and security is a shared task between all the involved parties and enhanced information and communications systems safety and security can only be achieved through close cooperation between owners and suppliers. Nonetheless, he stated that the balance between operational requirements and information and communications sys-

tems safety and security would always be a compromise. In his opinion, safety and security guarantees are difficult to make in a complex environment (some things may work in some infrastructures, but not in others). Suppliers can only make guarantees with respect to specific criteria.

A conference participant asked the same supplier representative about the requirements that suppliers imposed on their own employees regarding remote access to control systems at power network companies. According to the representative, his company had its own network into which its employees had to log on with usernames and passwords. The company also did background checks on its employees. Several suppliers had also discussed this issue with personnel from the Norwegian Water Resources and Energy Directorate. One of the suppliers recommended that system owners should do their own background checks of their suppliers because the owners are ultimately responsible for the safety and security of their organizations and systems. However, many conference participants noted that owners do not always have enough knowledge about threats and risks, and how to secure their systems. One of the conference participants asked the supplier representative what his company did with regard to this lack of knowledge. The representative answered that his company attempted to inform its customers about safety and security options, and conducted safety and security courses for its customers.

Another conference participant asked the supplier representative if his company employees had adequate knowledge of information and communications systems safety and security. He answered that the employees had sufficient knowledge. However, in his opinion, the suppliers and electric power supply companies had both contributed to building a culture that lacked a focus on information and communications systems safety and security. The power network companies did not set adequate requirements for their suppliers and software patches were not applied often enough. The control centers were required to operate 24 hours a day and, as a result, owners often waited too long to implement the necessary safety and security measures. The representative from the system supplier stressed that the suppliers and power network companies needed to cooperate to increase the focus on information and communications systems safety and security in the sector.

As mentioned above, regulations require that the Norwegian power network companies sign safety and security agreements with their industrial control system suppliers. On the other hand, the survey results revealed that 61.2% of the respondents answered positively (strongly agree or agree) on the item "In my organization, we always sign safety and security agreements with the suppliers of our ICT and ICS/SCADA systems" (Table 1). The results indicate that the power network companies do not sign safety and security agreements with their suppliers for all purchases of equipment and/or services.

According to the National Cyber Security Strategy for Norway of 2012 [18], owners of Norwegian critical infrastructure assets have limited awareness and knowledge about vulnerabilities, critical infrastructure interdependencies and the actions that enterprises must take to protect the infrastructure. Moreover,

Table 1. Distribution of scores for Item 22.

Response	Percentage	Number of Respondents
Strongly Disagree	1.0	1
Disagree	8.7	9
Neither Disagree or Agree	23.3	24
Agree	27.2	28
Strongly Agree	34.0	35
Not Relevant	0.0	0
Don't Know	5.8	6
Total	100	103

according to the interviewees from the Norwegian Water Resources and Energy Directorate, power network companies focus on what their industrial control systems provide (i.e., access to more information and operating in a simpler manner). However, there is not as much focus on, or awareness about, the risk of unwanted access to these systems, protection against malicious software, and so on. A previous study [24] also revealed that managers and employees of Norwegian power network companies perceive the risk of attacks on and malfunctions of their integrated information/communications and industrial control systems as relatively low.

The results of the current study show that there are challenges when it comes to the division of responsibilities for the safety and security of integrated information/communications and industrial control systems in the Norwegian electric power supply sector, and a lack of focus on information and communications systems safety and security in the sector. This leads to the second research question posed in this chapter:

- How should owners and suppliers of industrial control systems share the responsibility for information and communications systems safety and security in order to reduce the potential risks and threats to these systems?

As mentioned above, an earlier study showed that very few power network companies in Norway use technical standards. The increased use of standards and guidelines can help improve the cooperation between system owners and suppliers, and increase the focus on information and communications systems safety and security for industrial control systems in the Norwegian electric power supply sector. In fact, the NOU 2015:13 Report [7] recommends an increase in the use of international standards for information and communications systems safety and security.

Many published standards, guidelines and good practice documents provide recommendations for managing risks and threats to industrial control systems. One example is the NERC CIP set of eleven reliability standards. Another is the security standards developed over several years by the International Society of Automation (ISA) [10]. The ISA99 standards development committee,

which incorporates industrial cyber security experts from around the globe, has developed standards for industrial automation and control systems security, the first parts of which have been approved by the American National Standards Institute (ANSI). The original and ongoing ISA99 efforts are now being utilized by the International Electrotechnical Commission to produce the IEC 62443 series of multi-standards [10].

Meanwhile, the European Commission has set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) [8] to examine how a European certification scheme could improve industrial control systems security. ERNCIP is also studying resilience with the goal of operationalizing the concept to better understand how the resilience of critical infrastructures can be measured, enhanced and tested. Resilience is 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" [9].

According to the NIST 800-82 report [27], to properly address security in an industrial control system, a cross-functional cyber security team must apply its varied domain knowledge and experience to evaluate and mitigate risk to the control system. The NIST report also recommends that the cyber security team must consult with the control system vendor and/or integrator.

The NOU 2015:13 Report [7] recommends that industry associations should organize courses in information and communications systems safety and security for the Norwegian electric power supply industry. The report also recommends an increased focus on safety and security training exercises for industrial control systems that involve the participation of suppliers.

The Norwegian Oil and Gas Association (OLF) has developed safety and security guidelines based on ISO/IEC 27002 for integrating industrial control and information/communications systems. The guideline OLF104, Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems has been developed by information technology and control systems professionals from research institutions, government, consultants, major operators and suppliers [12]. As mentioned above, the Norwegian Water Resources and Energy Directorate's contingency planning regulations and guideline are comprehensive and devote considerable coverage to industrial control systems security. However, the Norwegian petroleum industry and electric power supply sector could benefit from more cooperation and improved sharing of the responsibility for information and control systems safety and security between industrial control system owners and suppliers.

According to CPNI's good practice guide for managing third-party risks [5], awareness and visibility of the third-party risks are the keys to enabling an organization to manage its risk. The recognition of potential security gaps enables an organization to seek appropriate engagement with suppliers/vendors and support organizations to mitigate the identified risks. To manage the risks from third parties, the CPNI guide recommends several good practice principles. Organizations can develop in-depth knowledge of product security func-

tions and can influence the security functionality of existing and new products by engaging in productive dialogs and developing relationships with industrial control system vendors.

CPNI [5] also recommends the creation of the correct contractual framework, which is an essential part of managing vendor risk. System owners should ensure that security clauses are detailed in all procurement contracts prior to their signing and that the appropriate clauses cascade down to sub-contractors. System owners should also engage with vendors on an ongoing basis and request vendors to provide security guidance for their current industrial control systems and roadmaps for future system development. System owners should attempt to influence their vendors' security cultures so that they meet or exceed their requirements. Moreover, they should ensure that appropriate levels of security awareness and training are in place, and they should work towards understanding the value chain and the dependencies that exist within it.

KraftCERT, a computer emergency response team (CERT) for the electrical power sector, was established in Norway in 2014. KraftCERT assists the power industry in preventing and handling security incidents. Counseling from KraftCERT could help power network companies make better safety and security demands and sign safety and security agreements with their suppliers, and help increase the cooperation between system owners and suppliers.

Norwegian industrial control system owners should also attempt to implement culture changes in their own organizations that place security priorities on par with operational priorities. According to Johnsen [12], key stakeholders who can influence the physical and organizational environments, social norms and cultural factors should be involved in exploring the safety and security of industrial control systems; these include regulators, industry associations, operators and suppliers/vendors. According to Jaatun et al. [11], different risk perceptions and situational understanding are best approached using discourse-based strategies, where the involved actors meet and discuss different viewpoints with the goal of arriving at a common understanding. Suppliers should also be involved in the risk and vulnerability analysis processes of power network companies. Finally, it is important that senior executives of power network companies are convinced about the benefits of information and communications safety and security management, and are willing to allocate the necessary human and financial resources.

6. Conclusions

This chapter has highlighted the important issue of responsibility for information and communications systems safety and security for industrial control systems and the challenges involved in dividing the responsibility between industrial control system owners and suppliers in the Norwegian electric power supply industry.

In Norway, system owners (power network companies in the electric power supply industry) are responsible for the safety and security of their own integrated information/communications systems and industrial control systems.

Suppliers of control systems are responsible for the safety and security of their products. However, the results of this study suggest that system owners do not always have enough knowledge about the threats and risks, and how to secure their systems. Many power network companies perceive the risk of attacks on or malfunctions in their integrated systems as low. They also appear to place considerable trust in the expertise of their suppliers, believing that the suppliers will create safe solutions and taking for granted that technological applications can address safety and security problems.

A key concern is that the observation studies indicate that Norwegian power network companies and their suppliers have contributed to the creation of a culture with a lack of focus on information and communications systems safety and security. Increased use of standards and guidelines can improve the cooperation between system owners and suppliers, and increase the focus on safety and security of industrial control systems in the Norwegian electric power supply sector. Industrial control system owners should also implement changes to the culture in their organizations and should influence the safety and security culture of their suppliers. Finally, power network companies need to place information and communications systems safety and security priorities on par with operational priorities, and they should become more vocal in demanding secure products from their suppliers.

References

[1] E. Adler and R. Clark, *An Invitation to Social Research – How It's Done*, Cengage Learning, Stamford, Connecticut, 2015.

[2] A. Sarri and K. Moulinos, Stocktaking, Analysis and Recommendations on the Protection of CIIs, European Union Agency for Network and Information Security, Heraklion, Greece, 2016.

[3] S. Antonsen, P. Almklov, J. Fenstad and A. Nybo, Reliability consequences of liberalization in the electricity sector: Existing research and remaining questions, *Journal of Contingencies and Crisis Management*, vol. 18(4), pp. 208–219, 2010.

[4] E. Byres, Revealing network threats, fears – How to use ANSI/ISA-99 standards to improve control system security, *InTech Magazine*, pp. 26–31, January/February 2011.

[5] Centre for the Protection of National Infrastructure, Good Practice Guide, Process Control and SCADA Security, Guide 5: Manage Third Party Risk, London, United Kingdom, 2015.

[6] Centre for the Protection of National Infrastructure, Security for Industrial Control Systems, Framework Overview, A Good Practice Guide, London, United Kingdom, 2015.

[7] Committee of Digital Vulnerabilities in Society, Digital Vulnerability – Secure Society: Protecting People and Society in a Digitalized World (in Norwegian), Official Norwegian Report (NOU 2015:13) to the Ministry of Justice and Public Security, Oslo, Norway, 2015.

[8] European Reference Network for Critical Infrastructure Protection, The ERNCIP Project Platform, Joint Research Centre, Ispra, Italy (erncip-project.jrc.ec.europa.eu), 2016.

[9] E. Hollnagel, J. Paries, D. Woods and J. Wreathhall (Eds.), *Resilience Engineering in Practice: A Guidebook*, Ashgate Publishing, Burlington, Vermont, 2011.

[10] International Society of Automation, ISA99: Industrial Automation and Control Systems Security, Research Triangle Park, North Carolina, 2015.

[11] M. Jaatun, E. Albrechtsen, M. Line, I. Tondel and O. Longva, A framework for incident response management in the petroleum industry, *International Journal of Infrastructure Protection*, vol. 2(1-2), pp. 26–37, 2009.

[12] S. Johnsen, Resilience at interfaces – Improvement of safety and security in distributed control systems by web of influence, *Information Management and Computer Security*, vol. 20(2), pp. 71–87, 2012.

[13] W. Knowles, D. Prince, D. Hutchison, J. Disso and K. Jones, A survey of cyber security management in industrial control systems, *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52–80, 2015.

[14] H. Leith and J. Piper, Identification and application of security measures for petrochemical industrial control systems, *Journal of Loss Prevention in the Process Industries*, vol. 26(6), pp. 982–993, 2013.

[15] M. Line and I. Tondel, Information and communications technology: Enabling and challenging critical infrastructure, in *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis*, P. Hokstad, I. Utne and J. Vatn (Eds.), Springer, London, United Kingdom, pp. 147–160, 2012.

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

[17] Norwegian Business and Industry Security Council, Norwegian Computer Crime and Security Survey – Information Security, Privacy and Data Crime (in Norwegian), Oslo, Norway, 2014.

[18] Norwegian Ministry of Justice and Public Security, National Cyber Security Strategy for Norway, Oslo, Norway (www.regjeringen.no/en/dokumenter/cyber-security-strategy-for-norway-/id729821), 2012.

[19] Norwegian Ministry of Petroleum and Energy, Facts 2013: Energy and Water Resources in Norway, Oslo, Norway (www.regjeringen.no/globalassets/upload/oed/faktaheftet/facts_energy_water.pdf), 2013.

[20] Norwegian Water Resources and Energy Directorate, Guideline for Contingency Planning Regulations, Guideline No. 1-2013 (in Norwegian), Oslo, Norway, 2013.

[21] E. Perez, U.S. investigators find proof of cyberattack on Ukraine power grid, *CNN*, February 3, 2016.

[22] R. Piggin, Are industrial control systems ready for the cloud? *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 38–40, 2015.

[23] R. Skotnes, 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(2), pp. 119–134, 2012.

[24] R. Skotnes, Risk perception regarding the safety and security of ICT systems in electric power supply network companies, *Safety Science Monitor*, vol. 19(1), article no. 4, 2015.

[25] R. Skotnes and O. Engen, Attitudes toward risk regulation – Prescriptive or functional regulation? *Safety Science*, vol. 77, pp. 10–18, 2015.

[26] A. Stefanini, G. Doorman and N. Hadjsaid, ICT vulnerabilities of power systems: Towards a roadmap for future research, in *Critical Information Infrastructures Security*, J. Lopez and B. Hammerli (Eds.), Springer, Berlin Heidelberg, Germany, pp. 13–24, 2008.

[27] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[28] J. Vatn, P. Hokstad and I. Utne, Defining concepts and categorizing interdependencies, in *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis*, P. Hokstad, I. Utne and J. Vatn (Eds.), Springer, London, United Kingdom, pp. 13–22, 2012.