Application of Cyber Resilience Review to an Electricity Company

Jouni Pöyhönen[1], Viivi Nuojua[1], Martti Lehto[1] and Jyri Rajamäki[1,2]
[1]University of Jyväskylä, Jyväskylä, Finland
[2]Laurea University of Applied Sciences, Espoo, Finland
jouni.a.poyhonen@jyu.fi
viivi.nuojua@jyu.fi
martti.j.lehto@jyu.fi
jyri.rajamaki@laurea.fi

Abstract: The functioning of a modern society is based on the cooperation of several critical infrastructures, whose joint efficiency depends increasingly on a reliable national electric power system. Reliability is based on the functional data transmission networks of the organizations belonging to the electric power system. Furthermore, reliability is linked to the confidentiality, integrity and availability of system data in the operational environment, whose cyber security risks are continuously augmented by the threatening scenarios of the digital world. In Finland, the electricity generation is in various ways distributed, which contributes to the reliability of the electric power system. There are about 120 electricity generation companies and about 400 power plants nationally, in which the electricity is produced using various production methods. The control of electric power system's operational processes is highly automated and networked. The major contribution of the paper is to apply the cyber resilience review to a single electricity company. The basis is in SWOT analysis, which is used for analyzing and that way for bettering the cyber security level of an organization. However, there is not such as perfect security. Security is based on trust, which can be developed with the help of preparedness planning. Resilience review can be seen as preparedness planning that also enables contingency planning. Resilience metrics framework proposed by Linkov et al. is utilized by applying the resilience measures to the organization's operational processes. In addition, open source intelligence and organization's operating networks are used for collecting significant security information and that way for updating the preparedness plan, i.e. resilience plan. In order to put the resilience plan into practice, the leadership of an organization must regard resilience measures related to cyber security as a strategic goal and communicate to their staff the importance of contingency planning in achieving the goals. As a result, the cyber security management of an electricity company is improved.

Keywords: critical infrastructure, cyber security management, electricity company, resilience, trust

1. Introduction

Electricity is produced at Finnish power plants in various ways, by using several energy sources and production methods. The major sources of energy include nuclear power, hydropower, coal, natural gas, wood fuels and peat. In addition to the sources of energy, production can be classified according to the production method. In Finland there are about 120 enterprises that produce electricity as well as around 400 power plants, over half of them hydroelectric power plants. Nearly a third of electricity is produced in connection with heat production. Compared with many other European countries, Finland's electricity production is distributed. A diverse and distributed electricity production structure increases the security of the national energy supply (Finnish Energy, 2015).

The global threats within the cyber environment have remained at a high level over the past few years, as stated in the annual international business world surveys by the World Economic Forum. Cyber threats are seen to be among the major global threats based on their likelihood and impact (World Economic Forum, 2018).

The electric power system with all its components belongs to critical national infrastructure: it is vital for the operations of a country, and its outage or destruction would weaken national security, economy, public health and safety as well as make the operations of state administration less effective. The criticality of a power system is expressed clearly in the seminar presentation "The power system as a basis for a functioning society" (in Finnish: "Sähköjärjestelmä yhteiskunnan toimivuuden perustana") given by the former chief executive officer of the National Emergency Supply Agency. Table 1 is an extract from the presentation. It describes the effects of power failure on the operations of society as a function of the duration of the failure. Endangered cyber security has been regarded as one of the most significant threats to the functioning of energy supply and energy networks (Kananen, 2013).

A diversified and distributed power production structure increases the national security of power supply. Considering cyber security in the different parts of the infrastructure further enhances trust in the services of

our society. The recent experiences of the disturbances in cyber operational environment (ICS-CERT, 2016) have showed that it is difficult to achieve perfect protection. Thus, the enterprises have acknowledged and accepted the fact that there will always be disturbances, and rather concentrate on preparing for them. The term resilience affiliates with tolerating disturbances. Generally, it means flexibility, and the ability to survive and adapt in unpredictable and surprisingly developing situations. According to Hilton, Wright and Kiparoglou (2012) there is not one universal definition for the word resilience. However, they approach the definition problem via systems thinking: resilience can be seen as an enterprise's capacity and capability to achieve its purposes in both predictable and unpredictable situations or under continuous stress.

According to Willis and Loa (2015) there are plenty of published reports on the resilience metrics applied to energy industry. They divide the reviewed metrics into five levels. The input level metrics depict the amount of the produced, transmitted or stored energy, or the number of people, facilities or equipment supporting the first-mentioned activities. The capacity level metrics depict the systems, policies and organizations supporting the energy capabilities. The capability level metrics depict the capability of energy systems for providing sources or factors. The performance level metrics depict the quality, amount and efficiency of the services provided by energy systems. Lastly, the outcome level metrics depict the influence of energy on health, safety and economy, i.e. societal welfare.

The EECSP-Expert Group (2017) emphasizes the following two high-level objectives as the goal of stakeholders in the energy sector: 1) The security of energy systems providing essential services to the European society, and 2) the data protection in the energy systems and the data privacy of the European citizen. In May 2018, the General Data Protection Regulation (GDPR) approved by the European Commission was entered into force, and the Directive on security of Network and Information Systems (NIS Directive) adopted by the European Parliament was supposed to be integrated in national laws. The purpose of the aforementioned GDPR and NIS directive is to better the trustworthiness of the online environment and that way the functioning of the EU Digital Single Market.

National Institute of Standards and Technology (NIST, 2018) introduces a cyber security framework that helps internal and external stakeholders to understand, manage and express cyber security risks in co-operation. It can be utilized for identifying and prioritizing actions in order to reduce cyber security risk. In addition, it can be used for aligning policy, business and technological approaches in order to manage that risk. The framework can be applied to the entire organization or to some specific critical service. So-called Framework Core guides in achieving specific cyber security outcomes and that way helps in managing cyber security risk.

Table 1: The consequences of power failure (Kananen, 2013)

Interruption time	Consequences
1 second	Sensitive industrial processes may stop. Data in information systems may be lost.
1 minute	Some industry and hospital processes will stop.
15 minutes	Shops will be closed. The failure may harm people's daily activities and cause traffic delays.
2–3 hours	Industrial processes may undergo significant damage. Mobile phone networks will face problems. Domestic animal production will be disturbed.
12–24 hours	Water supply to homes and offices will stop. Buildings will start to become cold in the winter. Frozen goods will begin to melt.
Several days	The operations of society will be seriously harmed. Industry and services will not function. Workplaces and schools will be closed. Buildings will suffer from frost damage.

This paper presents a process created with the help of aforementioned cyber security framework, and thus stands out from the previous papers. It pays attention to the cyber security of an energy company as part of the organization's overall resilience planning and that way continuity management.

Preparedness planning enables the proactive contingency planning for the operation's continuity management and that way building of trust in the management of cyber security related problematic situations, i.e. the promotion of cyber resilience. It includes preliminary planning of contingency, the plan for encountering disturbance situations and for how to recover and learn from those. In this research, the following two fundamental questions of resilience review have been explored:

- Is it possible to create such procedures for resilience review that help to do the planning as a continuous process for supporting the management?

- What are the most essential matters taken into consideration when planning the resilience of a Finnish electricity generation company?

A procedure suitable to answer our first research question can be found from the earlier national research related to the situational awareness of Finland's cyber security (Pöyhönen and Lehto, 2017). The basis is in a certain present state analysis, SWOT analysis, which is used for analyzing and that way for bettering the cyber security level of an organization. A case study into a typical regionally operating electricity generation company is chosen as a research strategy. It helps to figure out the factors related to the cyber management of a single electricity company, and how these factors should be taken into account in the structures of the company's operational processes. The focus of the research is in the main process of an electricity company, which consists of the raw material supplies, i.e. supplier network, production process and distribution network (= customers). A resilience metrics framework proposed by Linkov et al. (2013a) is utilized by applying the resilience measures to the organization's operational processes. In addition, an OSINT utilizing framework introduced by Lee and Shon (2016) is used for collecting significant security information, and that way for improving the organization's preparedness planning.

The rest of the paper is organized as follows. Section 2 describes electricity company's cyber-physical operational environment and how its situational awareness can be analyzed and improved. Section 3 provides tools for resilience planning. Section 4 introduces our proposed model for how to add a company's resilience. Section 5 concludes the paper.

2. Electricity company's cyber-physical operational environment and its situational awareness

2.1 The structure of an electricity company's cyber-physical operational environment

The highest levels of IT system hierarchy include the general information systems of administration and the enterprise resource planning (ERP) system. The top level of a typical ERP system includes overall process management by, for example, guiding the production volume. It also covers the restocking of raw materials, storing, distribution, payment traffic and human resources. If needed, between ERP software and control rooms there may be a manufacturing execution system (MES), which makes it possible to transfer the information obtained from the control room to the ERP system.

The industrial automation systems of production within an electricity company comprise their own hierarchy levels. Topmost of them is the control room, from which the operation of the entire process is presented to the supervisors in graphic form. Based on the information, process alarms are handled and the operation of the process is monitored and controlled. The next level consists of process stations, which house devices for process control, measuring and regulation. The same level also includes the actions taken to monitor faults and interferences in devices. The lowest level comprises the field equipment used to control and monitor process actuators and to gather measurement data.

Cyber-physical systems are software platforms that monitor, control and protect physical operational processes (Sadeghi, Wachsmann and Waidner, 2015). Their structure can be described as a five-layered structural model where each of the aforementioned systems and their parts can be placed. The structures are (Lehto, 2015):

- Cognitive domain
- *humane problem solution and interpretation environment*
- *the understanding and interpretation of the information's meaning*
- Service domain
- public and commercial network services
- operational and communicational services
- Semantic domain
- *information and data content controlled by the user*
- *the direction of the system operations controlled by the user*
- Syntactic domain

- *the control and management software of the system*
- *network protocols, error handling, handshakes*
- Physical domain
- *network devices, switches, routers*
- *wired and wireless communications*

Related to the research target the following cyber-physical systems were recognized:

- Supplier network (company level IT)
- Production process (ICS operator)
- Distribution network (company level IT / ICS operator)
- Real estate automation (ICS operator)
- Security system (company level IT / ICS operator)

These systems correlate in many ways, and via their data transmission networks they are also correlated to their operational environment.

2.2 The situational awareness of an electricity company's cyber security

The aforementioned IT and industrial automation systems are part of the common cyber world, in which the primary risks are related to the loss of money, sensitive information and reputation as well as to business hindrance. Security solutions are hereby the key elements in risk management. The vulnerabilities behind the risks can be analyzed as insufficient technology in relation to attack technology, insufficient staff competence or inappropriate working methods, deficiencies in the management of organizations, and lacks in the operating processes or their technologies. The most common motives of attackers are related to the aim of causing destructive effects on processes, making inquiries about process vulnerabilities, and anarchism or egoism. These attacks can even be carried out by state-level actors, but perhaps most commonly by organized activists, hackers or individuals acting independently (Lehto, 2015).

Harmful measures to the systems of an electricity company can be implemented by foisting mal- and spyware into the systems utilizing the staff; or they can include intruding or network attacks via wireless connections or the Internet. The intruders' goals may be related to the prevention of network services, the complete paralysis of operations, data theft or distortion, and the use of spyware. Components pre-infected with so-called backdoors, or the programming of components intentionally for the attacker's purposes is also increasingly common in today's cyber world (Lehto, 2015).

In the USA, the security threats to the electric power system concern power plant logistics. They involve interfering and harming raw material supply routes, doing physical damage to transmission and distribution networks as well as to the transformer and switching substations between them, or performing cyberattacks to the control and regulation systems of the power grid (Lewis, 2015).

The significance of the systems' usability is essential when considering the business result formation and the operation's reliability. In addition, the reliability and content integrity of the information included and used in the processes are essential objectives. As a result, the overall trust should be aimed to build. It is based on the targeted organization's realistic understanding of its own capabilities to manage reliably the challenges related to operating in cyber world. One solution for building up a company-specific understanding of the situational awareness is SWOT analysis (Pöyhönen and Lehto, 2017).

The term SWOT is an acronym of the words Strengths, Weaknesses, Opportunities and Threats. SWOT analysis is an important tool for analyzing an organization's performance and operating environment as a whole. The interviewing themes presented in Table 2 encompass perspectives linked to the cyber structure of a typical electricity company, which have been derived from the logistics framework of an electricity company and common IT and industrial automation systems.

In this study, a company's cyber security was analyzed from the perspectives of organizational strategy, operative measures, technological-tactical-level solutions and ability factors, with the company's cyber structure

and operation considered as part of a networked society. Taking into account these perspectives, the cyber security strengths and weaknesses can be analyzed by evaluating their mutual relationship. The most central factor in analyzing opportunities and threats is the change in the operating environment of a company – in this study, the cyber environment. The analysis of opportunities is then connected to the company's possibility to utilize measures supporting change in order to improve its opportunities to function. The assessment of threats comprises operating environment analyses and threat analyses, based on which measures can be taken to reduce threats.

3. Electricity company's resilience planning

3.1 The adaptation of the resilience metrics framework to the planning

The trust on organizations' operation and its continuous maintenance with efficient actions is an essential matter when thinking of the factors influencing cyber security. The security is based on trust. If there is no trust, there is no security and vice versa. It is good to acknowledge that perfect security cannot be achieved, either when operating in cyber world, which is dynamic and difficultly foreseeable operational environment. Thus, it becomes even more important to understand how significant our trust in cyber world and its security is. The significance of the operations building up trust is emphasized. When building the operations in cyber world on a solid base, we are able to utilize its diverse possibilities (Limnéll, Majewski and Salminen, 2014).

Trust can be developed by utilizing preparedness planning. Linkov et al. (2013a) introduce a resilience matrix framework (later: "Linkov model") that can be used for this planning. It combines the four stages of a system 1) plan/prepare, 2) absorb, 3) recover and 4) adapt with the four domains of a system 1) physical, 2) information, 3) cognitive and 4) social. Later on Linkov et al. (2013b) apply their model further to cyber systems. Their purpose is to develop efficient metrics to measure the resilience of cyber systems (Linkov et al., 2013a; Linkov et al., 2013b).

In case of cyber systems, the cells of the resilience matrix can be interpreted as follows: How capable the system is to prepare/absorb/recover/adapt in case of a cyber disturbance executed within the physical/information/cognitive/social domain? Adding one metric to a certain domain often requires adding metrics to other domains too. Resilience metrics are used for recognizing and prioritizing the needs, for tracking progression and for sharing resources. Thus, they constitute an essential part of planning and decision-making (Linkov et al., 2013b).

3.2 The maintenance of the planning with the help of OSINT

Open Source Intelligence (OSINT) can be used for the collection of significant security information. This kind of open or i.e. public references consist not only of newspapers and magazines representing traditional media but also of the Internet representing digital media (Lee and Shon, 2016).

Table 2: The SWOT analysis interview themes (Pöyhönen and Lehto, 2017)

Strengths and weaknesses	Opportunities and threats
management	acquisition of advanced technology
staff competence	new cooperation partners
cyber security products and services	new opportunities for development
situational awareness	analysing the operating environment
stakeholder approach	analysing cyber threats
ensuring continuity of operation	analysing the operating network
expert services	

Lee and Shon (2016) introduce an OSINT utilizing framework for examining the cyber threats of critical infrastructure. Their solution helps to improve the security level of critical infrastructure by analyzing previously unnoticed cyber threats, and that way making it possible to prevent zero-day vulnerabilities too. OSINT adapts particularly well to the critical infrastructure data network because of the nature of its communication models and environments. Lee and Shon's solution can be used for completing the signature-based threat detection methods and for anomaly detection (Lee and Shon, 2016).

According to Lee and Shon (2016), the OSINT utilizing intelligence has to fulfil two conditions: the content and reference of the analyzed information have to be confirmed, and the intelligence has to be useful and

meaningful in relation to its use. When making the OSINT plan, the target system is chosen first and then, the method and timetable for collecting the public information is decided. In the preparation phase, the internal information related to the target under examination is verified and based on that the initial intelligence database is created. Finally, the OSINT data collection tools are used for collecting the information about the target under examination. By utilizing the database created in the initial intelligence, the reliability of the collected information is verified, and at the same time, the initial intelligence information is updated (Lee and Shon, 2016).

3.3 The maintenance of the planning with the help of operating networks

The strategy-level strengths of electricity companies consist of the organization leaders who consider cyber security issues as a strategic goal, and a published cyber security policy and risk-based management as part of overall security and business activity. Nationwide clean networks are one of the main strengths for the electric power systems that provide a foundation for the entire critical infrastructure and its services. From an operational point of view, the strength of the stakeholder approach is based on the use of the best partners in outsourcing, clustering, public-private partnerships (PPP) and international cooperation. The strength of companies' situational awareness is the possibility to learn about threats often directly from the operating network or partners, and the use of announcements of the National Cyber Security Centre Finland. Competitive advantages include PPP activity and the possibility to create consistent situational awareness by using branch collaboration (Pöyhönen and Lehto, 2017).

4. Resilience adding operations

4.1 Resilience development as a continuous process

Establishing measures that increase cyber security and trust in a company is primarily the responsibility of corporate leadership. Integrating the necessary measures with the idea of ensured business activities increases their significance and benefits through better processes for the entire organization, interest groups and society. If security is not considered, risk analysis reveals potential damage as well as its costs and social consequences. The leadership's views and requirements brought out in the analysis play a central role in developing the security planning of the operating process. The costs and other resources allocated to the activities are simultaneously specified (Stouffer, Falco and Scarfone, 2011).

Systematical and good quality management of an organization is enabled with a proper management system. It pays attention to the customers, the significance of the staff, the efficiency and control of its operational processes, the continuous development of its operation and the interest group communication. The management system can also be used for controlling the operational processes of the cyber operational environment.

As a solution for research question 1, the resilience management process presented in Figure 1 was developed. It can be linked to the management system of an organization. When creating the resilience management process, we utilized the following: the definition of the target organization's cyber-physical systems, SWOT analysis, Linkov model, OSINT and the electricity companies' strength in utilizing its own operating networks for data collection.

After defining the target organization, the cyber-physical systems related to its operational processes are recognized and placed in the systems' cyber structure described in section 2.1. After that, SWOT analysis can be applied to the organization as a theme interview by taking into consideration the cyber structure. This enables the drafting of the resilience basic plan during the normal conditions (Linkov model stages 1–3) for all the domains (physical, information, cognitive and social). The Linkov model stage 4 includes all the aforementioned domains too but their final content must be defined based on the aftermath of the possible disturbance situation. The purpose is that the organization learns from the disturbance situations as efficiently as possible. The operations of the organization are developed by repeating SWOT analysis. As a result, the plans are updated for each of the Linkov model stage's part as a repairing operation. The preparedness planning of the normal conditions (stage 1) should continuously be maintained with the help of OSINT model and by utilizing the company's own data collection channels, such as operating networks, in the update process.

It should be noted that the resilience process can be utilized for the impact evaluation of the system correlations when revising the cyber-physical systems. The process model in Figure 1 is recommended to be included as part

of the organization's management system in order to accomplish practical operations. The implementation process of the resilience operations serves all the decision-making levels of an organization. In SWOT analysis, the analysis of the organization's performance and its operational environment on the whole supports especially the strategic planning. It also produces information to other decision-making levels in learning and problem recognition, evaluation and development of operational processes. Linkov model serves the planning and maintenance of the organization's operational continuity management, which supports the operation of the operational and technological-tactical levels.

4.2 The most essential resilience adding operations

The basis for trust adding operations is the envisioning of the company's operations in order to achieve the goals. It is made possible with the strategy definition derived from the vision. The electricity company's operational business processes include systems such as fuel logistics and input system, production system and its support processes, and electricity distribution operation. Because all the aforementioned components are needed in the operation of an electricity company, their mutual dependence, and the control and supervision of functionality solve the succeeding of the whole operation. In order to achieve a successful cyber security management, the different operations should be considered as equal. Linkov model and its different stages suit especially for the operational and technical-tactical level preparedness planning, and that way for ensuring the continuity of operation. Considering the structure of the previously described cyber-physical systems, it is possible to find those targets from the operation of an electricity company that are in a central position in preparedness planning. The company-specific content of the operations has to be based on the present state analysis carried out before using Linkov model, and on the situational awareness got from that in the form of target organization's strengths, weaknesses, possibilities, threats and their mutual relations. SWOT analysis described in section 2.2 gives a good overview of the cyber security of a critical infrastructure target against the managemental and national security requirements. Based on the analysis, the related needs of each organization can be planted on the planning stages of Linkov model (see Table 3).

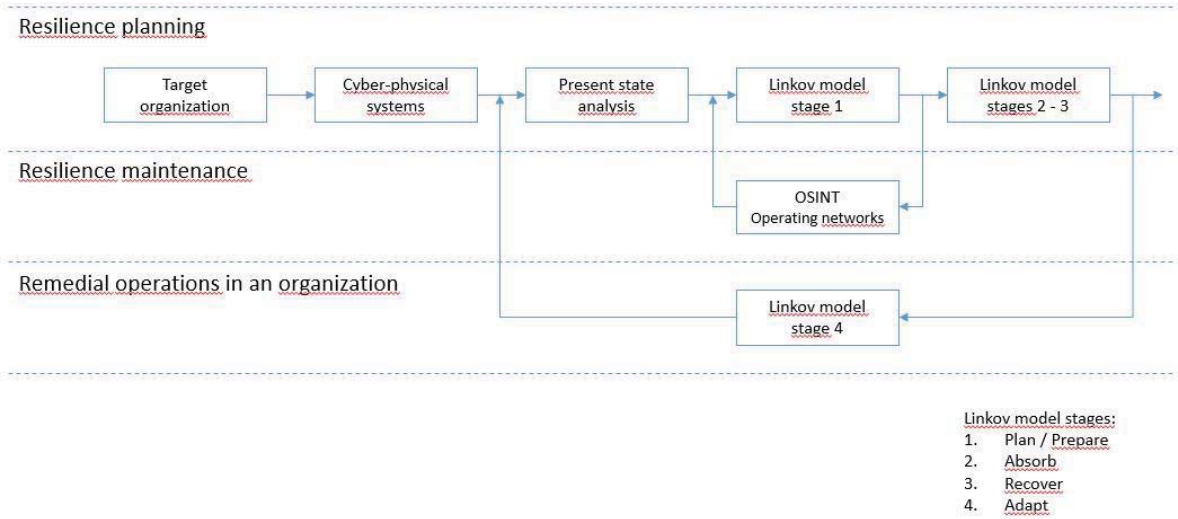

Figure 1: The implementation process of the resilience operations

Table 3: Research results planted on the Linkov model

	Plan/Prepare	Absorb	Recover	Adapt
Physical	technical situational awareness segmentation alternative resources	recognition of disturbances, their scope and impacts protection of sensitive information deployment of alternative resources isolation of disturbance	maintenance of situational awareness ramp-up testing	updates

	Plan/Prepare	Absorb	Recover	Adapt
Information	classification and prioritization of critical systems business impacts preparation of sensitive information protection communication plans	documentation informing of authorities and stakeholders	documentation informing of the press	aggregation of documents
Cognitive	perception of situational awareness scenarios and models situational management resourcing training and benchmarking feedback system	analysis of situational awareness additional resources prioritization censor information	allocation of expertise collection of data and log information	log analysis impact analysis situation analysis feedback analysis system updates continuous improvement
Social	naming of stakeholders' contact persons training for exceptional situations	informing about operations	informing about operations	staff training informing about development operations update of stakeholder information

The following operations of the planning and absorb stages within the physical domain of Linkov model were recognized: taking care of the functionality, supervision and control of the technology, planning of the system isolation and needed operational segments, and planning of the alternative networks and routes. In case of a disturbance situation, firstly, the situational awareness of the incidence, its nature, distribution and scope are clarified, as well as its impact. After that, the plans are put to use for their needed parts. In the recovery stage, the cleanliness and functionality of the systems is ensured for all of their parts. Then, the comprehensive ramp-up of the machines is guided through. The adaptation stage is determined by the experiences got from the incident, but at least the technical protection operations must be considered carefully.

The documentation planning is emphasized in the operations of information domain, by paying attention to the situation-specific documentation itself, and the critical operations and related requirements has to be documented already in the planning stage. The aforementioned documentation both serves the operation in a disturbance situation and enables the information documentation during the disturbance situation and in a recovery stage, so that the utilization of situation-specific experiences and learning in the adaptation stage is made possible. The informing of essential stakeholders and different authorities must also be included in each stage.

In our case study, the plan of cognitive domain grew the most of all domains. Thus, it can be seen very significant in both management, in building the situational awareness, in continuity management, in prioritizing the operations, and in managing and controlling different resources, including services. All these operations play a decisive role in a disturbance situation, in the recovery stage and in the adaptation stage when utilizing the knowledge gained from the previous stages.

The planning stage of the social domain consists of more specific communication plans than in the information domain, including the named contact persons, and both internal and external interest groups. The widescale situation-specific informing in the different stages results from the planning of the social domain. In addition, the planning of the social domain includes the whole staff training in managing all the different stages.

5. Conclusions

The national electric power system and its electricity generation is part of the national critical infrastructure. The operation of a modern society is based on a reliable national electric power system. To ensure the usability and reliability of the electricity companies' operational processes in all the operational environments is an essential part of the critical infrastructure's performance. Therefore, the electricity companies' operations to manage the cyber security of their processes form an important part in ensuring the reliability of electricity generation.

The most significant cyber environment related risks of the electricity company's operational processes require building up and maintaining the trust in all the business levels. The comprehensive cyber trust adding operations of the company together with the development of the cyber operational abilities improve its competitiveness too.

In the case study part of this research the process flowchart for the electricity company's resilience planning was developed, and a Linkov model compatible preparedness planning was made in a table format and on the title level to better the resiliency of the target organization. The previous research results of SWOT analysis have been utilized in this paper as described earlier, and the analysis has been targeted at the company's operational networks and its cyber-physical systems' structures. The Linkov model compatible tables were compiled by utilizing the SWOT analysis themes and by keeping in mind the structure of the target's cyber-physical systems. From the results an analogy between the structures of Linkov model and Lehto's cyber-physical systems can be drawn. Especially the planning of Linkov model's physical and cognitive domains benefits from the detailed knowledge of the system structure. The planning of the information domain is targeted also at the cyber-physical system covering all of its levels, and in addition, it is targeted at all the organization's interest groups. The social planning domain serves the consideration of all the interest groups. The conclusions from the usage of the models are the following:

- Linkov model expands the preparedness planning outside the cyber structure.
- The cyber structure of systems enables the detailed targeting of the planning at all the domains of cyber-physical systems.
- By combining the models, it is possible to get a comprehensive planning environment for the resilience review of the cyber-physical systems and for securing the continuity.

The preparation for cyber threats and a concrete preparedness planning form the basis for the organization's proactive preparation in its cyber operational environment, when it comes to the electricity company's cyber security management and to the development of trust in the operation. These cyber resilience adding plans and operations are recommended to be included as a fixed part of the company's overall security, when they support the management of an organization in all of its levels.

Since the energy companies are essential service providers for the society, the introduced process for developing the organization's resilience answers to the basic requirement of NIS Directive (The European Parliament and the Council of the European Union, 2016): "Operators of essential services and digital service providers should ensure the security of the network and information systems which they use".

Investigations have revealed that the extensive power failure in Ukraine on 23 December 2015 was caused by a coordinated cyberattack by an external party to the control systems and data warehouses of three enterprises in charge of power distribution. One potential target of the attack is suspected to be the industrial automation system, which the hackers may have managed to enter via a remote access service. When preparing for cyberattacks against industrial automation systems and trying to improve their resistance, organizations are recommended, in the first place, to introduce the best practices of cyber security management (ICS-CERT, 2016).

The generalization of the research results can be examined by utilizing the process flowchart of the resilience planning. It enables the repeatability of this research and the generalization of the material, such that the procedure can be applied to other energy companies too. In addition, a single case of the research target can be handled thoroughly enough by combining the domains of Linkov model, and the structure model of the cyber-physical systems presented by Lehto.

The further research needs are suggested to be targeted at developing the resilience of other critical infrastructure organizations.

References

EECSP-Expert Group (2017). Cyber Security in the Energy Sector. EECSP Report.

The European Parliament and the Council of the European Union (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council. Official Journal of the European Union.

Finnish Energy (2015). Electricity generation. [online] Available at: https://energia.fi/en/energy_sector_in_finland/energy_production/electricity_generation [Accessed 16 Nov. 2017].

Hilton, J., Wright, C. and Kiparoglou, V. (2012). Building resilience into systems. 2012 IEEE International Systems Conference SysCon 2012.

ICS-CERT (2016). Cyber-Attack Against Ukrainian Critical Infrastructure. [online] Available at : https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed 16 Nov. 2017].

Kananen, I. (2013). Sähköjärjestelmä yhteiskunnan toimivuuden perustana. National Emergency Supply Agency.

Lee S. and Shon T. (2016). Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures. 2016 Future Technologies Conference (FTC).

Lehto, M. (2015). Phenomena in the Cyber World. Cyber Security: Analytics, Technology and Automation. Springer.

Lewis, T. (2015). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. 2nd Edition. Wiley.

Limnéll, J., Majewski, K. and Salminen, M. (2014). Kyberturvallisuus. Jyväskylä: Docendo.

Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. and Seager, T. (2013a). Measurable Resilience for Actionable Policy. Environmental Science & Technology.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen J. and Kott, A. (2013b). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp. 471-476.

National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.

Pöyhönen, J. and Lehto, M. (2017). Cyber security creation as part of the management of an energy company. Proceedings of the 16th European Conference on Cyber Warfare and Security [also] ECCWS2017, Dublin, Ireland, June 2017. Academic Conferences International.

Sadeghi, A., Wachsmann, C., and Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. Proceedings of the 52nd Annual Design Automation Conference on - DAC '15.

Stouffer, K., Falco, J. and Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82.

Willis, H. H. and Loa, K. (2015). Measuring the Resilience of Energy Distribution Systems. [online] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR883/RAND_RR883.pdf [Accessed 27 May 2018].

World Economic Forum (2018). The Global Risks Landscape 2018. [online] Available at: http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape [Accessed 23 Jan. 2018].