Chapter 9
Cyber Security of an Electric Power System in Critical Infrastructure

Jouni Pöyhönen

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 functional data transmission networks in the organizations that belong to the power system. This chapter focuses on the procedures applied to cyber security management in the processes of an electricity organization, whereby different standards will also be utilized. The major contributions of the chapter are that it integrates cyber security management into the process structures of individual electricity production organization and that it utilizes the PDCA (Plan, Do, Check, Act) method in developing an organization's cyber security management practices. In order to put the measures into practice, the leadership of an electricity organization must regard trust-enhancing measures related to cyber security as a strategic goal, maintain efficient processes and communicate their implementation with a policy that supports the strategy.

Keywords Critical infrastructure · Power system · Electricity organization · Cyber security management · Trust

9.1 Introduction

The critical infrastructure consists several systems and services that are essential for national society. The functioning of a modern society is based on the cooperation of several operators, whose joint efficiency depends increasingly on a reliable national electric power system. Crucial in the cyber environment are also functional data transmission networks and the usability, reliability and integrity of systems and services in the operating environment, whose cyber security risks are continuously augmented by threatening scenarios of the digital world.

J. Pöyhönen (✉)
Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland
e-mail: jouni.a.poyhonen@jyu.fi

M. Lehto and P. Neittaanmäki (eds.), *Cyber Security*, Computational Methods in Applied Sciences 56, https://doi.org/10.1007/978-3-030-91293-2_9

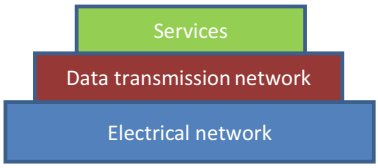

Fig. 9.1 Simplified composition of critical infrastructure

Security of supply means the ability to uphold society's vital functions in state of emergency and, in that sense, it is relevant to emphasize the importance of safeguarding the basic national structures and services. It is essential for the vital functions of society, including both physical facilities and structures as well as electronic functions and services. Collectively, they are called the critical infrastructure. Energy supplies, digital services, and logistics and transport must be safeguarded in the event of serious incidents and emergencies. In that sense it is also important to improve cyber security preparedness [9].

Based on the previous research results, the concept of national critical infrastructure can be simplified in accordance with Fig. 9.1. An energy supplies operator of electric power system can position its own strategic role and identify its operation as part of an entity whose other parts depend on a reliably functioning electrical network. This also facilitates the identification of cyber dependencies within the services of the service layer so that they can be secured with the most efficient and practical measures [24].

Finland's electric power system—comprising power plants, a nationwide transmission grid, regional networks, distribution networks and electricity consumers—is part of an inter-Nordic power system together with the systems of Sweden, Norway, and Eastern Denmark. In addition, there are direct current transmission links to Finland from Russia and Estonia in order to connect the Nordic system to the power systems of Russia and the Baltic countries. The inter-Nordic system is furthermore connected to the system in continental Europe via direct current transmission links [8].

Electricity is produced at Finnish power plants in various ways, using several energy sources and production methods. The major sources of energy include nuclear power, waterpower, 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 decentralized. A diverse and decentralized electricity production structure increases the security of the national energy supply [6].

The national significance of an electric power system is very similar irrespective of the country. For example, in the USA the power system is considered to be a critical infrastructure and a key resource for the functioning of the entire society. In the USA it can be seen that the grid represents a technologically highly advanced system entity and that its solutions call for the use of the most demanding technologies. Grid

technology and its control procedures constitute the principal areas in examining cyber security [17].

The electric power system with all its components belongs to critical national infrastructure: it is vital for the operations of the country and its outage or destruction would weaken national security, the economy, public health and safety as well as make the operations of state administration less effective. Even one second power failure can cause harm for sensitive industrial processes may stop. Data in information systems may be lost, fifteen minutes failure may harm people's daily activities and cause traffic delays, after few hours industrial processes may undergo significant damage, mobile phone networks will face problems, domestic animal production will be disturbed and finally after days the operations of society will be seriously harmed [12].

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. They are seen to be among the major global risks based on the probability and impact of their realization [29].

This chapter focuses on factors related to cyber security management in an electricity production organization of energy supplies that is typical part of power system. It will also examine the answer to the question: How the cyber security factors should be considered in the organization process structures while creating continuity in its operation within a dynamic cyber environment?

9.2 Organization's Cyber Structure

9.2.1 Structure of an Organization's Cyber World

According to EU commission "Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures (ICT infrastructures) form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures" [7]. Information and Communication Technology (ICT) systems are part of the organization's critical infrastructure and thus constitute a significant part of the operations that support an organization's core processes. Organization-level ICT systems are related to administration and to the management of information and material flows in the network. The production level includes industrial automation called Industrial Control Systems (ICS).

Martin C. Libicki has created a structure for the cyber world, his idea is based on the Open Systems Interconnection Reference Model (OSI). The OSI model groups communication protocols a broken down into seven layers. Each layer serves the layer above it and is served by the layer below it. The Libicki cyber world model has the following four layers: physical, syntactic, semantic and pragmatic [18].

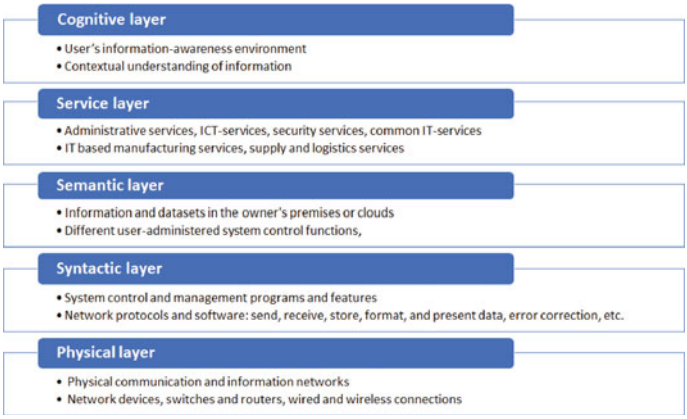

Fig. 9.2 Five-layer structure for the cyber world (modified from [16])

Martti Lehto, cyber security professor at the University of Jyväskylä, has updated the Libicki's four layers cyber world model by adding the fifth layer in order to consider an organization's networking needs. The structure is described in Fig. 9.2.

In the case of the five-layer model structure, the physical layer contains the physical elements of the ICT and ICS devices, such as computers, control devices, communications network devices (switches and routers) as well as wired and wireless connections. The syntactic layer is formed of various system control and management programs and features, which facilitate interaction between the devices connected to the different kind of networks, such as networks protocols, error correction, handshaking, etc. The semantic layer contains the information and datasets in the user's computer terminals as well as different user-administered and controlled functions. The service layer is the heart of the entire network. It contains administrative services, ICT-services, security services, IT based manufacturing services, supply and logistics services. The cognitive layer portrays the user's information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created.

9.2.2 Structure of an Electricity Organization's Cyber Environment

Organization's operational systems and supply chains are complex systems of systems characterized by a conglomeration of interconnected networks and dependencies. The general networks and working processes involved in the operation of an organization can be illustrated with a logistics framework that comprises a supplier network, a production process, a client network, and information and material flows that connect them [24].

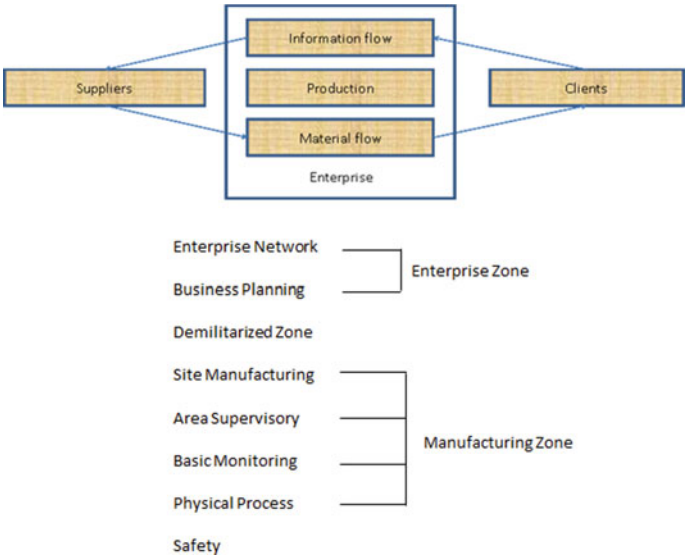

Fig. 9.3 Logistics framework of an electricity company (adapted) and common IT and industrial automation systems [3] (adapted from [14])

Information Technology (IT) systems are part of a company's infrastructure and thus constitute a significant part of the operations that support a company's core processes. Organization-level IT systems are related to administration and to the management of information and material flows in the network. The production level includes industrial automation and control systems (ICS). Figure 9.3 presents the structure of an organization's logistics framework and common ICT/IT and ICS systems.

The highest levels of IT system hierarchy include the general information systems of administration and the enterprise resource planning (ERP) system (Enterprise Zone). 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 ICS systems of production within an electricity organization comprise their own hierarchy levels (Manufacturing Zone). Based on their control systems and network structure, the Finnish Automation Society roughly classifies ICS systems into the following groups [2]:

1. Supervisory Control and Data Acquisition Systems (SCADA),
2. Programmable Logic Control (PLC),
3. Distributed Control Systems (DCS).

The transmission network of the Finnish national grid is owned by Fingrid Oyj. The distribution network consists of dozens of enterprises, and electricity is produced by about 120 enterprises and 400 power plants in different parts of the country. The power system structure is thus highly decentralized. Every organization of it is responsible for managing its own working processes. From the perspective of the entire power system of the critical infrastructure, the major threats to cyber security concern the transmission and distribution networks, switching and transforming substations, and power plants. A decentralized structure limits the potential consequences of these threats in the power system. On the other hand, decentralized power system requires good overall cyber security management for all of the electricity organizations as well as the capability to manage and control continuity of business processes in the cyber environment.

9.3 Main Cyber Security Threats in an Electricity Organization

When evaluating the role of electricity production systems in the cyber world as well as the factors that affect their cyber security, it is of primary importance to be aware of the most central features of the systems. For instance, the distributed industrial automation systems (DCS) used in controlling production processes can be characterized by saying that their operation is highly established and that their life cycles are long compared with other IT systems in a company. The life cycles of ICS systems can even be several decades, as far as the basic systems are concerned. Moreover, the structure of the basic systems is changed infrequently. The changes are mainly carried out as system life-cycle updates in connection with larger maintenance or alteration works.

The resources of ICS systems are also restricted, which is why it has not been possible to use typical technological information security solutions or cryptographies in them. Their user organizations are properly trained for their tasks and thus familiar with the devices as well as with the operating principles and operating environments of these devices. The data warehouses of ICS systems chiefly include process data, whereas administrative IT systems commonly include confidential business information. Unlike in administrative IT systems, no direct connection to the internet is usually needed in ICS systems. In the latter systems, IT devices are not used for purposes other than their decentralized tasks within the production process, its measurement and control tasks, and security functions. The monitoring of operations and staff in ICS systems is strictly controlled because of, for example, the availability and safety requirements of process operation [2].

Regarding the threats of information in ICT/IT and ICS environment terms such as, denial, loss, and manipulation are descriptive. Denial of useful information when it is needed is a condition which occurs only while the attack is active. Loss of information refers to sustained loss of an asset that continues after the active malicious interaction

has ceased. Manipulation alters the information asset and can be either loud and easy to detect or subtle and longer sustained.

The aforementioned ICT/IT and ICS 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 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 [15].

Harmful measures to the systems of an electricity organization 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 paralyzation 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 purposes of attackers is also increasingly common in today's cyber world [15].

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 [17].

Protecting the power system against threats implies measures taken based on risk assessment, and they ensure the availability of primarily digital information in the operating processes being examined. The measures are highly significant for the overall availability of the systems that support the processes. Availability plays a key role in achieving business results and promoting the reliability of activities. Further central goals include the reliability and content integrity of information within the processes and used by the processes. Overall trust should be built from these starting points, based on the target organization's realistic idea of its own capabilities to reliably manage the challenges involved in operations within the cyber world.

An organization can use their own capabilities to develop security in their cyber domain. By enhancing the capabilities of people, processes and technology, outcomes or effects applicable to the operational domain can be achieved [11].

9.4 Organization's Decision-Making Levels and System View

9.4.1 System-Level View of Organization's Cyber Security

In practice, all organizations of the power system operate in very complex, interrelated cyber environments, in which the new and long used information technical system entities (e.g., system of systems) are utilized. Organizations are dependent on these systems and their apparatus in order to accomplish their missions. The management must recognize that clear, rational and risk-based decisions are necessary from the point of view of business continuity. The risk management at best combines the top collective risk assessments of the organization's individuals and different groups related to the strategic planning, and also to the operative and daily business management. The understanding and dealing of risks are an organization's strategic capabilities and key tasks when organizing the operations. This requires, for example, the continuous recognition and understanding of the security risks at the different levels of the management. The security risks may be targeted not only at the organization's own operation but also at individuals, other organizations, and the whole society [23].

The Joint Task Force Transformation Initiative [23] recommends implementing an organization's cyber risk management as a comprehensive operation, in which the risks are dealt with from the strategic to the tactical level. That way, risk-based decision-making is integrated into all parts of an organization. In Joint Task Force Transformation Initiative's research, the follow-up operations of the risks are emphasized in every decision-making level. For example, in the tactical level, the follow-up operations may include constant threat evaluations about how the changes in an area can affect the strategic and operational levels. The operational level's follow-up operations, in turn, may contain, for example, the analysis of new or current technologies in order to recognize the risks to business continuity. The follow-up operations on the strategic level can often concentrate on an organization's information system entities, the standardization of the operation and, for example, on the continuous monitoring of the security operation [23].

In order to comprehensively build organization cyber security, organization leadership must define and guide actions at the strategic, operational and technical-tactical levels. The strategic level provides answers to 'why' and 'what' questions. The operational and tactical levels answer the 'how' question. The approach guided by questions ensures that the right things are done and that they are done in line with the set goal. The technical-tactical level must implement the goal-oriented activities defined at the strategic level, not create it. The organization's organizational capability in implementing the cyber security measures required by the technical-tactical level ultimately determines how the organization manages potential disturbance situations [20].

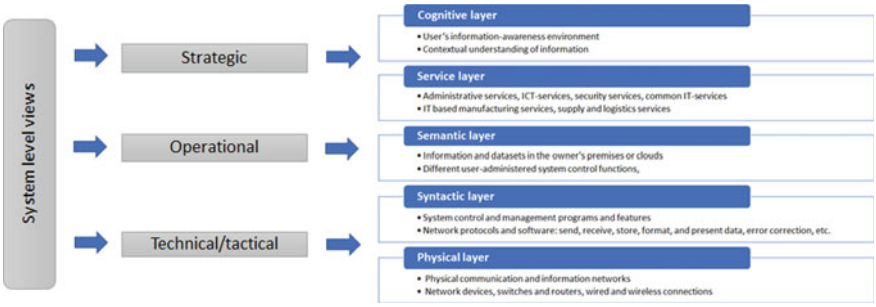

Fig. 9.4 System-level view of organization's cyber security

All three organization´s main decision-making levels can be integrated into the five-layer cyber structure in order to have a comprehensive system view of the organizations cyber security environment. It is a system thinking approach to the subsect of organization's cyber security. The principle is described in Fig. 9.4 [25].

The three decision-making levels are added to the five-layer cyber structure in order to have a comprehensive system view of the organizations cyber security environment. The following standards were utilized to support the idea to create a trust based cyber security architecture framework that is based on a comprehensive system view of the organizations cyber world.

NIST 800-39 publication places information security into the broader organizational context of achieving mission/business success. The objectives are as follows [23]:

1. Ensure senior leaders/executives recognize cyber security risks and manage such risks.
2. Ensure the risk management process is being conducted across the three tiers of organization, mission/business processes, and information systems.
3. Foster the awareness of cyber security risks so that mission/business processes are designed within designed within comprehensive enterprise architecture, and system development life cycle processes.
4. Help people in system implementation or operation understand how cyber security risks in systems affect the mission/business success (organization-wide risk).

The ISO/IEC 9000 standard family of quality management systems helps organizations ensure that they meet the stakeholders needs related to products or services. The main goal is the customers satisfaction. The fundamentals of quality management systems, including the seven quality management principles (customer focus, leadership, the engagement of staff, a process approach, continuous improvement, evidence-based decision-making, and relationship management) are the basic principles of the standard family [28].

The ISO/IEC 27,000 standard family provides recommendations for information security management system (integrated elements of an organization to establish

policies and objectives and processes to achieve those objectives), risk treatments and controls [10].

9.4.2 Systems Views and Trust-Enhancing Measures

According to process statistical management theory (Statistical Process Control, SPC) all processes involve operational variation, variation was classified into two types according to its causes: variation due to common causes (or the system itself) and variation due to special causes (i.e. named and assignable causes). Special causes come from outside of the process and usually generate more variation in the process than the common causes. In uncontrolled processes, deviation as a result of both types occurs simultaneously [19].

In principle, Lillrank's theory on the causes of process variation can also be generalized to the processes of an electricity organization. The measures taken by organization leadership can be targeted at reducing variations resulting from both aforementioned types of causes. Proper planning and control of process performance reduce variation generated by random causes. At a general level, it is always recommended to aim at reducing this variation. If corporate leadership, in particular, concentrates too much on process changes resulting from random causes, it can lead to overreactions in process control due to the measures chosen. At its worst, this can lead to loss of control in managing the overall process. The actions of corporate leadership should indeed be targeted primarily at proactively preventing variation generated by special causes. Almost without exception, serious cyber security disturbances occurring in the operating process cause blackouts. They are not in the normal range of variation. Taking these special causes into account in planning and proactively implementing security activities reduces related risks and improves the overall reliability of the organization's operations.

Excellence of an organization can be measured in its ability to recognize both causes of variation in operational processes at the right time and with the right attitude. In cyber security operations, this is mandatory in order to handle complicated technologies and complex system environment. To promote the most significant cyber security culminates in systems thinking and the point of views of strategy, operational and technical/tactical measures need to have comprehensive cyber trust.

One of the most fundamental cybersecurity tasks of the organization's uppermost management is the continuous development and maintaining of the trust in operation as part of the national critical infrastructure. The strategic choices relate to the reputation of an organization. The management is required to make concrete strategic choices and to support and guide the performance of the chosen operations through the whole organization. An important task of the management is to take care of the adequate resourcing of operations. The chosen operations must be communicated extensively with the organization's personnel and other interest groups. It is important to create a cybersecurity assessment model for the needs of the uppermost management. With the help of that model, for example, other organizations can

evaluate their cybersecurity level, become aware of their weaknesses and insufficient contingency planning, and take care of, at a minimum, the basics. The operations require strategic level decisions from the organization's uppermost management.

The operational level operations are used to advance strategic goals. Comprehensive security- and trust-adding operations require comprehensive cybersecurity management and maintaining the situation awareness of the cyber operational environment. Its starting point has to be the target's risk assessment, and the operation analyses carried out based on it. The operational level's concrete hands-on operations must be targeted at the confirmation of information security solutions and the composition of the organization's continuity and disaster recovery plans. The goal must be the continuous monitoring of the operational processes' usability, and the decision-making support in case of incidents that require analyzing and decisions.

At the technical/tactical level, the organization runs all operational processes and use such protection techniques in their ICT/IT and ICS systems that extend from the interface of the Internet and the organization's internal network right up to the protection of a single workstation or apparatus. These technical solutions make it possible to verify different harmful or anomalous observations. The typical technologies are related to security products such as network traffic analysis and log management (Security Information and Event Management, SIEM), firewall protection, intrusion prevention and detection systems (IPS and IDS) and antivirus. The situation awareness builds up to centralized monitoring rooms (Security Operations Centre, SOC). These technical solutions can be under the organization's control, or the service can be outsourced to the information security operator. A crucial goal is the situational awareness and protection of the business processes.

The key words of an organization's excellence are leadership, management, capabilities, and the measures to have continuous improvement actions. The cyber trust is related to the reliability of an organization. The summarized measures should be taken in all decision levels to increase an organizations cyber trust as illustrated in Fig. 9.5 [25]. The content of Fig. 9.5 is derived from the organization-wide risk management standard, NIST 800-39 [23] and perspectives from ISO/IEC 9000 standard family (seven quality management principles) and ISO/IEC 27000 standard family (information security management).

Building organization cyber security measures begins from the level of vision and strategy work. The visions created by leadership to enhance cyber trust are translated into strategic goals, operational-level actions, guidelines, and policy. The practical measures derived from the strategy are realized at the technological-tactical level. Organizational capability factors enable the success of the measures. Establishing measures that increase cyber world security and trust 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.

The continuous improvement of activities related to cyber security enhance the organization's capability to proactively prevent disturbances and tolerate potential changes to the operational processes. The competence and the possibilities open to fully influence the organization will help develop the overall operations of the

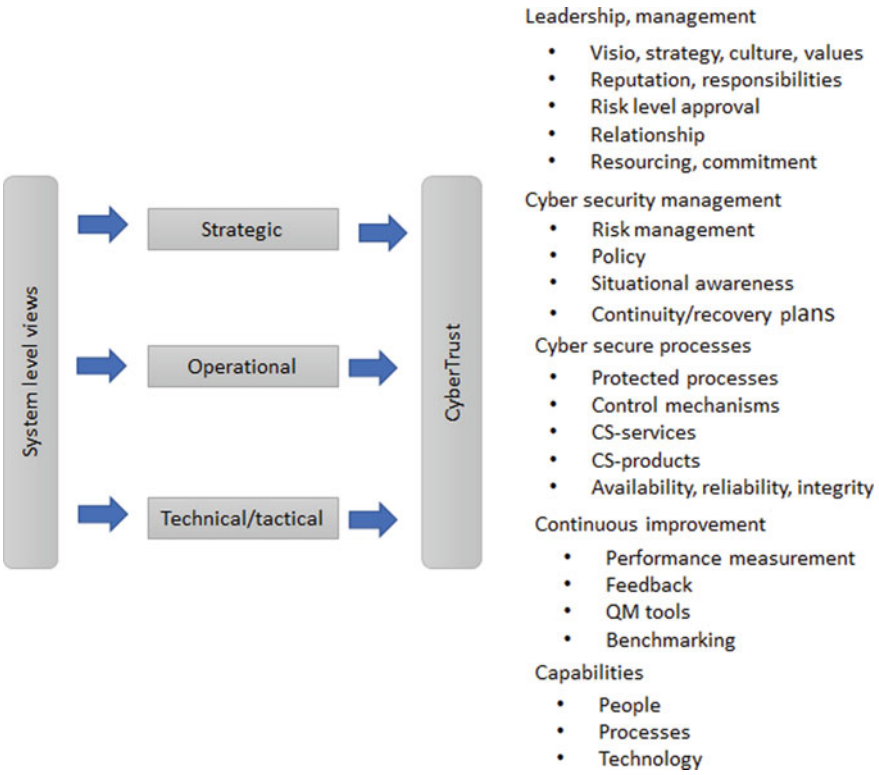

Fig. 9.5 Measures increasing an organization cyber trust

organization. The continuous development of activities and staff competence support the measures taken at the strategic, operational and technological-tactical levels.

The major cyber security excellence of the organization within the system thinking principles of leadership, management, process, and measures support that trust is enhanced and maintained at all levels of business activity. Comprehensive attitude to increase cyber trust, together with the development of capabilities related to cyber activity, also improve a company's competitive edge.

9.5 Implementing Measures to Enhance Cyber Trust

In this section, enhancing cyber trust is underlined. It is needed to understand risks, risk categorization, and system thinking approach in an organization. System thinking enables a trust-based cybersecurity architecture framework for an organization. It is then possible to make risk assessment for the whole organization.

There are still unidentified risks and therefore it is necessary to implement operations that add the resilience of the organization. They can be developed by utilizing preparedness process. At the end of the section, the PDCA (Plan, Do, Check, Act) method is recommended for developing cyber security activities and capabilities in an organization.

9.5.1 Trust-Enhancing Measures

In general risk assessment or classifications, it is assumed that every event is already identified, but it does not help to characterize unidentified risks. In the cyber world it is obvious that ICT/IT and ICS systems vulnerabilities can cause various risks. It is supposed that there is a very rare but well-known event. People know its identity but do not know if it will really happen. This event should be classified as unknown, because the occurrence and also the impact are uncertain.

In order to distinguish identified risks from unidentified risks, the level of knowledge about the risk occurrence should be about being able to identify the risk in advance or not. The level of knowledge about the impact of risk should include occurrence as well as impact since either occurrence or impact of a risk can be uncertain. A schematic structure of the risk categorization is shown in Table 9.1. In this model, events are categorized by "identification" and "certainty" [13].

As a solution to response to all listed challengers, a model of comprehensive system-level view in cybersecurity management is needed. It would be consisting of an organization's five-layer cyber structure and the strategic, operative and technical/tactical level approaches. These approaches include a survey of measures adding trust in the organization. An organization's architectural cybersecurity framework is constructed of these components and can be put to use in developing further steps in cybersecurity management on all levels of decision-making (strategic, operative and technical/tactical). Three practical measures for development are:

1. First, embedding high level and new technological solutions into the organization's piers cyber security structure (known known, unknown known),
2. Second, drafting comprehensive cyber security risk assessments (known unknown) and

Table 9.1 Schematic structure of the risk categorization [13]

	Certain (known)	Uncertain (unknown)
Identified (known)	Known-known (identified knowledge)	Known-unknown (identified risk)
Unidentified (unknown)	Unknown-known (untapped knowledge)	Unknown-unknown (unidentified risk)

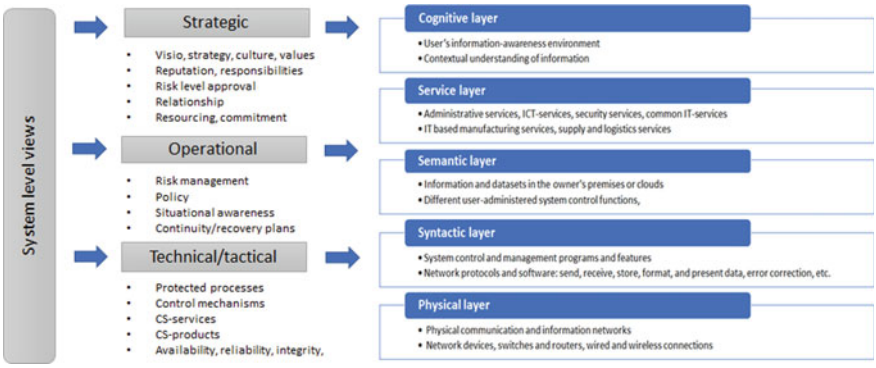

Fig. 9.6 Trust based cyber security architecture framework

3. Third, preparing contingency plans in order to improve an organization's resilience (unknown unknown).

Integration of the measures increasing an organization cyber trust (Fig. 9.5) and the system thinking approach to organization five-layer cyber structure (Fig. 9.2) makes it possible to have a trust based cyber security architecture framework (Fig. 9.6).

BusinessDictionary.com defines a capability in general as the "measure of the ability of an entity (department, organization, person, system) to achieve its objectives, especially in relation to its overall mission", and in quality perspective as the "total range of inherent variations in a stable process" [4]. Dickenson and Mavris [5] define a capability as "the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks" and also "the ability to execute a specified course of action". Thus, the capability of an organization can be seen also as an ability to learn from its experiences and use relevant information to improve the cyber security processes. Organization capabilities support actions of the architecture framework.

The process approach promoted by ISO/IEC 9001 systematically identifies processes that are part of organization quality system. Related to the quality management system, the PDCA cycle is a dynamic cycle that could be implemented in each process throughout the organization. It combines planning, implementing, controlling and continual improvement. That way an organization would achieve continual improvement once it implements the PDCA cycle [1].

9.5.2 Risk Analysis

The vision for achieving a company's goals is the point of departure for trust-enhancing measures. The definition of strategy derived from the vision guides the actions taken in order to achieve the goals. At the first stage, it is most practical to facilitate the definition of strategy by performing risk analysis on cyber threats.

When examining an electricity company, the targets of risk analysis are determined by the company's logistics framework and its IT processes. An electricity company's systems include a fuel logistic and feed system, a production system and its support processes, and the electricity distribution system. Due to all the aforementioned components being needed in the operation of an electricity company, their mutual dependence as well as operations management and monitoring are crucial for the success of overall production. In managing cyber security, the different functions of the logistics framework must be treated as subjects of equal value.

If an organization is familiar with the factors affecting the operation of processes, their most vulnerable points in the cyber world and the cyberattack methods most probably threatening the processes, it possesses the most relevant information for creating protective plans for potential treats. Vulnerability analysis against attack methods is a systematic tool for identifying and assessing risks related to process operations as well as for choosing the most suitable measures to enhance cyber security trust. The analysis provides a comprehensive overall picture of the needs to develop the processes.

The risk management standard ISO/IEC 27,005 of the ISO/IEC 27,000 standard family includes the risk management process (presented in Fig. 9.7), which can be utilized in analyzing the risks involved in the electricity production process. Risks can be classified in a treatment process according to Fig. 9.7. The aim should be to reduce or completely eliminate the highest risks using different measures. Corporate leadership prioritizes the highest risks to the processes based on risk identification and chooses the measures that best suit risk management and development of proactive measures in the cyber environment. Less significant risks can be retained, aiming to

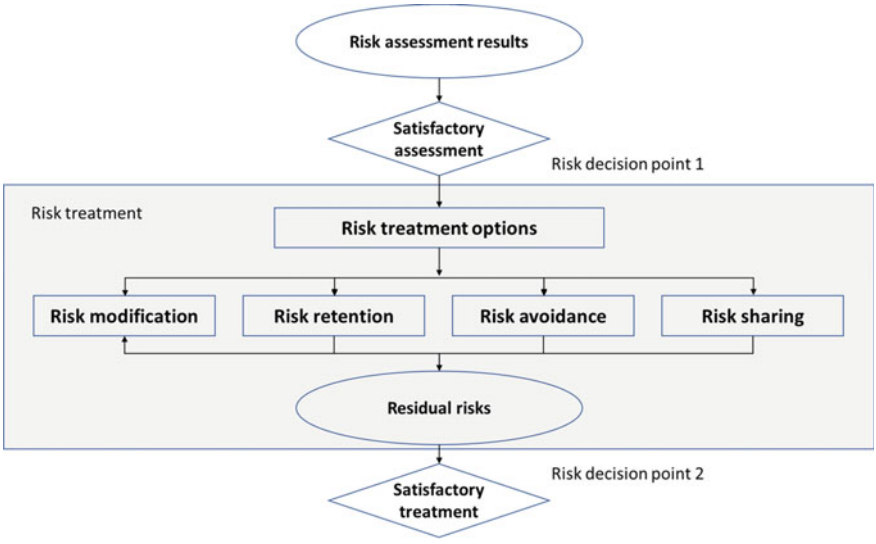

Fig. 9.7 ISO/IEC 27,005: risk management [27]

manage them. Risk transfer in the cyber environment of an electricity company can be possible through its logistics network. This means that responsibility questions must be resolved using a clear internal operations model within the network.

9.5.3 *Resilience Adding Operations*

Resilience adding operations can be developed by utilizing preparedness planning. Linkov et al. [21] introduce a resilience matrix framework (later the "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. [22] apply their model further to cyber systems. Their purpose is to develop efficient metrics to measure the resilience of cyber systems [21, 22].

The resilience management process (Fig. 9.8) was developed for the electricity company in the paper [26]. It can be linked to the management system of an organization. When creating the resilience management process, the following procedures would be utilized:

- the definition of the target organization's cyber-physical systems (ICT/IT and ICS systems),
- SWOT analysis (Strengths, Weaknesses, Opportunities and Threats),
- the Linkov model,
- Open Source Intelligence (OSINT), and
- the electricity organization's strength in utilizing its own operating networks for data collection.

After defining the target organization, the cyber-physical systems (ICT/IT and ICS systems) related to its operational processes are recognized and placed in the

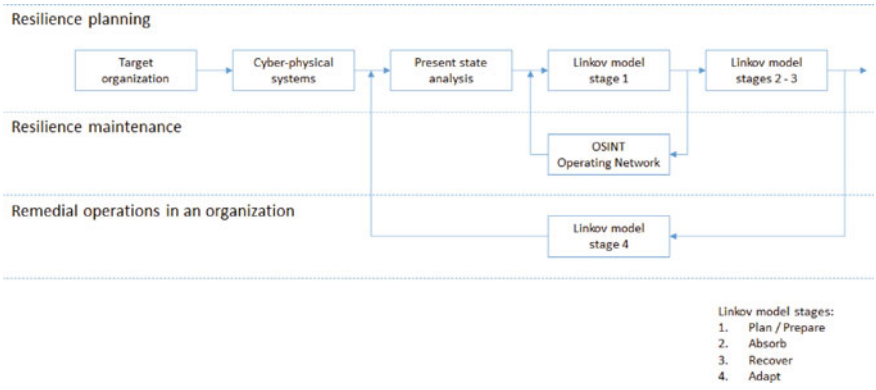

Fig. 9.8 Implementation process of the resilience operations

systems' cyber structure described in Sect. 2. After that, SWOT analysis can be applied to the organization as a theme interview by taking into consideration the cyber structure in order to describe the present state of the organization's cyber security situation. This enables the drafting of the resilience basic plan during the normal conditions (stages 1–3 of the Linkov model) for all the domains (physical, information, cognitive and social). Stage 4 of the Linkov model includes all the aforementioned domains also, 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 stage of the Linkov model as part of a repairing operation. The preparedness planning of the normal conditions (stage 1) should continuously be maintained with the help of the OSINT model and by utilizing the company's own data collection channels, such as operating networks, in the update process.

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 strategic planning. It also produces information to other decision-making levels in learning and problem recognition, evaluation, and development of operational processes. The 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.

The basis for trust adding operations is the envisioning of the company's operations in order to achieve its 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. Due to all the aforementioned components being 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.

The Linkov model and its different stages especially suit the operational and technical-tactical level preparedness planning, and ensures 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 the 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 from organizations cyber security capabilities gives a good overview of targets to be achieved in operations continuity enchantment and management against threats. Based on the analysis, the related needs of each power systems (electricity production) organization can be planted on the planning stages of the Linkov model (see Table 9.2).

Table 9.2 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
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 plan/prepare and absorb stages within the physical domain of the 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 used for their needed parts. In the recovery stage, the cleanliness and functionality of the systems is ensured for all their parts. Then, the comprehensive ramp-up of the machines is guided through. The adaptation stage is determined by the experiences received 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 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 as significant for 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 wide-scale 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.

9.5.4 PDCA Method as a Tool for Developing Activities

An organization's policy demonstrates that its leadership is committed to implementing strategic measures. In the business world, general strategic measures are mainly targeted at promoting the business activities, which means that taking cyber security into account as part of the overall strategy supports the business development targets. Cyber security as part of company policy is a way of communicating to staff and interest groups on the necessity and significance of development projects. Operational goals are formed as processes derived from the policy, whereby risk analysis has been considered. In order to create the measures, the organization must have a systematic approach to developing its operations.

The ISO/IEC 9000 Standard recommends the PDCA (Plan, Do, Check, Act) method for a systematic development of an organization's activities. The method is based on a cycle of four development phases. The first phase (Plan) comprises planning, during which the subject is analyzed, and alternative measures are created

based on the analysis. In the realization (Do) phase, the chosen measures are put into practice. Thereafter the functionality, efficiency and appropriateness of the chosen measures are checked in practice (Check). At the last (Act) phase of the cycle, the chosen measures are improved, if necessary, and established as standard practice. After the cycle has been implemented once, one will return to the first phase and start a new cycle with improvement actions based on a new situation analysis. Development can thus proceed as an endless process, in which a new level of activities is achieved after each cycle. The method is based on the idea of continuous learning and continuous improvement of activities.

The measures during one round of the cycle usually require a lot of planning, so sufficient time should be reserved for them. It is important to select the measures in relation to the resources needed for their implementation. The maturity level of the organization's development activities affects the evaluation of the implemented measures. When developing cyber security, at an initial stage the aim can be to recognize the need for cyber security management and to define cyber security risks for business. Hereby, the PDCA cycle may comprise the administrative actions most necessary according to risk assessment, such as a coherent information security policy in production, practical guidelines for maintaining information security in production, and potential preliminary system-specific cyber security checks. The targets for development must later be chosen according to risk prioritization.

The following is one possible process model for developing cyber security management with the PDCA method:

PLAN, planning phase

1. Choose the target for development based on risk assessment
   - present state
   - schedule and goal
2. Create a picture of the current cyber security situation
   - earlier measures, knowledge from partners
   - disturbances in the branch resulting from special causes
3. Analyze the problems and define corrective actions
   - identify relevant potential harms caused by the disturbances
   - choose the measures available to anticipate and manage the situation.

DO, implementation phase

4. Implement the chosen measures
   - choose the actors responsible for implementation
   - organize information and training for staff

CHECK, checking phase.

5. Check the impact of the measures
   - compare the results with the goals

- return to phase 3 if the goals have not been achieved

ACT; regularize the measures.

6. Regularize the chosen development measures
   - update necessary guidelines, technological solutions and services
   - continue staff training
7. Draw conclusions and make plans for the future
   - continue development according to new goals
   - update threat and risk analyses.

In this section, we have described one way of launching primary basic solutions related to cyber security management in an electricity production organization. These first steps provide a basis for later development activities and continuous improvement in a dynamic cyber environment.

9.6 Conclusion

The national power grid and its electricity production are part of a country's critical infrastructure—the operation of a modern society is based on a reliable electric power system. Ensuring the availability and reliability of processes in electricity organizations in all environments is vital for the efficient functioning of critical infrastructure. Therefore, the measures taken in electricity organizations in order to manage and control the cyber security of processes are an essential component of the reliability of production.

The major cyber environment risks within the processes of an electricity organization require that trust be enhanced and maintained at all levels of business activity. Comprehensive measures to increase cyber trust, together with the development of cyber security excellence of organization related to cyber activity, also improve a company case its competitive edge.

The initial measures taken to develop cyber security management and trust can be summarized and prioritized as follows:

1. It is ensured that the organization sees cyber security measures as strategic goals and that sufficient resources are allocated to the chosen measures.
2. Risk assessment is performed, the organization's policy is updated to meet the requirements of cyber security and the resilience management process is implemented.
3. The primary trust-enhancing development measures needed based on risk assessment are taken at the first development phase, using the PDCA method.
4. A continuous process is formed of the development actions by choosing the subjects of the next cycle, and the PDCA development cycle is repeated. This procedure will provide the organization with a culture of continuous learning

and improvement. The organization's capabilities and competitive advantage are enhanced.
5. The impact of the measures is monitored as part of the organization's audit and management procedures (e.g., as a part of the ISO/IEC 9001 Standard procedures).

References

1. 9001Quality (2020) The Plan Do Check Act (PDCA) cycle. 9001Quality http://9001quality.com/plan-do-check-act-pcda-iso-9001/. Accessed on 27 Jan 2020
2. Automaatioseura (2010) Teollisuusautomaation tietoturva: Verkottumisen riskit ja niiden hallinta. Suomen Automaatioseura ry, https://www.automaatioseura.fi/site/assets/files/2157/sas29_teollisuusautomaation_tietoturva.pdf
3. Bowersox D, Closs D, Helferich O (1986) Logistical management: a systems integration of physical distribution, manufacturing support, and materials procurement, 3rd edn. Macmillan, New York
4. BusinessDictionary (2020) BusinessDictionary.com. Online business dictionary. Available at http://businessdictionary.com/
5. Dickerson CE, Mavris DN (2010) Architecture and principles of systems engineering. CRC Press
6. ET (2020). Sähköntuotanto. Energiateollisuus ry (ET), https://energia.fi/energiasta/energiantuotanto/sahkontuotanto
7. EU (2009) Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience. 52009DC0149, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU Commission, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:HTML
8. Fingrid (2020) Electricity system of Finland. Fingrid Oyj, https://www.fingrid.fi/en/grid/power-transmission/electricity-system-of-finland/
9. Finlex (2018) Valtioneuvoston päätös huoltovarmuuden tavoitteista. Finnish Government, https://www.finlex.fi/fi/laki/alkup/2018/20181048
10. ISO/IEC (2018) ISO/IEC 27000:2018: Information technology, security techniques, information security management systems, overview and vocabulary. International Organization for Standardization (ISO), https://www.iso.org/standard/73906.html. Accessed 27 Jan 2020
11. Jacobs PC, von Solms SH, Grobler MM (2016) Towards a framework for the development of business cybersecurity capabilities. Business Manage Rev 7(4):51–61
12. Kananen I (2013) Sähköjärjestelmä yhteiskunnan toimivuuden perustana. Seminar presentation, Fingridin käyttövarmuuspäivän seminaari 2.12.2013, Fingrid, http://wms.magneetto.com/webcasts/hd1/fingrid/2013_1202_kayttovarmuuspaiva_02_Kananen/Attachment/02_Kayttovarmuuspaiva_021213_Kananen.pdf
13. Kim SD (2012) Characterizing unknown unknowns. In: Paper presented at PMI® Global Congress 2012—North America (Vancouver, 2012). Project Management Institute, Newtown Square, PA
14. Knowles W, Prince D, Hutchison D, Disso JFP, Jones K (2015) A survey of cyber security management in industrial control systems. Int J Crit Infrastruct Prot 9:52–80
15. Lehto M (2015) (2015). Phenomena in the cyber world. In: Lehto M, Neittaanmäki P (eds) Cyber security: analytics. Technology and Automation. Springer, Cham, pp 3–29
16. Lehto M (2018) The modern strategies in the cyber warfare. In: Lehto M, Neittaanmäki P (eds) Cyber security: power and technology. Springer, Berlin, pp 3–20

17. Lewis TG (2015) Critical Infrastructure protection in homeland security: defending a networked nation. eBook, 2nd ed, Wiley
18. Libicki MC (2007) Conquest in cyberspace: national security and information warfare. Cambridge University Press, New York
19. Lillrank PM (1998) Laatuajattelu: Laadun filosofia, tekniikka ja johtaminen tietoyhteiskunnassa. Otava
20. Limnell J, Majewski K, Salminen M (2014) Kyberturvallisuus. Docendo, Jyväskylä
21. Linkov I, Eisenberg D, Bates M, Chang D, Convertino M, Allen J, Flynn S, Seager T (2013) Measurable resilience for actionable policy. Environ Sci Technol 47:10108–10110
22. Linkov I, Eisenberg D, Plourde K, Seager T, Allen J, Kott A (2013) Resilience metrics for cyber systems. Environ Syst Decis 33(4):471–476
23. NIST (2011) Managing information security risk: organization, mission, and information system view. Joint Task Force Transformation Initiative, NIST Special Publication 800-39, National Institute of Standards and Technology (NIST), Gaithersburg, MD
24. Pöyhönen J, Lehto M (2017) Cyber security creation as part of the management of an energy company. In: ECCWS 2017: proceedings of the 16th European conference on cyber warfare and security, pp 332–340. Academic Conferences and Publishing International, Reading
25. Pöyhönen J, Lehto M (2020) Cyber security: trust based architecture in the management of an organization security. In: ECCWS 2019: proceedings of the 18th European conference on cyber warfare and security, pp 304–313. Academic Conferences and Publishing International, Reading
26. Pöyhönen J, Nuojua V, Lehto M, Rajamäki J (2018) Application of cyber resilience review to an electricity company. In: ECCWS 2018: proceedings of the 17th European conference on cyber warfare and security, pp 380–389. Academic Conferences and Publishing International, Reading
27. SFS (2012) SFS-käsikirja 327: Informaatioteknologia, turvallisuus, tietoturvallisuuden hallintajärjestelmät. Suomen standardoimisliitto SFS ry, Helsinki
28. SFS (2016) Johdanto laadunhallinnan ISO 9000—standardeihin: Kalvosarja oppilaitoksille. Suomen standardoimisliitto SFS ry, Helsinki, http://slideplayer.fi/slide/11133323/
29. WEForum (2020) The global risks report 2020. Insight report, 15th ed, World Economic Forum, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf