Assessment of cyber risk for energy utilities

Tommi Kantala

School of Science

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 27.05.2019

Supervisor

Prof. Ahti Salo

Advisor

MSc (Tech.) Lauri Haapamäki

Aalto University
School of Science

Aalto University
School of Science

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the master's thesis

Author Tommi Kantala

Title Assessment of cyber risk for energy utilities

Degree programme Mathematics and Operations Research

Major Systems and Operations Research **Code of major** SCI3055

Supervisor Prof. Ahti Salo

Advisor MSc (Tech.) Lauri Haapamäki

Date 27.05.2019 **Number of pages** 55 **Language** English

Abstract

Cyber risk assessment of industrial control systems and organizations using them is a challenging topic in risk analysis. In this Thesis, an approach to cyber risk assessment of energy utilities is proposed. The risk assessment is provided by a cyber security vendor for energy utilities. The aim of the approach is to be a rapidly deployable risk assessment method that does not require extensive modelling of the target organization. The approach also emphasises context establishment and cyber risk evaluation.

The risk assessment approach developed in this Thesis uses several different methods to reduce the dimensionality of industrial control systems and cyber threat environment. A modified annual loss expectancy model is used to calculate the cyber risk. Functional modelling of the target organization is used to identify critical business functions and costs of downtime. A questionnaire and interviews with the target organization help to establish context and the answers are used to modify strength of different cyber incidents. The controls and questions are based on industry standards for better coverage and to establish a common language with the target organization. The dimensionality is further reduced by categorising cyber incidents based on their threat source and impacts. Available data and expert assessment are used to create incident tables for the model with strength of attack and occurrence rates, which are modified based on the controls used by the target organization. The produced risk score and report communicates the current risk levels to the target organization and helps the decision makers in the risk treatment processes.

The risk assessment approach solves some of the common problems related to most cyber risk assessment methods. The proposed approach is provided by a vendor to a target organization. The discussions are used to communicate the importance of cyber risk to different decision makers within the target organization's management across different business functions. The interviews are used to verify that the cyber security processes and controls are adopted throughout the organization. The use of external vendor also enables more objective assessment. The produced risk score can be compared with peers and recommendations are given as a report, which assists the risk evaluation step of the risk management process.

Keywords cyber security, critical infrastructure, risk analysis, cyber risk assessment

Aalto University
School of Science

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi
Diplomityön tiivistelmä

Tekijä Tommi Kantala

Työn nimi Energiayhtiöiden kyberriskien arviointi

Koulutusohjelma Matematiikka ja operaatiotutkimus

Pääaine Systeemianalyysi ja operaatiotutkimus **Pääaineen koodi** SCI3055

Työn valvoja Prof. Ahti Salo

Työn ohjaaja DI Lauri Haapamäki

Päivämäärä 27.05.2019 **Sivumäärä** 55 **Kieli** Englanti

Tiivistelmä

Teollisten ympäristöjen kyberriskien arviointi on haasteellista. Tämän diplomityön tarkoituksena on muodostaa riskien arviointimenetelmä, jota kyberturvallisuusyritys voi hyödyntää energiayhtiöiden riskien arvioinnissa. Menetelmän tavoitteena on, että se ei vaadi raskasta kohdeympäristön mallinnusta ja se tukee riskienhallintaprosessin kontekstinmuodostus- ja riskienmääritysvaiheita.

Tässä työssä esitelty lähestymistapa hyödyntää useita menetelmiä kompleksisuuden vähentämiseksi. Kyberriskin laskemiseen käytetään muokattua vuotuisen tappion odotusarvion mallia. Kohdeorganisaatiota mallinnetaan liiketoimintojen avulla, jotta kriittiset komponentit voidaan tunnistaa ja niiden alasajokustannukset voidaan määrittää. Haastattelujen ja kyselyn avulla luodaan kontekstia ja kysymysten avulla selvitetään varautuminen kyberuhkiin, jota käytetään muokkaamaan erilaisten kybertapahtumien voimakkuutta mallissa. Kontrollimekanismit ja kysymykset perustuvat alan standardeihin, jotta ne ovat kattavat ja termit ovat kaikille osapuolille selkeät. Kybertapahtumien luokittelulla niiden vaikutusten ja tekijöiden perusteella pyritään edelleen vähentämään uhkaympäristön monimuotoisuutta. Apuna käytetään alan asiantuntijoiden arvioita ja saatavilla olevaa dataa, joiden avulla kybertapahtumista muodostetaan sektorikohtaisia taulukoita. Kohdeorganisaation päätöksentekoa tuetaan riskipisteytyksellä ja kirjallisella raportilla havainnoista ja niihin pohjautuvista suosituksista.

Työssä esitellyn lähestymistavan avulla voidaan ratkaista joitakin kyberriskien arviointiin liittyviä ongelmia. Sen avulla ulkoinen toimija kykenee objektiivisemmin arvioimaan riskejä kohdeorganisaation haastattelujen perusteella. Keskustelujen avulla voidaan myös kommunikoida kyberriskien merkityksestä eri toimijoille. Keskustelujen avulla voidaan varmistaa, että kohdeorganisaatio toteuttaa sen kuvaamia kyberturvallisuustoimia ja -prosesseja kaikissa toiminnoissaan ja yksiköissä. Riskipisteytyksen avulla organisaatiota voidaan verrata muihin alan toimijoihin ja raportti tukee kohdeorganisaation riskienhallintaprosessia.

Avainsanat kyberturvallisuus, kriittinen infrastruktuuri, riskianalyysi, kyberriskien arviointi

Preface

I want to thank my supervisor Professor Ahti Salo and my instructor MSc (Tech.) Lauri Haapamäki for their good guidance and Sectra for funding this Thesis project. I would also like to thank Finnish Energy (Energiateollisuus ry) and the organizations that participated in the interviews for their valuable input on the topic. Finally, I want to thank Jonna, my family and my friends for their support.

Helsinki, 27.05.2018

Tommi Kantala

Contents

Abbreviations

CI	Critical infrastructure
CPS	Cyber-physical system
DCS	Distributed control system
DHS	United States Department of Homeland Security
FRM	Functional reference model
ICS	Industrial control system
IEC	International Electrotechnical Commission
IT	Information technology
ISO	International Organization for Standardization
MTU	Master terminal unit
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operational technology
PLC	Programmable logic controller
PRA	Probabilistic risk assessment
RMA	Risk matrix approach
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
WAN	Wide area network

1 Introduction

Critical infrastructure (CI) is the vital backbone of any modern society, which is more and more dependent on the information network infrastructure. Within the critical infrastructure, several sectors, such as communications, manufacturing, financial, healthcare, energy, and transportation cooperate to provide necessary systems and assets for rest of the society. Specifically, energy sector is one of the most important sectors, since other sectors are heavily dependent on energy, especially electricity. Thus, energy sector is an attractive target for adversaries aiming to harm an energy organization, critical infrastructure or the society as a whole. [1, 2, 3]

Many operations of the energy sector rely on industrial control systems (ICS). For long, these automation, control and monitoring systems were separated into own local networks and used proprietary communications standard. Thus, an attack against energy sector were physical and affected physical assets of the organization. More and more of these systems are becoming increasingly interconnected for ease of monitoring and control. This means that some the networks might be exposed to public internet more or less directly, if necessary precautions are not taken. The connection to public networks creates a new attack vector for adversaries. Too often energy utilities have not implemented necessary security controls due to lack of investments, availability requirements or limitations of ICS equipment. The controls should be included in the risk management process of energy utility organizations. [1, 3, 4, 5]

The risk management process also includes the risk assessment. In this Thesis, the focus will be on the cyber risk assessment. There does not exist a unified risk model for critical infrastructure, industrial control systems or operational technology that would cover all possible scenarios. Especially high-impact low-frequency events are difficult for ICS risk assessments. The dynamic threat environment, outdated equipment and human elements create a constantly changing threat and vulnerability

landscape. The risk assessment in ICS environment is challenging. Qualitative methods do not provide objective information about the cyber risk. Quantitative methods can produce more objective results, but these methods are often probabilistic and suffer form lack of ICS cyber security data. Thus, there are several problems related to the cyber risk assessment in ICS relying organizations. [1, 4, 5]

1.1 Motivation

During the Thesis process Finnish electric utility organizations, especially distributors, were interviewed. The interviews gave some insight on the current state of cyber security in Finnish electric utilities. Other valuable information, for example cyber security standards used by Finnish organizations and on the impacts caused by failures, were collected.

Nine small to medium and two large electric utilities were interviewed in Fall 2018. In total, 17 persons participated in the interview sessions. Participants were mostly those who were responsible for day to day execution of cyber security, such as chief information (security) officer, IT manager or system specialist. In some organisations the participant was not part of the cyber security organisation. Some organisations have an external cyber or information security vendor or an external information security officer. In many organisations, the business unit managers and system specialist are responsible for cyber security.

The organisations reported varying threat levels of control systems, four answered *low*, two *medium*, four *high* and one reported the treat level to be *critical*. Despite the relatively high perceived threat level, cyber incidents affecting the OT or ICS network were not reported. However, some organisations reported that internal configuration errors and similar cases have caused minor problems, but malicious actions from internal or external sources were not reported. In IT networks, however, phishing and malware cases were reported but these incidents were limited to single computer in IT network with no access to OT or ICS networks. One third of the organisations did not expect a cyber incident in next 12 months. Rest of the organisations identified the possibility of a cyber incident but expect them to be minor.

Finnish electric utilities have mostly identified the importance of cyber security for safe and efficient operation. The interviews revealed that the current state of preparedness and awareness of cyber threats is varying. Larger organizations tend to be more aware of cyber threats and have established plans and procedures, while in smaller organization the level of cyber security is heavily dependent of the awareness and experience of the personnel. Active monitoring of ICS networks is often lacking

and while organisations have contingency plans against traditional disruptions, they do not include cases originating from cyber incidents. While the importance of cyber security is improving, there is still resistance against changes which would improve cyber security. Many of the smaller companies do not have cyber security plans or budget for it and responsibility is either placed on chief information officer or chief operations officer, instead of security personnel. As some organizations have rather limited willingness to spend on cyber security, it creates challenges for third party security vendors. From this standpoint, a risk assessment method must be relatively easily deployable, have valuable outcome and low cost. These challenges will be addressed in this Thesis.

The reminder of the Thesis is organised as follows. Section 2 reviews the critical infrastructure, energy industry, cyber threats and vulnerabilities and risk management. Section 3 describes methods and assumptions behind the presented approach to cyber risk assessment. In Section 4, the approach is presented and evaluated. Finally, Section 5 summarises the findings and reflects the results to literature.

2 Background

2.1 Critical infrastructure and industrial control systems

Critical infrastructure means infrastructure and systems that produce and distribute vital goods and services for a society. Transportation, communication systems, manufacturing, water supply, and energy generation, distribution and storage are examples of systems that are critical for the functioning of a modern society. Critical infrastructure forms a network-like structure, with dependencies (unidirectional) and interdependencies (bidirectional) between the components that often are complex systems themselves. They are considered critical, as their incapacity or malfunction has an impact on the health, well-being, economics, safety and security. Also, a failure in a component of critical infrastructure has a cascading effect. For example, a malfunction of electric grid can cascade geographically if other parts of the grid become overloaded. Further, the cascading effect can reach other critical sectors, such as rail transportation or critical manufacturing if the rely on the malfunctioning grid. [1, 2]

In this Thesis, the energy sector is used as an example of critical infrastructure. Within energy sector, especially electric utilities will be in the focus, as they include both local scale power plants and geographically spread distribution grids. Energy sector also heavily relies on automated control systems that are used to monitor and control production, distribution and storage.

Industrial control systems (ICS) consist of different computers, instruments and processes that under human supervision manage industrial tasks and processes. These systems can be found in all industrial sectors, including energy, utilities, manufacturing and transportation. Term operational technology (OT), defined by National Institute of Standards and Technology (NIST) as "hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise", is often used alongside ICS to

describe these systems, differentiating them from traditional information technology. ICS and OT are often used interchangeably. ICSs and OT are backbone for critical infrastructure (CI), which covers all assets needed for a functioning society and economy. The ICS term covers supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other systems such programmable logic controllers (PLC) and hybrid systems of the ones mentioned. The ICSs can be segmented in different ways. One way is to use enterprise, control and field zones as seen in Figure 1. The enterprise zone covers business and enterprise networks and systems, which are essentially information technology (IT) and based on IP protocol. This means that traditional IT security practices apply to this layer, but connections with operational technology must be considered and necessary ICS/OT security principles must be adopted also on this layer. Often, these systems are connected to control zone, where more specialized devices are used. Finally, the actual plant or process is automated and controlled at the field zone. This is where PLCs transform cyber to physical actions of pumps, valves, motors and sensors. The simplified zoning example in Figure 1 hides much of the connections and problems in the architecture of ICSs. [1, 2, 4, 5, 6]

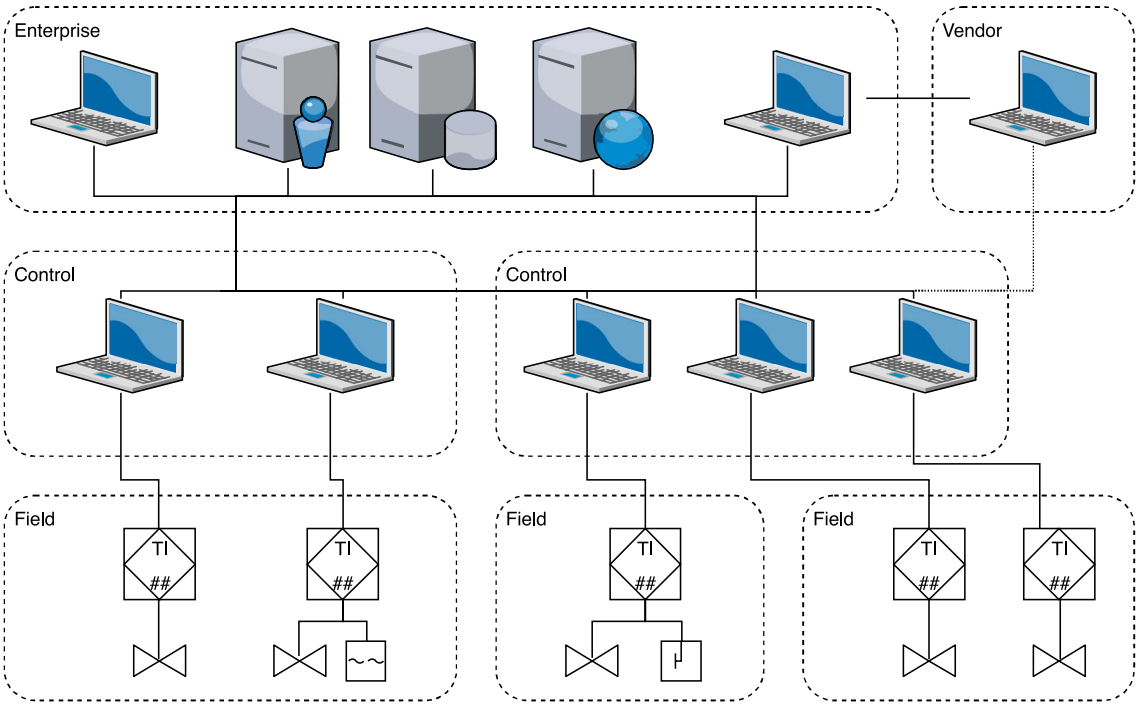

Figure 1: ICS zoning example. [4]

The ICSs are often complex systems with thousands of components. Moreover, these components can be geographically distributed and are controlled remotely using

wide area network (WAN). ICS components traditionally differ from information technology (IT) by running specialized hardware and software that are needed to physically interact with the world. The ICS components also typically have much longer lifecycles than IT components, often in the scale of dozens of years. Safety and reliability (in terms of fault tolerance) are important for ICSs and previously security only meant physical security, because that was the only way to tamper with these systems. ICSs differ from IT in several fashions. Most important differences are the performance and availability requirements of the ICS components and networks. The ICSs must work in real-time and the processes often cannot be stopped or restarted as they could be in IT environment, any production stops must be planned well ahead. The unavailability of an ICS could lead to severe physical consequences, such as environmental damage or injury to human operator. The ICS systems cannot be patched and updated like IT systems, because the software must be extensively tested, the availability cannot be compromised, the hardware and software can be proprietary and there may not be excess computational power to run the added (security) features. In traditional information security, a triad of confidentiality, integrity and availability in that particular order is used as a basis for policies and controls. In cyber security of industrial control systems, the order is availability, integrity and confidentiality. This highlights the traditional ICS cyber security approach, where system availability is crucial and there has been no need for confidentiality as system communication has been air-gapped, both logically and physically. There are also many intradependencies in ICSs, between ICS and enterprise systems and also between different ICSs, since critical infrastructure services are often connected. [2, 4, 5, 7, 8, 9]

The IT and ICS/OT systems have started to converge since the 1990s, as the cost of connectivity is decreasing and the desire for better connectivity has increased along with "smart" systems and internet of things (IoT) paradigms. Previously isolated proprietary systems are being connected to Internet and IT systems, which dramatically increases the number security threats, especially when systems not designed with cyber security in focus are exposed to Internet. Many of the ICS communications standards and components have not been developed with an emphasis on information security and rely on clear text communication without any authentication. New SCADA systems often use several communication media, such as cellular networks, radio frequencies, and Internet. Despite the convergence between IT and ICS/OT, the difference remains noteworthy and not all information security techniques and methods developed for IT can be applied to ICS/OT environments.

2.2 Cyber threats and vulnerabilities in industrial control systems

2.2.1 Cyber vulnerabilities

There are several definitions of vulnerability. One way to see vulnerabilities in ICS or CI is to consider them as global technical properties that, once exploited by a threat or hazard, can incapacitate or destroy a system or a component of it. The vulnerabilities are weaknesses, errors or flaws related to the design, implementation or management of a system or a component of it. [1]

Vulnerabilities in SCADA systems can originate from the underlying operating system vulnerability or from unencrypted communications standards. Legacy systems with long operational life are used in SCADA environments due to the high cost of components and availability requirements. Often these systems cannot be patched, which can lead to several vulnerabilities. All system components and protocols can also include back doors. As stated before, a wide variety of communications methods are used in modern control networks. This increases the number of access points for an adversary.

SCADA systems are complex and real-time operations are sensitive to small deviations. An adversary can exploit the sensitivity of the system. While cyber security often focuses on external adversaries exploiting technical vulnerabilities, insiders pose as equally important source of threat. They have access to the systems and can operate stealthily. External adversaries can also exploit insiders and employees of target organization by using social engineering methods. Thus, not all vulnerabilities are technical or "cyber", but cyber security is also closely tied to personnel and physical security. [5]

In SCADA systems, vulnerabilities can be divided into four categories. First, architectural vulnerabilities can be caused by poor separation between network layers, failures in firewalls or due to lack of authentication in communication between active components, such as actuators, remote terminal units (RTU) and SCADA servers. Second, security policy vulnerabilities, such as patching or access policies are not adequate and create opportunities for failures or exploitation. There are often also conflicting interests in the architectural design, monitoring and patching of systems. Third, software vulnerabilities are caused mostly by unpatched operating systems or applications. Finally, there can be vulnerabilities in the SCADA communication protocols, such as Modbus. The problem with SCADA communications protocols is that they lack checks for integrity or authenticity of components and packets and

controls against replay repudiation attacks. [2, 10] NIST 800-82 standard categorizes vulnerabilities into six categories: policy and procedure, architecture and design, configuration and maintenance, physical, software development, communication and network. Policy and procedure includes vulnerabilities such as lack of security training for personnel and lack of security policies and administration. Architecture and design, for example, covers vulnerabilities stemming from lack of security perimeters and security architecture design of systems. Configuration and maintenance vulnerabilities can be caused by unprotected data, poor access control mechanisms (local or remote), inadequate denial of service controls and such. Physical vulnerabilities include vulnerabilities such as loss of control environment, lack of physical access control and loss of power. Software development vulnerabilities originate from disabled security features in software and improper data validation. Communication and network vulnerabilities are caused by improper or inadequate use of firewalls and data flow controls. Insecure ICS communications protocols and lack of authentication and logging are also communication and network vulnerabilities. [5]

Energy sector is a good example of the spatial scale of CI and ICS. A small production plant can be considered an example of spatially local ICS, while a distribution network is an example of spatially distributed system. These spatial differences must be considered, because some threats can exploit threats in their local perimeter cause a cascading effect. [1] An electric utility, for example, can suffer from the geographical spread, because it increases the number of points of entry.

2.2.2 Cyber threat sources

Based on NIST's Guide to Industrial Control Systems (ICS) threats can be divided into four sources: adversarial, accidental, structural and environmental. All these sources have different characteristics, such as different intents, skills and consequences. [5]

Adversaries cause different levels of risk based on their capabilities, intents and targets. Not all attackers share the same skill set or goals. The demographics vary from "script kiddies" to nation-state supported persistent hacker with unlimited resources. Low-end hackers and "script kiddies" are attacking low hanging fruits with known vulnerabilities, often without certain goal. They can alter or block websites but are not often danger to operations. [5, 11]

Criminals, however, are seeking a monetary gain, either by stealing data and selling it or by taking information as a ransom. An example of this are ransomware attacks that became popular lately. Contractors and vendors that have permanent

or temporary access to system can either attack or steal data themselves or allow attackers use them as a backdoor against primary target. [5, 11]

Also, malicious insiders or disgruntled employees might want to gain financial benefit by selling data or revenge their grudges. Other companies and competitors might want to spy, steal intellectual property or damage competitors. Terrorist might want to cause damage to society by attacking vulnerable parts of critical infrastructure or to gain resources. [5, 11]

Finally, state sponsored adversaries could try to steal intellectual property, espionage other state, unsettle society or pressure decision makers. The consequences of adversarial threats greatly differ due to different targeting, intentions, goals and skills. A major problem with the identification of adversarial threats is that the adversaries can be capable of exploiting previously unknown vulnerabilities. These threats also depend on the unknown skillset of the adversary. One way to model the actions of an adversary is to use Cyber Kill Chain developed by Lockheed Martin seen in Table 1. [5, 11] NIST 800-82 standard also lists some threat events and incidents. Adversarial incidents can be control device reprogramming, malware in control system, denial of control, spoofing on status of the system, safety system modification or control logic modification. [5]

Accidental threat sources originate from human errors caused by erroneous actions by users or users with elevated privileges in their everyday actions. In contrast to previously mentioned insiders, these users do not have malicious intentions, but the incidents are caused by accident. [5]

Structural threats originate from hardware, software, resource, control or operational issues. These issues include equipment failures, problems related to software and hardware ageing, resource deficiencies or other causes of exceptional operating circumstances. [5]

Environmental threat sources include natural or man-made disasters and failures of critical infrastructure, such as fire, earthquake or telecommunications disruption. These situations are often considered force majeure, that is, the organization has no control over these events. Traditionally, these events are well understood but their magnitude and frequency and cascading effects can vary event to event. [5]

Some typical attack scenarios found in ICS are distributed denial of services attacks which prevent communications over internet, worm or malware infections, and phishing attacks, which are often used to gain credentials to attacker's targeted system. Attackers can also alter or block communications such that control of the industrial control system is lost or system reports false state to operators. An example

Table 1: Cyber kill chain [12, 13]

Phase	Description
Reconnaissance	Adversary identifies target, and gathers information by exploring public data, using social engineering, or exploiting vulnerabilities, among other methods.
Weaponisation & Delivery	Based on the recon information, adversary builds a malicious payload. The payload is delivered for example as an infected USB stick or email attachment.
Exploitation	The payload is executed using a vulnerability or bug, either known or zero-day, in order to gain access to files, network or machine(s). This happens as an infected USB drive is connected or a malicious email attachment is opened.
Installation	The payload installs on the target machine once it has been reached. The payload elevates the user privilege of the attacker and allows persistent access.
Command & Control	Adversary gains control of the system, allowing external connections and additional instructions to be executed. Essentially allows the attacker to have hands-on access to system.
Action	Adversary reaches goals, such has stealing data, halting system, or causing physical damage to system. From defender's perspective, prevention is not possible and recovery process must be started.

of a multistate attack with several of these attacks combined was Ukraine blackout attack in 2015. This attack included a reconnaissance phase of several months by the adversary, followed by exploitation of several technical vulnerabilities in firewalls, network protocols, encryption and VPN connections. The command and control phase included intercepting data packets and forging their contents in the SCADA network and control centre database and blocked remote control using malicious firmware. [10, 14]

2.3 Impacts of cyber incidents

One of the hurdles in the impact assessment of cyber incidents is that organizations lack capabilities to identify cyber related breaches in ICS. Organizations lack visibility into ICS networks, which then makes it difficult to detect incidents or to find the root cause of a failure or malfunction. This also makes it difficult to analyse the frequency of incidents. [15] Surveys and analyses on the impact of cyber incidents in ICS organizations yield ambiguous results. Ponemon Institute reported in 2018 that per capita cost of a data breach in energy sector is $167. In 2017, Ponemon Institute

reported that average annualized cost of cyber crime in utilities and energy sector is $14,460,000 (very limited sample size), whereas Business Advantage reported average annual cumulative financial loss by ICS cyber security breach to be $347,603 and $497,097 for companies with over 500 employees. [16, 17, 18]

In [19], three pipeline ruptures and other data sources were used to estimate the likelihood and impact of an oil pipeline rupture. In the model, single loss expectancy $SLE = \lambda \times t \times v$ depends on the range of values of severity of risk impact λ, the likelihood of attempted breach t and the likelihood of successful breach v, was used. Data was gathered to support the use of the model.

It was estimated that three ruptures had financial impacts of $11M, $12M and $135M. The range for impact was set $\lambda = [\$10M, \$150M]$. According to [19], t was set to 90%, since surveys showed that nine out of then organizations encounter a cyber incident each year. The likelihood of successful breach was set to 46%. This figure was based the average of two potentially overlapping values reported by surveys: 59% of detected incidents caused physical damage and 33% caused a business interruption. [19, 20]

Another way to obtain cyber security data is to use simulations or create experimental data using ICS or SCADA testbeds. [21] Testing in a live system is difficult, as there have been cases where an internal system scan has caused disruptions in the ICS operation, which is intolerable due to the availability constraints of these systems. Thus, for live analysis, a test bed must be used. Surveys, such as [15], can be used to collect data from organizations that have suffered from a cyber incident.

Upon discussion with Finnish electric utilities, it was concluded that standard compensations for power cuts are can be the most important source of monetary loss. Customers must be compensated for interruptions unless the electric utility or electricity retailer can show that the cause was unavoidable and unforeseeable by reasonable efforts. In Finland, these compensations are regulated by Electricity Market Act (588/2013). [22] The compensations are calculated from the annual network service fee of the customer and vary depending on the lengths of the interruption. For example, the smallest compensation is 10% of annual network service fee for an interruption between 12 to 24 hours. A 100% compensation is granted for an interruption length of 120 to 192 hours. The compensation is capped at 200% of the annual network service fee, that is granted for a power cut longer than 12 days. The absolute value of the compensation is capped at 2000€ per customer.

2.4 Cyber security controls and countermeasures

Since cyber risk management is a complex topic, several standards have been developed to aid the decision making and implementation of cyber security policies and procedures. While standards developed for IT centric risk management may apply also to cyber security, the ICS dependent organizations need a separate approach due to the criticality and availability constraints, complexity and design issues. Such standards are provided by several organizations, including ISO/IEC, NIST, North American Electric Reliability Corporation (NERC), United States Department of Homeland Security (DHS) and many national information security organizations. These standards offer guidelines for cyber security decision makers to create cyber security plans, identify vulnerabilities, threats and impacts and select suitable controls to mitigate. [5, 23, 24]

Robustness and resilience against cyber incidents must be considered on several levels. Typically, the cyber security controls should follow a defence-in-depth strategy, which means series of security controls and separation of information systems into layers based on their criticality, with increasing levels of security. [5] Foremost, organizations should have a risk management process that sets the goals and controls for cyber security. In order to prioritize impacts, organizations should have a clear understanding of the business process and the assets and resources needed to execute it. Thus, asset management is required, which further extends to inventories of information system resources, including configurations, backups, maintenance and authorization. The critical assets should be redundant and operate on redundant networks, for example using a ring topology. Vendors often have access to information systems in ICS environments. Thus, such connections should be documented, and contracts should include cyber security clause. [5, 25, 26] On a more technical level, networks should have domain separation and zoning or layering. The most critical systems should be on the most secure network separated from the less secure networks used for less critical operations. Networks should have firewalls at boundaries and within the layers. This helps containment of possible incidents. Further, the networks should be monitored for intrusion and malicious actions. Information assets should be patched if possible and correctly configured with limited access rights. [5, 23, 25] Humans pose a threat to information systems. Organizations should manage and monitor access. Actions of personnel should be monitored and identified. Insider policy should be in place and personnel should have adequate and role-based cyber security training. Cyber threats also have a physical dimension, hence physical security should be considered together with cyber security. [5, 24, 25]

There are often challenges related to implementation of cyber security controls and countermeasures. Organizations face ethical, environmental, cultural, personnel, financial, time, operational, and technical constrains. In the ICS context, especially technical and operational constrains are prevalent. [24] Since ICS systems have high availability requirements, patching and configuration changes can be rarely done. The life cycle of ICS components is much longer than that of IT components and new security features cannot be accommodated. Thus, cyber security controls need to be executed at the boundaries of network and by setting rules for operations of the organization.

2.5 Cyber risk management process

The cyber risk management process should be a systematic way for organizations to identify, analyse and evaluate cyber risk as part of the overall risk management process. It should serve as a starting point for actions and plans to mitigate cyber risks. ISO/IEC 27000 family of standards adopts the risk management process from ISO 31000 standard. The high-level view of the process is in Figure 2. The process should be an iterative one. [24] The base of the cyber risk management process is the definition of goals and current status of cyber security. The context establishment step should include the identification of system and its components. The value of assets and business functions should be identified with respect to the performance of operations as part of the risk identification process. This step should also include the identification of threats and threat sources. The risk analysis step is often based on the business impact analysis, which are based on scenarios and their direct impacts. The problem of this approach is the lack of data about and dynamic nature of cyber risk. The risk treatment process includes avoidance, mitigation, transfer and retention of cyber risks. Complete avoidance is impossible in a modern world, thus mitigating risks is the more popular approach. The mitigation strategies include controls mentioned in Section 2.4. Cyber insurance can be used as a risk transfer method. The residual risk after the insurance and mitigation strategies must be retained. The cyber risk management process must be continuously updated through the risk monitoring process, because the cyber landscape is constantly changing. [27, 28] NIST divides the risk management process into four components: framing, assessing, responding and monitoring that should be used on three tiers: organization level, business process level and information system (IT or ICS) level. The objective of the risk management process should be to continuously improve the risk-related activities of the organization. [5]

There is an ongoing shift in risk management from system robustness to resilience. While robustness requires the system to be hardened against certain threats, resilience approach emphasises the recovery capabilities of the system. A robust system can withstand incidents, but once something breaks the system, the recovery is difficult, whereas a resilient system could lose some of the functionality but is able to recover back to a fully operational state0. [1]

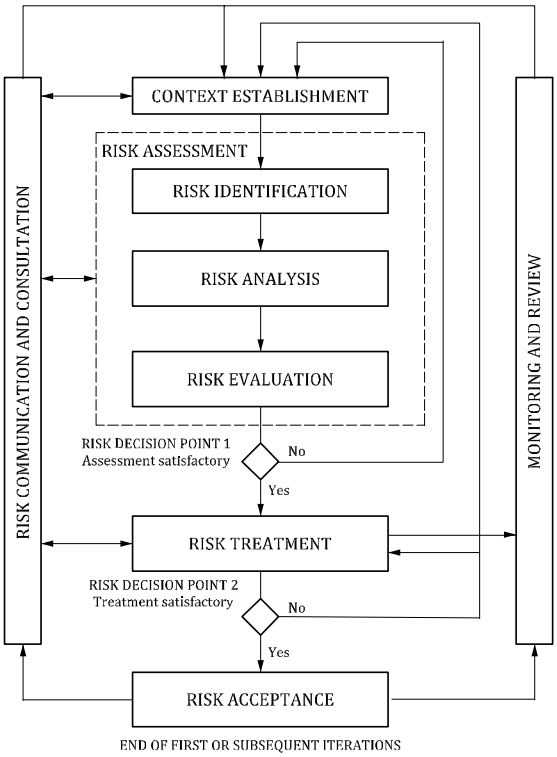

Figure 2: Information security risk management process according to ISO/IEC 27000 family of standards. [24]

2.5.1 Cyber security standards

Several cyber security standards have been created to aid the decision makers in industrial organizations. Some standards provide a general cyber security perspective, while some methods focus on ICS or CI applications and/or provide more technical perspective. ISO/IEC 27000 family of standards, NIST800-82 and ISA/IEC 62443 (ISA99) family of standards are some of the popular standards used especially in the energy sector. [5]

Despite these standards have been updated, a slightly outdated comparison by Sommestad, Ericsson and Nordlander [9] still highlights the different approaches

in standards. The comparison covered SCADA security standards *Good Practice Guide, Process Control and SCADA Security* by Centre for the Protection of National Infrastructure, *Cyber Security Procurement Language for Control Systems* by Department of Homeland Security, *21 steps to Improve Cyber Security of SCADA networks* by U.S. Department of Energy, *CIP-002-1 - CIP-009-1* by North American Electric Reliability Corporation, *Guide to Industrial Control Systems (ICS) Security* and System Protection Profile – Industrial Control Systems by NIST, *ANSI/ISA-99.00.1-2007* by the International Society of Automation and *Cyber Security for Critical Infrastructure Protection* by U.S. Government Accountability Office. These standards are also compared to more general international cyber security standard *ISO 27002 (previously called ISO/IEC 17799).* The document quantitatively analysed most common countermeasures suggested by the standards. It was observed that the standards place a different weight to countermeasure groups. Most common countermeasures recommended were authentication, cryptography, firewall, auditing and vulnerability scanning, intrusion detection and authorization. The least popular countermeasures were security organization, system administration tools and system resilience. Also, threats were analysed using same the methods. The focus of the standards was on malicious code, denial of service, spoofing, replay, interception and modification of data, information gathering and threats from employees. The attention to human aspect was modest while the emphasis on malicious code dominates the standards. The paper states that many electric power utilities rely on the more general *ISO 27002* standard which puts more attention to administrative and organizational issues such as security organization, security policies, business continuity and third party collaboration. Compared to SCADA security standards, the *ISO 27002* puts clearly less weight on technical countermeasures such as firewalls. The authors recommend that users of *ISO 27002* should adapt also more technical countermeasures from other SCADA cyber security standards. [9]

While ISO/IEC 27000 family of standards is a general-purpose information security standard, it is used also in an industrial context. While most of the ISO/IEC 27000 documents do not provide direct instructions, they serve as a starting point for risk management and provide guidelines for cyber risk management process and risk controls. ISO/IEC 27019 document provides guidelines for energy utility industry. ISO/IEC 27019 redefines and supplements ISO/IEC 27002 controls to suits the needs of the energy utility industry (excluding nuclear energy). [23, 29]

2.6 Risk assessments methods and challenges

In general, risk analysis methods can be divided into two major categories: qualitative and quantitative. Qualitative methods aim to utilize expert assessments, relative importance or likelihood of incidents without statistical approach. Commonly this is done by assessing labels, such as "high", "medium" and "low". A traditional example of qualitative risk analysis method is the development of risk matrices, in which probability and impact are estimated and used to find focus for actions and countermeasures. [30] Classification into quantitative and qualitative methods is not binary as some risk analysis methods can be described as semi-quantitative. Some risk matrix methods can be extended to semi-quantitative ones. These are widely used in risk analysis despite their limitations. While risk matrices lack mathematical robustness of quantitative methods, they are still a useful tool, as they are well received in many industries due to their intuitive graphical presentation and easy-to-apply-and-understand nature. [31] Quantitative methods utilize probabilities and statistics to estimate the risk objectively. Probabilistic risk assessment (PRA) and the extensions of it are one of the most commonly used risk assessment methods. Due to the widespread use and relative importance, PRA and extensions will be reviewed in more detail. [32]

Many probabilistic risk assessment methods are scenario-based. These methods use the definition of risk presented in Eq. 1 by finding the set of undesired events and end states and corresponding initiating events that can lead to these states. These methods can combine historical data with expert assessments as the basis for probabilities needed to. PRA can be combined with fault tree analysis (FTA) and event tree analysis (ETA). FTA is a deductive method that graphically represents the system of interest. It can be used to model logical relationships between systems so that the cause of a component failure can be extrapolated backwards in the system. In the context of ICS, this means that a system failure can be traced through the IT and OT system. This also means that the system must be extensively covered to ensure that all (or at least the most important) paths that can cause a failure are considered. The method needs also failure data as an input, and for ICSs, this often means an expert elicitation. The method is more suitable for predicting component failures. ETA is similar to FTA but uses an inductive approach. In ETA, an initiating event starts a chain on actions, which leads to paths towards a failure. The yields a tree of conditional probabilities for success or failure at each node. This method, too, needs historical data or an expert elicitation. These two methods can be combined into a bow-tie analysis, where the path to an event is first deductively analysed using

FTA and then the consequences are inductively analysed using ETA. So far, the methods have not taken into account adversarial users. To handle adversarial events instead of just random failures, attack trees can be used. The method models a system as a tree, where an adversary can attack on an attack surface, from where on the attack scenarios are modelled through the system to see the probability and consequences if the attacker can reach the target component. Furthermore, the attack tree can be combined with FTA, ETA or bow-tie to broaden the coverage. Most of the problems related to PRA also apply to FTA, ETA, bow-tie and attack trees. [33, 34]

As previously seen, cyber risk assessment is one part of the risk management process. Risk assessment methods might cover one or multiple steps of the risk management process. A typical risk assessment answers three questions: what can go wrong, what is the likelihood of this happening and what are the consequences. Mathematically, the risk can be written as

$$R = \{s_i, p_i, x_i\}, i = 1, 2, ..., N, \tag{1}$$

where R is risk, $\{\}$ is set of N possible system damaging scenarios s, probabilities of scenarios p, and consequences x with suitable measure such as time or direct costs. For an ICS system, the previous equation can be interpreted as

$$R = tvx_{tv}, \tag{2}$$

where t is a threat, v is a vulnerability and x_{tv} is the consequence of a threat exploiting a vulnerability successfully. This means that the adversary, either external or internal, must find a vulnerability that is successfully exploited in order to cause consequences. There are also several other metrics that are used to quantify the security. *Core metrics* measure the number of vulnerabilities in the system with information drawn from vulnerability databases. *Structural metrics* measure the path length from attack to attacker's goal node, for example by evaluating the shortest path or mean path length. Also, resilience of a system can me modelled, measured and analysed. [1, 33, 35, 36]

2.6.1 Risk assessment methods in CI and ICS

General risk assessment methods have several extensions designed for risk analysis in critical infrastructure, industrial control system and SCADA environments. The categorisation of ICS risk assessment methods is not easy. In [34], the current

state of the decision science is reviewed to improve cyber security of ICS. In this paper, more than dozen different technique categories were identified. Many of these are closely related, such as very common probabilistic risk assessment methods, which can be combined with fault tree analysis (FTA), event tree analysis (ETA), bow-tie analysis, attack trees. Other categories include Monte Carlo simulations, Markov models, failure modes, effects and criticality analysis, hazard and operability (HAZOP) method. Cherdantseva et al. (2016) use different categorisation methods to classify SCADA risk assessment methods in their review of 24 risk assessment methods used in or developed for SCADA environments. [33] Level of detail and coverage can be used to divide methods into *guidelines* which broad coverage and low level of detail with a set of steps for the user, *activity-specific methods* which cover narrower part of the risk management process but with greater detail, and *elaborated guidelines* which may cover all the stages of risk management process with high level of detail at each stage. Cherdantseva et. al (2016) categorize most of the methods reviewed into *activity-specific methods*. The SCADA risk assessment methods can also be divided into *formula-based* or *model-based methods*. The former are based on mathematical model of the risk with a set of formulas. Supporting information is presented in tabular or textual form. The latter are based on a graphical model supporting the use of mathematical models and qualitative analysis. This analysis is often probabilistic. These methods can be further classified into *graph-based models* and other models. Even further, the *model-based methods* can be divided by their *attack- or failure-oriented approach*, *goal-oriented-approach*, or *dual approach*. A more traditional approach is to categorize the methods into *quantitative* or *qualitative methods*. The 24 methods included in [33] and their categorisation are in Table 2. Some of the methods reviewed in [33] will be discussed more closely shortly, along with other methods from the literature.

Table 2: Articles in [33].

Author(s)	Year	Method title	Category 1	Category 2	Category 3
Baiardi et al.	2009	Hierarchical, Model-Based Risk Management of Critical Infrastructures	Probabilistic	Model (D)	Elaborated guideline
Beggs and Warren	2009	Cyber-Terrorism SCADA Risk Framework	Qualitative	-	Guideline
Byres et al.	2004	Attack Trees for Assessing Vulnerabilities in SCADA	Qualitative	Model (A)	Activity-specific method
Cardenas et al.	2011	Risk Assessment, Detection, and Response	Probabilistic	Formula	Activity-specific method
Chittester and Haimes	2004	Risk Assessment in GPS-based SCADA for Railways	Qualitative	Model (G)	Activity-specific method
Francia et al.	2012	CORAS-based Risk Assessment for SCADA	Qualitative	Model (A)	Activity-specific method
Gertman et al.	2006	Scenario-based Approach to Risk Analysis in Support of Cyber Security	Probabilistic	Formula	Elaborated guideline
Guan et al.	2011	Digraph Model for Risk Identification and Management in SCADA Systems	Non-probabilistic	Model (G)	Activity-specific method
Henry and Haimes	2009	Network Security Risk Model (NSRM)	Probabilistic	Model (A)	Elaborated guideline
Henry et al.	2009	Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis	Non-probabilistic	Model (A)	Activity-specific method
Hewett et al.	2014	Cyber-Security Analysis of Smart Grid SCADA Systems with Game Models	Probabilistic	Model (A)	Activity-specific method
Le May et al.	2010	Adversary-driven State-Based System Security Evaluation	Probabilistic	Model (A)	Activity-specific method
Markovic-Petrovic and Stojanovic	2014	Improved Risk Assessment Method for SCADA Information Security	Probabilistic	Formula	Activity-specific method
McQueen et al.	2006	Quantitative Cyber Risk Reduction Estimation Methodology	Probabilistic	Model (A)	Elaborated guideline
Patel and Zaveri	2010	Risk-Assessment Model for Cyber Attacks	Probabilistic	Formula	Activity-specific method
Patel et al.	2008	Two Indices Method for Quantitative Assessment of the Vulnerability of Critical Information Systems	Probabilistic	Model (A)	Activity-specific method
Permann and Rohde	2005	Vulnerability Assessment Methodology for SCADA security	Not specified	-	Guideline
Roy et al.	2010	Attack Countermeasure Tree	Probabilistic	Model (A)	Activity-specific method
Song et al.	2012	Cyber Security Risk Assessment in Nuclear Power Plants	Qualitative	-	Guideline
Ten et al.	2010	Cybersecurity for Critical Infrastructures: Attack and Defence Modelling	Probabilistic	Model (A)	Elaborated guideline
Woo and Kim	2014	Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems	Non-probabilistic	Formula	Activity-specific method
Yan et al.	2013	PMU-based Risk Assessment Framework for Power Control Systems	Probabilistic	Model (A)	Elaborated guideline
Yu et al.	2006	Vulnerability Assessment of Cyber Security in Power Industry	Probabilistic	Formula	Activity-specific method

The approach by Patel and Zaveri [37] identifies attack types, probabilities of attacks and their impacts in terms of control loss, product loss, staff-time loss, equipment damage and prevention. A revenue loss function is used to estimate total probable financial losses. They use a real-life example of chemical engineering plant, identifying seven attack types: replay (message capture and resending), spoofing (faking to be remote or master terminal unit (MTU)), denial of service (block control by spamming messages), control message modification, modification of MTU files, manipulate RTU responses or modify RTU files. They note that the impacts carried with these attacks are not mutually exclusive. The authors estimate the daily revenue of the system under both automatic and human control, also under loss on certain percentile of equipment. They also estimate the staff time loss for different percentiles of lost equipment and costs of equipment replacement and fixing in situ. The authors state that this type of model should be useful for determining insurance premiums and the users can update the system and modify it with, for example, non-linear cost structures. [33, 37]

One of the ways to model cyber risk is ADversary VIew Security Evalution (ADVISE) by LeMay et al. (2011). This approach is designed for system architects for the purpose of evaluating security trade-offs when deciding architecture. It models an adversary which plans several steps ahead and mimics real life preferences, goals and skills. The adversary has a decision function, which determines most attractive attack paths. [38]

Simulation methods, including Monte Carlo methods and Markov models, can be used to model a cyber physical system and its security. Monte Carlo simulation can be used to model the randomness of seemingly deterministic systems. In the Monte Carlo simulation, at each time step or iteration, a random number generator is used to determine whether a component of the system fails or not. Then, it can be analysed how a failure in some component affects the availability and operability, but it may also reveal new failure conditions. In the Markov model, the components of the system can transition from one state to another at each time-step. These models use the Markov property, which means that the system has no memory so that the previous state does not affect the probability of transition. It is also possible to use higher order Markov processes, where n previous states can be considered. Often these transitions are from normal state to failure, but other states are also possible. The method resembles the Monte Carlo simulation and offers similar advantages in terms of revealing previously unnoticed connections between the failures of the components. [33, 34]

Dondossola, Garrone and Szanto (2009) combine the cyber kill chain and test bed data with Markov model to test the risk of a SCADA system. They use the Cyber-Power Risk index $R_{ICT_{Power}} = \sum_j P^j \times (\gamma^j | P_S)$, where j is a specific intrusion type, P_j is the probability of successful intrusion and $\gamma | P_S$ is the impact factor of j conditional to P_S of system being in state S. The probability P^j is a composite of conditional probabilities of intrusion type, intrusion step, vulnerability, threat and attack successfulness.[21]

Bayesian networks (BN) are graphs that use Bayes' rule $P(A|B) = \frac{P(B|A)P(A)}{P(B)}$ to combine non-representative data with prior belief (experts' opinion) to form a posterior distribution. The model can be updated as new data is available, which makes the method flexible and it can solve some problems caused by the lack of data. However, the data of ICS cyber attacks is not often available. Bayesian networks can be extended into influence diagrams, which are a graphical way of presenting relationship between decisions and random nodes. Influence diagrams are similar to decision trees, but are often more flexible, since nodes do not have to depend on preceding nodes. Adversarial risk analysis is based on influence diagrams and game theory. These models allow systems to be modelled as stochastic networks, that feature random, decision and utility nodes. The model allows multiple players to interact, allowing users to model the actions and utility of an adversary using defend-attack, attack-defend, and defend-attack-defend graphs. These methods still need the system to be greatly simplified, similar to other methods mentioned before. [33, 34, 39, 40]

2.6.2 Challenges

Many of the risk assessment methods focus only on some parts of the risk assessment process. As noted in Section 2.5, risk management is a multistage process. Analysis of risk assessment methods has shown that most of the SCADA specific methods focus only on risk identification and risk analysis. Much less emphasis is placed on risk evaluation, context establishment, monitoring and review, and communication and consultation. In [33], none of the risk assessment methods reviewed established a process of comparing the results of risk assessment with risk criteria. Moreover, most papers did not discuss the acceptable levels of the risk metrics used. Cyber risks do not originate only from technical vulnerabilities, but also from non-technical sources, such as organizational cyber security culture or business processes. Especially quantitative methods often disregard the context establishment process and only focus on the network or system and its components. Such focus leaves many of the

non-technical risks out. [33]

Cherdantaseva et al [33] suggest that risk assessment methods should adopt a goal-oriented modelling approach, in which the successful operation is in focus, instead of considering what are the failure modes. These methods do not rely on historical data and can be used for incomplete sets of threats. They should also lay more emphasis on context establishment but also on risk identification and risk assessment stages. [33]

Probabilistic methods are the most common family of risk assessment methods for SCADA cyber security. They are also very prevalent in risk assessment in general, especially in the analysis of high reliability systems, when data is available. However, there are some obstacles. First, the models do not account for unknown threats, vulnerabilities or impacts. In Eq. 1, when the set of system damaging scenarios is formulated, it is limited to known scenarios or a subset of them. This also means, that it needs continuous updating in order to keep the vulnerabilities, threats and impacts up to date. It is often also impossible to cover all the threats and vulnerabilities, especially when using a attack- or fault-tree method, since the ICS systems are very complex and have indirect and feedback relationships, are time to time poorly documented, threats and vulnerabilities are unknown and constantly evolving and the computation and modelling suffers from curse of dimensionality. Probabilistic methods use historical system data to quantify the uncertainties, which is often not available, is not comprehensive or is subjective. Probabilistic methods also often disregard high-impact low-frequency, often called as black swan events, which may have a catastrophic impact on the organization. [33, 34]

There are foundational and other challenges in risk assessment both in general and in critical infrastructure, specifically. Some foundational problems are related to terminology. There are several definitions of risk and no clear concept of uncertainty has been established yet. As discussed earlier, there are problems with the probabilistic risk assessment methods: they fail to address (lack of) information and knowledge that cannot be directly translated into probabilities. Especially in security applications, probabilities are problematic representation of knowledge. The attack probabilities are affected by the risk management process, for example. Some issues are more related to risk assessment in critical infrastructure. One of the issues is the complexity of systems and system of systems to be considered in the analysis, feedback loops found in the systems, variety of threats and vulnerabilities of varying type. [1, 32]

Zio [1] presents a general outlook of a vulnerability and risk analysis goals

for CI. While not directly cyber related, he highlights important key points to consider when building a risk analysis framework. First, damage causing and loss inflicting event sequences should be identified relative to the planned objectives of a system. Second, initiating events and cascading effects to a system or its components should be considered. Third, the event set should be as complete as possible, yet manageable. This can be achieved by identifying the most important event sequences and clustering the less important ones into larger categories. Finally, (inter-)dependencies based on the initiating events, event sequences and outcomes should be analysed, along with couplings of different orders. He also mentions that systems must be modelled for the vulnerability and risk analysis to be feasible. The modelling should cover physical attributes, such as structure and dependencies, operation and management attributes, such as communication and human factors, performance and safety attributes, economic attributes, social attributes and environmental attributes. However, a single modelling methodology alone is not sufficient for capturing all the attributes of a CI system.

Two very different methods, penetration testing and game theoretic methods, have been proposed as a solution to the difficult task of ICS risk quantification. However, especially penetration testing is an inefficient method and no framework has been established for such an activity. IT and OT personnel often lack common vocabulary and a common architectural model understood by both parties is a necessity. Another problem with penetration testing is that ICS systems might not be able to cope with destructive testing. Thus, non-destructive methods are needed. One way to build data on ICS cyber risk is to use simulation tools. Test beds or cyber ranges offer a synthetic environment, where different scenarios can be tested. [34]

3 Methods

3.1 Requirements and limitations

The proposed risk assessment approach is to be used by a cyber security vendor organization. Often, the risk assessment methods are designed that organizations can on their own evaluate the risks using a risk assessment tool. If, for example, an electric utility assesses the risk themselves using a tool, results may be more biased than if an external vendor assesses the risks. The utility organization will now on be called a *target organization* and the cyber security vendor will be called a *vendor*. The aim of the approach proposed in this Thesis is to be a rapidly deployable, flexible and economic way to model risk in organizations relying on operational technology. The approach should be flexible so that the use of the model does not dramatically change between different sectors, while the input to the model might.

The approach will be used as a base for a risk assessment tool in a cyber security vendor organization. As an external vendor, the user of the tool does not have direct visibility and whole architecture of the target organization at hand. Thus, a questionnaire and interviews are to used to establish context and check current state of cyber security at the target organization. Based on identified business needs, experiences and literature, some requirements have been set for the risk assessment tool developed. First, in order to establish a common language and compatibility with the client, the risk assessment tool should be based on industry standards such ISO/IEC and NIST. This is to ensure that the target organization of the assessment understands the questions and can provide data for the risk model. The input for the underlying model presented later should include top-level architecture of the organization, interdependencies and current state of the cyber security. The model should have enough coverage to ensure reasonable risk estimates. It should also require limited input from the target organization. The model should result in a risk metric, whether may it be monetary, time or score. One of the requirements

is that the results for different target organizations can be compared. The risk assessment is done as one-off project, as required in the use case proposed by the vendor organization. However, if the cyber security environment or the current state of the cyber security of the target organization dramatically changes, the assessment must be redone. Incremental changes that have been planned but not executed during the assessment process can be added to the model later once completed. These requirements will be discussed later in more detail.

The approach must be quite inexpensive, rapidly deployable and flexible because at least Finnish electric utility organizations are moderate at cyber security spending. The risk assessment tool altogether draws needs from business perspective instead of academic. For the electric utilities, this risk assessment approach helps with risk analysis, asset identification and context establishment. The proposed approach is not designed to replace the risk management process, but to provide security decision makers in the target organization with an external view, discussions and recommendations. The tangible asset for the target organization is a report with description of the current state of cyber security, including cyber risk scores and key recommendations based on the findings and current industry best practices.

3.2 Modified annual loss expectancy

For risk assessment purposes, annual loss expectancy (ALE) can be used as a measure of cyber risk. In [27], the effectiveness of cyber security investments is analysed. In the article, annual loss expectancy ALE is used to measure the cyber risks. ALE can be defined as

$$ALE = SLE \times ARO, \tag{3}$$

where SLE is single loss expectancy and ARO is annual rate of occurrence. In [27], SLE is further decomposed into two components $SLE = AV \times EF$, where AV is asset value and EF is exposure factor. Moreover, ALE is used to cover the sum of direct losses DL_j related to attacks modified by indirect costs W_i and scaling based on the strength of the attack W_A such that ALE can be written as

$$ALE = W_A \prod_{i=1}^{N} W_i \left(\sum_{j=1}^{M} DL_j \right) \times ARO, \tag{4}$$

where N is the set of conditions that affect indirect costs and M is the set of different direct losses. Indirect costs include cover sanctions, environmental damage and recovery costs, while direct loss includes costs related to interruptions and failures in

production process. [27]

The ALE formulate presented in [27] has some shortcomings, such as the estimate being zero if any indirect cost is zero. Thus, some changes are necessary, also to incorporate some requirements mentioned earlier. The estimation of loss is a difficult task in complex process control environments. Direct book value of assets is not sufficient measure of loss. Hence, the impact of attack strength and effects on system performance should be accounted for. [27] Instead of annual or single loss expectancy, a loss related to downtime of business function is used in this assessment. The loss related to disruption or downtime of the functions can be estimated from perspective of loss of revenue, damage to assets and compensations, all considered as direct costs in this risk assessment approach. The use of functional reference model presented in Section 3.4 makes it possible to analyse the business process and costs related to incident in different business functions. The analysis of indirect costs will be excluded from the assessment, because direct costs are considered more relevant for coverage of the analysis. The definition of direct costs includes some costs that [27] considers indirect, such as the standard compensations.

In the risk model, the strength of attack modifiers are based on a sector specific tables, which summarize available data and expert assessments. Further, the strength of attack will be modified based on the current state of cyber security controls and processes in the target organization. The modifiers will be discussed more in Section 3.3. In essence, the cyber security controls are mapped against different incident categories and positive actions reduce the strength of attack. The direct loss DL_j includes costs directly related to loss of service in different business functions. The downtime cost of business functions is estimated based on expert assessment and interviews with target organization. The model can be modified to use downtime instead of costs related to it instead if necessary. Based on the discussions with Finnish electric utilities, standard compensations are major source of costs related to downtime of services. Thus, indirect cost modifier W_I is excluded. Also, instead of annual rate of occurrence, the ALE function is modified to accommodate the changes, such that is becomes

$$modifiedALE = \sum_{i}^{N} \sum_{j}^{M} W_{A_{ij}} \times DL_j \times LH_{A_i}, \tag{5}$$

where W_{A_i} is the strength of attack of different incident categories, DL_j is the cost of downtime and LH_{A_i} is the likelihood of incident category, N is the number of incident categories or cases and M is the number of business functions included in

the analysis. The data to support the model will be discussed next.

3.3 Cyber security questionnaire

To build the model and use it effectively, some data must be obtained from the target organization and used in the model to effectively convert the input data into a good output. Since it is suggested in the literature to use monetary or other metrics to measure the impact of a cyber incident, relevant but not directly applicable data can be used to support the model and assessment of impacts for sector specific incident and impact tables. A failure of an ICS component can be caused by bad luck, accident or a malicious action in both physical and cyber environment, but the impact is almost always physical due to the cyber-physical nature of the system. This means that data for normal production disruptions and respective costs can be used to model also cyber incidents. Impacts of failures can be also measured on business function level. This allows to model the system at functional level instead of component level which reduces the dimensionality of the system.

In order to generate a quantitative risk level for an organization relying ICS, input data for the model is needed. A questionnaire and interviews with key security personnel and business owners are essential part of establishing context. The interview and questionnaire process strongly aid the context establishment process, which is often lacking. [24, 33] Interviews also highlight discrepancies within the organization. Instead of simply allowing the target organization of the risk assessment fill a questionnaire, answer can be cross-checked with different people. It also helps to assess the current state of cyber security plans and procedures, which are often created and then updated on ad-hoc basis without proper steering. A questionnaire highlights the critical factors of cyber security of the organization. [41]. The questionnaire and interviews alone are useful for the client of the risk assessment, as it forces them to consider and explain their processes to an external security analyst. All organizations benefit also from an objective review of cyber security controls and processes. Organizations often focus on external threats, while internal threats are equally important. The discussions also reveal the engagement and attitude towards cyber security at different levels of management. Cyber security decisions might be made by insufficiently cyber aware decision makers, such as by plant manager, who might not have any education or training on cyber security. The organization as a whole must be engaged into the cyber security control and process decision making and central management and business units must cooperate. [41] The interviews are the most important step of the risk assessment process and require most input and

time from both the target organization and the vendor. Key security personnel, such as chief information security officer, chief information officer, chief operations officer, chief financial officer, chief security officer, IT personnel, business unit owners and maintenance managers. The availability and responsibilities in cyber security affect the time needed for the interview. Often chief information officer or information security officer along with IT department is responsible for execution of cyber security. Thus, most of the interviews and discussion can be done with the information or security department. These discussions often require several hours. Discussions and cross-checks with business unit owners and similar managers require less time. The interviews, review of the system and business architecture and cross-checks require approximately two working days. Further, the target organization is expected to be able to provide the required input data. An example of the questions is in Figure 3. The answer can be supported with clarifying comments, if necessary.

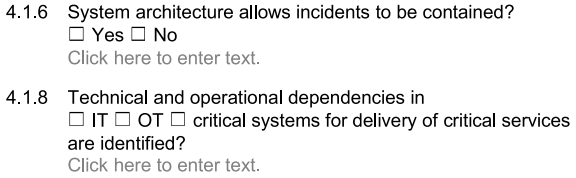

Figure 3: Example of questions used to assess the current state of cyber security.

The questionnaire follows the contents of ISO/IEC 27000 family of standards and NIST 800-82 standards. Since ISO/IEC is more risk management process oriented, more technically oriented NIST standard is used also. The benefits of NIST 800-82 standard are the technical components and the classification of controls. Baseline controls have been categorised into low-medium-high classes based on the impact level of ICS. This allows the model to weight the importance of different controls and approached adopted by target organizations. Using the NIST categorisation, controls can be mapped against different levels of incidents based also on the skills set of threat profile, because typically the high-level controls are against more sophisticated attacks. The use of standards also helps to establish a common language with the client. Based on the interviews with Finnish electricity distribution organizations, ISO/IEC standards are mostly used. ISO/IEC 27019:2017 standard includes cyber security controls for energy utilities. [5, 23, 24, 25, 29] ISO/IEC 27019:2017 standard provides information security controls for the energy utility industry. This standard is used in this example to focus the questionnaire for use in energy sector. Compared to ISO/IEC 27002:2013, the standard provides controls more suitable for ICS and energy utility industry use. On a high level, 14 different topics are used to divide

the controls into different categories. Controls found in NIST 800-82 have slightly different focus than the ISO/IEC 27019:2017. While the comparison in Table 3 is not exhaustive as only topic levels have been matched to best effort, it can seen that there is some differences in focus. NIST standard emphasises operations security with several different topics against only one found in ISO/IEC. While this comparison is crude and many of the topics on either standard could be matched against several if they were split, there is a good reason to use both to cover different aspects of controls against cyber threats. A deeper look into the standards shows that NIST has more technical detail whereas ISO/IEC focuses more on the coverage and process. ISO/IEC standard emphasises more supply chain security, which is one of the most important attack vectors but often overlooked. Many organizations allow third parties, such as vendor or suppliers to have physical or logical access to critical systems, creating a path for attack where organizations depend also on the cyber security of third party. The standards go much more into detail than Table 3. Especially the NIST standard establishes very concrete recommendations for cyber security controls. [5, 23, 29]

3.4 Functional reference modelling in ICS

In the financial industry, operational risk and its quantification are interest to regulators, academics and practitioners. Operational risk is defined by Basel Committee as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". [42] While the definition of operational risk is done with financial industry and organizations in mind, it is applicable to any industry. Industrial control systems are an essential source for risk stemming from human errors, failures in internal processes and external events. While many methods have been developed for operational risk quantification in financial industry, they do not generalise well to other industries. [43] Nevertheless, operational risk in other industries can be studied by modelling the risk flow of the organization. Businesses model their operations and functions by vertically splitting them or analysing different flows (monetary, information, product or service). Identification and analysis of flows offers and end-to-end visibility to interconnected sub-functions and processes. [43]

The risk flow approach allows to identify and analyse the two components of operational risk: direct and indirect costs. Direct costs have only a financial impact and they do not affect the flow. As there is no network effect, the direct costs can be summed. An example of direct cost is a repair of a machine that is not in use. Indirect costs, on the other hand, have a network effect which makes analysis more difficult. For example, a machine failure causes direct costs in terms of reparation,

Table 3: A high level comparison of ISO/IEC27019:2017 controls against information security threat for energy utility industry and NIST 800-82 controls for ICS. [29, 5]

ISO/IEC 27019:2017	NIST 800-82
Information security policies	Organization-wide information security program management controls
Organization of information security	Risk management
Human resource security	Personnel security
	Awareness and training
Asset management	Media Protection
Access control	Access control
	Identification and Authentication
Cryptography	
Physical and environmental security	Physical and environmental protection
Operations security	Auditing and accountability
	Security assessment and authorization
	Configuration management
	System and information integrity
	Planning
Communications security	Systems and communications protection
System acquisition, development and maintenance	Maintenance
	System and services acquisition
Supplier relationships	
Information security incident management	Incident response
Information security aspects of business continuity management	Contingency planning
Compliance	

but also indirect effect by affecting the flow, causing the failure to cascade in the value chain. [43] The cascading effect is especially prevalent in industrial control systems, where highly interconnect complex systems are used. The indirect costs are often much important as was found out during discussions with Finnish electric utilities. Some utilities noted that standard compensations are the largest cost of a typical power outage, before equipment repair costs or loss of income.

In [44], hierarchical graph representation is used to model robustness of system-of-systems critical infrastructure. The method models the components and product or service flows in CI and measures the delivery capability of the system as metric for robustness. The modelling of the system is done by identifying the input (production), demand (load) and transmission arcs, also allowing feedback loops. The paper also presents clustering techniques to reduce the complexity of the system to different levels of detail. While the clustering reduces the levels of detail, it allows for an elementary analysis of the robustness with reduced time use. The results show that

using clustering and hierarchical graph representation, results between different levels of detail provide consistent results. While the original method simulates a critical infrastructure and system-of-systems, in this work similar approach of dimension reduction is applied on a single organization level. In a similar fashion of using a clustering technique to reduce the dimensionality, functional reference modelling approach will be used to reduce dimensionality. This suits the needs presented in Section 3.1, as it streamlines the application process, and helps use of same framework structure to different sectors of critical infrastructure by changing necessary components. [44] However, compared to the hierarchical graph representation, the proposed approach further simplifies the modelling and relates more to business process modelling. While Figure 4 includes many processes and functions, only a critical subset of functions is needed for the analysis of the cyber risk, as many of the components do not result in loss of production or distribution of electricity or heat. Thus, a flow approach is used to identify necessary components based on the interview with the target organization. The dependencies of the functions are also considered, allowing risk flow to be influencing factor in the total cyber risk. [43] The dependencies are used as a weighting factor in the modified ALE formula. The functional modelling can be also used to model the dependencies in the system. If the functions are highly connected and dependent on each other, a cyber incident has more dramatic effects. Such dependencies and interconnections should be considered in the risk assessment. High interconnectedness creates cascading events, especially if larger infrastructure is considered. [1, 43] The functional reference model can be also extended if other functions exist. The model is scaled according to number of business functions.

Another benefit of relying on a functional model of the organization is that it requires the participation of different business lines and owners to the risk assessment process and adequate documentation and communication between central management and business lines. This also allows the identification of importance of functions and the analysis of cascading effects, as dependencies can be modelled between functions. The simplified model of organization also allows the analysis of whole organization. The dependencies between business units can be modelled between functions in different branches or between the functions of business units and central management components. The dependencies further increase or decreases the cyber risk. [46] The target organization should be able to provide business architecture, which is often relatively close to functional architecture, or can be translated into such. If such documentation does not exist, more time is required to build the func-

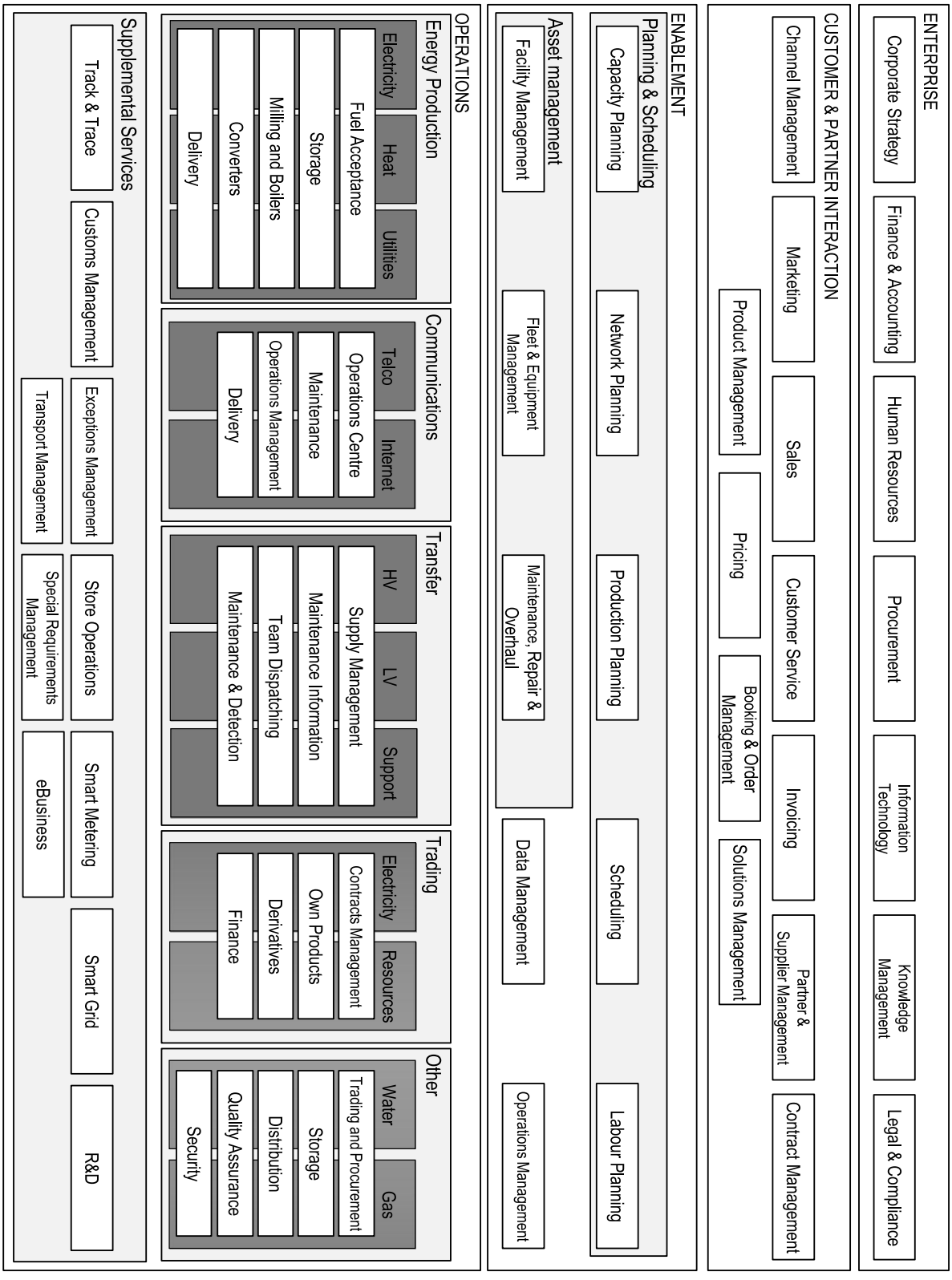

Figure 4: Example of functional reference model for an electric utility organization. [45]

tional architecture and the dependencies. The lack of documentation also affects the strength of attack modifiers. If the organization does not have clear understanding of the business process and architecture, it is difficult to respond effectively to possible cyber incidents.

The analysis of cascading effect should be limited in the analysis, otherwise the analysis may become too extensive. For example, if one were to analyse an electric utility company and a power outage, certain boundaries for the analysis of losses should be set to only analyse losses caused for the organization in scope. If one were to analyse, for example, the critical infrastructure of Finland and the society around it, a power outage will cascade to consumers of electrical power and cause losses there. The scope of the analysis should be clearly indicated. In this case, only the effects within the target organization's boundaries will be evaluated.

3.4.1 Incident and impact clustering

There is limited data on the cyber threats, vulnerabilities and impacts. In PRA, a complete set of threats must be established for the analysis to be exhaustive. However, this is rarely possible as new vulnerabilities emerge constantly, not all vulnerabilities are known and threat sources have varying motivations and skill sets. The concept of resilience emphasises the organizations ability to operate under changing conditions, whereas in traditional risk management, robustness against anticipated events is the focus of preparations. In cyber security, only some level of robustness can be achieved as threats and vulnerabilities are constantly evolving. By not resorting to fully probabilistic approach and using the concept of resilience as a guideline, exact set of threats may not be needed. This makes it possible to cluster the incidents. It can be argued that by considering incidents and different scenarios on a higher hierarchical level the need to identify and analyse all vulnerabilities and threats exploiting them is reduced. It is still possible to consider the skill set of the attacker, so that strength of attack is modified accordingly.

NIST proposition of ICS impact levels in Table 4 is based on ISA99 standard. It categorizes ICS impacts into low, moderate and high categories. [5] As another example, European Network of Transmission Systems Operators for Electricity categorizes incidents into four categories: Anomalies, Noteworthy incidents, Extensive incidents, and Wide area incident or major incident. The categorisation of ICS risks into these categories will compress the dimensionality. [47] For a resilient organization, the type of incident is not as crucial as for a robust organization, but more important is the ability to withstand and recover effectively form variety of incidents. Approaching

cyber security from this standpoint allows the categorisation of incidents and risks. [48] While the financial impact of incidents is still important, the damages and costs can be evaluated for different incidents based on expert assessment and statistics on actual incident cases.

Table 4: ICS impact levels based on ISA99 standard in NIST 800-82 standard. [5]

Impact category	Low-impact	Moderate-impact	High-impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life of limb
Financial loss	$1,000	$100,000	Millions
Environmental release	Temporary damage	Lasting damage	Permanent damage
Interruption of production	Minutes	Days	Weeks
Public image	Temporary damage	Lasting damage	Permanent damage

Based on the literature, statistics, reports and expert assessments, a table of incidents can be created. Incidents will be categorized based on their impact and similarity in other metrics, such as the threat source and skill set required. Common threat sources will be matched to different incident scenarios along with expert assessment of strength of attacks, which is a ratio with respect to downtime of different business functions and costs related to it. The strength of attack, however, is based on external data and not on the downtime costs of the target organization. Thus, the strength of attack modifiers are sector specific and objective from the perspective of the target organization. Strength of attack of different categories will be used to modify the client provided costs of downtime of different business functions. The strength of attack is also modified by the controls adopted by the target organization.

Further, the occurrence rate of incidents will be evaluated based on statistics and expert assessment. The occurrence rates will be recorded on a qualitative likelihood scale. This approach allows the controls and level of security to modify the strength of attack and occurrence rates of incident types. The mapping of controls to respective incidents can be supported by use of guides, such as [49], which maps operational cyber security risk to NIST 800-53 standard. The NIST 800-82 standard is an extension to NIST 800-53. [5]

4 Proposed approach

The proposed approach to cyber risk assessment is a combination of different methods. The model uses different types of input data to improve its validity and avoid problems related to purely quantitative or qualitative assessment. The use of different data sources is in Figure 5. The model utilises the modified annual loss expectancy as the mathematical model and available data and expert assessment are used to support the model. The impact and probability data are based on available statistics and data, combined with expert assessment. This approach to data should be acceptable considering the lack of statistical data of cyber incidents. Due to close resemblance to probabilistic methods, the proposed approach needs constant improvement. However, the process is less tedious due to incident modelling done on sector level instead of organizational or system level. The model also addresses the dependencies of different business functions using the functional reference model for the sector it is applied. The security control questions also highlight the importance of supplier relationships. [1, 26] Also, the target organization is involved in the risk assessment process by the use of interviews, questionnaire and functional modelling.

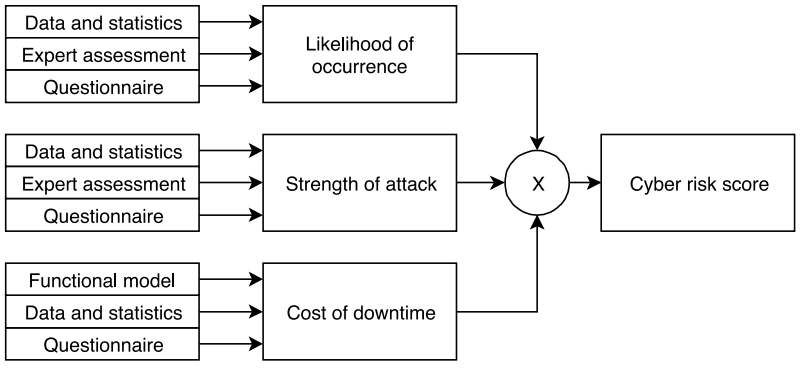

Figure 5: Proposed cyber risk assessment model and its data sources.

While the model and questionnaire component do not emphasize resilience over

robustness, the approach leans towards the concept of resilience, by clustering the cyber incidents instead of considering all separate event chains and controls against them. While the questionnaire and controls are based on the ISO/IEC 27000 family of standards and NIST 800-82, which do not emphasise resilience approach, some controls can be considered more resilience than robustness based. However, the role of respond and recovery was not considered adequate and those topics have been extended in the questionnaire, by adding questions of policies and controls. [1]

The proposed approach supports several phases of ISO information security risk management process. The functional modelling of the organization and operations can be considered context establishment, because they are done together with the client. Risk identification in the model is sector specific. It is not as in-depth risk identification processes as often is done. However, considering the requirements and limitations given for the model, the sector specific risk identification and clustering gives enough coverage. The proposed approach also covers the risk analysis and risk evaluation steps, by considering cyber incidents and controls in order to evaluate a risk score. Because this assessment is executed by an external party instead of the client performing it using solely their own resources, the risk communication and consultation can be considered to be covered. The produced report includes two layers of detail, one suitable for executive level and rest aimed at cyber security experts within the organization. [1, 24] The risk assessment can be performed rather quickly. The interviews and the questionnaire require one to two working days with the key security and management personnel of the target organization. After this, a report is created, requiring some analyst work hours. This, however, ensures that the client receives a tangible report on the current cyber risk, state of cyber security and some recommendations of actions. The proposed method is not designed to cover all the steps of the risk management process. Risk evaluation, monitoring and further actions are left for the target organizations risk assessment process. The vendor provided risk assessment should be used along with the target organization's internal risk assessment tools.

The process of the proposed risk assessment approach is in Figure 6. The process starts with the project proposal and once accepted, interview sessions can be scheduled. One to two analysts from the vendor organization are typically required to carry the initial presentations and the following discussion. If possible, the core cyber security team or IT department is interviewed first and then business line managers, CEO, CFO, and other managers are interviewed to verify the architecture and adapted cyber security controls. The cross-checking will highlight possible gaps.

The risk assessment tool is built as a Microsoft Excel template to ensure compatibility within the vendor organization. The questionnaire is also included in the template, allowing answers to be directly transformed into quantitative modifiers. Once the questionnaire is complete and verified by the target organization, the risk score is ready. At current state, report writing is manual process and requires one to two days from the vendor organization. It is possible to automatically populate some parts of the report and in future more of the report can be automated. It is still necessary to manually create content, as not all communication with the analysts and target organization representatives can be recorded in the questionnaire answers.

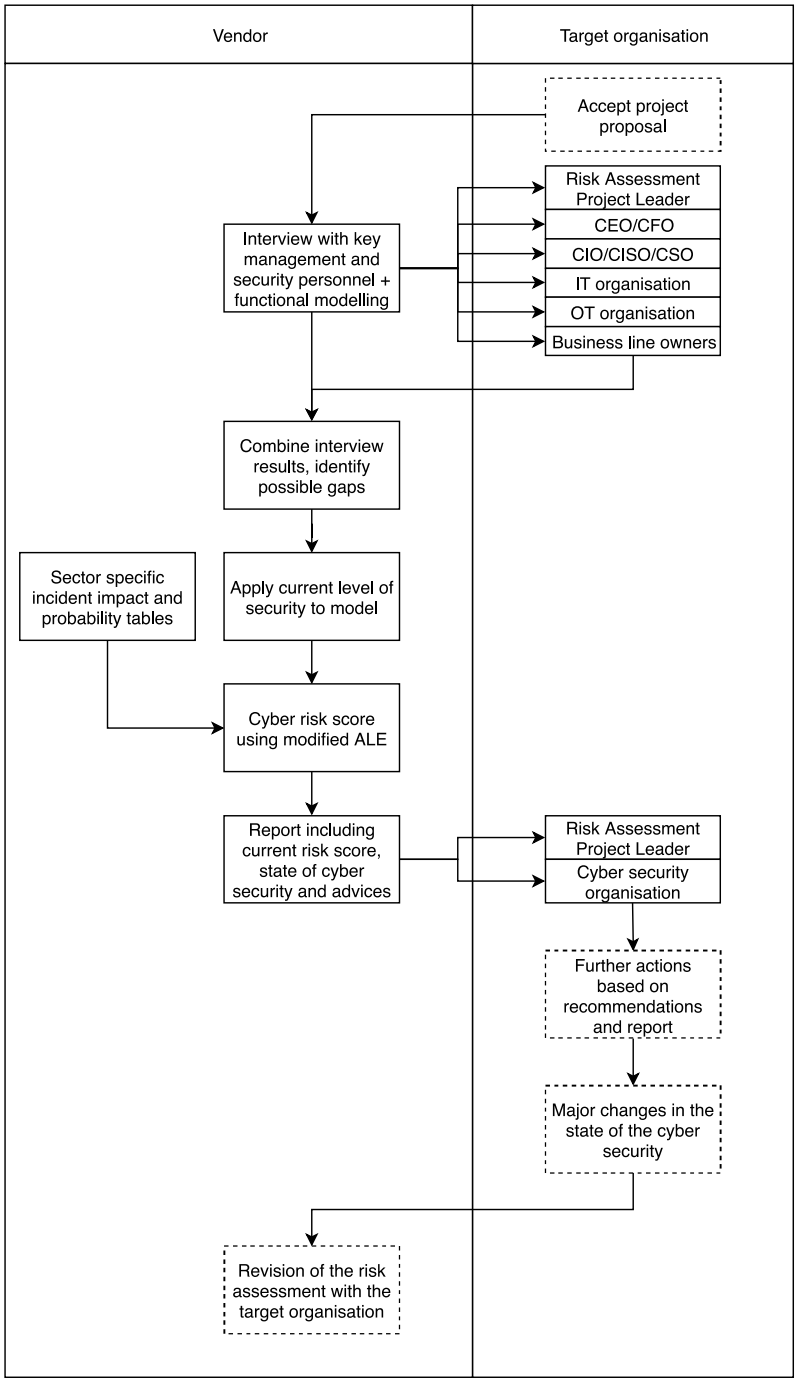

Figure 6: Example of the risk assessment process.

5 Discussion

5.1 Strengths of the approach

The aim of this Thesis was to create and describe a cyber risk assessment method for use in a variety of industrial organizations. It was required that the model should be based on cyber security standards. The proposed model offers a relatively easy to implement approach to cyber risk assessment for use with energy utilities that heavily rely on industrial controls systems. The approach combines qualitative and quantitative approaches into a semi-quantitative approach, in which statistics and expert assessments of monetary impacts and occurrence rates are scaled based on interviews and questionnaire with the target organization. The use of traditional methods in the CI risk assessment is not sufficient, but the analysis should be based on a combination of four different approaches according to [1]. These four approaches are topological, logical, functional and flow methods. In a sense, the proposed approach implements many of these. The functional reference model is a combination of the four methods mentioned and the modified ALE function with data drawn from statistics, experts and the organization itself can be considered at least partially logical method. The proposed method also aims to focus on the important cyber incident sequences and group the less important ones, as proposed by [1].

According to Cherdantseva et al [33], a "good" risk assessment approach should be comprehensive, adherent to evidence, logically sound, practical and politically acceptable, open to evaluation, based on explicit assumptions, compatible with institutions, conducive to learning, attuned to risk communication and innovative. [33, 50] Some of the requirements for "good" risk assessment are difficult to analyse but some are apparent. While the proposed approach is not revolutionary, it manages to combine different methodologies into one assessment. For example, both formula-based and model-based approach are used, counting for some levels of innovativeness. The proposed method focuses on risk communication and context establishment. The

management of the target organization is widely interviewed during the assessment process, which communicates the risks and risk awareness to different parts of the upper management. The organization also receives a report with an external view to the current cyber security status and culture along with key recommendations that CIO/CISO can use to communicate with rest of the management and organization. It also supports the learning of the target organization. The method is neutral politically, the logic is documented and the results do not depend on the risk inspector. Difficulties mostly arise from the incident impact and occurrence table, but they are same for all organization, thus resulting comparable results. Due to business value, the exact logic cannot be disclosed, thus not allowing review or evaluation. The proposed risk assessment method is not unique in that sense, commercial risk assessment tools often have business value that is wanted to be kept a secret.

One of the strengths of the proposed approach is that it requires a limited workload from both vendor and target organization, after the incident impact and occurrence tables, modifiers and questions have been set. The method does not require extensive modelling but aims to standardise organizations within each industry sector, in this case within energy sector. The standardized approach reduces costs and increase cost-benefit for the target organization, increasing the attractiveness of such assessment. During the discussions with the Finnish electric utilities it became apparent that organizations are somewhat hesitant on the cyber security spending. Thus, reducing the costs is important to increase the number of assessments and make it more available for smaller organizations with limited budgets. The method could be extended relatively easily to automatically create recommendations based on the threat landscape and current security status. The method could be also used to follow changes in the cyber security environment and later create automatic recommendations for organizations based on their previous state of cyber security and changed requirements. This could further increase the attractiveness of the risk assessment method.

Despite reducing the workload, the proposed risk assessment method covers several stages of the risk management process. The cyber risk management process based on ISO standards was presented in Figure 2. By using an interview and questionnaire, the proposed method can be used for context establishment purposes. Many other methods only focus on the network or technical components of the target organization, whereas the proposed approach includes also nontechnical questions and can exploit "hidden" information during the interviews. The workload is reduced by using the incident tables instead of separate risk identification for each target organization

and using the answers to questionnaire as the modifiers for the modified annual loss expectancy that acts as the risk metric in the risk analysis phase. Cherdantseva et al [33] concluded that little attention is paid to risk evaluation, which means that the results of the risk analysis are not explained. In the proposed approach, not only a risk score is given to the target organization, but the report also includes description of the current state of the cyber security and recommendations for future actions. Risk treatment and further steps are left for the target organization.

The proposed model can also be used in other sectors of business. This requires some changes in the questionnaire, because currently some of the questions are based on the ISO/IEC 27019 standard aimed for energy utilities. Nevertheless, most of the topics covered in the standard are applicable on other fields. Possible changes in the cyber incident tables are needed, since the cyber threats vary between different industries, especially if industries are more dependent on IT services than OT system. More changes are needed for the functional reference model, which are unique for each sector. Nevertheless, by creating sector specific components, the proposed approach can be used in different industries as long as they are dependent on industrial control systems.

5.2 Challenges and improvements

While the current state of the proposed risk assessment method is functional, there are some drawbacks and clear areas for improvement. The method has not yet been tested against other risk assessment methods to evaluate the produced risk scores. With the current use case, the risk scored do not have to be directly comparable with the outputs and risk scores of other risk assessment methods. Further testing and calibration of the model is needed along with updates to the controls and incident tables. The model does not currently emphasize the human factors more than what ISO/IEC 27000 and NIST 800-82 standards do. Zio [1] recommends that human factors should not be underestimated in the risk analysis of critical infrastructure.

One of the challenges of the model is related to the cyber risk metric itself, which is one of the requirements for a risk assessment method. [33] The risk metrics or security indicators are needed for informed cyber security decision making within the target organization. When modifiers are used, the metrics are comparable between different organizations. While monetary terms are used in the risk metric, the resulting scores do not reflect real cyber risk. In order to produce a more realistic risk metric in terms of time or money, the modifiers need to be adjusted to reflect better actual losses related to cyber incidents. One way to do this is to gather data from

organizations that have been assess before and have since suffered a cyber incident. Another way is to use real incident scenarios and estimate modifying weights based on these events. Either way, creating "realistic" risk score is challenging and it is more feasible to consider the produced risk score as a relative one. While the used cyber risk score is more abstract, the observations and recommendations in the report are more tangible for cyber security decision making.

The lack of cyber security data continues to be a problem for cyber risk assessments. When available, objective data is used, but currently expert assessments are needed to support the scarce data. The use of expert assessment also has some drawbacks. When used, attention should be paid to the techniques used to capture, formalize and transferring the expert assessments into numerical values. In the proposed approach, expert assessments are used with historical data whenever it is possible. Expert assessments may be even more valuable than some historical data. [33] This may be due to the rapidly changing threat environment. Reports and statistics may lag behind, or organization might not disclose publicly details of cyber incidents, while experts may have insight of the hidden details. One proposed method for combining expert assessments with statistics is fuzzy logic. Currently, the use of fuzzy methods is limited. [33]

One of the dimensions not covered in this description of the proposed risk assessment called strength of knowledge. The term is used to describe the uncertainty related to assumptions with respect to the criticality of the topic or component. The uncertainty and strength of knowledge should be analysed to improve the validity of the model. The strength of knowledge would inform the decision makers where the gaps in the analysis are and if surprises between the assessment and reality can be expected. Zio [1] recommends that strength of knowledge analysis should be focused on the most critical risk or criticality scoring. In the proposed approach, there are multiple ways to assess the criticality in order to focus the strength of knowledge analysis. One way is to focus on the incident scenarios that are expected to have major impacts. This is aided by the clustering of the incidents. Another approach would be to focus the strength of knowledge assessment based on the criticality of components identified in the function architecture review for each of target organization separately. A third approach would be to assess the strength of knowledge of the controls and related modifiers based on the NIST 800-82 ranking of the controls. While this is not done at the current state of the model, it would be beneficial and make the model more reliable. The strength of knowledge should increase the longer the model is in use and updated, when expert assessments can

be replaced with incident data, whenever it becomes available. The modifiers of strength of attack are most suspect to knowledge gaps, imbalance and bias, since the scaling of modifiers is difficult. While this is problematic in some ways since it can create imbalance to the risk score, it is acceptable in the use case, where risk scores are compared between organizations. This allows some ranking bias in the importance of the modifiers if the expert assessment is susceptible to it. Data and standards can be used to reduce the bias, as discussed earlier.

The model could benefit from Bayesian approach. Especially influence diagram-based modelling would be beneficial, since the functional reference model allows reduces the need for unique models. The use of influence diagrams could help transform the model more towards resilience, as several steps of incident from several threat sources could be simulated. [34, 39] The model does also not include the analysis of strength of knowledge. Implementing such a mechanism to the model would add important information to be used in the decision-making process. [1, 51] While more probabilistic approach requires more input, it might be a necessary change in the future to improve the method.

5.3 Conclusions

The cyber risk assessment in critical infrastructure continues to be challenging. Much research is still needed and while proposals for better methods exist, the cyber risk assessment methods struggle keeping up with rapidly changing cyber threat environment and complex networks found in industrial systems. The area needs cooperation between researchers, cyber security companies and organizations that need risk assessments. Organizations should be more open about the cyber vulnerabilities and incidents so that comprehensive databases could be collected. organizations should also invest more extensively in cyber security, which could boost advances in risk analysis and cyber security. The proposed approach avoids some of the common issues related to cyber risk assessment, but improvements are still needed. The proposed method consists of separate modules, allowing them to be updated as the research advances.

References

[1] E. Zio. Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 152:137–150, 2016.

[2] S. Nazir, S. Patel, and D. Patel. Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, 70:436–454, 2017.

[3] L. A. Maglaras, K.-H. Kim, H. Janicke, M. Amine Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz. Cyber security of critical infrastructures. *ICT Express*, 4(1):42–45, 2018.

[4] A. Kott, C. Aguayo Gonzalez, and E. J. M. Colbert. Introduction and Preview. In E. J. M. Colbert and A. Kott, editors, *Cyber-security of SCADA and Other Industrial Control Systems*, pages 1–13. Springer International Publishing, Cham, 2016.

[5] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication*, 800:82, 2015.

[6] National Institute of Standards and Technology Computer Security Resource Center. Operational technology. Online glossary, 2017. https://csrc.nist.gov/glossary/term/Operational-technology (Accessed 23.12.2018).

[7] A. Hahn. Operational Technology and Information Technology in Industrial Control Systems. In E. J. M. Colbert and A. Kott, editors, *Cyber-security of SCADA and Other Industrial Control Systems*, pages 51–68. Springer International Publishing, Cham, 2016.

[8] C.-N. Huang, J. J. H. Liou, and Y.-C. Chuang. A method for exploring the interdependencies and importance of critical infrastructures. *Knowledge-Based Systems*, 55:66–74, 2014.

[9] T. Sommestad, G. N. Ericsson, and J. Nordlander. SCADA system cyber security—A comparison of standards. In *2010 IEEE Power and Energy Society General Meeting*, pages 1–8. IEEE, 2010.

[10] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi. An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. In *3rd International Conference on Human System Interaction*, pages 679–686, 2010.

[11] E. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, 38(2):226–241, 2018.

[12] B. Hoffman, N. Buchler, B. Doshi, and H. Cam. Situational Awareness in Industrial Control Systems. In E. J. M. Colbert and A. Kott, editors, *Cyber-security of SCADA and Other Industrial Control Systems*, pages 187–208. Springer International Publishing, Cham, 2016.

[13] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 11:39–50, 2015.

[14] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318, 2017.

[15] B. Gregory-Brown. Securing Industrial Control Systems 2017. *A SANS Survey. SANS Institute*, 2017. https://www.sans.org/reading-room/whitepapers/ICS/paper/37860. (Accessed 23.4.2019).

[16] Ponemon Institute. 2018 Cost of a Data Breach Study. 2018. https://www.ibm.com/downloads/cas/861MNWN2 (Accessed 12.1.2019).

[17] Ponemon Institute. 2017 Cost of Cyber Crime Study. 2017. https://www.ponemon.org/library/2017-cost-of-cyber-crime-study (Accessed 12.1.2019).

[18] Business Advantage. The State of Industrial Cybersecurity 2017. 2017. https://go.kaspersky.com/rs/802-IJN-240/images/ICS(Accessed 14.2.2019).

[19] D. Young, J. Lopez, M. Rice, B. Ramsey, and R. McTasney. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14:43–57, 2016.

[20] The Aspen Institute. Critical infrastructure readiness report: Holding the line against cyberthreats. Technical report, 2015. https://www.thehaguesecuritydelta.com/media/com_hsd/ort/43/document/Critical-Infrastructure-Readiness-Report—Holding-the-Line-against-Cyberthreats.pdf (Accessed 24.3.2019).

[21] G. Dondossola, F. Garrone, and J. Szanto. Supporting cyber risk assessment of Power Control Systems with experimental data. In *2009 IEEE/PES Power Systems Conference and Exposition*, pages 1–3, March 2009.

[22] Sähkömarkkinalaki 588/2013 [Electricity Market Act 588/2013]. Online, 2013. Accessed 23.12.2018.

[23] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27002:2013. *Information technology – Security techniques – Code of practice for information security controls*, 2013.

[24] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27005:2018. *Information technology – Security techniques – Information security risk management*, 2018.

[25] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27001:2017. *Information technology – Security techniques – Information security management systems - Requirements*, 2017.

[26] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27036-2:2014. *Information technology – Security techniques – Information security for supplier relationships - Requirements*, 2014.

[27] J. Markovic-Petrovic and M. Stojanovic. An improved risk assessment method for SCADA information security. *Elektronika ir Elektrotechnika*, 20(7):69–72, 2014.

[28] M. Eling and W. Schnell. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5):474–491, 2016.

[29] International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 27019:2017. *Information technology – Security techniques – Information security controls for the energy utility industry*, 2017.

[30] S. E. Ramona. Advantages and disadvantages of quantitative and qualitative information risk approaches. *Chinese Business Review*, 10(12):1106–1110, 2011.

[31] H. Ni, A. Chen, and N. Chen. Some extensions on risk matrix approach. *Safety Science*, 48(10):1269 – 1278, 2010.

[32] T. Aven and E. Zio. Foundational issues in risk assessment and risk management. *Risk Analysis*, 34(7):1164–1172, 2014.

[33] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56:1–27, 2016.

[34] A. Cook, R. Smith, L. Maglaras, and H. Janicke. Measuring the risk of cyber attack in industrial control systems. In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016*. BCS eWiC, 2016.

[35] S. Kaplan and B. J. Garrick. On the quantitative definition of risk. *Risk Analysis*, 1(1):11–27, 1981.

[36] S. Abraham and S. Nair. Predictive cyber-security analytics framework: A non-homogenous Markov model for security quantification. *arXiv preprint arXiv:1501.01901*, 2015.

[37] P. Sandip and J. Zaveri. A risk-assessment model for cyber attacks on information systems. *Journal of Computers*, 5(3), 2010.

[38] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke. Model-based security metrics using ADversary VIew Security Evaluation (ADVISE). In *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, pages 191–200. IEEE, 2011.

[39] D. Rios Insua, A. Couce-Vieira, J. A. Rubio, W. Pieters, and D. Garcia Rasines. An adversarial risk analysis framework for cybersecurity. *arXiv preprint arXiv:1903.07727*, 2019.

[40] R. A. Howard and J. E. Matheson. Influence diagrams. *Decision Analysis*, 2(3):127–143, 2005.

[41] J. F. Broder and E. Tucker. *Risk Analysis and the Security Survey.* Butterwoth-Heinemann, Elsevier, Boston, MA, 2011.

[42] Basel Committee on Banking Supervision. *International Convergence of Capital Measurement and Capital Standards - A revised framework.* Bank for International Settlements, 2006.

[43] G. R. Finke, M. Singh, and S. T. Rachev. Operational risk quantification: A risk flow approach. *Journal of Operational Risk*, 5(4):65–89, 2010.

[44] E. Ferrario, N. Pedroni, and E. Zio. Evaluation of the robustness of critical infrastructures by hierarchical graph representation, clustering and Monte Carlo simulation. *Reliability Engineering & System Safety*, 155:78–96, 2016.

[45] Sectra AB. Functional Architecture. Adapted on permission of copyright holder.

[46] B. Suh and I. Han. The IS risk analysis based on a business model. *Information & Management*, 41(2):149–158, 2003.

[47] European Network of Transmission System Operators for Electricity. Incident Classification Scale. Technical report, 2018.

[48] P. E. Roege, Z. A. Collier, J. Mancillas, J. A. McDonagh, and I. Linkov. Metrics for energy resilience. *Energy Policy*, 72:249–256, 2014.

[49] L. R. Cebula, J. L.and Young. A taxonomy of operational cyber security risks. Technical report, Carnegie-Mellon University Pittsburgh PA Software Engineering Institution, 2010.

[50] Y. Y. Haimes and C. G. Chittester. A roadmap for quantifying the efficacy of risk management of information security and interdependent scada systems. *Journal of Homeland Security and Emergency Management*, 2(2), 2005.

[51] J. Shortridge, T. Aven, and S. Guikema. Risk assessment under deep uncertainty: A methodological comparison. *Reliability Engineering & System Safety*, 159:12–23, 2017.