energies

Article

Expert-Guided Security Risk Assessment of Evolving Power Grids

Seppo Borenius [1,*], Pavithra Gopalakrishnan [1,2], Lina Bertling Tjernberg [2] and Raimo Kantola [1]

[1] Department of Communications and Networking, School of Electrical Engineering, Aalto University, 02150 Espoo, Finland; pavithra.gopalakrishnan@aalto.fi (P.G.); raimo.kantola@aalto.fi (R.K.)

[2] Division of Electric Power and Energy Systems, KTH Royal Institute of Technology, 10044 Stockholm, Sweden; pavgop@kth.se or linab@kth.se

* Correspondence: seppo.borenius@aalto.fi

Abstract: Electric power grids, which form an essential part of the critical infrastructure, are evolving into highly distributed, dynamic networks in order to address the climate change. This fundamental transition relies on extensive automation solutions based on communications and information technologies. Thus, it also gives rise to new attack points for malicious actors and consequently, increases the vulnerability of the electric energy system. This study presents a qualitative assessment of power grid cybersecurity through expert interviews across countries in Europe and the U.S. to gain understanding of the latest developments and trends in the cybersecurity of future electric energy systems. The horizon of the assessment is 10 years spanning until the early 2030s. Thereafter, the study identifies how and to which extent the risks identified to be most significant are understood and addressed in the latest research and industry publications aiming at identifying areas deserving specific further attention. The most significant threats based on the assessment are False Data Injection (FDI), Denial of Service (DoS) supply chain, and ransomware and malware attacks.

Keywords: smart grids; power grids; cybersecurity; security risk assessment

Citation: Borenius, S.; Gopalakrishnan, P.; Bertling Tjernberg, L.; Kantola, R. Expert-Guided Security Risk Assessment of Evolving Power Grids. *Energies* **2022**, *15*, 3237. https://doi.org/10.3390/en15093237

Academic Editors: Paulo Fernando Ribeiro, Yuri Rodrigues and Maira Monteiro

Received: 23 March 2022
Accepted: 27 April 2022
Published: 28 April 2022

1. Introduction

The electricity sector has a central role in the decarbonization of the energy system and consequently, in the efforts to meet climate targets and to achieve net zero emissions. Efforts are now taking place to electrify industry, transportation, and heating. In addition, the power grids are evolving into dynamic meshed smart grids consisting of distributed, renewable low-inertia generation, electricity storage and active consumers. While this evolution is vital in order to address climate change, it also poses a challenge for grid management and control. Currently, distribution grids typically utilize communications and information technologies only in a relatively limited manner. In the future, the grid management and control challenge will require extensive automation solutions based on communications and information technologies. However, this fundamental transition will also expose the grid to attacks by malicious actors, thereby increasing the vulnerability of electric energy systems.

Real-world cybersecurity incidents show that power grid Information and Communication Systems (ICS) infrastructures, Supervisory Control and Data Acquisition (SCADA) and other critical infrastructure assets are primary targets for cyberwarfare [1]. Well-known cyberattacks targeting critical energy infrastructures include the attack on uranium enrichment facilities in Iran 2010 to destroy the centrifuges and the attack on the Ukrainian power grid which caused a major blackout in December 2015 [2,3]. In the former, a worm called Stuxnet was utilized while in the latter, Black Energy malware was used to gain access to operational systems (OT, Operational Technology) through corporate information networks (IT Information technology). A ransomware attack on the Colonial Pipeline in the U.S. in April 2021 led to major fuel shortages in the gas stations on the U.S. east coast.

The attackers gained access to Colonial Pipeline's information network through compromised virtual private network passwords. According to the European Union Computer Emergency Response Team (EU-CERT), many cyberattacks are not reported publicly due to confidentiality issues and reluctance to report such incidents because of the potential reputational damage [4]. In 2020, major publicly reported cyber security attacks on power grids included disruptive attacks on European energy firms in March, a ransomware attack on at least eight major energy companies in April 2020, the so-called Berserk Bear Group's advanced persistent threat activity targeting critical infrastructure in Europe and the U.S. in May, and an Italian energy firm compromised by Netwalker ransomware in October [4].

The novelty and contribution of this paper is in providing insights into what senior power grid domain experts in Europe and North America consider to be the most significant cybersecurity risks and trends, followed by an analysis on how well those risks and trends are currently analyzed and understood in academia and industry. More specifically, a qualitative risk assessment is carried out by interviewing 19 senior experts, followed by a focused state-of-the art analysis of the latest research and industry publications. This paper focuses on issues attributable to deliberate, malicious digital attacks on networked systems. Consequently, it excludes issues resulting from other causes, such as natural disasters and technical failures.

The rest of the paper is organized as follows. Section 2 describes the risk assessment method applied in the interviews. Sections 3–7 present in detail the outcome of risk assessment and how the experts see the most significant cybersecurity risks and trends. Section 8 continues by analyzing how the most significant identified risks and trends are covered in the most recent academic research and industry publications. Finally, Section 9 identifies research gaps and areas deserving specific attention before providing the summary.

2. Methods

The risk assessment methodology is based on the well-established framework of the international ISO/IEC 27005:2018 standard [5], comprising three major phases (Figure 1): risk identification, risk analysis, and risk evaluation. The first two phases are relevant to the scope of this paper. The risk assessment process forms part of the overall information security risk management process defined in the ISO/IEC 27005:2018 standard [5].

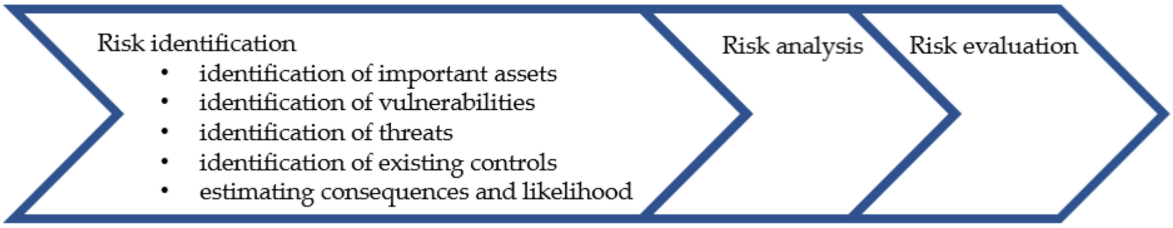

Risk identification
• identification of important assets
• identification of vulnerabilities
• identification of threats
• identification of existing controls
• estimating consequences and likelihood
Risk analysis
Risk evaluation

Figure 1. ISO/IEC 27005:2108 risk assessment phases.

The risk identification phase aims at gaining an understanding of the types of harmful events that could take place as well as possible mechanisms and reasons leading to these events. The risk identification phase consists of five steps: identification of important assets, identification of vulnerabilities, identification of threats, identification existing controls, and estimating consequences. After the risk identification phase, the risk analysis phase continues by analyzing the potential significance of the harmful events identified in the preceding phase. A risk related to a harmful event is defined as a product of the potential consequence and likelihood of the event. Risk evaluation relates to determining, against predetermined criteria, whether the risk level is acceptable or not. In the latter case, a specific risk treatment action could be carried out after completion of the risk assessment [5].

A risk assessment, covering the risk identification and risk analysis phases, was carried out during the spring and summer of 2021 in co-operation with a panel of experts. The typical size of the panel in these kinds of studies is 10 to 50 [6]. Our panel of interviewees consisted of 19 senior experts from Europe and the U.S. The organizational background and geographical distribution of the interviewees are summarized in Table 1. The European experts were recruited from Belgium, Finland, Italy, Luxembourg, and Sweden.

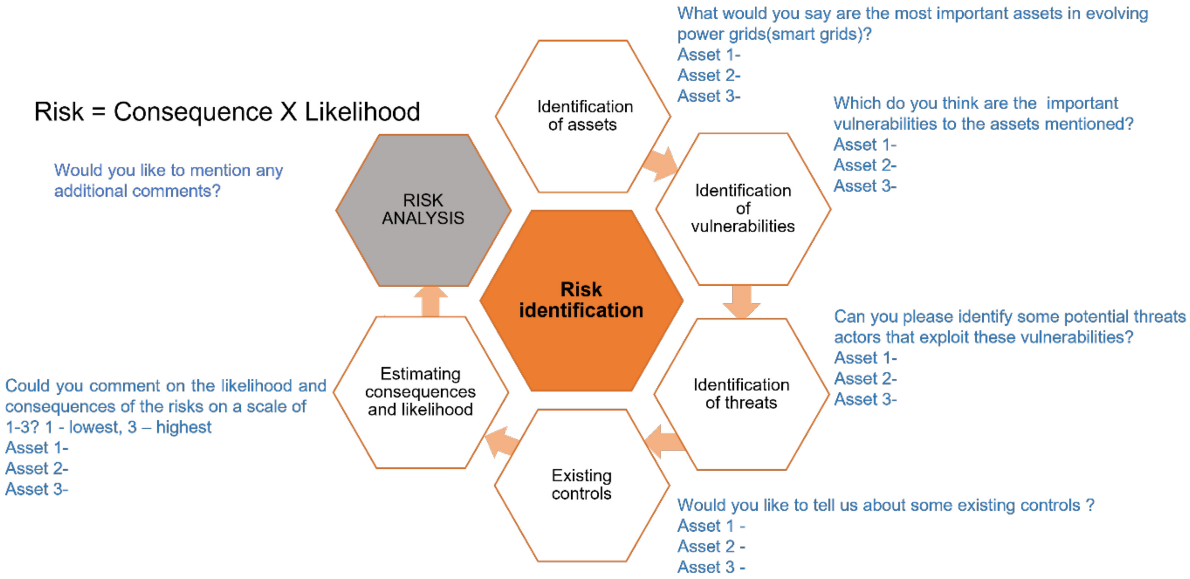
Table 1. Power grid experts interviewed for the risk assessment: background and geography.

Organizational Background	Geography	Number of Experts
Distribution system operators (DSOs)	Europe	3
Transmission system operators (TSOs)	Europe	1
Regulatory bodies	U.S.	2
	Europe	1
Technology companies	Europe	4
	U.S.	1
Academics	Europe	7
Total		19

During the risk identification phase, all the experts were interviewed by utilizing a structured set of questions on cyber-physical security ISO/IEC 27005:2108 risk assessment steps (Figure 2). The questions in the interviews were not specific to any organization or institution but are aimed at a generic perspective on the country's power grid. Furthermore, the opinions stated by the interviewees are their own and are not necessarily shared by their organizations. The experts were asked to identify up to three power grid assets. They assessed consequences based on factors such as power outages, number of people remaining without power, business, or monetary loss due to the attack. The likelihood of occurrence is a measure of attack probability which is impacted by the time taken to mount the attack, expertise or knowledge level, and equipment required by the attacker to mount a successful attack. The interviewed experts were asked to estimate values for both the consequences and likelihood of an attack on scales of 1 to 3, with 3 being the highest for each individual asset on this descriptive scale. Subsequently, in the latter phase, the risk analysis was carried out together with the interviewees to elaborate on the results. If a particular asset had, for example, a consequence of 2 and a likelihood of 3, the total qualitative indication of the risk was deemed to be 2 × 3 = 6. The numeric evaluation of risks was carried out to give a clear indication of the risk level as perceived by each individual interviewees as well as to facilitate discussion during the risk analysis phase. The numeric values for consequences, likelihood, and the total risk are not directly comparable between the experts and assets due to the subjective nature of those numeric values.

Risk analysis is often first carried out qualitatively or qualitatively in order to gain an understanding of the big picture, the potentially most significant issues [5]. In this paper, we apply qualitative risk analysis for the very same reason, i.e., to gain the latest insights into the power grid cybersecurity landscape and major global trends projected to occur within the next 10 years until 2030. A qualitative risk assessment is made based on interview responses concerning risk identification, subjective estimation of consequences, and the likelihood of risks. Such an assessment, although not statistically representative, provides elaborative insights and new inputs by interviewing people and obtaining expert opinion, unlike other techniques such as filling in questionnaires and surveys, where expert opinions could be confined to a few pre-defined options. Consequently, it can be claimed that the interview results give a good indication of the most targeted assets and the attack vectors.

The most important terms for security risk assessment are assets, vulnerabilities, threats, and controls. These terms are defined in Table 2, and their interrelationships are depicted in Figure 3 [5,7]. Figure 3 provides a pictorial representation of the defined risk elements used in the security assessment inspired by ISO 13335-4 [8], an earlier version of the standard ISO/IEC 27005:2018 [5]. Threat actors represent malicious persons or organizations who carry out malicious actions with a deliberate intent to harm the assets. T1, T2, T3, T4 signify the threats, and C1 and C2 are the controls that aim at preventing these threats from harming the asset in the center. V1, V2, 3, V4 are the vulnerabilities in the system that may allow the threats to reach the asset.


Risk = Consequence X Likelihood
RISK ANALYSIS
Identification of assets
Identification of vulnerabilities
Risk identification
Identification of threats
Existing controls
Estimating consequences and likelihood

What would you say are the most important assets in evolving power grids(smart grids)?
Asset 1-
Asset 2-
Asset 3-

Which do you think are the important vulnerabilities to the assets mentioned?
Asset 1-
Asset 2-
Asset 3-

Can you please identify some potential threats actors that exploit these vulnerabilities?
Asset 1-
Asset 2-
Asset 3-

Would you like to tell us about some existing controls ?
Asset 1 -
Asset 2 -
Asset 3 -

Could you comment on the likelihood and consequences of the risks on a scale of 1-3? 1 - lowest, 3 – highest
Asset 1-
Asset 2-
Asset 3-

Would you like to mention any additional comments?

Figure 2. Interview questionnaire.

Table 2. Key risk assessment terminology.

Term	Definition
Asset	Anything that has value to the organization and which, therefore, requires protection.
Vulnerability	A weakness in a system that could be accidentally or intentionally exploited to damage assets.
Threat	Action that has the potential to harm assets such as information, processes, and systems and, therefore, organizations. Threats harm assets by exploiting the vulnerabilities
Controls	Measures trying to prevent a threat from reaching the assets.
Threat actor	A person, a group of people, an organization or a nation state taking an action (threat) aiming at harming an asset.

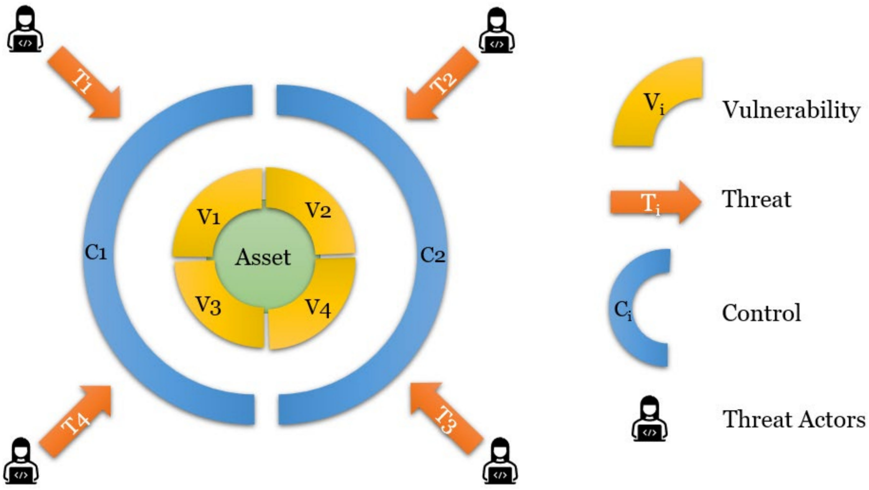


Figure 3. Interactions between assets, vulnerabilities, threats, threat actors, and controls [8].

The Smart Grid Architecture Model (SGAM), developed by the CEN/CENELEC/ETSI joint working group [9], is utilized to categorize the important assets identified by the experts. As depicted in Figure 4 (adapted from [9]), the assets can be grouped into four categories (i.e., architecture layers): the physical power grid layer, field and station layer, communication layer, and operation layer.

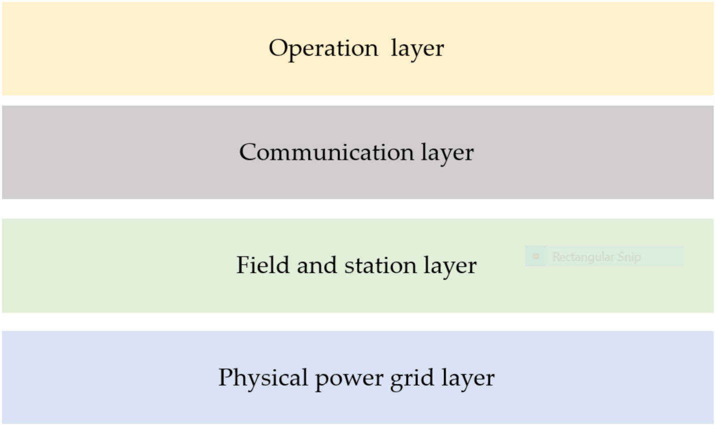


Figure 4. High level categorization of power grid assets for analysis of interview results.

The physical power grid layer includes physical equipment directly involved in the electricity flow and all participating components directly connected to the process, such as generation systems, substations, electric power lines, and power electronic devices. Field and station layer includes equipment that protects, controls and monitors the physical power grid layer, including protection relays, Intelligent Electronic Devices (IEDs), Remote Terminal Units (RTUs), and Substation Automation Systems (SAS). The communication layer focuses on the communication network and the infrastructure that connects the operation layer, field layer, and station layer as well as the assets within these layers. The assets included in the communication layer consist of the network infrastructure and communication systems. The operation layer hosts central information systems for power system control and operation, such as Supervisory Control and Data Acquisition system (SCADA), Energy Management System (EMS), Advance Metering Infrastructure (AMI), and Advanced Distribution Management Systems (ADMS).

3. Expert Interviews Assessing Physical Power Grid Layer Security Risks

According to the classification shown in Figure 4, the physical power grid layer consists of assets involved in the transformation of energy and all participating components. The experts identified the four most important assets to be generators, substations, electric power lines, and power electronics devices (Tables 3–6).

The first asset is the generation systems, which include both bulk generation systems that are connected to transmission systems and Distributed Energy Resources (DERs) that are directly connected to the public distribution grid. Table 3 consolidates the risk assessment of generation systems based on the interviews. The power grid experts identified three vulnerabilities in the generation systems: lack of diversity in energy mix, poor physical security for remotely located DERs, and common mode failures.

According to the experts, physical attacks to generation systems include tripping generators of a less diverse energy mix, attacking fuel lines, and creating a fuel shortage during unfavorable times. Although most components of power systems are designed for at least N-1 contingency criteria, a targeted cyber-hack to shut down a couple of critical generators could lead to major power outages, resulting in large penalties for failing to deliver the committed amount of power to the market. Non-physical threats include manipulation of signals and injection of false measurements to disrupt generation, such as tampering with wind speed measurements to shut down wind generators in remote locations. Potential threat actors identified by the interviewed experts can include disgruntled people, nation states, and people with malicious intent to disrupt or exploit energy markets.

Table 3. Risk assessment of generation systems.

Physical Power Grid Layer—Risk Assessment of Generation Systems			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Lack of diversity in energy mix • Common mode failure • Insufficient physical security for DERs in remote locations	• Malicious actors who physically trip generators • Criminals who cause a shortage of generation fuel	• Hackers disrupting multiple generators simultaneously • People who meddle with electricity markets • Disgruntled people • Nation states or malicious actors who manipulate signals, inject false measurements (FDI)	• Physical security perimeter • Contingency design • Skilled workforce and training • Electronic security perimeter violation tickets • Vendor compliances to NERC CIP standards for utilities, audits
Risk level indication: medium			

Table 4. Risk assessment of substations.

Physical Power Grid Layer—Risk Assessment of Substations			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Poor camera surveillance • Poor access control systems • Long replacement time for damaged equipment • Internal redundancy constraints within substation • Usage of personal workstations	• Vandals, terrorists carrying out a dynamite attack on multiple transmission substations • Trespassing • Vandal attacks on hardware	• Attackers penetrating through IT network, causing blackouts	• Security cameras, prevent tailgating • Optimal level of redundancy among components • Malware protection, antivirus solutions
Risk level indication: low			

Table 5. Risk assessment of electric power lines.

Physical Power Grid Layer—Risk Assessment of Electric Power Lines			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Poor surveillance in unmanned locations • Difficulty in monitoring long lines	• Vandals cutting wires • Suicidal attack on high voltage lines	• Not specifically brought up by the interviewed experts	• Physical security—fences, burgling alarms, camera surveillance • Increasing redundancy in power lines. Structural meshing of networks • Purchasing from different fibre optic companies
Risk level indication: medium			

Table 6. Risk assessment of power electronic devices.

Physical Power Grid Layer—Risk Assessment of Power Electronic Devices			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Information of assembly and dispatch • Lack of periodic updates • Lack of knowledge on internal workings	• Not specifically brought up by the interviewed experts	• Malicious persons triggering common mode failure through malware on inverters • Hackers gain remote control access to inject bot net attacks • Supply chain attacks	• Mandatory cybersecurity standards • Monitor firmware updates in future • Patch management and good cyber hygiene
Risk level indication: medium			

These threats can be prevented from leading successful attacks by implementing control measures such as tightening physical perimeter security, electronic security perimeter violation tickets, and selecting trusted vendors compliant with North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards [10]. NERC provides a comprehensive list of reliability and CIP standards for effective functioning of Bulk Electric Systems in North America. These CIP standards comprise guidelines to categorize cyber assets and outlines in CIP-002 to CIP-014 various recommended controls, including physical security, electronic security perimeter, skilled personnel and training, operational and procedural requirements, information protection, as well as change management [11].

The risk outcome is calculated for each asset by multiplying the values of consequence (1–3) by the likelihood of attack (1–3), as obtained from the interviewed experts. Further, the obtained risk outcome is scaled across low (1–3), medium (4–6), and high levels (7–9). The three different experts who mentioned generation systems as an important asset rated consequences as 3, 3, and 2. Similarly, their corresponding likelihoods are 2, 1, and 3. The resultant risk outcome is obtained by multiplying respective consequence and likelihood values, then averaging over the number of interviewees. As a result, the risk outcome for generation systems is a value of 5 (medium).

The second asset under the physical power grid layer is the substation. As defined by IEC, substations are the part of an electrical system that includes ends of transmission or distribution lines, electrical switchgear and control gear, buildings and transformers. The second asset also includes safety or control devices [12]. Among the interviewed experts, substations were one of the most frequently mentioned assets in the risk identification of this study. Table 4 consolidates the risk assessment of substations based on the interviews.

According to experts, threats to the substation can be both physical and cyber in nature. Vulnerabilities affected by these threats include poor camera surveillance, poor access control systems, and usage of default or weak passwords. An unavoidable vulnerability in the design of substations is the inability to create internal redundancy, for example, with respect to the number of busbars or transformers. Therefore, a balance must be maintained by increasing redundancy or by managing the complexity of the system, costs involved, and the resulting level of security achieved. Experts emphasize the need for dedicated engineering stations to tune and configure devices in a substation. Usage of personal workstations with insufficient security measures introduce weaknesses into the system. The threat actors mentioned most by the experts include vandals and terrorists who attempt to penetrate through IT networks to interrupt the power supply. Disgruntled employees could exploit substations by introducing malware to personnel in the engineering station. Apart from cyberattacks, in locations with insufficient physical security perimeter protection, physical threats can also result in damage to hardware in substations by vandals. The level of asset security can be increased within a substation by strengthening existing controls, such as increasing camera surveillance, a higher but optimal level of redundancy, effective malware protection, and antivirus software.

In the estimation of consequences and likelihood step of the risk analysis phase, four experts rated the consequences as 2, 2, 3, 3, and the corresponding likelihood as 1, 1, 1, 1 (Table 2). Based on these values, we obtain an overall risk outcome of 2.5 (low), on a scale of 1 to 9, with 9 representing the highest overall risk.

The third asset under the physical power grid layer is the electrical power lines, including physical overhead wires, underground cables, and networks between the different stages of power transmission among the power systems. Table 5 consolidates the risk assessment for the electric power lines based on the interviews.

Due to a lack of surveillance, power lines in unmanned locations are considered to be easier attack points substations in terms of physical security. The difficulty in monitoring also arises due to the length of these lines. Threats of physical damage, such as deliberately cutting wires, identified by the experts, especially in remote locations. These physical security attacks could be averted through control measures, such as installation of fences, burgling alarms, camera surveillance, redundant power lines, and structural meshing of networks. Two experts brought up power lines as an important asset. Through risk analysis based on the consequences (3, 1) and likelihood (3, 3) of malicious actors attacking electric power lines, the risk outcome is a value of 6 (medium).

The final asset subsumed under the physical power grid layer is power electronic devices such as inverters and convertors, whose main function is to convert and control electric power [13]. Table 6 consolidates the risk assessment of power electronic devices based on the interviews.

The vulnerabilities of these devices are due to fragmentary supply chain information and their inherent nature as black boxes in the system. Potential threats to these devices can include supply chain attacks, injection of bad code to create power outages, or introduction of a common mode failure, such as a malicious code switching off all inverters at a particular frequency. Importantly, such attacks can be remotely initiated by botnets or malicious replicating code. Threat actors were identified as malicious persons who intend to disrupt the energy systems of a country through the above attacks. The security of power electronics could be enhanced by effective controls, such as purchasing software from trusted vendors, mandatory cyber standards, cyber hygiene, and effective patch management. Although power electronic devices are currently isolated and do not allow firmware updates, the risks over the next 10 years may require enhanced security controls and efficient protection from malware. The two experts rated the consequences of the threat to devices as 2 and 3, and the corresponding likelihood as 2 and 2. The overall risk outcome value calculated from the above values is 5, thus indicating a medium level of risk for power electronic devices. Table 4 documents the interview responses along with the calculated risk outcome from corresponding values of the consequences and the likelihood for power electronics.

4. Expert Interviews Assessing Field and Station Layer Security Risks

This layer includes protection, control, and monitoring equipment, including field devices and automation systems. According to the interviewed experts, the most important assets in this layer are field devices such as Intelligent Electronic Device (IEDs), Remote Terminal Unit (RTUs), protection relays, and Substation Automation Systems (SAS). Although there is a minor overlap between components in these two assets, it can be noted that the term "field" accounts for operation of individual devices in this layer, whereas "station" represents an aggregation of field level devices and their co-operation.

Table 7 consolidates the risk assessment of the field devices based on the interviews. Most vulnerabilities in this layer can be attributed outdated environments (a culture of using legacy components until repair or end of life), challenges in asset management (inconsistent maintenance records, outdated inventory records), open ports, unencrypted communication, unsecure protocols, unreliable or unqualified technology providers, as well as usage of default passwords.

Table 7. Risk assessment of field devices.

Field and Station Layer—Risk Assessment of Field Devices			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Legacy components • Improper asset management, documentation of maintenance • Un-updated, unpatched environments, usage of default passwords • Unencrypted communication, open ports, unsecure protocols • Unreliable technology provider	• Not specifically brought up by the interviewed experts	• Ransomware attack by nation states • Terrorists injecting malware on maintenance laptops without knowledge of contractor • Social engineering, blackmail • Criminals who attack smart grids for fun or to challenge to disrupt their availability	• Physical access policies, SOCs obtain logs from systems, network devices • Firewalls on network, monitoring and raising alarms • Self-monitoring relays • Patch management, human resources (only authorized people)
Risk level indication: low			

In addressing the above vulnerabilities, the main challenge lies in the maintenance and asset management of field devices. Given the innumerable connected devices, major vulnerabilities can arise due to various deficiencies, including documentation of assets along with their ownership, keeping a record of the latest software updates, and password changes. Software updates in field devices are often not tracked as long as the legacy components continue to work. Moreover, a potential cyber threat faced by field devices can even include undetected malware in maintenance laptops. The motive for malicious actors who attack this asset category could be either ransom or proving one's capability to disrupt the electricity supply. The experts identify possible malicious actors as nation states as well as terrorists who blackmail for ransom. It is worth noting that companies are most often discreet about attacks and their sources, thus making it difficult to precisely identify malicious actors in smart grid security.

Some controls that could help to enhance the security of this asset include enforcing stringent physical access control, access log monitoring through Security Operation Centers (SOCs), patch management, and ensuring trusted human resources. The three experts who mentioned field devices as an important asset rated the consequence as 1, 1, 2, and the respective perceived likelihood as 2, 1, 3. Thus, the field and station layer had an overall risk outcome of 3, indicating a low-risk category.

The second asset, Substation Automation System (SAS), comprises the hardware and software components that monitor and control an electrical system, both locally and remotely [14]. These components are responsible for all data-acquisition process, control, monitoring, and alarming functions associated with a high-voltage apparatus related to primary equipment, as well as similar functions related to secondary substations [15]. Table 8 consolidates the risk assessment of Substation Automation Systems (SAS) based on the interviews.

Experts from DSOs commented that unlike SCADA systems, patch management has not been effectively implemented for substation automation systems, as they are fully isolated from IT systems. Another reason could be due to the need for investments in patching, as well as cost constraints that prevent organizations from following stringent patch policies in substation automation systems. The vulnerabilities in these systems are mainly due to unencrypted communication, poor access control and monitoring, open ports (no firewalls, accessible from any IP address), and poor cyber-hygiene (e.g., use of infected USB sticks).

Ransomware attacks by potential threat actors, such as criminal organizations and nation states, can affect the Substation Automation System. The security of these systems could be improved through controls such as effective patch management, Security

Information & Event Management (SIEM), and stringent access control. The two experts mentioning Substation Automation Systems as an important asset rated the consequence as 3 and 3, and the respective perceived likelihood as 2 and 1. The resulting risk outcome obtained from these values is 4.5, thus signifying a medium level risk.

Table 8. Risk analysis of Substation Automation Systems (SAS).

Field and Station Layer—Risk Assessment of Substation Automation Systems (SAS)			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Lack of patching policy • Lack of monitoring and logging • Open ports, lack of firewall • Unencrypted communication • Poor cyber hygiene	• Not specifically brought up by the interviewed experts	• Malicious actors deploying ransomware • Disgruntled employees injecting malicious content through USB sticks	• Patch management • Security Information & Event Management (SIEM) • Authorized access to human resources, maintenance personnel
Risk level indication: medium			

5. Expert Interviews Assessing Communication Layer Security Risks

With the increasing complexity of smart grids, dependency on communication technologies has increased as well. This section analyzes the third layer illustrated in Figure 4, the communication layer. This layer includes network infrastructure and communications systems across different domains of smart grids, namely, end-user premises, transmission grids, distribution grids, and generation. The concept of network infrastructure partially overlaps with communications systems. The network infrastructure focuses more on the individual communications device level, while communications systems focus on the network level, i.e., networks built by using individual communications devices.

Table 9 consolidates the risk assessment of the network infrastructure based on the interviews. Threats faced by network infrastructures are predominantly cyber threats. According to the experts, major vulnerabilities in network infrastructure are due to old unsecure protocols, poor access control, default passwords, lack of surveillance at network end points in remote areas, poor patching, and encryption.

Table 9. Risk assessment for network infrastructure.

Communication Layer—Risk Assessment of Network Infrastructure			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Old unsecure protocols • Poor access control, default passwords • Lack of surveillance at network end points in remote areas • Poor patching, encryption	• Not specifically brought up by the interviewed experts	• Criminals deploying ransomware • Black hat hackers initiating botnet attacks by hijacking PCs	• Secure protocols, firewalls, data protection • Design by standardization • Security by design for microgrids, verification of new configurations • Secure wireless protocols, patching of wireless connected devices • Penetration testing
Risk level indication: medium			

In network devices between IEDs and SCADA, a misconfiguration leading to online availability of unpatched devices may enable threat actors, such as nation states and terrorists, to gain access. Furthermore, due to its inherent wide attack surface, network infrastructures are prone to botnet attacks by criminals for ransom and black hat hackers. In industry, protocol updates are usually slow mainly due to cost constraints on investments made in cybersecurity. The overall security of networks can be enhanced by implementing secure, updated protocols along with protocol analysis during the design of microgrids. Other controls include effective firewalls, patch management for wireless connected devices, change management, and penetration testing to prevent the aforementioned threats from becoming successful attacks. The two interviewed experts rated the consequences of potential risks to network infrastructure as 2 and 2, and their respective likelihoods as 2 and 3. These values gave an overall risk outcome of 5, indicating a medium-risk category for network infrastructure.

The second asset under this category is the communications systems. Table 10 consolidates the risk assessment of communications systems based on the interviews. The vulnerabilities faced by communications systems include usage of open networks by customer premises routers, which are prone to hacking. Further, vulnerabilities in access control and authentication could pose the threat of data manipulation. General threat actors mentioned by the experts include hackers, teenagers, nation activists who attempt by-passing firewalls, trigger Denial of Service DoS, and False Data Injection (FDI) attacks. These integrity issues could be tackled through implementation of controls such as two-phase authentication, careful monitoring of access control lists, and multilayer passwords for IT systems. Furthermore, the overall cybersecurity of information systems could be ensured using general controls such as network segmentation in IT, efficient antivirus software, and protocols.

Table 10. Risk assessment for communication systems.

Communication Layer—Risk Assessment of Communications Systems			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Poor access control or authentication verification • Customer premises routers use public networks making them prone to unauthorized access.	• Not specifically brought up by the interviewed experts	• Hackers bypassing firewalls • National activists who launch DoS, False Data Injection • Malicious teenagers or any malicious actor with moderate knowledge of the power system	• Double authentication of access, signal verification, Limit access control lists, multilayer passwords • Antivirus, segmentation of IT, Information security training for employees • Protocols, systems to ensure cybersecurity, standardization, e.g., IEC 62351, 61850 • Sharing cyberattack incident information to avert similar attacks
Risk level indication: medium			

The three experts who mentioned this asset rated the consequences of an attack against communications systems as 2, 2, and 1, and the corresponding likelihood as 3, 2, and 2. Calculating the risk outcome as an average of their products, we obtain a value of 4, indicating a medium-risk category for communications systems.

6. Expert Interviews Assessing Operation Layer Security Risks

The operation layer hosts central information systems for power system control and operation. The experts highlighted four of these systems: the Supervisory Control and Data Acquisition system (SCADA), Energy Management System (EMS), Advanced Distribution Management Systems (ADMS), and Advance Metering Infrastructure (AMI).

The SCADA system is a core component of the Industrial Control Systems (ICS). In smart grids, SCADA systems are used in monitoring the electricity distribution network to ensure reliability of the power supply [16]. Table 11 consolidates the risk assessment of SCADA systems based on the interviews. According to the interviewed experts, the following vulnerabilities make them prone to malicious attacks: compatibility of installed systems having different ages and life spans (e.g., outdated software, legacy OT systems whose updates are not on par with IT systems), lack of cybersecurity by design (e.g., devices initially not planned to work online have now been upgraded with network and remote access facilities), lack of clear cybersecurity strategy, and unprepared manpower.

Table 11. Risk assessment for SCADA systems.

Operation Layer—Risk Assessment of SCADA Systems			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Compatibility with legacy systems • Lack of security by design • Accessible by remote control • Lack of a clear cybersecurity strategy	• Not specifically brought up by the interviewed experts	• Criminals initiating ransomware • Nation states, criminals creating cyberwar to show their power on nation's power grid • Cyberhackers working with terrorists on ransomware • Disgruntled employees	• SCADA is located in control centres within offices, isolated from typical office networks, staff • Identity Access Management (IAM) • Business Continuity & Incident Management (BCIM)
Risk level indication: high			

Threats to SCADA systems identified by the interviewed experts included FDI, Distributed Denial of Service (DDoS), ransomware, social engineering, and falsification of signals. Potential threat actors who may target the SCADA systems consisted of nation states, criminals who intend to initiate a cyberwar, cyberhackers working with terrorists, and disgruntled people seeking revenge on employers. An inherent control for SCADA systems is that they are located in control centre offices, physically well isolated from office networks and the Internet. Other important controls include Identity Access Management (IAM), Business Continuity and Incident Management (BCIM), purchasing software from trusted vendors, authorizing only trusted maintenance personnel, and implementing sophisticated algorithms for bad data detection.

For the risk analysis, the two experts rated the consequences of an attack on SCADA systems to be high, a value of 3. The corresponding likelihood was rated as 3 and 2. Calculating the risk outcome as an average of their products, we obtain an overall risk outcome of 7.5, indicating a high-risk category for SCADA systems.

The second asset under the operation layer is the Energy Management Systems (EMS), which is a computer-aided tool used by Power Systems Operators (PSOs) to monitor, control, and optimize energy generation. The purpose of an EMS is "to determine power generation or power demands that minimize a certain objective such as generation cost, power loss, or environmental effect" [17]. Table 12 consolidates the risk assessment of the Energy Management Systems based on the interviews.

Table 12. Risk assessment of Energy Management Systems (EMS).

Operation Layer—Risk Assessment of Energy Management Systems (EMS)			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Lack of sufficient hardening • Unsafe security practices, sharing of login credentials • Asset management and ownership • Compatibility of life span of installed systems	• Physical shooting attacks on control centres	• False Data Injection attacks by nation states, cyber terrorists • Disgruntled employees installing malware • Foreign actors who want to disrupt energy markets • Supply chain attack	• Anomaly detection used by asset owners • Sophisticated algorithms for bad data detection • Purchasing software from trusted vendors
Risk level indication: medium			

The accuracy of an EMS depends on reliable inputs. Since these inputs must be communicated at very high rates, the authentication and verification must occur very rapidly. This creates an inherent vulnerability in EMS, as pointed out by the power grid experts. Other vulnerabilities of the EMS systems and control centres included people working in control centres susceptible to attacks, insufficient hardening, single user logins, usually everyone logs in as admin, challenges in asset management and ownership, outdated software, legacy systems, and the long lifespan of power systems.

Potential threats to EMS arise from disgruntled employees or someone who has been blackmailed to install malware. Other possible threats to the EMS include FDI attacks carried out by foreign actors and cyber terrorists who intend to disrupt power systems or exploit energy markets for financial gain. These threats can be addressed by establishing controls for efficient asset management combined with anomaly detection, as well as Security Operation Centres (SOCs). SOCs help in detecting anomalies in the systems and heuristically monitor access logs. A successful FDI attack efficiently masks data, which can be identified only with the help of sophisticated bad data detection algorithms. Furthermore, the security of EMS against supply chain attacks can be enhanced by purchasing software from trusted vendors and enforcing stringent cyber controls for authorized authentication.

Experts from different countries and backgrounds, including DSOs, regulatory bodies, and academia, rated the consequences as 2, 3, 3, 3, and 2, and the likelihood of attacks on EMSs was rated as 2, 3, 1, 1, and 3, respectively. Calculating the risk outcome as an average of their products, we obtain an overall risk outcome of 5, signifying a medium level risk.

The third asset under the operation layer is the Advanced Distribution Management System (ADMS), whose function is to automate restoration of outages and to optimize the overall performance of the distribution grid. ADMS is a software platform that supports outage restoration and performance optimization of distribution power grids [18]. Table 13 consolidates the risk assessment of the ADMSs based on the interviews.

OT systems often use legacy software and Operating Systems (OS) versions, which are often not kept up-to-date or not even supported anymore by their suppliers, thus making them prone to cyber-attacks. Threats to ADMS include lateral movement from an IT network to OT, for example, through the introduction of malicious content by email or malware in the system. Potential threat actors include professional hacking groups collaborating with nation states or terrorists targeting distribution management systems.

Controls for securing these systems include ensuring isolation of OT systems from IT network, implementing efficient firewalls wherever necessary, and periodically testing systems for malware. According to an expert from a European DSO, the consequences and likelihood were the highest for an attack on ADMS. Therefore, they were rated the highest values of 3 each, resulting in an overall risk outcome of 9, indicating a high risk.

Table 13. Risk assessment of Advanced Distribution Management Systems (ADMS).

Operation Layer—Risk Assessment of Advanced Distribution Management Systems (ADMS)			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Software updates not on par with IT systems • Usage of legacy OS versions	• Not specifically brought up by the interviewed experts	• Nation states or hacking groups involved in lateral movement • Cyber terrorists who inject malicious content or malware from IT network to OT	• Isolation of OT from IT network • Firewalls • Periodic malware testing
Risk level indication: high			

The final asset under the operation layer is the Advanced Metering Infrastructure (AMI), which is a system of smart meters for energy utilities that connect to data management systems through computer networks. AMI enables a bidirectional exchange of data between the consumer and the utility company [19]. Smart meters are the core of AMI, performing functions such as measuring customer electricity consumption, voltage levels, as well as communicating these readings to utility providers and back to customers for billing and providing energy feedback [20]. Table 14 consolidates the risk assessment of the Advanced Metering Infrastructure based on the interviews.

Table 14. Risk assessment of Advanced Metering Infrastructure (AMI).

Operation Layer—Risk Assessment of Advanced Metering Infrastructure (AMI)			
Vulnerability	**Physical Threats**	**Cyber Threats**	**Controls**
• Poor isolation from the Internet • Low physical security • Poor data protection	• Malicious actors who attempt to gain access to networks through physical attacks	• Criminals who corrupt metering data, control switches • Nation states or criminal organizations who initiate ransomware attacks with stolen customer data • Casual hackers who challenge penetration into IT distribution grid.	• Physical security hardening of smart meters • Whitelisting techniques for access control for electricity vendors • Network segmentation • Security audits
Risk level indication: low			

Vulnerabilities of smart meters can be due to poor isolation from the Internet, low physical security (i.e., network hijacking), and poor data protection. Improper access control could result in various threats, including data theft, corruption of metering data, unauthorized access to control switches, and penetration of the IT distribution grid. Threat actors include criminals, criminal organizations, and foreign states that could initiate ransomware attacks on stolen customer data from smart meters. The probability of attacks against AMI can be reduced and the consequences of such attacks can also be minimized by physical hardening of smart meters, whitelisting authorized users of energy companies, securing data storage locations, conducting security audits for external vendors on storage of accessed data.

All the interviewed experts rated the likelihood of attacks against AMI with the lowest value of 1, while the consequences varied between 2 and 3, thus indicating a low overall risk outcome of 2.66 for AMI.

7. Summary of the Expert-Guided Security Risk Assessment

The four preceding sections, Sections 3–6, presented the risk assessment for each of the four smart grid architecture layers. Figure 5 summarizes the experts' view on the most significant risks for each of the layers, while Table 15 consolidates the experts' perception on the most significant threat actors for each of the layers. The area of the boxes in the tree map of Figure 5 indicates the extent of different threats on the assets within the four layers. As can be seen in Figure 5, the majority of the interviewees focused on threats affecting assets in the operation layer. This could be attributed to the central role played by assets in this layer, such as SCADA and EMS for the control and operation of various other components within the power grid.

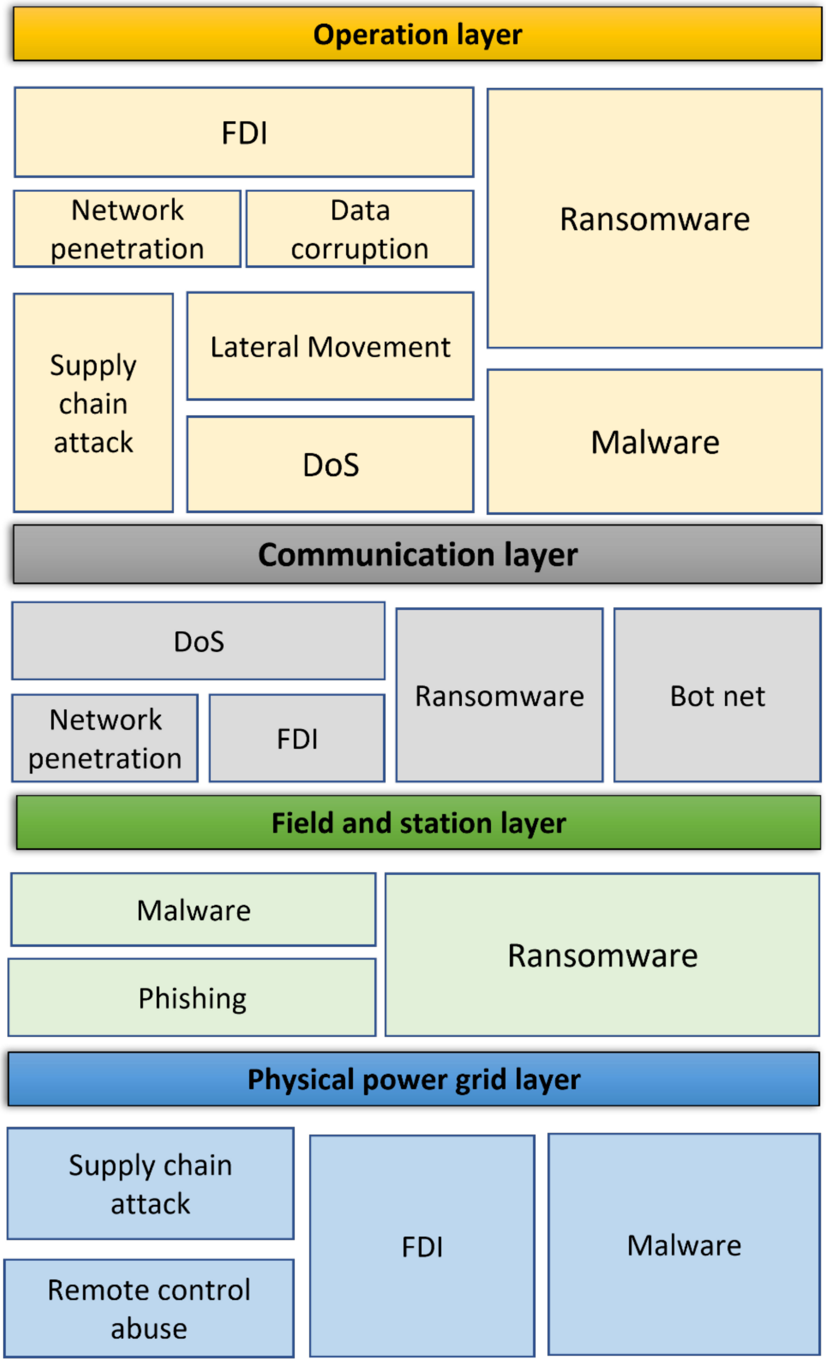


Figure 5. Tree map of the most significant threats on different power grid layers.

Table 15. Cyber threat profile across layers.

Layer/Threat Actors	**Cyber Terrorists & Criminals**	**Hackers & Skilled Malicious Individuals**	**Nation States**	**Disgruntled Employees**	**Market Competitors**	**National Activists**	**Malicious Teenagers**
Operation layer	■	□	■	□	□		
Communication layer	▣	▣	□	□		□	□
Field and station layer	▣	□	□	□			
Physical power grid layer		■	□	□	□		

The darker the color, the more the threat actor is targeting assets on that particular power grid asset category.

Table 15 summarizes how the experts see the main threat actors on each of the smart grid architecture layers. The darker the color, the more the particular threat actor is targeting assets on that particular power grid asset category level. The most commonly mentioned potential threat actors are cyber terrorists and criminals and hackers, followed by nation states. According to the risk assessment, cyber terrorists and criminals and nation states mostly target the operation layer, while hackers and malicious individuals focus on the physical power grid layer. It is also worth noting that apart from financial and politically related threats such as ransomware and state-sponsored attacks, several interviewees also mentioned market competitors and disgruntled employees as potential threat actors who might disrupt smart grids.

Based on the extent of different threats on the assets within the four layers (Figure 5) as well as related detailed discussions with the experts, the major threats were identified as False Data Injection (FDI), Denial-of-Service (DoS), supply chain and ransomware and malware attacks. Next, we move on to study how well these most significant risks have been understood and addressed in the latest research and industry publications aiming at identifying areas deserving further specific attention.

8. The Research and Industry View on the Threats Identified in the Expert-Guided Security Risk Assessment

This section provides a review of the latest academic research and industry views on the major identified threats: False Data Injection (FDI), Denial-of-Service (DoS), supply chain, and ransomware and malware attacks. Section 9 will build on Section 8 by discussing the differences and gaps between the experts' views and those of academic research and industry presented in Sections 8.1–8.4

8.1. False Data Injection (FDI)

Much research has been devoted to False Data Injection (FDI) attacks on power grids, state estimation, phasor measurement units, protection, voltage stability, and microgrids. Many of these studies have also focused on evaluating the feasibility and performance of Machine Learning (ML) algorithms in detecting FDI attacks.

To address FDI attacks, Musleh et al. [21] provide a review of model-based and data-driven algorithms, as well as describing the strengths and limitations of these algorithms. The article classifies cyber-physical attacks based on their method of delivery into four main categories: cyber-based, network-based, communication-based, and physical-based cyberattacks. The authors demonstrate how an FDI attack is applicable to each of these categories and targets different systems and layers of the smart grid. In model-based detection algorithms, smart grids are modelled based on dynamic real time measurements and static system data, such as substation configuration and other system parameters, to identify any deliberate manipulation of these measurements or data. In contrast, data-driven algorithms are model-free and largely depend on historic data of the system to enable Machine Learning (ML) techniques. The ultimate goal of the article is to develop an optimal algorithm with minimum limitations.

FDI attacks on Phasor Measurement Unit (PMU) based state estimation have been investigated in [22]. To detect FDI attacks, the authors develop a Phase Locking Value (PLV) technique, which has the advantage that it requires no training. The proposed approach is tested by using Monte Carlo simulation and applying multiple grid configurations. The simulations show that the proposed algorithm can efficiently detect FDI attacks.

In [23], a Logical Analysis of Data (LAD)-based method was proposed to detect FDI attacks early and to safeguard power grid protection systems from FDI attacks. The proposed method focuses particularly on online protection applications and identifies a minimum set of secured sensors to maintain the necessary fault detection capabilities. The effectiveness of the method is verified by simulations.

A new detection algorithm that calculates an indicator to identify the attack on PMU data was proposed in [24] for possible cyber-physical attacks on the voltage stability monitoring system of power transmission systems. The advantage of this algorithm is that it requires no historical data, since the algorithm is based on analytical techniques. The algorithm is able to detect and combat sophisticated attacks which utilize the power flow equations of the system.

In [25], the Nejabatkhah et al. discuss the cyber-physical systems in smart microgrids, their threats and impacts, with a detailed focus on FDI attacks. In this survey article, cyber-physical systems are classified into four groups roughly similar to those presented in [21]. An FDI attack that compromises data integrity in communication network is considered the most challenging threat to smart grids. The authors in [25] review recent cyber-security projects, standards (e.g., NERC CIP and IEC62351) and protocols. Further, they discuss attacks on data availability, integrity, and confidentiality along with their physical, technical, and economic impacts. The authors also elaborate on FDI attacks targeting state estimation, voltage control, frequency control, and protection systems, as well as their corresponding defensive strategies. Finally, an example is provided to illustrate the process of constructing and detecting an FDI attack in power electronic intensive microgrids.

8.2. Denial of Service (DoS)

The main purpose of DoS attacks is to block or delay the data communications. Unlike the FDI attack that targets data integrity, DoS and Distributed Denial of Service (DDoS) attacks attempt to compromise data availability in power systems. These attacks can be initiated from a single source or multiple sources by transferring malformed packets to the target device or flooding the network or communication layer by exhausting the processing capacity of the router, network bandwidth, or servers [25]. In addition to FDI attacks, Nejabatkhah et al. also discuss Denial of Service (DoS) attacks with a particular focus on microgrids [25].

In its report on DDoS [26], the European Union Agency for Network and Information Security (ENISA) defines DDoS as the stage when users of a system or service are unable to access the relevant information, services, or other resources. In such situations, DDoS attacks exhaust the service or overload components of the network infrastructure. The report shows that botnet attacks are on the rise, with China, Brazil, and Iran being the countries most infected by botnets. Such sophisticated attacks can be used as reconnaissance activities, which are exponentially increasing, along with expansion of botnet networks and connectivity among devices. The total number of DDoS attacks rose by 241% between the Q3 of 2018 and the same period of 2019. Among the different techniques used by threat actors, SYN flood has been observed to be the most challenging. The proposed actions for mitigating SYN flood include identifying critical resources and locations of overload, as well as prioritizing defense accordingly. Other mitigation actions could be to incorporate a DDoS managed service provider, to develop a proactive defensive posture and to maintain a risk register of critical assets.

The Cybersecurity for energy sector report published by the European Cyber Security Organization (ECSO) [27] provides a synthesis of present-day cybersecurity challenges affecting the energy sector, with a focus on the cybersecurity gaps in the electricity sector.

As the reason for such challenges, the report lists three major changes presently occurring in the energy sector: a shift in the energy source mix, digitalisation of energy infrastructures, and an increase in threats due to ICT. According to the report, threats are the highest in the energy sector, followed by the financial and ICT sectors. The topmost attacks are malware, DoS/DDoS, and cyber espionage within the energy sector. Interestingly, this report is one among the very few publications that attempts to classify the origin and type of threat actor in terms of different historical attacks on energy infrastructures over the years.

In [28], a threat analysis approach was developed to study system level vulnerabilities for emerging dynamic control centres. Key technologies such as PMUs and digital twins are incorporated in these control centres to enhance monitoring and control capabilities of conventional SCADA systems. The threat analysis approach implements a four-stage methodology focusing on PMU and SCADA communication, the Human–Machine Interface (HMI), and the process database at the control centre. Further, the article calculates risk scores which are found to be the highest for PMU and SCADA communication in the presence of DoS, spoofing, and injection attacks. Overall, the article discusses the critical nature of security in dynamic control centres and establishes a foundation for future research towards resilient designs.

In [29], the authors introduce a token authentication service for use in an Energy Management System (EMS) and propose an encryption verification mechanism. The effectiveness of their mechanism has been verified in the Smart Green Science City in Taiwan. SCADA systems and the Internet of Things (IoT) have been used to achieve increased connectivity, complete system integration and overall improvement in the working efficiency of Industrial Control Systems (ICS). However, due to the dependence of SCADA systems on public networks, the SCADA systems become vulnerable to information security attacks and cyber threats. Methods for mitigating DoS attacks include attack inspection, traffic filtration, and multiple verification techniques. The major challenge is to prevent hackers from using the external Internet to attack firewalls and Intrusion Detection and Prevention Systems (IDPS), thereby enabling access to EMS, and then ultimately mounting a DoS attack against the SCADA server. Therefore, this paper proposes an encrypted verification mechanism based on tokens and the transport layer security (TLS) protocol to ensure the internet security of SCADA and protect industrial networks. In addition to DoS, the encryption mechanism can also prevent man-in-the-middle, replay, and impersonation attacks.

8.3. Supply Chain Attacks

The European Union Agency for Network and Information Security (ENISA) published a report [30], that describes the nature of threats to ICT supply chains and proposes strategies to counter these threats. ENISA defines supply chain integrity as an “indication of the conformance of the supply chain to good practices and specifications associated with its operations”. The ICT supply chains include distribution of software and firmware, as well as chip designs in soft formats across geographies. The study begins by exploring possible threats to the ICT supply chain, focusing on technical manipulations by untrustworthy suppliers. A major contribution of this report is its recommendations for improving trust models, evaluation, and integrity verification techniques, as well as technology solutions to prevent counterfeiting and to improve inventory management.

ENISA’s “Threat landscape for supply chain attacks” [31] describes an increasing trend in supply chain attacks, resulting from a shift from organizations to their suppliers as the initial target of attackers. The report claims that 24 supply chain attacks occurred between January 2020 and July 2021, with almost 50% of these attacks originating from APTs (Advanced Persistent Threats), well known cybercrime groups, including APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413, and TA428. Malware has been reported as the major attack technique applied by attackers. To identify the key characteristics and techniques used in these attacks, the report analyzes recent attacks such as the SolarWinds attack that affected large entities (e.g., governmental organizations) and the Kaseya attack that disrupted service providers. Finally, the report ends by recommending methods for assessing the cybersecurity maturity of suppliers and the level of exposure to the risk arising from the customer–supplier relationship. Ultimately, to reduce supply chain attacks, it is essential that the customers take into account the overall quality of the products and the cybersecurity practices of their suppliers, including enforcement of secure development procedures.

In [32], the authors modelled and analyzed the threats to the cyber supply chain along with examples from the smart grid. The attacks were modelled using the Structured Threat Information eXpression (STIX) method to identify potential attacks, such as penetration and manipulation that impact organizational goals. The authors describe the methods used by threat actors to exploit supply chain lifecycles at different stages of development, distribution, or operation. Examples of such methods included not only injection of exfiltrated code during the software development phase to attack a third-party website or database server in later stages, but also APT attacks and replacement of legitimate software with modified versions. Based on threat intelligence gathered from the analysis, the article recommends improvements for controlling access, assets, and update management throughout the supply chain.

Deloitte's report on "Managing cyber-risk in the electric power sector, Emerging threats to supply chain and industrial control systems" [33] discusses cyberattacks that demonstrate a threat to the power sector through supply chains. An example of such a cyberattack is the attack carried out by Dragonfly, aka Energetic Bear, which breached utility ICSs in the United States and other countries through commonly visited industry websites in order to spread malicious content. Investigations have classified Dragonfly as an APT backed by a nation state for reconnaissance purposes. The report then discusses the NotPetya attack, where the attackers hacked into a Ukranian accounting software service provider using corrupt software updates. This attack infected at least six local electric utilities as well as affected the health and transport sectors, leading to over USD 10 billion in damage. The report suggests using blockchain technologies to track components throughout the supply chain by maintaining an automated tracking ledger to follow the digital record of the product's lifecycle and access control. Blockchain and cloud computing techniques would decentralize data and ensure the authenticity of tracking records. Overall, cyber supply chain risks can be reduced by ensuring accountability and ownership, as well as by identifying and mapping critical assets across the industry.

The paper presented in [34] aims to revise trust in all relationships to avoid internal threats to corporate networks. A zero-trust architecture provides a checklist of controls to analyze the gaps and improve security in the overall cyber supply chain. The proposal presented in the paper is based on the Zero Trust principle introduced by the National Institute of Standards and Technology (NIST), which provides standards and guidelines, such as standard SP 800-207 Zero Trust architecture. This study has a very similar approach to the risk assessment methodology devised in this paper, as it identifies critical components in the supply chain. Adherence to the principles of Zero Trust can be verified by performing individual analyses of each component. For organizing the controls, the paper discusses six domains of Zero Trust adapted from Microsoft's Zero Trust Guidance Center and the Zero Trust Maturity Model. The paper ends by proposing a security roadmap for improvements based on the gap analysis.

In [35], cyberattack ontology concepts are explored to provide semantic mapping and relationships for determining attack patterns and risks. To address growing cyber supply chain threats, the lack of threat intelligence, and issues of trust, it is essential for organizations to understand and map the security relationships in a supply chain. This approach includes analyzing properties such as goals, actors, Tactics, Techniques and Procedure (TTP), attacks, and vulnerability. The paper uses a protégé tool to model the relationships that enable interoperability in a machine interpreted method for expressing the meaning, structure, and syntax of cyberattack incidents and their cascading impacts on the cyber supply chain domain. Secondly, the paper models a cyberattack ontology for semantic mapping and knowledge representation. Finally, the concepts of threat intelligence and knowledge reuse are discussed, and results show that the cyberattack ontology concepts could be used to improve cyber supply chain security.

8.4. Ransomware and Malware

Ransomware and malware have been the topic of much investigation. Threatpost provides an overview of ransomware trends and how this criminal activity is organized in its comprehensive report "2021: The Evolution of Ransomware" [36]. The report identifies utilities as the second most common ransomware attack target after the healthcare sector, followed by the legal and insurance sectors. Similarly, Check Point states in its "Cyber Security Report 2021" that the number of ransomware attacks are increasing and that healthcare organizations appear to be the primary target [37]. The report makes the observation that most of the ransomware attacks have been made during weekends and holiday seasons, when abnormal behavior and odd symptoms are less likely to be detected, since most of the staff are not physically present in the office. Consequently, the report recommends constant systematic monitoring 24/7, in addition to prompt patching and user training, to protect IT and OT systems. The risk of being caught has been low, since some nation states silently allow ransomware groups to operate within their jurisdiction by assuming that they do not pose a threat to these states themselves. Interestingly, one of the most well-known ransomware groups, REvil, also mentioned in Threatpost's report, was arrested in Russia in January 2022 based on information provided by U.S. Intelligence [38].

David Nicol provides an overview of recent ransomware attacks on energy systems and discusses the motivations of the attackers, typical attack vectors, and potential methods for addressing the increasing ransomware threat [39]. In addition to monetary gain, political reasons such as environmental or political activism could place pressure on companies and politicians to achieve activists' targets. Nicol points out that malware can directly reach OT systems, for example, through software updates or the laptops of experts troubleshooting the OT system, instead of first compromising the IT system. Ransomware attacks on energy systems are typically divided into two phases. In the first phase, attackers demonstrate that they have access to the energy system and can control it, for example, by opening and closing circuit breakers without actually causing major harm, followed by monetary or political demands. If the energy company does not accept the demands, the attacker damages the energy system. If the company accepts the demand, the attacker delivers a key to remove the malware. Thus, the attacker does not need to have access to the OT after having presented the demand, thereby making countermeasures more challenging. Further work will be required to develop methods not only for rapidly launching countermeasures without the attacker noticing these actions, but also for rapidly reinstalling the whole OT system from non-infected backups.

ENISA has identified ransomware as the prime threat for 2020–2021 in the ENISA Threat landscape report published in [40]. Cybercriminals are increasingly motivated by monetization of activities such as ransomware. Cryptocurrency remains the most common pay-out method for threat actors. According to this report, understanding the trends related to threat actors, their motivations, and their targets greatly assists in planning cybersecurity defenses and mitigation strategies. The report considers following four categories of cybersecurity threat actors: state-sponsored actors, cybercrime actors, hacker-for-hire actors, and hacktivists. The focus on Ransomware as a Service (RaaS) type business model has increased during 2021, making it difficult to precisely attribute these attacks to individual threat actors.

ENISA's threat landscape on "Sectoral/thematic threat analysis" [41] predominantly identifies malware as an increasingly popular form of attack. This report analyses threats introduced by three emerging technologies: 5G, Internet-of-Thing (IoT), and smart cars. These technologies are analyzed using an asset-based risk assessment approach. This report analyses eight important asset groups: core network, access network, physical 5G infrastructure, human factors, software design, IoT and car sensors, actuators, and communication network protocols for smart cars. The report also presents sectoral incident statistics to aid in understanding the dynamics of cyberthreats and emerging trends in different sectors based on factors such as adversary motives and exposure of assets.

According to ENISA's "Main incidents in the EU and worldwide" [42], up to five ransomware attacks were reported between 2019 and 2020. One of these occurred in July 2020 affected the Johannesburg energy supply. Malware is considered to be one of the top threats according to [42]. The report also lists 16 incidents between 2019 and April of 2020, including the attack on ENTSO-E in March 2020. This report indicates the growing importance of supply chain attacks in technology sectors. Further, social engineering is considered to be the main threat behind up to 84% of the cyberattacks recorded. The report finds that the average time taken to detect a data breach can be as long as six months, state-sponsored APT groups are increasingly active, and that organized crime, nation states, and insiders are the three main threat actors.

9. Discussion and Conclusions

Having carried out the expert-guided security risk assessment (Sections 3–7) and having explored how and to which extent the most significant identified risks are understood and addressed in the latest research and industry publications (Section 8), we shall now move on to compare these results from Sections 3–7 with the findings from the latest research and industry publications in order to identify areas deserving specific further attention.

Although the state-of-the-art research shows that Artificial Intelligence (AI) methods are being actively researched in order to develop methods for detecting FDI attacks, AI was rarely mentioned in the expert interviews. There could be two reasons for this discrepancy. One reason might lie in the interviewees' field of expertise, which focused primary on power systems rather than, for example, computer science. Another reason could be that the academic research is forward-looking (as academic research in general should be). Thus, in the future, we might increasingly see AI utilized in attack vectors. This development would be in line with the increased (non-criminal) utilization of AI in various industries and everyday applications.

Technical academic publications on smart grids have focused primarily on identifying different types of attacks, as well as developing detection algorithms and to some extent on controls against these attacks, as seen in Section 8. Most of these publications have studied the effectiveness of data-driven and analytical approaches, suggested more efficient algorithms, or have specialized in detection methods specific to particular types of attacks, such as FDI. However, few studies in the scientific literature have attempted to carry out an asset level risk assessment, such as that conducted in this study, which identifies critical assets, vulnerabilities, and controls. The reason behind this may be a lack of sufficient historical incident data, statistics on attacks, or information on compromised assets. Other reasons could include difficulties in conducting an asset-oriented security risk assessment due to the complex connections and interdependencies between these assets within smart grids, or simply due to confidential nature of security incidents.

Traditional OT systems (e.g., SCADA) at power systems companies have been fairly detached from IT systems and open public networks—a fact that is rapidly changing due to the smart grid evolution. Based on the security risk assessment carried out in this study, it would be most likely that the power grid operations layer will become the primary target for cyberattacks, since an attack on system level control solutions could have a wide adverse impact. With the enhanced connectivity of the operations layer, it can become increasingly vulnerable to traditional straightforward attack mechanisms, such as DoS attacks, thus obviating the need for more demanding mechanisms requiring domain knowledge, such as FDI on PMU measurements, to cause essential damage. In addition, the expanded role of software-based solutions in power grid management can be expected to further increase the vulnerability to supply chain attacks. As discussed in Section 8.3, supply chain attacks are becoming more prominent and are challenging to combat due to the multiple separate organizations involved. Clearly, the increasing amount of supply chain attacks is an issue that will also require specific attention in the electric energy sector.

Based on recent trends concerning cyber-attacks reported in the literature, it is notable that even though the power industry is an important target for cyber-attacks, it is less targeted than other industries such as the health sector. This could be due to the expertise required to mount these attacks in power systems as compared to other sectors. Attacking power grids and creating essential damage requires not only generic IT and communications expertise, but also domain specific knowledge on power system devices and operations. Furthermore, the reward gained by malicious actors for successfully attacking other industries could be higher when the primary motivation is a monetary benefit.

However, power systems become important targets during crises (i.e., war or pre-war situations) due to the crippling societal consequences of a major blackout. Furthermore, countermeasures particularly against cyber physical attacks are difficult due to the vast geographic coverage of electric power grids. The electric power systems do not have a clear and limited physical perimeter, as is the case, for example, with factories, hospital campuses, or the computer centers of financial institutions. The most impactful cyber-physical attacks would require cyberattacks (e.g., on SCADA) coordinated in parallel with physical attacks (e.g., on major substations and power lines). Such coordinated attacks are a complex endeavor requiring a major professional organization, such as a nation state. What makes cyberattacks particularly compelling during pre-war times is the difficulty in providing credible attribution. Nevertheless, in-depth research focusing on threat actors behind such cyberattacks cannot—to the best of our knowledge—be found in state-of-the-art academic publications. In contrast, industry reports released by cybersecurity organizations, such as ENISA and ECSO, discuss threat actors to a considerable extent, though mostly in a generic sense, not from a power grid perspective. ENISA's report on "Main incidents in the EU and worldwide" [42] indicates that organized crime groups (60%) and nation states (16%) comprised the most active threat actors in security incidents between 2019 and 2020. This finding is in line with our observation from the interviews in Sections 3–7. Other actors such as disgruntled employees and teenage malcontents are discussed to a lesser extent in both the interviews and the publications by EU cybersecurity organizations. In addition to identifying the main threat actors, the interviews also provided a mapping between them and the power grid assets, as discussed in Sections 3–7.

Finally, most of the literature is focused on tackling one small issue of security at a time. Works that would take an overall view on the problem and seek to find solutions that would provide security on a significantly higher level than what we are used to in IT are rare. The need for a significant leap forward in security compared to traditional IT is motivated by the fact that attacks in the electricity system can cause major societal disruption in the physical world, which is much more than what we expect for impacts in the digital world where the damage is most likely limited to loss of information and or money.

In this study, we conducted a qualitative risk assessment on power grid cybersecurity based on interviews across countries in Europe and in the U.S. to gain understanding of the latest developments and trends in the cybersecurity of future electric energy systems. The most exposed assets were identified to be the OT systems on the operation layer, in particular, SCADA and ADMS, with the most significant threats being False Data Injection (FDI), Denial of Service (DoS), supply chain, and ransomware and malware attacks. From the literature, we also identified how and to which extent these most significant risks are understood and addressed in the latest research and industry publications. The academic research on AI points out that AI techniques will be increasingly utilised in attack vectors, thus requiring industry to take anticipatory actions. On the other hand, academia should pay more attention to gaining a deeper understanding of the threat actors targeting power systems. Lastly, supply chain attack models from other industries could provide valuable insights into the types of incidents that could more frequently affect the power industry in the future.

Author Contributions: Conceptualization, S.B.; methodology, S.B.; investigation P.G. and S.B.; resources, R.K. and L.B.T.; data curation, P.G.; writing—original draft preparation, P.G. and S.B.; writing—review and editing, L.B.T. and R.K., visualization, P.G. and S.B.; supervision, R.K. and L.B.T.; project administration, S.B.; funding acquisition, R.K., S.B. and L.B.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Finnish public funding agency for research, Business Finland under the project "5G VIIMA", grant number 6430/31/2018.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Nor applicable.

Data Availability Statement: The data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

ADMS	Advanced Distribution Management System
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
APT	Advanced Persistent Threats
BCIM	Business Continuity and Incident Management
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIP	Critical Infrastructure Protection
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DoS	Denial of Service
DSO	Distribution System Operator
ECSO	European Cyber Security Organization
EMS	Energy Management System
ENISA	European Union Agency for Cybersecurity
ENTSO-E	European Network of Transmission System Operators
ETSI	European Telecommunications Standards Institute
EU	European Union
FDI	False Data Injection
FDIA	False Data Injection Attack
HMI	Human Machine Interface
IAM	Identity Access Management
ICS	Information and Communication Systems
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Standardization Organizations
IT	Information Technology
ML	Machine Learning
NERC	North American Reliability Corporation
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OS	Operating system
OT	Operational Technology
PMU	Phasor Measurement Unit
PSO	Power System Operator

RTU	Remote Terminal Unit
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SGAM	Smart Grid Architecture Model
SIEM	Security Information and Event Management
SOC	Security Operation Center
STIX	Structured Threat Information eXpression
TC	Technical Committee
TSO	Transmission System Operator
U.S.	The United States
USB	Universal Serial Bus

References

1. The European Union Agency for Cybersecurity (ENISA). *Smart Grid Security Annex II. Security Aspects of the Smart Grid*; The European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2012.
2. Liu, C.; Alrowaili, Y.; Saxena, N.; Konstantinou, C. Cyber Risks to Critical Smart Grid Assets of Industrial Control Systems. *Energies* **2021**, *14*, 5501. [CrossRef]
3. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* **2021**, *14*, 5894. [CrossRef]
4. Koutepas, G. Grid Attacks in Europe. European Union Computer Emergency Response Team (EU-CERT), 21 October 2021. Available online: https://www.edsoforsmartgrids.eu/save-the-date-4th-e-dso-encs-entso-e-event-on-cybersecurity-enhancing-our-grid-resilience/ (accessed on 20 November 2021).
5. *SFS-ISO/IEC 27005:2018*; Information Technology—Security Techniques—Information Security Risk Management. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
6. Iqbal, S.; Pipon-Young, L. The Delphi Method. The British Psychological Society. Available online: https://thepsychologist.bps.org.uk/volume-22/edition-7/delphi-method (accessed on 16 March 2022).
7. Gollmann, D. *Computer Security*; Wiley: Hoboken, NJ, USA, 2016.
8. *ISO/IEC 13335-1:2004*; Information Technology—Security Techniques—Management of Information and Communications Technology Security. International Standards Organization (ISO): Geneva, Switzerland, 2004.
9. CEN-CENELEC-ETSI Smart Grid Coordination Group. *Smart Grid Reference Architecture*; CEN-CENELEC-ETSI Smart Grid Coordination Group: Valbonne-Sophia Antipolis, France, 2012.
10. North American Electric Reliability Corporation. About NERC. 2021. Available online: https://www.nerc.com/AboutNERC/Pages/default.aspx (accessed on 28 January 2022).
11. North American Electric Reliability (NERC). Standing Committees. 2020. Available online: https://www.nerc.com/comm/Pages/default.aspx (accessed on 17 January 2022).
12. International Electrotechnical Commission (IEC). Generation, Transmission and Distribution of Electricity-General. 1985. Available online: https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=601-03-02 (accessed on 18 November 2021).
13. Institute of Electrical and Electronics Engineers (IEEE). Power Electronics. Available online: https://ewh.ieee.org/soc/pels/home/Control-Theory.php (accessed on 19 November 2021).
14. EATON. Substation Automation: Fundamentals of Substation Automation. 2021. Available online: https://www.eaton.com/us/en-us/products/utility-grid-solutions/grid-automation-system-solutions/fundamentals-of-substation-automation.html (accessed on 19 November 2021).
15. Padilla, E. *Substation Automation Systems: Design and Implementation*; Wiley: Hoboken, NJ, USA, 2016.
16. Chuan, S.; Yao, Y.; Fu, Q.; Yang, W. A cyber-physical model for SCADA system and its intrusion detection. *Comput. Netw.* **2021**, *185*, 107677. [CrossRef]
17. Shamseldein, M.; Abdelaziz, A. Energy Management for Medium-Voltage Direct Current Networks. In *Medium Voltage Direct Current Grid*; Academic Press: Cambridge, MA, USA, 2019. [CrossRef]
18. Gartner Glossary. Information Technology Gartner Glossary. 2021. Available online: https://www.gartner.com/en/information-technology/glossary/advanced-distribution-management-systems-adms (accessed on 8 November 2021).
19. IBM. IEC CIM Advanced Metering Infrastructure. IBM Corporation. 2013. Available online: https://www.ibm.com/docs/en/netcoolomnibus/8?topic=integrations-iec-cim-advanced-metering-infrastructure (accessed on 11 November 2021).
20. U.S. Department of Energy (DOE). *Advanced Metering Infrastructure and Customer Systems*; Office of Electricity Delivery and Energy Reliability: Washington, DC, USA, 2016.
21. Musleh, A.; Chen Guo, D.; Zhao, Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
22. Almasabi, S.; Alsuwian, T.; Javed, E.; Irfan, M.; Jalalah, M.; Aljafari, B.; Harraz, F. A Novel Technique to Detect False Data Injection Attacks on Phasor Measuremnet Units. *Sensors* **2021**, *21*, 5791. [CrossRef] [PubMed]
23. Das, T.; Ghosh, S.; Koley, E. Prevention and detection of FDIA on power-network protection scheme using multiple support set. *J. Inf. Secur. Appl.* **2021**, *63*, 103054. [CrossRef]

24. Ghafouri, M.; Au, M.; Kassouf, M.; Debbabi, M.; Assi, C.; Yan, J. Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids. *IEEE Trans. Smart Grid* **2020**, *11*, 3004303. [CrossRef]
25. Nejabatkhah, F.; Li, Y.; Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2020**, *14*, 27. [CrossRef]
26. The European Union Agency for Cybersecurity (ENISA). *Distributed Denial of Service ENISA Threat Landscape*; The European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2020.
27. European Cyber Security Organization (ECSO). *Energy Network and Smart Grids: Cyber Security for the Energy Sector*; European Cyber Security Organization (ECSO): Brussels, Belgium, 2018.
28. Kummerow, A.; Rösch, D.; Nicolai, S.; Brosinksky, C.; Westermann, D.; Naumnann, A. Attacking dynamic power system control centers—A cyber-physical threat analysis. In Proceedings of the 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16–18 February 2021. [CrossRef]
29. Yang, Y.-S.; Shih-Hsiung, L.; Wei-Che, C.; Chu-Sing, Y.; Yuen-Min, H.; Ting-Wei, H. Securing SCADA Energy Management System under DDos attacks using token verification approach. *MDPI Appl. Sci.* **2022**, *12*, 530. [CrossRef]
30. Cadzow, S.; Giannopoulos, G.; Merle, A.; Storch, T.; Vishik, C.; Gorniak, S.; Ikonomou, D. *Supply Chain Integrity—An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward*; The European Union Agency For Network And Information Security (ENISA): Athens, Greece, 2015.
31. The European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape for Supply Chain Attacks*; The European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2021.
32. Yeboah-Ofori, A.; Islam, S. Cyber Security Threat Modeling for Supply Chain Organizational environments. *Future Internet* **2019**, *11*, 63. [CrossRef]
33. Deloitte. *Managing Cyber-Risk in the Electric Power Sector, Emerging Threats to Supply Chain and Industrial Control Systems*; Deloitte: London, UK, 2019.
34. Amara, T.; Gondim, J. Integrating Zero Trust in the cyber supply chain security. In Proceedings of the 6th Workshop on Communication Networks and Power Systems (WCNPS 2021), Brasilia, Brazil, 5 December 2021. [CrossRef]
35. Yeboah-Ofori, A.; Ismail, U.; Swidurski, T.; Boateng, F. Cyberattack Ontology: A Knowledge Representation for cyber supply chain security. In Proceedings of the International Conference on Computing, Computational Modelling and Applications (ICCMA), Brest, France, 14–16 July 2021. [CrossRef]
36. Threatpost. 2021: The Evolution of the Ransomware. April 2021. Available online: https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf (accessed on 17 January 2021).
37. Check Point Software Techologies Limited. *Cyber Security Report 2021*; Check Point Software Techologies Limited: Ramat Gan, Israel, 2021.
38. BBC. Revil Ransomware Gang Arrested in Russia, 14 January 2022. Available online: https://www.bbc.com/news/technology-59998925 (accessed on 17 January 2021).
39. Nicol, D. The Ransomware Threat to to Energy-Delivery Systems. *IEEE Secur. Priv.* **2021**, *19*, 24–32. [CrossRef]
40. The European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2021—April 2020 to Mid-July 2021*; The European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2021.
41. The European Union Agency for Cybersecurity (ENISA). *Sectoral/Thematic Threat Analysis ENISA Threat Landscape*; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2020.
42. The European Union Agency for Cybersecurity (ENISA). *Main Incidents in the EU and Worldwide*; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2020.