

# Cybersecurity in Power Grids: Challenges and Opportunities

Tim Krause<sup>a</sup>, Raphael Ernst<sup>a</sup>, Benedikt Klaer<sup>b,c</sup>, Immanuel Hacker<sup>b,c</sup>, Martin Henze<sup>a</sup>

<sup>a</sup>Cyber Analysis & Defense, Fraunhofer FKIE, Wachtberg, Germany

<sup>b</sup>Digital Energy, Fraunhofer FIT, Aachen, Germany

<sup>c</sup>High Voltage Equipment and Grids, Digitalisation and Power Economics, RWTH Aachen University, Aachen, Germany

---

## Abstract

Increasing volatilities within power transmission and distribution force power grid operators to amplify their use of communication infrastructure to monitor and control their grid. The resulting increase in communication creates a larger attack surface for malicious actors. Indeed, cyber attacks on power grids have already succeeded in causing temporary, large-scale blackouts in the recent past. In this paper, we analyze the communication infrastructure of power grids to derive resulting fundamental challenges of power grids with respect to cybersecurity. Based on these challenges, we identify a broad set of resulting attack vectors and attack scenarios that threaten the security of power grids. To address these challenges, we propose to rely on a defense-in-depth strategy, which encompasses measures for (i) device and application security, (ii) network security, (iii) physical security, as well as (iv) policies, procedures, and awareness. For each of these categories, we distill and discuss a comprehensive set of state-of-the-art approaches, and identify further opportunities to strengthen cybersecurity in interconnected power grids.

**Keywords:** Critical infrastructure, Cyber-physical security, Cybersecurity, Power grid, Power system communication

---

## 1. Introduction

Historically, power grids have grown from simple, localized grids to large, physically wide-spread grids, often spanning multiple nations or even whole continents [1]. Despite its importance to modern society, the energy sector has adapted slower than other industries to digital technology due to its size and need for high system availability. Because of the need for more efficiency, digital technology gets more widespread and new technologies in the power grid heavily rely on high-frequency monitoring cycles and adaptation to bottlenecks in the grid [2]. This trend is boosted with the rise of renewable energy (ranging from large off-shore wind farms matching the power generation of traditional power plants to a single household feeding solar energy into the grid) [3, 4], which leads to power generation becoming more distributed and thus less reliable, resulting in difficult to organize transmission and distribution of energy [5, 6].

This results in a less controllable situation than in the past, when only a small number of bulk power production plants were required. While increasing power demands can be satisfied with more traditional or renewable power plants, the grid itself needs to support the transportation of the generated power. However, extending the grid by adding new lines is prohibitively expensive and often slowed down, e.g., by regulations or resistance of residents. Fortunately, digital technology can aid in better utilizing the existing grid, leading to an increased deployment of digital technology to control, monitor, and maintain transmission and distribution of power [7].

This increasing use of digital technology requires more and more networking capabilities and connects previously isolated components with larger communication networks [8–10], re-

sulting in a large variety of new dataflows [11]. The resulting increasing interconnection of power grids raises severe security concerns [12]: Protocols and systems originally developed for power grids were not designed with security in mind. Yet, these systems are still used alongside modern technology and increasingly exposed to outside networks such as the Internet. Likewise, the increasing use of digital and decentralized technology provides a larger attack surface [13–15]. Indeed, different cyber attacks have successfully targeted essential parts of the power grid [16, 17]. Resulting disruptions and wide-scale outages of electrical power have extensive social and economic consequences [18].

**Contributions.** This paper specifically targets the security challenges originating from the increasing interconnection of power grids, especially at the transmission and distribution level. To this end, we motivate the need for cybersecurity when operating power grids and outline promising approaches that improve security at different levels of abstraction. More specifically, our contributions in this paper are:

1. We provide a high-level overview over the communication infrastructure of power grids and derive resulting fundamental challenges w.r.t. cybersecurity risks (Section 2).
2. As a foundation to secure power grids, we identify a comprehensive set of attack vectors and scenarios based on these security challenges (Section 3).
3. We distill and discuss promising approaches that provide security for interconnected power grids to protect against serious attack vectors and scenarios (Section 4).

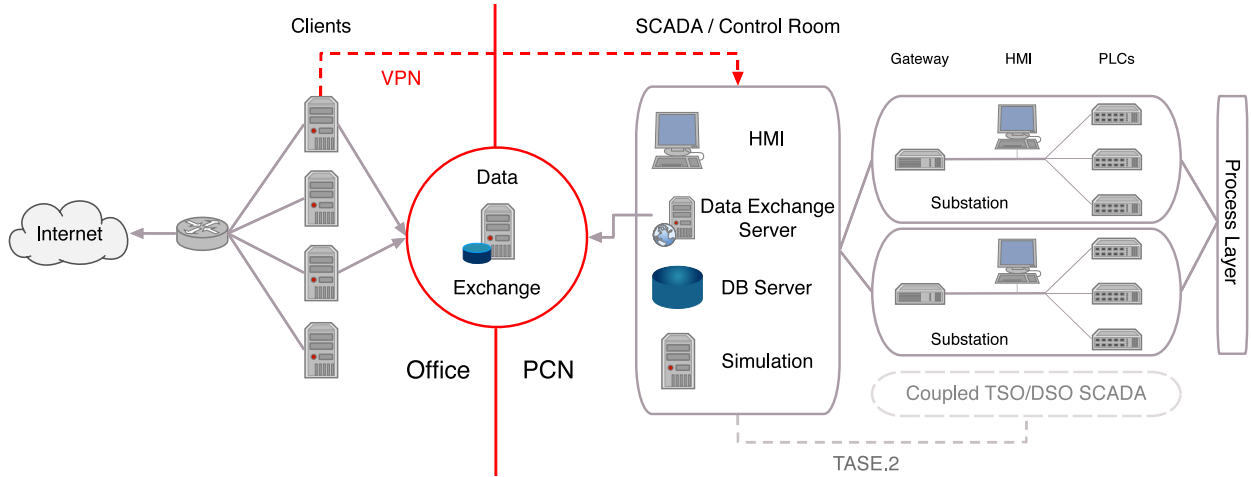


Figure 1: A simplified view of a TSO/DSO network, separated into office network (connected to the Internet, typical data processing tasks) and process control network (SCADA traffic, connecting the control room with substations and field devices). While data should only be exchanged through a dedicated data exchange server, in reality, these networks are often interconnected, e.g., with VPNs.

As such, our contributions are relevant for both, cybersecurity researchers who are usually not familiar with the processes and terminology of electrical engineering, as well as electrical engineers and power grid operators who have a decent understanding of power grids but are often unaware of the extent and specifics of cybersecurity challenges.

## 2. Communication Infrastructure of Power Grids and Resulting Cybersecurity Challenges

With the increasing digitalization of power grids, operators are confronted with rapid changes regarding the amount of necessary communication and the means through which this communication is conducted. As a result, more and more communication is introduced to power grids. In the following, we first describe the communication infrastructure of power grids, before focusing on the fundamental security challenges resulting from an increasing interconnection of power grids.

We use the term *grid* exclusively to refer to the power grid and the term *network* for digital communication networks. Furthermore, the information contained in this paper mainly focuses on European power grids. However, many of the proposed changes to cybersecurity also apply to other regions. In this context, we refer to *transmission* of power as the transportation of energy over long distances (e.g., between distant cities, not within a city) and *distribution* of power as the transportation on a local scale such as a single city or small region. The transmission of power is overseen by *Transmission System Operators* (TSO), while the distribution of power is carried out by *Distribution System Operators* (DSO).

### 2.1. Communication Infrastructure of Power Grids

To illustrate the typical communication infrastructure found in power grids, we provide a simplified view of the network of a grid operator, i.e., a TSO or DSO, in Figure 1. Typical to such a network is the separation between *office network* and *process control network* (PCN). The office network is similar to

any usual corporate network with, e.g., email traffic or data processing. Contrary, the PCN connects the control room of grid operation companies with their substations and field devices, typically using DNP3 [19] (North America and parts of Asia) or IEC 60870-5-104 [20] (rest of the world) as protocol. Resulting control messages are usually interpreted by a *programmable logic controller* (PLC) and then passed to the process layer. The control room typically contains a *human-machine interface* (HMI), a database (DB) server managing grid information, and a simulation server for pre-computing the effects of grid changes. Furthermore, the control room is connected to multiple substations (each containing at least a gateway, an HMI, and multiple PLCs) and can be coupled with other TSO/DSO SCADA systems for mutual control.

Data exchange between office network and PCN should only be handled through a dedicated data exchange server, where every file is checked for malware before being passed through. Sometimes though, as seen in the Ukraine attacks [16], there are other communication channels, such as VPNs, which allow direct communication between the office network and the PCN or remote maintenance lines for vendors or contractors.

### 2.2. Fundamental Cybersecurity Challenges

While the increasing digitalization of power grids is necessary to deal with changing power demands and generation, it raises fundamental security challenges. In the following, we introduce and highlight the most important challenges or mechanisms in electrical power grids impacting cybersecurity.

#### 2.2.1. CIA Triad: Availability is Key

The triad of confidentiality, integrity, and availability (CIA) [21] as the fundamental concept of information security has to be interpreted slightly differently in the energy sector. In traditional cybersecurity, it is generally preferable to ensure confidentiality and integrity and sacrifice (some) availability. In power grids, however, availability is by far the most important measure of the triad as the consequences of downtimes can be

severe [18]. The longer a blackout lasts and the more of the grid is affected, the harder it is to rebuild the grid [22]. To illustrate the race for availability, the German power grid had an end-consumer availability of 99.9995% in 2017 [23], compared to the allegedly highly available Google services with 99.978% (no scheduled downtime) [24]. When measured in time, the power grid has a more than 45-fold higher availability. As availability is the most important measure in power grids, any measures ensuring the confidentiality and integrity of systems should never interfere with the availability of power delivery.

### 2.2.2. Balancing Generation and Consumption

Electrical power grids rely on a stable grid frequency of either 50 Hz or 60 Hz due to the use of alternating current. The frequency is only stable if power generation and consumption are at an equilibrium. If more power is generated than consumed, the frequency rises and vice versa.

The operation reserve ensures the equilibrium between production and consumption at any given time. In Europe, the operation reserve is separated in three different stages: primary operation reserve, secondary-reserve, and minute reserve. The primary control is a continuous frequency load control, where the controller is implemented as a droop control distributed to different power plants. Thereby, the amount of primary operation reserve is 3 GW which is the power rating of two mayor generation units (e.g., nuclear power plants). The secondary-reserve and minute-reserve will be activated if the frequency derivation holds on. More specifically, the secondary reserve has to be activated after 5 minutes of frequency derivation and will be replaced by the minute reserve after 15 minutes. These are both activated centrally by the grid operator in whose grid area the power deviation occurred. However, at deviations of 1 Hz, either some consumers, possibly multiple cities, have to be disconnected from the grid (in case of decreased grid frequency) or power plants have to be downregulated to save the generators from damage [25, 26].

The sensitive equilibrium between generation and consumption can be exploited by attackers, as they only need to control a comparably small amount of consumption or generation to use cascading effects within the grid to create a system-wide blackout [27, 28], as power generation and consumption in the operating reserve have time delays.

### 2.2.3. Decentralization of Power Generation

The rise of renewable energy has empowered many individuals and companies to enter the energy sector [29]. For example, individual households can now feed their excess solar energy into the grid. Naturally, the security of their systems is not as tightly controlled as those of traditional energy companies. As a result, the hardware and software use by individuals to operate power generation are often not as secure as it should be or misconfigured [30], potentially impacting transmission and distribution in the grid.

Assuming a vulnerability in a large number of, e.g., solar installations, is found, attackers may control the power fed into the grid. Consequently, an attacker can do considerable damage even when controlling only a comparably small section

of the grid by exploiting cascading effects (see above) [29]. By controlling the feeding of power into the grid, an attacker could exploit these cascading effects with the goal to cause a system-wide blackout, impacting distribution and transmission [27, 28].

### 2.2.4. No Security in Process Control Networks

Most devices used in power grids, such as protection devices or PLCs, are designed for multiple-decade use. Often, they are neither patched nor replaced. The most widespread protocols are DNP3 [19] (mostly used in North America and parts of Asia) and IEC 60870-5-104 [20] (predominantly used by the rest of the world). These protocols have been developed more than 20 years ago with no security concerns in mind [31]. Despite their wide-spread use by DSOs and TSOs, neither protocol supports basic security mechanisms such as authentication or integrity protection, which have been taken for granted for years in other commercial sectors. For example, IEC 60870-5-104 [20] as used by DSOs and TSOs is susceptible to man-in-the-middle, denial-of-service, replay, and spoofing attacks [32–34]. Similar observations have been made for the DNP3 [19] protocol [35–37]. While the standard IEC 62351 provides additional cybersecurity concepts [38], it is not (yet) supported by many devices and networks such that its deployment is rather slow or even non-existent.

As grid operators often use their own separated networks over dedicated physical cables, they could neglect further security mechanisms in the past, leading to networks which do not necessarily use cryptography, authentication, or integrity checks. Past attacks have shown that office networks (connected to the Internet) are often not sufficiently separated from the PCN, allowing attackers lateral movement between the two networks [16]. Once an attacker gains access to an unsecured PCN, simple tools enabling communication in the specific protocol may be used to control devices crucial for grid operation.

### 2.2.5. Difficulties of Physical Network Changes

Field devices in power grids have planned lifetimes which are measured not in years but decades [39]. Information technology has much faster development cycles, allowing the development of attacks for devices which may have to be in use for many more years. It is very unlikely that all energy companies will be able to always follow current security best-practices by simply exchanging devices for newer models, which, e.g., support more modern protocols such as IEC 61850 [40].

If possible at all, modern security mechanisms have to be implemented in software only and run on the available hardware or be able to interface directly with the specialized devices used by grid operation companies, without affecting the availability of electricity supply. However, many devices in use may not have the computational power to support additional security functionality [41–45]. Even if certain devices are eventually exchanged or upgraded with new software, they are often required to support legacy protocols to be able to communicate with older devices still relying on these protocols. Consequently, distribution and transmission system operators suffer from the well-known problem of insecurity by inheritance [46].

	Scope	Difficulty	Impact	Examples
<b>Lateral Movement</b>	Single Operator	High	High	[16, 59, 60]
<b>Physical Access</b>	Local	Medium	Medium	[48–51]
<b>Remote Maintenance Access</b>	Multiple Operators	High	High	[52–54]
<b>Third-Party Exploit</b>	Multiple Operators	High	Medium	[17, 55, 58]
<b>Overcoming Air Gap</b>	Local	High	Medium	[59, 60]
<b>Insider Attack</b>	Single Operator	Low	High	[48, 63]
<b>Cascading Effects</b>	Multiple Operators	High	High	[27, 28]

Table 1: Classification of attack vectors specific to the energy sector and power grids.

### 2.2.6. Weakest Link Problem

For attacks to have devastating consequences, an attacker does not have to target the largest grid operator. As long as the victim of an attack has control over enough power to affect the grid frequency, the attacker can leverage cascading effects to affect the whole power grid. As smaller operators often lack the means to harden their devices and networks as much as larger operators, such targets may be more attractive to attackers. Furthermore, attacks do not have to be limited to grid operators: An attacker controlling a larger number of consumer electronics, e.g., solar power cells, might still be able to influence the frequency within the grid [28].

As a result, there is a need to develop solutions which can be used by all relevant actors in interconnected power grids and are not only deployable by larger grid operators.

## 3. Attack Vectors and Scenarios

Practical cybersecurity in interconnected power grids is impacted by a diverse set of fundamental security challenges (cf. Section 2.2). As a foundation to overcome these challenges and thus provide security for distribution and transmission grids, we now identify attack vectors and attack scenarios that result from the fundamental security challenges. In the following, we first discuss the most important attack vectors before we present the attack scenarios enabled by these vectors.

### 3.1. Attack Vectors in Distribution and Transmission Grids

Attackers can leverage different attack vectors to compromise the network of a transmission or distribution system operator with the goal of causing a blackout or at least considerable disturbance in the power grid. To achieve this goal, an attacker will likely aim to compromise the PCN of the target system. From there, the attacker can compromise substations or field devices, thus gaining control over parts of the grid. In the following, we discuss the most important attack vectors an attacker can exploit to access a PCN. We provide a summary of our classification of attack vectors in Table 1.

#### 3.1.1. Lateral Movement from the Office Network

In the attacks on Ukrainian grid operators in 2015 [16], attackers gained access to the PCN through lateral movement from the office network (cf. Figure 1). Allowing communications between PCN-connected devices and the office network

might be necessary, e.g., to transfer certain information such as environment data between office network and control room. An attacker can comprise an office network, e.g., by sending spear-phishing emails to certain employees or by exploiting vulnerabilities in applications such as web browsers or office suites [47]. Once access to a machine in the office network has been gained, the attacker can passively listen for user credentials and search for, e.g., a VPN tunnel to the PCN. Lateral movement from the office network is one of the most dangerous attack vectors for power system operators. An attack would, however, be limited to a single network.

#### 3.1.2. Physical Access

Energy providers often use their own dedicated cable networks for PCN communications (cf. Section 2.2.4). While this certainly provides an extra level of security, it does not offer any protection once an attacker has gained physical access to one device in the network. For example, substations are usually connected to the PCN and are controlled remotely without personnel being present. Therefore, an attacker can gain physical access to the network by breaking into a substation and then manually use available systems or connect its own device to the PCN [48]. Break-ins in substations already happen today [49, 50], although mostly with the intention to steal and then sell copper cables [48, 51]. Hence, such a theft could be used as camouflage by cyber attackers to deter grid operators from even looking for traces of a cyber attack. Such an attack could have a large influence on grid operations but does not scale well, as it necessitates physical presence at (possibly multiple) substations.

#### 3.1.3. Remote Maintenance Access

Manufacturers of control room software and hardware usually have a maintenance contract with the grid operators using their systems. To be able to debug these systems remotely or to deploy software updates, these systems are typically equipped with some form of remote maintenance access [52]. Depending on the technology used and security measures in place, attackers may try to exploit this maintenance access to gain access to the PCN. Such maintenance access is typically hardened against cyber attacks. However, if a vulnerability is found, an attack could have a considerable impact at multiple operators and wide-ranging control over the PCN is likely. As an example, in 2014 ICS-CERT reported on a security breach at a public

utility where the attacker used standard brute forcing techniques to gain access to a password-protected remote access [53]. The risk of this attack vector is further illustrated by an incident from 2013, in which attackers compromised a vendor of a large power producer in the US and Canada to exfiltrate passwords potentially used for remote maintenance access [54].

#### 3.1.4. Third-Party Exploit

Attack vectors are not limited to the premises of grid operators. In fact, exploiting third-parties such as suppliers or subcontractors is one of the most dangerous and hard to control attack vectors. For example, the actors behind the Dragonfly malware, which specifically targets energy systems, compromised three different manufacturers of ICS equipment and inserted their malware into software available on the manufacturers' websites [55]. Likewise, for the attack on the Ukrainian power grid in 2016 [17], attackers compromised manufacturers of field devices and manipulated firmware update installers on the publicly available websites of the manufacturers. Employees at the affected DSO then downloaded and deployed these updates, consequently unknowingly installing the attackers' malware which allowed the attackers to gain access to PCN-connected devices.

Moreover, in case the manufacturer of the control room software is compromised, attackers may have direct access to the remote maintenance access of multiple grid operators. This becomes especially relevant when relying on cloud resources [39, 56, 57]. In a different case, the turbine control system of a power company in the United State was unintentionally infected with a virus through an infected USB drive plugged in by a third-party technician during maintenance [58]. A special case of a third-party exploit would be a compromise of the supply chain during the manufacturing of field devices. If attackers are able to tamper with devices before they are installed at the grid operator, they might, e.g., install a covert channel for remote access. The impact of such an attack would be high and could result in extensive access to the PCN. A single exploit could be used to gain control over multiple grid operators.

#### 3.1.5. Overcoming Air Gap

Even if PCNs are air-gapped, i.e., physically isolated from other networks such as the office network to prevent lateral movement, attackers can still try to attack a PCN by strategically placing USB drives containing malware around a facility they are targeting. Consequently, curious or helpful employees may unknowingly compromise air-gapped systems by connecting such drives to devices in company networks. Such an attack would likely be local in scope with a medium impact, as attackers could only execute previously determined attacks. Because of the air gap, there will be no immediate feedback on the attacks' success to an adversary. Indeed, malware-infected USB drives are one suspected attack vector of Stuxnet [59, 60]. Notably, air-gapped systems in areas with even stronger security requirements such as military bases [61] or the international space station [62] have shown to be susceptible to such attacks, especially using USB drives.

#### 3.1.6. Insider Attack

If an attacker already works within the energy sector or compromises an employee of a grid operator, the attacker might have direct access to the control room or field devices and could therefore directly control devices or introduce malware, even to air-gapped systems. Insider attacks are hard to predict and protect against. In the case of an insider, no further compromise of systems may be necessary, as the attacker has legitimate access to the PCN. Different examples of disgruntled employees misusing their authority have been reported by Brdiczka [63]. For example, a disgruntled employee caused a power outage during the 2002 Winter Olympics by knocking out a substation in Salt Lake City [48]. An insider attack can have a high impact on the grid, especially since insiders typically have decent knowledge of the inner workings of grids and potential security measures in place, thus being able to carefully pick their target.

#### 3.1.7. Cascading Effects

Instead of having to compromise the network of one or more grid operators, an attacker may leverage cascading effects in the power grid to cause a power outage (cf. Section 2). For example, by remotely gaining control over a large number of consumer electronics such as solar power cells [64], an attacker can take advantage of the mechanics of the operating reserve to influence the frequency within the grid [28]. There are also companies that centrally manage many distributed solar or wind plants, e.g., within the scope of a virtual power plant [65]. A compromise at one of these service providers may allow attackers to leverage similar effects. An attack exploiting cascading effects could be global in scale with a medium to high impact (depending on the amount of power under the attackers' control) but has a high technical difficulty, as a comparably large number of devices has to be exploited and controlled simultaneously. However, already today, larger botnets, e.g., Conficker, Hajime, or WannaCry, control hundreds of thousands to millions of devices [66–69] making such attacks less unlikely than it appears. The problem might further exaggerate with the rise of electric mobility, as electric cars as well as their charging infrastructure [70] will be networked, facing their own cybersecurity risks combined with a high amount of energy consumption under their control.

### 3.2. Attack Scenarios

Different vectors can be used to attack distribution and transmission systems to disrupt vital control systems. We assume an attacker accessing a PCN to aim at disrupting the power grid and do not specifically consider pure passive attacks such as industrial espionage. In the following, we briefly discuss the three most important methods an attacker with access to the PCN can employ.

#### 3.2.1. Disconnecting Resources

If an attacker has gained full access to the PCN, we can assume that the attacker is able to send arbitrary control commands to connected control systems, since commonly used communication protocols lack even basic authentication or authorization features. Thus, an attacker can, e.g., control switches in

substations which disconnect entire power lines or power plants from the grid, possibly leading to an immediate loss of the power supply to consumers. In the attack on Ukraine in 2015, 225 000 consumers were disconnected from the grid, as attackers were able to control switches in multiple substations [16].

### 3.2.2. Injecting False Information

If an attacker can only gain control over a small subset of field devices, he can still indirectly influence the power grid, e.g., by sending forged or manipulated sensor readings to the control room [71, 72]. The operators in the control room may act on the wrong data and take steps to correct a non-existent problem [73, 74], which may lead to disruption in the power grid, e.g., unintentionally overloading a power line because sensor readings show a normal load. Depending on the sophistication of the attack, SCADA software may be able to identify a problem through bad data detection algorithms. However, these have been shown to not always be effective [75].

### 3.2.3. Denial of Service

Even if attackers neither have full access to the PCN nor can inject (false) information, they may still be able to manipulate certain devices and effectively render them non-functional, resulting in a denial of service attack against parts of the power grid [71]. For example, in the attacks on the Ukraine power grid in 2016 [17], the CRASHOVERRIDE malware used by the attackers was able to disable Siemens SIPROTEC devices, manipulate the firmware of serial-to-ethernet devices, and hence disrupt crucial substation functions such as protection, automation or measurement. In future attacks, similar methods could, e.g., allow attackers to overload power lines even if these are secured by protection devices, potentially leading to physical damage.

## 4. Providing Cybersecurity for Interconnected Power Grids

Given the tremendous threats resulting from the diverse set of attack vectors and scenarios, providing security for power transmission and distribution within the grid is a paramount objective. We claim that future improvements in the security of power grids will have to be a combination of technical approaches, awareness measures, and closer collaboration between the electrical engineering community and cybersecurity experts. To provide a way forward for security in interconnected power grids, we thus identify a set of diverse security solutions and approaches including both, security software as well as organizational measures such as security training, which complement each other nicely. More specifically, we draw from the principle of *defense-in-depth* [76–78] as illustrated in Figure 2, to provide a comprehensive set of security measures at different layers. These measures encompass approaches for (i) device and application security, (ii) network security, (iii) physical security, as well as (iv) policies, procedures, and awareness. While discussing all four aspects in more detail in the following, we specifically focus on approaches to provide network security, since the need to protect communication becomes especially important with an increasing interconnection of power grids.

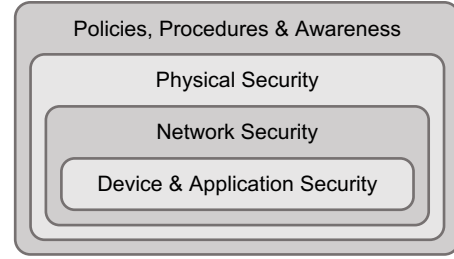


Figure 2: Following the principle of defense-in-depth, providing security for interconnected power grids needs to encompass a comprehensive set of measures for (i) device and application security, (ii) network security, (iii) physical security, as well as (iv) policies, procedures, and awareness.

### 4.1. Device & Application Security

As a foundation to provide defense-in-depth, all devices and applications deployed in power grids have to be secured. This becomes especially important considering an increasing interconnection in power grids, thus exposing potentially vulnerable devices and applications to larger attack surfaces. Especially in the context of interconnected power grids, one promising approach consists of device and application diversity, i.e., using a wide range of different hardware and software to thwart a worst-case scenario where malware pervasively compromises all equipment [79]. Before integrating new devices into the network or deploying updates to devices, static firmware analysis [80] can be used to detect susceptibility to vulnerabilities as well as malware and default credentials contained in a firmware image. Following a different direction, security assessments allow to additionally detect insecure configurations and test for vulnerabilities at runtime [81–83]. Such approaches also show promising benefits for device and application security in power grids [84, 85].

Once firmware has been analyzed, assessed for security, and subsequently deployed on devices controlling the power grid such as PLCs, operators have to ensure that the applications running on these devices do not get compromised. To this end, different approaches for hardware-based [86] or software-based [87] remote code attestation allow to verify the integrity of code, its execution, and updates. Within the context of interconnected power grids, remote attestation can, e.g., be used to detect compromised devices based on changes in their physical memory [79, 88]. Likewise, hardware performance counters can be utilized to detect modifications in firmware of critical infrastructure components [89]. From a different angle and complementing approaches to provide network security, deploying security agents to individual components such as PLCs aids in applying security patches, maintaining end-to-end-security, as well as managing alarms [90–92].

### 4.2. Network Security

The increasing use of digital technology in power grids demands for more and more networking capabilities, resulting in the connection of previously isolated components to larger communication networks [8, 10]. To address resulting security concerns, we require methods to proactively prevent security incidents, most prominently using *network separation*, and to

detect security incidents that successfully bypassed preventive measures using *intrusion detection systems*.

#### 4.2.1. Network Separation

Traditional network separation through demilitarized zones (DMZ) and virtual networks is a standard tool for securing networks. These techniques make it harder for attackers to get a comprehensive view of the network through simple reconnaissance methods and restrict lateral movement within the network. DMZ and virtual networks are already used today by grid operators [84] and their deployment is often enforced through laws [93]. More recently, software-defined networking (SDN) provides a more flexible alternative to DMZ and virtual networks, which are usually configured once at the creation of a network and cannot easily be changed during operation. With SDN, changes to network separation can be configured quickly, e.g., to counter cyber attacks. Likewise, SDN can be used to enforce network compliant behavior, e.g., specified using communication rules by the operator of the communication network [94, 95]. Dong et al. [96] and White et al. [97] provide more information on the opportunities and challenges of using SDN for smart grid resilience. The main challenges of SDN approaches for securing power grids result from availability concerns of grid operators.

#### 4.2.2. Intrusion Detection Systems

Intrusion detection systems (IDS) are used in most company networks to detect attackers through suspicious network activities [98, 99]. While not all companies in the energy sector are using IDS to secure their PCNs today, often citing availability concerns, we assess that IDS are especially well-suited to provide security in interconnected power grids: In contrast to office networks of large companies, traffic in PCNs is well defined as only certain protocols are used and, in most cases, any piece of software or hardware communicating over the network is known in advance [100]. An IDS in a PCN can, therefore, be much more restrictive without affecting operations than in an office network, where a large number of protocols and devices might communicate with each other and unknown Internet endpoints. Still, an attacker doing active reconnaissance (e.g., a port scan) could even easily be detected by a simple traditional IDS which is not specialized on industrial control systems.

Existing IDS deployments can be classified into network-based and host-based approaches [77]. We assess that combining both approaches to secure PCNs offers significantly more value than relying on a single approach only. Furthermore, distributed and process-aware IDS allow to further strengthen security in interconnected power grids. In the following, we discuss the different approaches for IDS and their application to the energy sector.

Most of the communication in a PCN in the energy sector is conducted between the control room and substations or field devices. Consequently, a *network-based IDS (NIDS)* should be deployed at nodes in the network such as switches to be able to monitor any traffic within the PCN, especially those sent from the control room or towards it. Such an IDS can then easily detect reconnaissance measures, e.g., port scans. Moreover, as

traffic in PCNs is well defined, a network-based IDS can detect further suspicious network activity, e.g., an increase in the number of packets sent from a network node or communication between network nodes that have not communicated beforehand. An emerging challenge in NIDS within a PCN is the question of how to cope with the ever changing and dynamic smart grid environment [72, 98].

A *host-based IDS (HIDS)* runs on a single host in a networked environment and is therefore only able to monitor the incoming and outgoing traffic on this device. But in contrast to NIDS, HIDS also monitor log files, system policies, and other relevant data concerning the host they are installed on. These systems should be used wherever possible to supplement network-based IDS in the PCN. Not all switches in a network may offer a monitoring port or there might be other restrictions, why network-based systems cannot be used for parts of the network. In such cases, HIDS can be used to still monitor most parts of the traffic. HIDS can, e.g., detect and block a denial-of-service attack targeting a device within the PCN. However, within a PCN a challenge for HIDS are the specialized hardware used. It will only be possible to install host-based IDS on a certain subset of systems. For highly at-risk hardware, e.g., some PLCs, a host-based IDS could be implemented by using a gateway between the network and the PLC to monitor any incoming and outgoing traffic [101].

A *distributed IDS* for the power grid combines network-based and host-based IDS and centrally aggregates and correlates data provided by the systems distributed within the PCN [102]. Such a distributed IDS allows a more complete view on the traffic within the PCN compared to many individual systems. Attacks from multiple points within the network can be correlated and dealt with more specifically. Moreover, compromised devices may be more easily identified. The collected data can be processed at a central location and could be used to help the operators in the control room to make well-founded decisions. A major challenge for distributed IDS within a PCN is the placement of the nodes as this influences the quality of the aggregated data.

A *process-aware IDS* employs context information about the environment in which it is placed. Chromik et al. [103] recently developed such a system for local substation networks. In their approach, which employs the event-based network security monitor Bro (now Zeek) [104], they check incoming control commands for consistency with safety requirements and physical constraints. Their approach maintains a model of the local system, which is updated through sensor readings and commands sent through the IEC 60870-5-104 protocol. At the current stage, inconsistent commands yield an alert message, which has to be acted on manually. Such systems could, e.g., be extended to block commands if their execution would lead to an inconsistent state, especially when adapted to more modern grid communication protocols.

The concept of process-aware IDS is especially interesting in a SCADA and industrial control systems (ICS) environment, where valid traffic is well-defined and commands lead to physical changes in the controlled system [105]. In combination with distributed IDS, such approaches can lead to substantially more



secure grids, while introducing a minimum of extra hardware into the PCN. However, the main challenge for deploying such a system lies in the considerable knowledge which is required about the individual environment. Future work is necessary to automatically adapt to differences between grid operators, e.g., w.r.t. used hardware, software, protocols, and topologies.

#### 4.3. Physical Security

As grid operators often use their own physical networks for communication, physical security is directly related to cybersecurity. For example, a motivated attacker could break into a substation and infect local devices with malware or tamper with the available access to the PCN in another way. Physical security for substations differs widely between grid operators but might be as low as a wire fence paired with no means of surveillance or access control [49]. Recommended measures to ensure physical security for substations include the protection of information on substations such as engineering drawings and power flow models, surveillance and monitoring measures such as video cameras and motion detectors, as well as the restriction of physical access [50].

More sophisticated physical security may not only deter attackers but also act as a part of a general IDS. For example, if a physical security violation is detected at a substation [106], subsequent malicious activities in the PCN could be correlated with this violation, helping in attack response. A major challenge will be integrating (automatically) detected physical security violations [106] into an overall security solution involving intrusion detection on the network side. With an increasing integration of novel, easily-accessible assets such as smart meters [107] and charging infrastructure for electronic vehicles [70, 108] into the communication infrastructure of smart grids, the challenge of physical security further exaggerates.

#### 4.4. Policies, Procedures & Awareness

To date, the most devastating cyber attacks on power grids all specifically exploited human behavior either through spear-phishing, most prominently using emails, or manipulated downloads [16, 17]. These problems cannot solely be solved by using more sophisticated security technology. Consequently, employees need to be trained to increase awareness towards security-related behavior [109].

Especially workers who have direct access to vital equipment need to be aware of social engineering techniques and empowered to detect simple attacks such as spear-phishing. For example, phishing experiments are valuable to raise employees' awareness for spear-phishing at companies in the energy sector [110]. However, as long as office networks and operational networks are not completely separated (which might be difficult to achieve), a general increase in security awareness is necessary to increase overall security. A challenge of security-related awareness training is its adaptation to the constantly changing cyber attack landscape.

Additionally, even with the best security measures and awareness trainings in place, eventually a (potential) security incident will occur [111]. As such, corresponding incident response

plans and guidelines need to be created, maintained, and trained. However, most existing guidelines for responding to security incidents are mainly concerned with information chains and organizational processes [112, 113], and not with actually remediating security incidents.

Consequently, grid operators need to develop and maintain actionable incident response plans and guidelines, supporting their employees with precise instructions also at the technical level on how to react to security incidents. To further decrease incident response times, it is recommended to keep the number of involved parties small, e.g., by operating own networks, and thus reduce the need for synchronization and communication during incident response [111]. Notably, proper preparation for cybersecurity incidents also requires to regularly train the response to cybersecurity incidents, e.g., using a corresponding training simulator [114, 115]. To be valuable for training employees of grid operators, such training environments need to closely model typical process control network as found in power grids [12, 116].

### 5. Conclusion

With increasing digitalization and decentralization, grid operators are faced with rapid changes in the amount of necessary communication and how this communication is conducted. As a result, more networking is introduced, creating a wider attack space for attackers. In this paper, we highlighted resulting fundamental security problems and attack vectors, which still have to be addressed in the coming years in order to maintain a high level of security and availability of power grids as a critical infrastructure.

To provide security in interconnected power grids, we discussed a set of diverse security solutions and approaches. Depending on the country and the specific grid operation company, current security measures range from non-existent to state-of-the-art. However, even if attackers are only able to control a small fraction of the power generation or consumption, they can still leverage mechanisms inherent to today's large power grids to cause considerable damage. Thus, only an overall increase in the security of a country's power grid provides an effective defense against sophisticated attacks. Consequently, we identified a combination of software and organizational approaches, including intrusion detection systems, software-defined networking, and awareness training, as promising candidates for achieving this goal.

The cyber landscape within power grids is drastically changing: To continually provide ubiquitous power, new cybersecurity threats have to be taken into consideration and protected against. Achieving these goals requires tight collaboration between cybersecurity experts and grid operators to develop and implement cybersecurity solutions that are tailored to the unique requirements of power grids. To this end, our theoretical contributions consolidated in this survey paper provide the foundation for deeper practical research and experimental studies to pave the way forward to provide a high level of cybersecurity for interconnected power grids.



## References

- [1] X. He, R. C. Qiu, Q. Ai, L. Chu, X. Xu, Z. Ling, Designing for situation awareness of future power grids: An indicator system based on linear eigenvalue statistics of large random matrices, *IEEE Access* 4 (2016) 3557–3568. doi:10.1109/ACCESS.2016.2581838.
- [2] T. Wang, Q. Long, X. Gu, W. Chai, Information Flow Modeling and Performance Evaluation of Communication Networks Serving Power Grids, *IEEE Access* 8 (2020) 13735–13747. doi:10.1109/ACCESS.2020.2966489.
- [3] N. Javaid, G. Hafeez, S. Iqbal, N. Alrajeh, M. S. Alabed, M. Guizani, Energy efficient integration of renewable energy sources in the smart grid for demand side management, *IEEE Access* 6 (2018) 77077–77096. doi:10.1109/ACCESS.2018.2866461.
- [4] A. L. Figueroa-Acevedo, C.-H. Tsai, K. Gruchalla, Z. Claes, S. Foley, J. Bakke, J. Okullo, A. J. Prabhakar, Visualizing the Impacts of Renewable Energy Growth in the U.S. Midcontinent, *IEEE Open Access Journal of Power and Energy* 7 (2020) 91–99. doi:10.1109/OAJPE.2020.2967292.
- [5] N. Phuangpornpitak, S. Tia, Opportunities and Challenges of Integrating Renewable Energy in Smart Grid System, *Energy Procedia* 34 (2013). doi:10.1016/j.egypro.2013.06.756.
- [6] S. D. Ahmed, F. S. Al-Ismael, M. Shafiullah, F. A. Al-Sulaiman, I. M. El-Amin, Grid Integration Challenges of Wind Energy: A Review, *IEEE Access* 8 (2020) 10857–10878. doi:10.1109/ACCESS.2020.2964896.
- [7] B. Klaer, Ö. Sen, D. van der Velde, I. Hacker, M. Andres, M. Henze, Graph-based Model of Smart Grid Architectures, in: *Proceedings of the 3rd International Conference on Smart Energy Systems and Technologies (SEST)*, 2020. doi:10.1109/SEST48500.2020.9203113.
- [8] M. Henze, J. Hiller, R. Hummen, R. Matzutt, K. Wehrle, J. H. Ziegel-dorf, Network Security and Privacy for Cyber-Physical Systems, in: *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*, Wiley-IEEE Press, 2017. doi:10.1002/9781119226079.ch2.
- [9] J. Pennekamp, R. Glebke, M. Henze, T. Meisen, C. Quix, R. Hai, L. Gleim, P. Niemietz, M. Rudack, S. Knape, A. Epple, D. Trauth, U. Vroomen, T. Bergs, C. Brecher, A. Bührig-Polaczek, M. Jarke, K. Wehrle, Towards an Infrastructure Enabling the Internet of Production, in: *Proceedings of the 2nd IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*, 2019. doi:10.1109/ICPHYS.2019.8780276.
- [10] J. Hiller, K. Komanns, M. Dahlmanns, K. Wehrle, Regaining Insight and Control on SMGW-based Secure Communication in Smart Grids, in: *Proceedings of the 2019 AEIT International Annual Conference (AEIT)*, 2019. doi:10.23919/AEIT.2019.8893406.
- [11] J. Pennekamp, M. Henze, S. Schmidt, P. Niemietz, M. Fey, D. Trauth, T. Bergs, C. Brecher, K. Wehrle, Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective, in: *Proceedings of the 5th ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*, 2019. doi:10.1145/3338499.3357357.
- [12] D. van der Velde, M. Henze, P. Kathmann, E. Wassermann, M. Andres, D. Bracht, R. Ernst, G. Hallak, B. Klaer, P. Linnartz, B. Meyer, S. Ofner, T. Pletzer, R. Sethmann, Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures, in: *Proceedings of the 6th IEEE International Energy Conference (ENERGY-CON)*, 2020. doi:10.1109/ENERGYCon48941.2020.9236523.
- [13] H. Zhang, X. Jin, Y. Li, Z. Jiang, Y. Liang, Z. Jin, Q. Wen, A Multi-Step Attack Detection Model Based on Alerts of Smart Grid Monitoring System, *IEEE Access* 8 (2019) 1031–1047. doi:10.1109/ACCESS.2019.2961517.
- [14] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, H. Leung, A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids, *IEEE Access* 7 (2019) 80778–80788. doi:10.1109/ACCESS.2019.2920326.
- [15] M. Serror, S. Hack, M. Henze, M. Schuba, K. Wehrle, Challenges and Opportunities in Securing the Industrial Internet of Things, *IEEE Transactions on Industrial Informatics* (2020). doi:10.1109/TII.2020.3023507.
- [16] E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid (2016).
- [17] Dragos, CRASHOVERRIDE – Analysis of the Threat to Electric Grid Operations (2017).
- [18] T. Petermann, H. Bradke, A. Lüllmann, M. Poetzsch, U. Riehm, What Happens During a Blackout: Consequences of a Prolonged and Widespread Power Outage, *BoD*, 2014.
- [19] IEEE, Distributed Network Protocol (DNP3), *IEEE Standard 1815-2012* (2012).
- [20] International Electrotechnical Commission, IEC 60870-5-104 Standard (2000).
- [21] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Syngress, 2014. doi:10.1016/C2013-0-18642-4.
- [22] U. G. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management*, Wiley, 2001. doi:10.1002/9781118878323.
- [23] Bundesnetzagentur – Security of supply, [https://www.bundesnetzagentur.de/EN/Areas/Energy/Companies/SecurityOfSupply/QualityOfSupply/QualityOfSupply\\_node.html](https://www.bundesnetzagentur.de/EN/Areas/Energy/Companies/SecurityOfSupply/QualityOfSupply/QualityOfSupply_node.html).
- [24] Google, Reliability, <https://support.google.com/googlecloud/answer/6056635>.
- [25] ENTSO-E, *Operation Handbook*.
- [26] J. Wang, X. Wang, Y. Wu, Operating Reserve Model in the Power Market, *IEEE Transactions on Power Systems* 20 (1) (2005). doi:10.1109/TPWRS.2004.841232.
- [27] S. Amini, F. Pasqualetti, H. Mohsenian-Rad, Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes, *IEEE Transactions on Smart Grid* 9 (4) (2018). doi:10.1109/TSG.2016.2622686.
- [28] A. Dabrowski, J. Ullrich, E. R. Weippl, Grid Shock: Coordinated Load-Changing Attacks on Power Grids, *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC)* (2017). doi:10.1145/3134600.3134639.
- [29] R. W. Kenyon, J. Maguire, E. Present, D. Christensen, B.-M. Hodge, Bulk Electric Power System Risks from Coordinated Edge Devices, *IEEE Open Access Journal of Power and Energy* 8 (2021) 35–44. doi:10.1109/OAJPE.2021.3052433.
- [30] M. Dahlmanns, J. Lohmöller, I. B. Fink, J. Pennekamp, K. Wehrle, M. Henze, Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments, in: *Proceedings of the Internet Measurement Conference (IMC)*, 2020. doi:10.1145/3419394.3423666.
- [31] J. P. Chapman, S. Ofner, P. Pauksztelo, Key factors in industrial control system security, in: *Proceedings of the IEEE 41st Conference on Local Computer Networks (LCN)*, IEEE, 2016, pp. 551–554. doi:10.1109/LCN.2016.90.
- [32] P. Maynard, K. McLaughlin, B. Haberler, Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks, in: *Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, 2014. doi:10.14236/ewic/ICSCSR2014.5.
- [33] E. Hodo, S. Grebeniuk, H. Ruotsalainen, P. Tavalato, Anomaly Detection for Simulated IEC-60870-5-104 Traffic, in: *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*, 2017. doi:10.1145/3098954.3103166.
- [34] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, E. Panaousis, Attacking IEC-60870-5-104 SCADA Systems, in: *Proceedings of the 2019 IEEE World Congress on Services (SERVICES)*, Vol. 2642, 2019. doi:10.1109/SERVICES.2019.00022.
- [35] M. Robinson, The SCADA Threat Landscape, in: *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, 2013. doi:10.14236/ewic/ICSCSR2013.4.
- [36] I. Darwish, O. Igbe, O. Celebi, T. Saadawi, J. Soryal, Smart Grid DNP3 Vulnerability Analysis and Experimentation, in: *Proceedings of the IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 2015. doi:10.1109/CSCloud.2015.86.
- [37] Y. Xu, Y. Yang, T. Li, J. Ju, Q. Wang, Review on Cyber Vulnerabilities of Communication Protocols in Industrial Control Systems, in: *Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2017. doi:10.1109/EI2.2017.8245509.
- [38] International Electrotechnical Commission, IEC 62351 Standard (2020).

- [39] M. Henze, The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation, in: Proceedings of the 6th IEEE International Workshop on Security and Privacy in the Cloud (SPC), 2020. doi: 10.1109/CNS48642.2020.9162199.
- [40] International Electrotechnical Commission, IEC 61850 Standard (2004).
- [41] R. Hummen, J. Hiller, M. Henze, K. Wehrle, Slimfit - A HIP DEX Compression Layer for the IP-based Internet of Things, in: 1st International Workshop on Internet of Things Communications and Technologies (IoT), 2013. doi: 10.1109/WiMOB.2013.6673370.
- [42] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms, in: Proceedings of the sixth ACM Conference on Security and privacy in Wireless and Mobile Networks (WiSec), 2013. doi: 10.1145/2462096.2462107.
- [43] J. Hiller, M. Henze, M. Serror, E. Wagner, J. N. Richter, K. Wehrle, Secure Low Latency Communication for Constrained Industrial IoT Scenarios, in: Proceedings of the 43rd IEEE Conference on Local Computer Networks (LCN), 2018. doi: 10.1109/LCN.2018.8638027.
- [44] J. Hiller, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko, K. Wehrle, Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments, in: Proceedings of the 27th IEEE International Conference on Network Protocols (ICNP), 2019. doi: 10.1109/ICNP.2019.8888033.
- [45] E. Wagner, J. Bauer, M. Henze, Take a Bite of the Reality Sandwich: Revisiting the Security of Progressive Message Authentication Codes, arXiv preprint arXiv:2103.08560 (2021).
- [46] P. Ackermann, Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems, Packt, 2017.
- [47] M. Ligh, S. Adair, B. Hartstein, M. Richard, Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code, Wiley, 2010.
- [48] J. Xie, A. Stefanov, C.-C. Liu, Physical and cyber security in a smart grid environment, Wiley Interdisciplinary Reviews: Energy and Environment 5 (5) (2016) 519–542. doi: 10.1002/wene.202.
- [49] Florida Public Service Commission, Office of Auditing and Performance Analysis, Review of Physical Security Protection of Utility Substations and Control Centers (2014).
- [50] P. W. Parfomak, Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations, Congressional Research Service (2014).
- [51] Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, An Assessment of Copper Wire Thefts from Electric Utilities (2007).
- [52] Kaspersky Lab ICS CERT, Threats posed by using RATs in ICS, <https://securelist.com/threats-posed-by-using-rats-in-ics/>.
- [53] ICS-CERT, Internet Accessible Control Systems at Risk, ICS-CERT Monitor Newsletter ICS-MM201404 (2014).
- [54] R. M. Lee, M. J. Assante, T. Conway, ICS Defense Use Case (DUC) # 4: Analysis of the recent reports of attacks on US infrastructure by Iranian Actors, SANS ICS (2016).
- [55] Symantec, Dragonfly: Cyberespionage Attacks Against Energy Suppliers, Symantec Security Response, Version 1.21 (2014).
- [56] M. Henze, R. Matzutt, J. Hiller, E. Mühmer, J. H. Ziegeldorf, J. van der Giet, K. Wehrle, Practical Data Compliance for Cloud Storage, in: Proceedings of the 2017 IEEE International Conference on Cloud Engineering (IC2E), 2017. doi: 10.1109/IC2E.2017.32.
- [57] M. Henze, R. Matzutt, J. Hiller, E. Mühmer, J. H. Ziegeldorf, J. van der Giet, K. Wehrle, Complying with Data Handling Requirements in Cloud Storage Systems, IEEE Transactions on Cloud Computing (2020). doi: 10.1109/TCC.2020.3000336.
- [58] ICS-CERT, Malware Infections in the Control Environment, ICS-CERT Monitor Newsletter ICS-MM201212 (2012).
- [59] N. Falliere, L. O. Murchu, E. Chien, W32.Stuxnet Dossier, Symantec Security Response (2011).
- [60] J. P. Farwell, R. Rohozinski, Stuxnet and the Future of Cyber War, Survival 53 (1) (2011) 23–40. doi: 10.1080/00396338.2011.555586.
- [61] W. F. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs 89 (5) (2010) 97–108.
- [62] N. Hannan, An Assessment of Supply-Chain Cyber Resilience for the International Space Station, The RUSI Journal 163 (2) (2018) 28–32. doi: 10.1080/03071847.2018.1469249.
- [63] O. Brdiczka, Insider attacks pose a serious threat to critical U.S. infrastructure, <https://blog.vectra.ai/blog/insider-threats-in-critical-us-infrastructure>.
- [64] D. J. S. Cardenas, A. Hahn, C.-C. Liu, Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations, IEEE Access 8 (2020) 61161–61173. doi: 10.1109/ACCESS.2020.2983313.
- [65] D. Pudjianto, C. Ramsay, G. Strbac, Virtual power plant and system integration of distributed energy resources, IET Renewable Power Generation 1 (1) (2007). doi: 10.1049/iet-rpg:20060023.
- [66] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmman, C. J. Dietrich, H. Bos, SoK: P2PWNEED – Modeling and Evaluating the Resilience of Peer-to-Peer Botnets, in: Proceedings of the 2013 IEEE Symposium on Security and Privacy, IEEE, 2013. doi: 10.1109/SP.2013.17.
- [67] H. Asghari, M. Ciere, M. J. van Eeten, Post-Mortem of a Zombie: Conficker Cleanup After Six Years, in: Proceedings of the 24th USENIX Security Symposium, 2015.
- [68] ThaiCERT, WannaCry Ransomware, TLP:WHITE (2017).
- [69] S. Herwig, K. Harvey, G. Hughey, R. Roberts, D. Levin, Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet, in: Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS), 2019. doi: 10.14722/ndss.2019.23488.
- [70] R. Falk, S. Fries, Electric Vehicle Charging Infrastructure – Security Considerations and Approaches, in: Proceedings of the Fourth International Conference on Evolving Internet (INTERNET), 2012.
- [71] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, H. Zhu, Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges, IEEE Communications Magazine 50 (8) (2012) 38–45. doi: 10.1109/MCOM.2012.6257525.
- [72] S. Sridhar, A. Hahn, M. Govindarasu, Cyber-Physical System Security for the Electric Power Grid, Proceedings of the IEEE 100 (1) (2012). doi: 10.1109/JPROC.2011.2165269.
- [73] M. R. C. Acosta, S. Ahmed, C. E. Garcia, I. Koo, Extremely Randomized Trees-Based Scheme for Stealthy Cyber-Attack Detection in Smart Grid Networks, IEEE Access 8 (2020) 19921–19933. doi: 10.1109/ACCESS.2020.2968934.
- [74] D. Xue, X. Jing, H. Liu, Detection of False Data Injection Attacks in Smart Grid Utilizing ELM-Based OCON Framework, IEEE Access 7 (2019) 31762–31773. doi: 10.1109/ACCESS.2019.2902910.
- [75] Y. Liu, P. Ning, M. K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Transactions on Information and System Security (TISSEC) 14 (1) (2011) 13. doi: 10.1145/1952982.1952995.
- [76] D. Kuipers, M. Fabro, Control Systems Cyber Security: Defense in Depth Strategies, Tech. Rep. INL/EXT-06-11478, Idaho National Laboratory (2006).
- [77] B. Pranggono, K. McLaughlin, Y. Yang, S. Sezer, Intrusion Detection System for Critical Infrastructure, in: The State of the Art in Intrusion Prevention and Detection, 2014. doi: 10.1201/b16390.
- [78] A. Ashok, M. Govindarasu, J. Wang, Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid, Proceedings of the IEEE 105 (7) (2017) 1389–1407. doi: 10.1109/JPROC.2017.2686394.
- [79] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical Security of a Smart Grid Infrastructure, Proceedings of the IEEE 100 (1) (2011) 195–209. doi: 10.1109/JPROC.2011.2161428.
- [80] Fraunhofer FKIE, FACT - The Firmware Analysis and Comparison Tool, [https://fkie-cad.github.io/FACT\\_core/](https://fkie-cad.github.io/FACT_core/).
- [81] M. Caselli, F. Kargl, A Security Assessment Methodology for Critical Infrastructures, in: Proceedings of the 9th International Conference on Critical Information Infrastructures Security (CRITIS), 2014. doi: 10.1007/978-3-319-31664-2\_34.
- [82] M. Combs-Ford, Security Assessment of Industrial Control Supervisory and Process Control Zones, in: Proceedings of the 17th Annual Conference on Information Technology Education and the 5th Annual Conference on Research in Information Technology (SIGITE/RIIT), 2016. doi: 10.1145/2978192.2978219.
- [83] L. Roepert, M. Dahlmanns, I. B. Fink, J. Pennekamp, M. Henze, Assessing the Security of OPC UA Deployments, in: Proceedings of the 1st ITG Workshop on IT Security (ITSec), 2020. doi: 10.15496/publikation-41813.
- [84] A. J. McBride, A. R. McGee, Assessing Smart Grid Security, Bell Labs

- Technical Journal 17 (3) (2012) 87–103. doi:10.1002/bltj.21560.
- [85] E. Winter, M. Rademacher, Fuzzing of SCADA Protocols used in Smart Grids, *Energy Informatics* 3 (Suppl 2), P1 (2020). doi:10.1186/s42162-020-00113-9.
- [86] M. Henze, J. Hiller, O. Hohlfeld, K. Wehrle, Moving Privacy-Sensitive Services from Public Clouds to Decentralized Private Clouds, in: *Proceedings of the 2016 IEEE International Conference on Cloud Engineering (IC2E) Workshops*, 2016. doi:10.1109/IC2EW.2016.24.
- [87] A. Shah, A. Perrig, B. Sinopoli, Mechanisms to Provide Integrity in SCADA and PCS devices, in: *Proceedings of the International Workshop on Cyber-Physical Systems-Challenges and Applications (CPS-CA)*, 2008.
- [88] X. Yang, X. He, W. Yu, J. Lin, R. Li, Q. Yang, H. Song, Towards a Low-cost Remote Memory Attestation for the Smart Grid, *Sensors* 15 (8) (2015) 20799–20824. doi:10.3390/s150820799.
- [89] X. Wang, C. Konstantinou, M. Maniatakis, R. Karri, ConFirm: Detecting Firmware Modifications in Embedded Systems using Hardware Performance Counters, in: *Proceedings of the 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, IEEE, 2015. doi:10.1109/ICCAD.2015.7372617.
- [90] D. Wei, Y. Lu, M. Jafari, P. M. Skare, K. Rohde, Protecting Smart Grid Automation Systems Against Cyberattacks, *IEEE Transactions on Smart Grid* 2 (4) (2011). doi:10.1109/TSG.2011.2159999.
- [91] A. Anwar, A. N. Mahmood, Cyber Security of Smart Grid Infrastructure, in: *The State of the Art in Intrusion Prevention and Detection*, 2014.
- [92] M. Dahlmans, J. Pennekamp, I. B. Fink, B. Schoolmann, K. Wehrle, M. Henze, Transparent End-to-End Security for Publish/Subscribe Communication in Cyber-Physical Systems, in: *Proceedings of the ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS)*, 2021. doi:10.1145/3445969.3450423.
- [93] Federal Republic of Germany, *Energiewirtschaftsgesetz (EnWG)*, § 11 (2018).
- [94] M. Serror, M. Henze, S. Hack, M. Schuba, K. Wehrle, Towards In-Network Security for Smart Homes, in: *Proceedings of the 2nd International Workshop on Security and Forensics of IoT (IoT-SECFOR)*, 2018. doi:10.1145/3230833.3232802.
- [95] M. Rademacher, K. Jonas, F. Siebertz, A. Rzycka, M. Schlebusch, M. Kessel, Software-Defined Wireless Mesh Networking: Current Status and Challenges, *The Computer Journal* 60 (10) (2017) 1520–1535. doi:10.1093/comjnl/bxx066.
- [96] X. Dong, H. Lin, R. Tan, R. K. Iyer, Z. Kalbarczyk, Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges, in: *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (CPSS)*, 2015. doi:10.1145/2732198.2732203.
- [97] K. J. White, D. P. Pezaros, C. W. Johnson, Using Programmable Data Networks to Detect Critical Infrastructure Challenges, in: *Proceedings of the 9th International Conference on Critical Information Infrastructures Security (CRITIS)*, 2014. doi:10.1007/978-3-319-31664-2\_22.
- [98] P. I. Radoglou-Grammatikis, P. G. Sarigiannidis, Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems, *IEEE Access* 7 (2019) 46595–46620. doi:10.1109/ACCESS.2019.2909807.
- [99] S. Northcutt, J. Novak, *Network Intrusion Detection*, New Riders, 2002.
- [100] K. Wolsing, E. Wagner, M. Henze, Poster: Facilitating Protocol-independent Industrial Intrusion Detection Systems, in: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2020. doi:10.1145/3372297.3420019.
- [101] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, An Integrated Security System of Protecting Smart Grid against Cyber Attacks, in: *Proceedings of 2010 Innovative Smart Grid Technologies (ISGT)*, 2010. doi:10.1109/ISGT.2010.5434767.
- [102] S. R. Snapp, J. Brentano, G. Dias, T. L. Goan, L. T. Heberlein, C.-L. Ho, K. N. Levitt, DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype (2017).
- [103] J. J. Chromik, A. Remke, B. R. Haverkort, Bro in SCADA: dynamic intrusion detection policies based on a system model, in: *Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR)*, 2018. doi:10.14236/ewic/ICS2018.13.
- [104] Zeek Network Security Monitor, <https://www.zeek.org/>.
- [105] J. Appiah-Kubi, C.-C. Liu, Decentralized Intrusion Prevention (DIP) Against Co-Ordinated Cyberattacks on Distribution Automation Systems, *IEEE Open Access Journal of Power and Energy* 7 (2020) 389–402. doi:10.1109/OAJPE.2020.3029805.
- [106] C. Cheh, U. Thakore, B. Chen, W. G. Temple, W. H. Sanders, Leveraging Physical Access Logs to Identify Tailgating: Limitations and Solutions, in: *2019 15th European Dependable Computing Conference (EDCC)*, 2019. doi:10.1109/EDCC.2019.00032.
- [107] H. Khurana, M. Hadley, N. Lu, D. A. Frincke, Smart-Grid Security Issues, *IEEE Security & Privacy* 8 (1) (2010). doi:10.1109/MSP.2010.49.
- [108] A. Palomino, M. Parvania, Data-Driven Risk Analysis of Joint Electric Vehicle and Solar Operation in Distribution Networks, *IEEE Open Access Journal of Power and Energy* 7 (2020) 141–150. doi:10.1109/OAJPE.2020.2984696.
- [109] J. F. Clemente, *Cyber Security For Critical Energy Infrastructure*, Tech. rep., Naval Postgraduate School Monterey (2018).
- [110] H. Holm, W. R. Flores, G. Ericsson, Cyber Security for a Smart Grid – What About Phishing?, in: *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)*, IEEE, 2013. doi:10.1109/ISGTEurope.2013.6695407.
- [111] A. R. Metke, R. L. Ekl, Security Technology for Smart Grid Networks, *IEEE Transactions on Smart Grid* 1 (1) (2010). doi:10.1109/TSG.2010.2046347.
- [112] Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001 (2017).
- [113] German Bundestag, *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)* (2015).
- [114] C. Vellaithurai, A. Srivastava, S. Zonouz, SECPSIM: A Training Simulator for Cyber-Power Infrastructure Security, in: *Proceedings of the IEEE Fourth International Conference on Smart Grid Communications (SmartGridComm)*, 2013. doi:10.1109/SmartGridComm.2013.6687934.
- [115] R. Uetz, L. Benthin, C. Hemminghaus, S. Krebs, T. Yilmaz, BREACH: A Framework for the Simulation of Cyber Attacks on Company’s Networks, in: *Proceedings of the Digital Forensics Research Conference Europe*, 2017.
- [116] M. Henze, L. Bader, J. Filter, O. Lamberts, S. Ofner, D. van der Velde, Poster: Cybersecurity Research and Training for Power Distribution Grids – A Blueprint, in: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2020. doi:10.1145/3372297.3420016.