Threat analysis and adversarial model for Smart Grids

Javier Sande-Ríos
University Carlos III of Madrid
Madrid, Spain
jsande@pa.uc3m.es

Jesús Canal-Sánchez
University Carlos III of Madrid
Madrid, Spain
100488671@alumnos.uc3m.es

Carmen Manzano-Hernández
University Carlos III of Madrid
Madrid, Spain
100489177@alumnos.uc3m.es

Sergio Pastrana
University Carlos III of Madrid
Madrid, Spain
spastran@inf.uc3m.es

***Abstract*—The power grid is a critical infrastructure that allows for the efficient and robust generation, transmission, delivery and consumption of electricity. In the recent years, the physical components have been equipped with computing and network devices, which optimizes the operation and maintenance of the grid. The *cyber* domain of this smart power grid opens a new plethora of threats, which adds to classical threats on the *physical* domain. Accordingly, different stakeholders including regulation bodies, industry and academy, are making increasing efforts to provide security mechanisms to mitigate and reduce cyber-risks. Despite these efforts, there have been various cyberattacks that have affected the smart grid, leading in some cases to catastrophic consequences, showcasing that the industry might not be prepared for attacks from high profile adversaries. At the same time, recent work shows a lack of agreement among grid practitioners and academic experts on the feasibility and consequences of academic-proposed threats. This is in part due to inadequate simulation models which do not evaluate threats based on attackers full capabilities and goals. To address this gap, in this work we first analyze the main attack surfaces of the smart grid, and then conduct a threat analysis from the adversarial model perspective, including different levels of knowledge, goals, motivations and capabilities. To validate the model, we provide real-world examples of the potential capabilities by studying known vulnerabilities in critical components, and then analyzing existing cyber-attacks that have affected the smart grid, either directly or indirectly.**

***Index Terms*—Smart Grid, Cybersecurity, Adversarial Model, Power Grid, Critical Infrastructures**

1. Introduction

The provision of electricity is crucial for the well-being of the society and industry. As such, the power grid is one of the most critical infrastructures for every nation. Yet, recent incidents show that attacks on the Smart Grid are not only possible, but also can cause severe consequences such as black-outs [5], [34]. Thus, it is essential to understand how attacks might occur, so as to prepare appropriate cyber-physical defenses [57]. Attacks highly depend on factors such as the attack surface, knowledge, goals and capabilities of an adversary, i.e., the *Adversarial Model*. Understanding these factors allow to better prepare for the potential Techniques, Tactics and Procedures (TTPs) used by cyberattacks, and to foresee how these might evolve in the future. This knowledge, together with the understanding of the organizational critical assets, facilitates the design and implementation of appropriate countermeasures for prevention, detection and risk mitigation [45]. Still, the literature on Smart Grid security have mostly focused on the analysis of attacks and defenses (see §2.2), without considering the actual motivation, capabilities and knowledge that an adversary might have to conduct such attack. Thus, there is a gap on the analysis of the adversarial model on real world settings. This is one of the reasons that leads to disconnection between real-world, operational and academic-proposed threats, since often academic works rely on incomplete simulated scenarios or unrealistic adversarial models [57].

To address this gap, in this work we provide a comprehensive analysis of adversaries against the Smart Grid. We first describe the different factors that compose the adversarial model, i.e., attack surface, motivations, goals, knowledge and capabilities. We infer this information from the exiting academic literature, and by studying the history and evolution of cyberattacks on Smart Grids, from which we can analyze the TTPs used, and the goals, targets and impacts of these. We also conduct a study of existing vulnerabilities in critical devices used in operational Smart Grids, which allow us to foresee the potential capabilities that the adversary can exploit to penetrate (and attack) the network. This way, we first formalize an Adversarial Model focusing on the different roles for adversaries against Smart Grids. Then, we use this model to map real-world attacks, e.g., those that targeted and turn-off part of the Ukrainian power grid [7].

This paper is structured as follows. First, §2 presents a theoretical background about the Smart Grid, and the related work. Then, §3 describes the different factors for adversaries, and formalizes an adversarial model. §4 describes different real-world attacks and maps the proposed adversarial model on these. Finally, §5 provides the conclusions of the paper.

2. Background and Related Work

This section first describe theoretical concept of the Power Grid and its evolution to the 'smart' concept, and then describes the related work.

2.1. The power grid

Electricity is an essential aspect of the society. Consumers have an easy and transparent access to electricity provided by a proper functioning of the electrical grid: a network of synchronized power providers and consumers connected by transmission and distribution lines and operated by one or more control centers. In a nutshell, an electrical grid is composed by: i) **Power Stations**, for the generation of electrical power (e.g., carbon or nuclear plants, solar panels or wind turbines); ii) **Electrical Substations**, that transform high voltage electricity (as generated from the power stations) into low voltage, and vice versa, by means of transformers; iii) **Electric Power Transmission**, which is the infrastructure, usually transmission lines, that enables the movement of high-voltage electrical energy (i.e., greater than 39kV) from power stations to electric substations; and iv) **Electric Power Distribution**, where the electricity is delivered to the final consumers from a local substation that reduces the high or medium voltage level of the electricity to an usable voltage, typically 230V, which is is then delivered to the final customers.

2.1.1. The smart power grid. A *smart* power grid is a cyber-digitally enhanced power grid that optimize grid operation, leveraging modern Power Automation Systems (PAS), IoT devices and custom communication protocols. It allows to reduce cost in the generation, transmission and delivery of electricity, and also enables real-time monitoring of the distribution and demand of electricity [48]. A key feature introduced by Smart Grids is the decentralization of power production, allowing end-users to become part of the network, e.g., by generating electricity through domestic solar panels. While this reduces costs and energy losses, it simultaneously increases the complexity of the control and management [23].

The Smart Grid involves different entities (i.e., cyber-physical systems, or CPS, computer systems, and the individuals or organizations) operating in different domains [23]: the **Customer** domain is where electricity is mostly consumed, but it can also be produced (e.g., households, commerce, industries, etc.); the **Market** domain balances the production based on estimated consumption and consumer demands; the **Service** domain includes tasks such as commercializing, customer management, or installation and maintenance of equipment; the **Operation** domain, responsible for the smooth function of the Smart Grid, involves tasks such as monitoring, analysis, control, maintenance, etc.; the **Generation** domain, where actual production takes place (e.g., coal-fired or nuclear power station), including Distributed Energy Resources (DERs) located at the consumer side (e.g., domestic solar panels); the **Transmission** domain, focused in the transportation of electricity through different substations; and finally, the **Distribution** domain, focused on the delivery of electricity from substation to end customers. §3.1 revisits these domains as key attack surfaces for adversaries, and describes the main components exposed on each domain.

2.2. Related work

The cybersecurity in Smart Grids is an active area of research in academia, with several papers being published each year. As such, there are various surveys on Smart Grid security [17], [25], [37], [46], [49], [57]. Since our work is focused on attackers, we review recent works that analyse attacks or adversaries, which we have used to better understand the current landscape and to inform our proposed model.

Peng et al. disscused various attacks at a high granularity (i.e., generation, transmission, distribution or consumption), with general activities (i.e., reconnaissance, scanning, exploitation and access) [46]. Ding J, et al. analyzed vulnerabilities on devices of the Smart Grids from a technical perspective, i.e., the capabilities of the adversary, and also the potential impacts of these, showing real attacks performed on Smart Grids infrastructures worldwide [17]. Reda et al. focused on existing False Injection Attacks, providing an interesting taxonomy on these attacks, including attack models (e.g., knowledge or capabilities required), targets (e.g., Intelligent Electronic Devices, or IEDs) and impact (i.e., goals) [49]. Kamrul Hasan et al. provide a survey on Smart Grid cybersecurity, including types of attacks that might incur damage on the confidentiality, integrity and availability of data and system on Smart Grids [25]. They also provide a taxonomy of attacks based on the 'layer' being affected (i.e., control, communication, physical or cyber layer), and on the impact and goals of these (e.g., economic or physical disruption). Finally, the work of Nafees et al. analyse actual attacks and survey existing countermeasures and to overview existing gaps for cyber-physical situational awareness, including a threat model [37]. This threat model is composed by an adversary model (i.e., understanding the motivation or resources of different actors), and asset/vulnerability model (i.e., types of components and how these could be exploited), and an attack model (i.e., particularities of attacks, like initial access, propagation or impact).

Different from previous work, we particularly focus on the adversarial model, considering potential attack surfaces, and the actual capabilities, knowledge, motivation and goals of adversaries. Indeed, a recent paper by Singer et al. shows a disconnection between real-world operational security (dealing with real systems) and academic works (using simulation and models), showing that threats that could lead to a real impact on the grid are less frequent as those proposed by the academia [57]. They surveyed cyber-security operators, asking for academic-proposed attacks, and concluded that misperceptions on simulation tools and incomplete models lead to inconsistent scenarios. This work motivated our study, where we propose an adversarial model showing how it can be mapped to real world actors that have attacked the grid (§4), and studying vulnerabilities in actual products that could potentially enhance adversarial capabilities (§3.4). We believe this is a further step towards more realistic simulations with Smart Grids.

3. Adversarial model

When modeling an adversary, it is crucial importance to pinpoint four key elements: their attack surface, objectives, knowledge, and capabilities. We next describe each of these aspects with respect to Smart Power Grids.

3.1. Attack surface

The attack surface represent the potential entry points for attacks. As introduced in §2, the Smart Grid is a complex system composed of a diverse range of infrastructures and devices. For the analysis of its characteristics, we will categorize them into the domains defined in §2.1.1, where each domain represents a distinct aspect of the Smart Grid infrastructure. Examining these domains individually allows for a focused analysis of specific vulnerabilities and potential attack vectors.

3.1.1. Power generation. The generation of energy primarily takes place in power stations. Among these stations, a diverse set of infrastructures exists, involving variations in the type of energy generated (coal, nuclear, wind, solar, etc.), as well as differences in size and age. Many power plants, particularly those dedicated to fossil fuels, exhibit significant age, resulting in original equipment that was not designed with connectivity and cybersecurity in mind. The challenge arises when attempting to adapt and upgrade such outdated systems, posing a formidable obstacle both technically and financially [53]. The outdated equipment now presents a significant cybersecurity risk, providing malicious actors with opportunities to exploit vulnerabilities. Given the critical role of power generation, in the event of an attack on these infrastructure, an adversarial entity with malicious intentions could manipulate the amount of generated energy, potentially destabilizing the entire network [6].

Energy generation can also occur on the consumer side through Distributed Energy Resources (DERs), e.g., solar panels or wind turbines. While an attack on a DER would have a smaller impact than an attack on a generation plant, the aggregated effect of a cooperative attack against those generation devices can have a substantial influence on the network [15], [33]. This poses an escalating risk as the deployment of DERs increases.

3.1.2. Transmission. The transmission of electricity, from generation to consumption, involve various systems and infrastructures which are potential targets by adversaries.

Substations are facilities placed along the grid that convert the voltage level of the electricity from high to low or vice versa [32]. Substations are of various sizes and complexities. Some substations cover small areas and may only contain one bus-bar and several circuit breakers. Larger substations cover a significant area and require more components, such as switching, protection and control equipment. Due to the equipment contained and operations performed within, substations are considered a critical part of the power grid and a potential target for attackers [27].

The equipment for this domain primarily consists of **transformers** and **protection equipment**. Transformers are used to adapt the voltage levels of electricity to meet the requirements of each grid segment. Meanwhile, protection equipment (e.g., relays, circuit breakers, or disconnect switches) is employed to interrupt the flow of electricity in case of faults or network overload. When these devices detect abnormal operating conditions, they automatically trigger switching equipment to isolate the faulty section and protect the electrical equipment and the grid [9]. This equipment plays a critical role in maintaining grid stability and safeguarding physical equipment on the grid or at customer endpoints, and thus, it is an attractive target for attacks aimed at manipulating protection devices, disabling protections, or causing false positives leading to denial of service [72].

3.1.3. Operation. The operation domain includes control equipment that serves to monitor and manage the electricity flow, allowing to remotely supervise and maintain the grid's stability. This includes various essential systems. We next describe these systems, including the risks they are exposed to within the grid and the potential impact than an attack could have on the rest of the structure.

Advanced Metering Infrastructure (AMI) provides real-time metrics for energy consumption and production. At its core, AMI relies on smart meters, which receive information about the energy consumption, e.g., from final users, and other metrics such as battery information, or the amount of energy produced by solar panels [74]. These devices enable direct communication between end-users and the grid. AMI devices are often placed at end-user facilities, and due to ease of physical access, they are highly exposed. Indeed, smart meters are susceptible to physical tampering, leading to fraudulent activities, such as injecting false consumption data to manipulate electricity bills [3]. Furthermore, as these meters are often integrated with other systems such supporting apps for remote consumer consultation, they become potential targets for remote attackers [24].

Geographic Information Systems (GIS) are responsible for collecting and geographically aggregating real time information from metering devices deployed in the grid [22]. GIS improves decision-making by adding a spatial dimension, helping, for instance, to identify DERs locations or network areas at risks. GIS provides insights which allow the system to react accordingly to maintain the grid stability. GIS establish remote connections with smart meters and other IoT devices, acquiring the necessary data for predictions. However, this exposure poses a risk, as attackers may exploit vulnerabilities in these systems to gather information about connected devices, their topology, or potentially compromise the integrity and confidentiality of received data [40].

Power Automation Systems (PAS) are software systems used to monitor electrical substations, retrieving information regarding the part of the grid in which they are deployed. This functionality enables quick and accurate response according to the specific necessities. Moreover, PAS act as an integrator in the grid by incorporating standardized communication protocols, facilitating the exchange of information among different components of the grid. Given their presence across diverse substations within the grid, PAS systems are susceptible to deficiencies in the security measures of these facilities [19], [70]. Vulnerabilities present on these systems pose a threat to

the whole structure of the grid, due to their role in monitoring substation activities and their inherent connection to the devices deployed within it.

Demand Response Systems (DRS) manage the electricity usage based on supply conditions, pricing, or grid state, leveraging real-time data and communication and optimize energy consumption, costs, and enhancing grid stability [28]. The automated response facilitated by smart switches and the integration with AMI, facilitates automatic energy management, ensuring timely responses to grid fluctuations or emergencies [15]. DRS utilize a combination of hardware devices (such as smart switches) and software solutions responsible for automation and communication with metering and control devices. Consumer devices might include DRS for efficiency (e.g., turning on/off a laundry machine depending on market prices and energy consumption), and thus they are vulnerable to potential compromise, both through the local network of the user or via physical manipulation. This poses a threat to the integrity and confidentiality of the information sent to the Demand Response control infrastructure.

These mentioned systems are composed of both software and hardware equipment for data collection, remote operation and task automation. Key devices integral to this functionality are: i **Supervisory Control And Data Acquisition (SCADA)** systems, which receive information from different sources and, based on a predefined configuration they manage and act upon the information [63]. SCADA systems are in the operation center of Smart Grids, thus, an attack on these systems could end in a disruption of the service of the grid. Additionally, if they are affected by network vulnerabilities, its compromise could lead to other components of the grid being also compromised [65]; ii **Remote Terminal Unit (RTU)** are critical components that enable automatic and remote control of grid operations. Moreover, nowadays most of them allow for wireless communication, and thus they are exposed to attackers that can either get in the network through other devices on the same network, or attackers that find vulnerabilities directly in the devices. Since they are a crucial part of the structure of Smart Grids, compromising an RTU would pose at risk the whole network of a Smart Grid [51], [62]; iii **Programmable Logic Controller (PLC)** are responsible for executing specific tasks based on pre-programmed logic [54]. In Smart Grids PLCs are deployed in various facilities, such as substations and power plants, where they oversee and regulate essential processes. Given their inherent connectivity, they are susceptible to potential cyber threats [47]. Attackers targeting PLCs could manipulate critical processes, disrupt energy flow, or compromise the integrity of the grid.

3.1.4. Market. The electricity market is highly complex, and its mechanisms vary depending on the region. Nevertheless, in most of these markets, consumption forecasting is a fundamental factor [36]. Since electricity cannot be stored at a large scale, the power grid must maintain a balance between the generation and consumption of electric power. Consumption forecasting allows suppliers to optimize power production, thereby reducing waste and lowering operational costs. Accurate forecasting is also critical in the integration of renewable energy sources, aligning their intermittent generation patterns with the overall demand [2].

The diverse consumption patterns of consumers pose a challenge for suppliers, requiring them to align power production with the dynamic nature of real-time consumption. Understanding energy demand is crucial for planning and allocating generation. This prediction relies on algorithms that receive information about past consumption under similar conditions to those being forecasted (same day the previous year, day of the week, weather conditions, etc.) [35]. AMI plays a primary role for the collection of consumption data. A failure in forecasting can have serious consequences; overestimation may lead to unnecessary energy generation and economic losses, while underestimation can result in unpreparedness for energy demand and subsequent blackouts. Hence, forecasting algorithms play a pivotal role in the network and may be targeted in attacks aimed at manipulating them [15].

3.1.5. Service. The service domain include user management systems, where sensitive information such as payment data, addresses, and consumption details are stored and managed. Safeguarding this information is crucial to protect user privacy. The systems within this domain share similarities with other ICS, such as water distributors, gas providers, telecommunications companies, etc. and are susceptible to similar types of threats. These attacks may attempt to exploit potential vulnerabilities in their servers to extract customer information, employ social engineering tactics to impersonate a client, or even cause a denial of service, disrupting the network's proper functioning [4].

3.1.6. Customer. The consumer domain is closely related with other domains such as service, market, and operation. Customer consumption and its associated information can be leveraged to manipulate electricity prices and forecast (market), billing statements (service), status and consumption information read by smart meters (operation), or even power generation through DERs. This connection with other domains establishes the consumer as a potential entry point for numerous threats. These include previously mentioned attacks like energy injection through DERs or manipulation of consumption through IoT devices. Furthermore, consumers themselves may become the target of attacks, facing threats such as denial of service, or data leaks that pose risks to their privacy.

A transversal attack surface which affects all the previous domains is the **human factor** (though differently in terms of the capabilities, goals, and impact that they entail). This includes customers, operators and employees from the Smart Grid. As we describe in §4, compound APT attacks often start with a Social Engineering attack targeted at strategically selected employees, i.e., by means of an spearphishing attachment which gives the initial access to the corporate network [5], [37].

3.2. Knowledge

Having knowledge of the intricacies of the Smart Grid, including the topology and systems involved, is key to conduct a successful attack. Indeed, the reconnaissance phase is the first step used by adversaries to gain knowledge and plan future attacks [37], [67]. Academic

and official resources about the Smart Grid, including international standards, often offer only a high-level description. Moreover, the majority of communication protocols and security measures adhere to public standards, closely aligning with those employed in various industrial systems, albeit with notable complexity. Consequently, a detailed study of these standards and protocols allows an adversary to identify concrete elements and potential exploitation of the communication protocols. The electrical grid introduces a degree of opacity at a certain level. While obscurity is not explicitly considered as a security measure, various aspects of the Smart Grid implementation, infrastructure, and topology are deemed confidential by governments [11]. This veil of secrecy surrounding the grid creates a substantial knowledge gap for malicious actors. Consequently attaining a clear understanding of the network's topological structure, operational processes, chain of command in control centers, and their practical implementation remains challenging. Based on these considerations, we distinguish three sources of knowledge:

1) **Knowledge through the standards and official sources.** Adversaries at this level are informed about the established standards that govern the operation and security of the grid [30]. Furthermore, attackers can access information about the grid through official documentation publicly available [16], which still might be only superficial and lack of details. Based on this knowledge, adversaries can exploit vulnerabilities and weaknesses of the standards or base their attacks on a estimation of hardware used. Since these standards are open, adversaries could even replicate a production system in order to analyze the system for misconfigurations, weaknesses, or even vulnerabilities in the protocols.
2) **Knowledge through the interaction with the grid equipment.** The grid is deployed in an open field, and its infrastructure is accessible at specific locations, such as smart meters in clients' homes, data collectors within residential buildings, or security equipment at the transport domain and substations. This accessibility might be a substantial source for obtaining valuable information about the grid's operation. Importantly, many of the devices utilized in the Smart Grid are generic and commonly employed in other industrial environments, such as relays, RTUs and SCADA systems. Moreover, detailed documentation for these devices is often publicly available, including their vulnerabilities (see, e.g., §3.4.3). Consequently, the knowledge acquired through interaction with the grid equipment can be combined with publicly accessible information about these devices, empowering potential adversaries to formulate targeted attacks based on a partial understanding of device functionality in the grid.
3) **Insider Knowledge**. Attackers at this level have technical knowledge about both the physical and cyber layers, as well as practical knowledge of the actual implementation of a Smart Grid. Attackers are not only familiar with the standards and the hardware used but also possess a strategic understanding of its topology, organizational structures and emergency response mechanisms, making their potential threats even more sophisticated and challenging to counter. This depth of knowledge encompasses details about the specific devices utilized on the grid, including their manufacturers and versions, and providing adversaries with a significant advantage in identifying potential attack vectors and vulnerabilities. Such level of insight into the grid is typically obtainable only to individuals with direct involvement in the infrastructure, such as insiders within the targeted grid, or adversaries backed by nations, institutions, or companies capable of providing such intricate details about the power industry.

These knowledge sources are not mutually exclusive. For instance, the understanding of standards can be combined with information gathered from an opportunistic interaction with specific grid devices, providing the adversary with an higher level of knowledge. It is not only the source of knowledge but also its depth that shapes and amplifies the adversary's capabilities to execute an attack.

3.3. Motivations and Goals

The electrical grid is one of the most valuable critical infrastructure for nations, their institutions and citizens. Also, generation, transportation, and distribution of energy constitute an important economic asset, involving transactions totaling billions of dollars annually in each country. Given the intricate web of stakeholders in the electrical grid, potential cyber threats pose a multifaceted challenge with various objectives and motivations. Understanding an adversary in this context requires delving into what motivates them to take action, and what specific outcomes they aim to achieve. Thus, we make a distinction between the general motivations for adversaries, and their more targeted and concrete goals.

3.3.1. Motivations. We distinguish the following motivations for attacking the grid.

Geopolitics. Attackers may seek to exploit the electrical grid as a strategic asset. Motivated by geopolitical considerations, these attackers aim to exert influence, control, or disrupt energy systems to advance broader political goals. The manipulation of the electrical grid can serve as a tool for coercion, influencing regional dynamics, or establishing dominance in the global geopolitical landscape. The electrical grid has become a potent weapon in modern conflicts, employed as a means to weaken adversaries as witnessed in recent conflicts such as the war in Ukraine [42].

Inflict damage on the sector. Adversaries with this motivation may aim to deliberately sabotage the functioning of the energy sector or a specific company within it.

Inflict harm on the user(s). Certain actors may target end-users, intending to compromise their safety, privacy, or property through disruptions in their energy supply.

Financial benefit. For some adversaries, the primary motivation could be financial gains, whether through ransom demands, market manipulations, or other means of economic exploitation.

Fame and recognition. In some instances, attackers might be driven by the desire for notoriety or acknowledgment within certain circles, seeking recognition for their actions.

3.3.2. Goals. Based on their motivations, attackers conduct activities to achieve any of the following goals.

Reconnaissance. An adversary with this goal seeks to obtain information about critical assets and weakest points of failure. The motivation behind such actions may involve utilizing this information to orchestrate a more intricate attack with a distinct goal or gaining advantages by offering the acquired data to third parties [37]. This includes information regarding its topology, implemented security measures and critical assets, such as substations, power generation facilities, and control systems. Moreover, the attacker may seek to gather information about human personnel, which can be subsequently employed for social engineering attacks [8]. Successful reconnaissance enables adversaries to increase their knowledge.

Service disruption. This category encompasses attackers aiming to instigate blackouts or disruptions in the electrical grid, potentially causing chaos and impacting various sectors. The objective here could be not only to disrupt daily operations but also to inflict lasting and profound damage, strategically impacting a nation's infrastructure, economy, and overall resilience.

Data theft. The objective here is to obtain sensitive information, e.g., users' consumption habits. Other valuable data managed by electric companies, such as personal or financial information, may also be targeted. This information can be used to commit other actions, such as blackmailing or fraud, and also it might allow to conduct further steps of a cyberattack.

Market manipulation. Some adversaries may seek to distort data related to energy consumption, potentially for purposes of influencing market dynamics or cause economic losses.

Manipulating the electricity bill. A more specific economic goal is to manipulate systems to reduce the cost of bills, e.g., for personal gain or to undermine the provider company. This is often the case for customer fraud.

3.4. Adversarial capabilities

Capabilities are a key factor when characterizing an adversary. They define the spectrum of actions that an attacker can undertake, and in many cases, these coerce the actual goals (i.e., the purpose of the attacks is restricted by the capabilities of the adversary). Also, the capabilities are associated with the knowledge (i.e., the more knowledge and adversary has, the larger capability it has to conduct the attack). Finally, the capabilities highly depend on the attack surface exposed and targeted.

3.4.1. Capabilities modeling. Following well-known models for capabilities we differentiate between access, exploitation, lateral movement, and persistence [12]. Each category significantly shapes the potential of attackers to achieve their objectives on different phases of the attack.

Access. The access refers to the attacker's capability to infiltrate the Smart Grid. With **physical access**, adversaries possess the capability to manipulate or gain entry to targeted devices through their physical layer. This capability may be associated with opportunistic adversaries, such as insiders, or with devices that are not adequately protected at the physical level and exposed to third parties. This might occur either by bad security practices (e.g., an improper access control into a substation), or due to the intrinsic nature of the device (e.g., a smart meter in end-users' homes, or a transmission cable in the field). The exploitation of physical access requires a knowledge of the physical layer, e.g. to understand how to break in the devices or where to act to conduct a disruption. With **remote access**, attackers possess the capability to infiltrate the intricate networks that constitute the infrastructure. Communication protocols, such as Modbus [60], employed by devices like RTUs or PLCs interfacing with SCADA systems, introduce a diverse range of potential threats. This opens an avenue for virtually any attacker with the required ability to eavesdrop or infiltrate a network, thus jeopardizing the integrity and security of the entire grid. In this case, the adversary requires knowledge of the IT layer and its standards, in order to infer what protocols are being used, and how to exploit weaknesses on these to gain access. Also, recent work propose the use of Web-based PLC malware for modern PLCs, which allows to re-use well-established web-based attacks for industrial PLCs [47].

Exploitation. The Smart Grid offers multiple exploitation vectors, increasing those for the traditional power grid. These attack vectors are strongly tight to the aforementioned capabilities and most of them are only possible with the corresponding level of access. While acknowledging the vast array of diverse attack strategies and threats, we draw attention to four generic exploitation capabilities:

- **Command injection [68].** With this capability, the adversary might gain control over Smart Grid devices, allowing the execution of malicious commands that can compromise its integrity and operation. While remote command execution poses a risk due to the characteristics of the Smart Grid, this threat also encompasses taking control of devices through physical manipulation (e.g., by an attacker with access to the HMI of a SCADA system, or any mechanical activator of a security device).
- **False data injection [49].** It involves introducing false data into the system, usually to manipulate the recorded consumption. This type of action can have various objectives, such as altering the perception of actual demand, distorting estimations, or even triggering incorrect actions in the operational management of the system leading to a denial of service.
- **Denial of service (DoS) [26].** Attacker can impact the availability of the grid or some of their components. This capability is achieved through various means, which can be related with previously mentioned capabilities, e.g., controlling over devices via command injection, inducing false positives on security devices through the injection of false data, or directly by exploiting vulnerabilities leading to DoS.
- **Eavesdropping [69].** It is the ability to exploit communication protocols and obtain data of interest, such as user consumption. An attacker with this capability could, for example, intercept data traveling between smart meters and GIS. Also, to observe traffic between control elements and other devices, with the aim of using this information in combination with other capabilities such as false data injection or

command injection to, for example, conduct a replay attack. Eavesdropping is strongly tied to two primary knowledge sources: standards and direct interaction. First source allows attackers to understand the data being intercepted, whereas second provides insights into how data interception can be achieved. Furthermore, this capability is not solely reliant on knowledge from direct device interaction. It can also be employed to gather additional information about the devices operation and communication mechanisms.

Lateral Movement and privilege escalation. After discussing the potential capabilities of an adversary to access the grid systems and exploit them, we shift our focus to their ability to move laterally to other elements of the network and escalate privileges once they are inside. This capability is crucial in the execution of complex attacks. In attacks on major infrastructures, such as control or generation stations, direct access to control systems from external sources is rarely feasible. Therefore, in most cases attackers gain entry through systems exposed to the public, or through social engineering attacks targeting employees. Once an adversary gains access to one of these devices, it must have the capability to move laterally within internal networks until they successfully access control systems. Leveraging access to local accounts with limited permissions, adversaries exploit systems' vulnerabilities, such as default or hardcoded credentials [13], [39], gaining access to restricted resources. This capability is closely tied to the adversary's knowledge. The more they know about the internal structure and hierarchy of the organization, the greater their ability to navigate through it. Additionally, operational knowledge of the grid and their communication protocols are essential.

Persistence and evasion. These capabilities define the attackers' capacity to endure within the compromised systems without detection. This capability varies, ranging from minimal instances where adversaries may execute discrete acts of sabotage, to more sophisticated scenarios where attackers establish clandestine backdoors, providing them with the means to sustain access and control over the system. Once again, we observe a correlation with the attackers' level of knowledge; a deeper understanding of the cyber layer enhances their ability to navigate countermeasures effectively and maintain their activities discreetly. Moreover, possessing detailed knowledge about both layers empowers adversaries to execute Living-of-the-Land attacks [61]. In such instances, they leverage existing tools and services within the target environment, evading detection and maintaining persistence [66], [67].

3.4.2. Malicious activities. The extent of damage that can be caused by an attacker employing the mentioned capabilities depends on the nature of the affected devices and the scale of the attack. The malicious activities can span from localized domains, involving the manipulation of user or facility consumption and availability, to broader calamities such as blackouts encompassing city or country-wide areas. Within the spectrum of potential attacks that can leverage the presented capabilities, we differentiate the following malicious actions:

Modification of Energy Generation. In instances where an adversary gains remote or physical access to a power generator device, it can manipulate the amount of energy injected into the network, causing an overload or voltage drop [1]. These sophisticated attacks require access and control over devices in critical infrastructure, such as generation plants, or the widespread control of DER located at the customer's end [33]. Moreover, the injection of false data could be used to trick the demand-reponse system into responding to a fake generation and consumption imbalance scenario, resulting in the injection of excess or reduced power into the network. Finally, the deactivation of generators can also be achieved through denial of service capabilities targeting the generation plant systems.
Modification of Energy Consumption. Similar the exploitation of DERs to modify power generation, adversaries can manipulate energy demand to destabilize the network [15]. Seizing control or disrupting the availability of a substantial quantity of loads connected to the grid, such as high-consumption IoT devices, could disturb the delicate balance of the electrical system.
Manipulation of Security Elements. With the required capabilities an adversary can modify security elements, in order to either cause false positives affecting availability or evade the detection of hazardous situations in the grid. The combination of this manipulation with other attacks, such as altering the amount of energy generated, can not only result in a denial of service but also cause irreversible damage to the infrastructure and connected devices. For example, an adversary with command execution capability over a remote relay can modify the threshold at which current transmission is cut, leading to a blackout in a the area protected by the relay [73]. Similarly, an attacker with false data injection capability could activate a security element by simulating a dangerous state of the grid through manipulated data. Lastly, the availability of security elements can be disrupted by exploiting denial of service capabilities targeted at the vulnerable systems.

3.4.3. Case study: real-world vulnerabilities. To overview and confirm that the previous capabilities are possible in real world deployments, we conduct a study to gather evidence from various products, both specific of Smart Grids (e.g., AMI or PAS) and also generic to other ICS (e.g., PLCs and RTUs). Appendix B describes the methodology used for this study, related to a selected set of devices from three of the top vendors in this field: Siemens, Esri, and ABB.

Table 1 enumerates the number of products considered in devices from these vendors (i.e., GIS, PAS, AMI and DRS), together with the corresponding CPE identifier [38] and CVEs identifier [14]. We provide overall analysis for these vulnerabilities in Appendix B, and the detailed identifiers in an online appendix.[1] Here, we provide a classification based on which capabilities would be granted to the adversary, shall the vulnerability be exploited. To achieve this, we categorized them according to their potential for providing access, command and false data injection, eavesdropping, Denial of Service (DoS), lateral movement & privilege escalation, persistence and other functionalities. This classification is not mutually

1. https://github.com/jsande-uc3m/adversarial-model-smart-grids

Component	#Products	#CPEs	#CVEs
Geographic Info. Sys. (GIS)	16	86	83
Power Automation Sys. (PAS)	9	15	36
Advance Meter. Infras. (AMI)	4 + 1*	14 + 4*	17
Demand Resp. Sys. (DRS)	1	4	2
Remote Terminal Unit (RTU)	7	13	11
SCADA	7	8	40
Program. Logic Contr. (PLC)	5	20	14
Total	**50**	**164**	**203**

TABLE 1. OVERVIEW CVES IN OPERATION SYSTEMS AND DEVICES

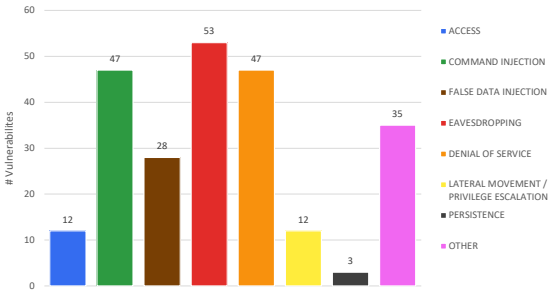

Figure 1. Capabilities enabled by exploiting known vulnerabilities

exclusive, allowing for the potential association of a single vulnerability with multiple capabilities concurrently.

The results of this classification are depicted in Figure 1. In terms of access, we identified 12 vulnerabilities that, for instance, allow unauthorized users to gain access to resources or administration controls by circumventing authentication systems. Conversely, we also pinpointed a similar number of vulnerabilities facilitating command injection, eavesdropping, and denial of service, with 47, 53, and 47 CVEs respectively. Moreover, we unearthed vulnerabilities breaking data integrity, thereby enabling false data injection. Equally significant as the access vulnerabilities, we uncovered vulnerabilities allowing lateral movement and privilege escalation, empowering authenticated users, for instance, to access resources beyond their permissions or passwords from other accounts. The persistence capability is possible facilitated through 3 vulnerabilities (although it is worth noting that persistence could also be achieved through other capabilities such as command injection). Lastly, categorized as "others", we identified 35 vulnerabilities, predominantly linked to social engineering attacks where an adversary redirects legitimate users to rogue websites.

As we can observe, vulnerabilities provide adversaries with the necessary knowledge and potential to exploit security flaws, thereby acquiring the capabilities defined in this section. Some of these vulnerabilities have been exploited in critical cyberattacks, as we discuss in §4.

3.5. Adversarial model

Once we have presented the different features that might define an adversary against Smart Grids, we wrap up with a definition of potential roles based on different models. Table 2 presents and characterize these roles, which we briefly discuss next.

First, **state-sponsored** refers to the highest profile actor, mostly with geopolitical motivation (i.e, threatening the Smart Grid of an enemy country with any goal). As such, we assume that it has the highest knowledge (i.e., insider, by means of a sabotaging insider or cyber-espionage) and capabilities, and would act on any domain. Then, a **cyber-terrorist** is an actor that resembles a state-sponsored, but its motivations are more aligned with ideology and its goal is to harm the society or individual users of a targeted victim, i.e., with a main goal of disrupting the generation of energy. Due to potentially having less resources, it might posses fewer capabilities for lateral movement and persistence or evasion. Instances of this threat have been observed [43], alongside attacks on the physical layer of energy infrastructure perpetrated by extremists [21]. The next role, **cyber-criminal**, refers to an actor which seeks to gain financial benefit from the victim (e.g., a ransomware gang), targeting the grid remotely and by means of classical cyberattacks such as command injection or DoS on the operation and service domains. A subset of the previous, less skilled actor, is what we refer as **script-kiddie**, which different from the previous, it might want to gain notoriety on underground communities before they evolve towards a higher profile [44]. An important role, since it might be transversal to the others (e.g., he/she can be coerced or suborned by state-sponsored actors), is the **sabotage insider**, which mostly refers to an actor with capabilities to threat the sector from the inside, e.g., and employee. Depending on the role and permissions of this actor, its capabilities and targeted domain might differ (e.g., depending on whether he/she has administrative privileges on the industrial network, or if he/she can tamper with particular devices within the grid). Finally, we consider the role of a **fraudulent user**, which is an adversary that resembles a final customer willing to tamper their local smart meter to report lower readings, and thus to reduce the electricity bill [3].

Overall, our adversarial model helps to understand the different characteristics to understand threats on Smart Grids, and from these, to define different roles. We showcase the benefits of our model by studying real-world attacks, mapping these to the adversarial role.

4. Modeling Adversaries from Real Attacks

This section describes the main cyberattacks that have targeted the power Smart Grid, and maps these attacks to the adversarial model proposed before. To this end, we rely on public information gathered from news and security reports. First, we describe targeted malware designed specifically to attack the Smart Grid. Then, we examine more generic malware designed to attack diverse ICS, including ransomware attacks that, despite not being its primary goal, they have impacted the electrical industry with diverse consequences.

4.1. Cyberattacks targeting the Smart Grid

In recent years, the number of attacks against the Smart Grid have increased [29]. Table 3 presents a list of the major cyber-incidents that have directly targeted and caused significant impact on power grids. As it can be observed, they all targeted the power grid of Ukraine. The BlackEnergy-3 malware used in the 2015 Ukrainian blackout is not a malware specifically designed to attack power grids but is a multi-purpose malware that has been active since 2007 (in earlier versions) and was used since

Role	Motivation	Goals	Knowledge	Capabilities				Attack Surface
				Access	Exploitation	Lateral movement	Persistence/ Evasion	
State-sponsored	Geopolitics	Reconnaissance Service Disruption Data theft Market manipulation	Insider	Physical Remote	Command Inj. False Data Inj. Eavesdropping DoS	High	High	All domains
Cyber-terrorist	Damage sector Harm users	Service Disruption	Official Field	Physical Remote	Command Inj. False Data Inj. Eavesdropping DoS	Medium	Medium	Generation
Cyber-criminal	Financial benefit	Service Disruption Data theft Market manipulation	Official Field	Remote	Command Inj. DoS	Medium	Low	Operation Service
Script-kiddie	Fame and recognition	Any	Official Field	Remote	Eavesdropping DoS	Low	Low	Operation Customer
Sabotaging insider	Damage sector	Service Disruption	Insider	Physical Remote	Command Inj. False Data In. Eavesdropping DoS	Medium	Medium	Operation Generation Transmission Service
Fraudulent user	Financial benefit	Bill manipulation	Field	Physical	False Data Inj. DoS	None	None	Customer

TABLE 2. SMART GRID ADVERSARIAL MODELS.

Year	Target	Cyber-weapon	Impact
2015	Various substations (Ukraine)	BlackEnergy-3	Blackout
2016	Pivnichna substation (Ukraine)	Industroyer / CrashOverride	Blackout
2022	Unknown (Ukraine)	Industroyer-2	None[†]

TABLE 3. CYBERATTACKS TARGETING THE UKRANIAN SMART GRID FOR SERVICE DISRUPTION. ([†]THE ATTACK WAS STOPPED BY THE NATIONAL CERT BEFORE INCURRING ANY FURTHER DAMAGE)

then in multiple campaigns. In contrast, the Industroyer and Industroyer-2 malware pieces, used in the 2016 and 2022 attacks respectively, were specifically designed to attack power grids. This means that they are a more sophisticated and dangerous threat to power grids because they attempt to exploit specific features and protocols used in electrical substations. These attacks, summarized in Table 3, have the same pattern, i.e., they all have geopolitical motivation and the goal for disruption. Despite subtle differences, mostly in terms of sophistication, they all fall under the same adversarial model, i.e., state-sponsored. We next describe the first attack (2015), mapping each of the actions to the proposed adversarial model.

4.1.1. Ukrainian blackout (2015). The first known cyberattack that caused a blackout in a populated city took place in Ukraine on December 23, 2015. The cyberattack caused several power outages, which affected 225,000 customers approximately, in different regions of Ukraine, and lasted for almost 6 hours [18] **[goal-disrupt]**. The attack was attributed by various security firms and hacking experts to the Russian hacking group Sandworm [34] **[motivation-geopolitical]**.

This attack that led to the black-out was not an isolated incident, but rather a continuation of multiple attacks carried out by Russia against Ukraine's critical infrastructure. Indeed, the first step the attackers took before executing the actual attack was a reconnaissance phase **[goal-reconnaissance]**, in which they tried to gather all possible information about the potential targets **[goal-data-theft]**. Once they had all the necessary information, the actors developed custom malware for the attack. The adversaries employed spear-phishing against employees of the different Ukrainian substations **[capability-false-data-injection]**, sending e-mails with weaponized Microsoft Office documents with an embedded installer of the BlackEnergy3 (BE-3) malware [59]. The BE-3 malware established connection to its Command and control (C2C) server for further instructions **[capability-command-injection]**. After reaching this point, they performed lateral movement through the internal corporate network in order to discover new targets and expand the invasion **[capability-lateral]**, and they also gained access to critical devices within the ICS network. Allegedly, the attackers reached this point around six months before the actual date of the black-out, collecting necessary data and gaining knowledge from the infrastructure to conduct the attack (**[knowledge-insider]**).

Once this phase was reached, the hackers placed the KillDisk malware on a network share and added a policy in the domain controller to retrieve this malware and execute upon system reboots **[capability-persistence]**. Next, they prepared a new attack to launch in parallel to the actual black-out. This attack consisted on cutting the uninterruptible power supply (UPS) of the telephone communications server and the substation data center servers to prevent users from reporting the loss of power and thus making the outage last longer **[capability-DoS]**.

For the attack, the attackers "pulled the plug" by remotely controlling the computers of the substation's employees and issuing unauthorized commands **[capability-command-injection]** that opened the circuit breakers, interrupting the power supply to more than 225,000 customers **[goal-disrupt]**. Once the hackers cut the power, they delivered a malicious firmware update to the target devices to disable serial to Ethernet converters. Consequently, operators were unable to remotely close the breakers, requiring to manually close the breakers at each substation, increasing the recovery time and the impact of the attack **[capability-persistence],[capability-DoS]**. Also, the attackers cut the phone communication server and data center server of the substations through a DoS attack, tampering the reporting for the customers**[capability-evasion],[capability-DoS]**. Once the attack took place, the actors executed the KillDisk mal-

ware again to erase all the records and log data from the victim's machines from both the corporate and ICS networks [18] [59] **[capability-evasion],[capability-DoS]**.

4.2. Cyberattacks affecting the power grid

In this section, we describe cyberattacks that had an impact on the power grid, but with a lower level of planning and sophistication than the targeted cyberattacks described previously. Table 4 shows the attacks that employ more-generic malware, not explicitly designed to attack power Smart Grids. We next discuss them in detail.

In 2016 a cyberattack against the Israel Electric Authority was reported by the national government, claiming that they were targeted by severe cyberattacks causing several computers to shut down. In response, officials chose to switch off segments of the country's power grid, hindering its operation [64] **[goal-disruption]**. A later report from Dragos Security contradicts the version given by the government, claiming that the cyberattack was actually an undisclosed ransomware delivered via spearphishing that infected an employee from Israel's Electric, taking off some computers from the Electric Authority but not incurring into important outages affecting the power grid **[goal-financial],[capability-dos]**. Since no further information was disclosed, we can not model the potential adversary. However, this case shows how a cyber-criminal, potentially seeking financial gain, was able to alarm an energy operator, ultimately leading to a deprivation of a national critical infrastructure.

The 2017 attack against EirGrid, a power company that provides electricity across Ireland and Northern Ireland, resembles a state-sponsored attack, though there is not official attribution. According to multiple reports, adversaries gained access by using a MITM (Man-In-The-Middle) technique (**[capability-eavesdropping]**) and installing a virtual tap on Vodafone's Direct Internet Access (DIA) service in Shotton, Wales [10]. The wiretaps were discovered in July 2017 and have allegedly been active since April of that same year. In these 4 months, hackers were able to intercept communications and steal information (**[goal-data-theft],[knowledge-insider]**. The extent of data compromised by the hackers and the potential installation of additional malware remain undisclosed. However, as mentioned previously, attackers might seek to gain knowledge and persist before conducting further attacks **[goal-reconnaisance]**. At the time of this writing (March'24) no further information have been made public regarding these incidents in Ireland's power grid [10].

In 2019, a ransomware attack against City Power, a major electricity provider in South Africa, encrypted all their databases, applications and network **[motivation-financial],[capability-DoS]**. The attack disrupted prepaid customers' ability to purchase electricity units, consequently leading to an eventual shortage of supply **[goal-disruption]**. The number of customers who were affected by this problem was over 250,000. The ransomware used, whereas it has been allegedly identified, has not been disclosed publicly at the time of this writing [4]. This is another example of a cybercriminal adversary, that, seeking for financial benefit, and by targeting the service domain, has disrupted a critical infrastructure due to the way the market domain was designed.

Year	Target	Cyber-weapon	Impact
2016	Electricity Authority (Israel)	Ransomware	Operability
2017	EirGrid (Ireland)	None (MITM)	Unknown†
2019	City Power (South Africa)	Ransomware	Operability

TABLE 4. CYBERATTACKS WITH EFFECTS ON THE OPERATION. (†ALLEGEDLY, DATA LEAKAGE OR MALWARE INSTALLATION)

4.2.1. Ransomware attacks that hit the electrical sector. Various cyberattacks, even not directly targeting the grid operation (i.e., distribution, generation or transmission domains), have affected the electricity industry, concretely the service, customer and market domains. Table 5 in Appendix A includes the ransomware attacks against utilities in the electricity sector that could be identified. For this analysis, we rely on the CIRA dataset [50]. Even though the dataset starts taking data from 2017 onward, the number of ransomware attacks against companies in the electrical sector has been increasing since 2017. This is expected and consistent with the popularity and prevalence of these attacks in the last years [20]. The most common approach used for initial exploitation is via phishing e-mails to company employees **[capability-false-data-injection]**. The consequences for companies are, in most cases, financial losses, e.g., payments to recover the data or prevent data leakage, and also reputational, since these attacks degrade the confidence and trust into these companies **[goal-financial],[goal-market-manipulation]**. However, in some minor but relevant cases, such as the ones discussed before, these attacks entail operational problems, meaning that their cyber-physical systems have been temporarily shut down because of the attack.

5. Conclusions and discussion

The Smart Grid is a critical infraestructure that needs to be properly protected, and the attacks in the Ukrainian grid showed the impact that a high-profile adversary can incur on the society. To better prepare, detect and respond to these incidents, it is important to understand the attacks surfaces, as well a the knowledge, capabilities, motivations and goals of the adversary, i.e., to know the adversarial model. We define a model by considering attacks from the research literature, exiting vulnerabilities, and by analysing the Tactics, Techniques and Procedures (TTPs) from real-world attacks. This model allows to define different actors (roles) for these incidents, with different levels of skills and goals. Our work allows to better understand the risks to which the Smart Grid is exposed, and consequently, to apply appropriate and reasonable countermeasures to mitigate these.

Acknowledgments

As part of the open-report model followed by the Workshop on Attackers & CyberCrime Operations (WACCO), all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO/tree/main/WACCO-2024. This work was supported by Grant TED2021-132170A-I00 funded by MCIN/AEI/10.13039/501100011033 and by the "EU NextGenerationEU/PRTR".

References

[1] Sridhar Adepu, Nandha Kumar Kandasamy, Jianying Zhou, and Aditya Mathur. Attacks on smart grid: Power supply interruption and malicious power generation. *International Journal of Information Security*, 19:189–211, 2020.

[2] Tanveer Ahmad, Hongcai Zhang, and Biao Yan. A review on renewable energy and electricity requirement forecasting models for smart grid and buildings. *Sustainable Cities and Society*, 55:102052, 2020.

[3] Mahmoud M Badr, Mohamed I Ibrahem, Hisham A Kholidy, Mostafa M Fouda, and Muhammad Ismail. Review of the data-driven methods for electricity fraud detection in smart metering systems. *Energies*, 16(6):2852, 2023.

[4] BBC News. Ransomware hits johannesburg electricity supply, 2019. Accessed: 30-05-2023.

[5] Chris Brook. Blackenergy apt group spreading malware via tainted word docs, 2016. Accessed: 16-03-2023.

[6] Clementina Bruno, Luca Guidi, Azahara Lorite-Espejo, and Daniela Pestonesi. Assessing a potential cyberattack on the italian electric system. *IEEE Security & Privacy*, 13(5):42–51, 2015.

[7] CERT-UA. Cyberattack of the sandworm group (uac-0082) on energy facilities of ukraine using industroyer2 and caddywiper malware (cert-ua-4435), 2022. Accessed: 04-03-2023.

[8] Anton Cherepanov and Robert Lipovsky. Industroyer 2 - sandworm's cyberwarfare targets ukraine's power grid again, 2022. Accessed: 04-03-2023.

[9] Robert Lipovsky & Anton Cherepanov. Industroyer2: Sandworm's cyberwarfare targets ukraine's power grid again, 2022. Accessed: 13-03-2023.

[10] Graham Clueley. Attack on ireland's state-owned power provider blamed on state-sponsored hackers, 2017. Accessed: 30-05-2023.

[11] Federal Energy Regulatory Commission et al. Critical energy/electric infrastructure information (ceii). https://www.ferc.gov/ceii, 2019. Accessed: 2024-02-22.

[12] Mitre Corporation. Mitre att&ck. https://attack.mitre.org/, -. Accessed: 2024-02-16.

[13] Mitre Corporation. Hardcoded credentials. https://attack.mitre.org/techniques/T0891/, 2022. Accessed: 2024-03-16.

[14] The MITRE Corporation. Common vulnerabilities and exposures. https://www.cve.org, -. Accessed: 2024-03-16.

[15] Adrian Dabrowski, Johanna Ullrich, and Edgar R Weippl. Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, pages 303–314, 2017.

[16] Comunidad de MADRID. Planificación de la red de transporte de electricidad 2015-2020. https://www.ree.es/sites/default/files/01_ACTIVIDADES/Documentos/planificacion/madrid_v2.pdf, 2014. Accessed: 2024-02-22.

[17] Jianguo Ding, Attia Qammar, Zhimin Zhang, Ahmad Karim, and Huansheng Ning. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, 15(18), 2022.

[18] E-ISAC. Analysis of the cyber attack on the ukrainian power grid, 2016. Accessed: 14-02-2023.

[19] Ahmed Elmasry, Abdullatif Albaseer, and Mohamed Abdallah. Openplc and lib61850 smart grid testbed: Performance evaluation and analysis of goose communication. In *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE, 2023.

[20] Guy Faulconbridge. Russia's gru military intelligence agency explained, 2018. Accessed: 08-03-2023.

[21] Eric Geller. Physical attacks on electrical grid peak amid cyber threats. *Politico*, December 2022.

[22] Lavanya Gnanasekaran and Sean Monemi. Gis role in smart grid. *2018 IEEE Conference on Technologies for Sustainability (SusTech)*, pages 1–5, 2018.

[23] Avi Gopstein, Cuong Nguyen, Cheyney O'Fallon, Nelson Hastings, David Wollman, et al. *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology ..., 2021.

[24] Yutian Gui, Ali Shuja Siddiqui, Suyash Mohan Tamore, and Fareena Saqib. Security vulnerabilities of smart meters in smart grid. In *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, volume 1, pages 3018–3023, 2019.

[25] Mohammad Kamrul Hasan, AKM Ahasan Habib, Zarina Shukur, Fazil Ibrahim, Shayla Islam, and Md Abdur Razzaque. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*, 209:103540, 2023.

[26] Alvin Huseinović, Saša Mrdović, Kemal Bicakci, and Suleyman Uludag. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access*, 8:177447–177470, 2020.

[27] Shahbaz Hussain, Javier Hernandez Fernandez, Abdulla Khalid Al-Ali, and Abdullatif Shikfa. Vulnerabilities and countermeasures in electrical substations. *International Journal of Critical Infrastructure Protection*, 33:100406, 2021.

[28] iea. Demand response. https://www.iea.org/energy-system/energy-efficiency-and-demand/demand-response, 2023. Accessed: 2023-10-09.

[29] International Energy Agency. Cybersecurity: is the power system lagging behind?, 2023.

[30] International Organization for Standardization (ISO). Information technology – security techniques – information security management guidelines based on iso/iec 27002 for process control systems specific to the energy utility industry, 2017.

[31] Amber Jackson. Top 10: Smart grid companies. https://energydigital.com/top10/top-10-smart-grid-companies, 2023. Accessed: 2023-11-09.

[32] A Leonardi, K Mathioudakis, A Wiesmaier, and F Zeiger. Towards the smart grid: substation automation architecture and technologies. *Advances in electrical engineering*, 2014, 2014.

[33] Martin Lindström, Hampei Sasahara, Xingkang He, Henrik Sandberg, and Karl Henrik Johansson. Power injection attacks in smart distribution grids with photovoltaics, 2021.

[34] Mandiant. Sandworm team and the ukrainian power authority attacks, 2016. Accessed: 11-03-2023.

[35] Piotr Mirowski, Sining Chen, Tin Kam Ho, and Chun-Nam Yu. Demand forecasting in smart grids, 2014.

[36] Amir Motamedi, Hamidreza Zareipour, and William D. Rosehart. Electricity price and demand forecasting in smart grids. *IEEE Transactions on Smart Grid*, 3(2):664–674, 2012.

[37] Muhammad Nouman Nafees, Neetesh Saxena, Alvaro Cardenas, Santiago Grijalva, and Pete Burnap. Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Computing Surveys*, 55(10):1–36, 2023.

[38] NIST. Official common platform enumeration (cpe) dictionary. https://nvd.nist.gov/products/cpe, -. Accessed: 2023-10-09.

[39] NIST. Cve-2016-8566 detail, 2017. Accessed: 2024-03-16.

[40] NIST. Cve-2021-29114. https://nvd.nist.gov/vuln/detail/CVE-2021-29114, 2021. Accessed: 2024-02-22.

[41] NIST. Vulnerability metrics, 2022. Accessed: 2023-10-09.

[42] Patrick Howell O'Neill. Russian hackers tried to bring down ukraine's power grid to help the invasion. https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/, 2022. Accessed: 2024-03-16.

[43] Pierluigi Paganini. Isis cyber caliphate. *Security Affairs*, 2015.

[44] Sergio Pastrana, Alice Hutchings, Andrew Caines, and Paula Buttery. Characterizing eve: Analysing cybercrime actors in a large underground forum. In *Research in Attacks, Intrusions, and Defenses: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings 21*, pages 207–227. Springer, 2018.

[45] Sergio Pastrana, Juan E Tapiador, Agustin Orfila, and Pedro Peris-Lopez. Defidnet: A framework for optimal allocation of cyberdefenses in intrusion detection networks. *Computer Networks*, 80:66–88, 2015.

[46] Chen Peng, Hongtao Sun, Mingjin Yang, and Yu-Long Wang. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(8):1554–1569, 2019.

[47] Ryan Pickren, Tohid Shekari, Saman Zonouz, and Raheem Beyah. Hey, you, get off of my market: detecting malicious apps in official and alternative android markets. In *NDSS*, 2024.

[48] Theta Learning Point. Difference between smart grid and conventional grid. https://www.thetalearningpoint.com/2023/01/difference-between-smart-grid-and-conventional-grid.html, 2023. Accessed: 2023-10-09.

[49] Haftu Tasew Reda, Adnan Anwar, and Abdun Mahmood. Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts. *Renewable and Sustainable Energy Reviews*, 163:112423, 2022.

[50] A. Rege. Critical infrastructure ransomware attacks (cira) dataset. Online, 2023. Accessed: 26-04-2023.

[51] Engla Rencelj Ling, Jose Eduardo Urrea Cabus, Ismail Butun, Robert Lagerström, and Johannes Olegard. Securing communication and identifying threats in rtus: A vulnerability analysis. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ARES '22, New York, NY, USA, 2022. Association for Computing Machinery.

[52] Emergen Research. Top 10 companies advancing smart grid technology to create sustainable energy future. https://www.emergenresearch.com/blog/top-10-companies-advancing-smart-grid-technology-to-create-sustainable-energy-future, 2023. Accessed: 2023-11-09.

[53] Carla Rubí. The challenges of upgrading the power grid for a decarbonised electric future. https://informaconnect.com/the-challenges-of-upgrading-the-power-grid-for-a-decarbonised-electric-future/, 2019. Accessed: 2024-02-22.

[54] Gabriel Salles-Loustau, Luis Garcia, Pengfei Sun, Maryam Dehnavi, and Saman Zonouz. Power grid safety control via fine-grained multi-persona programmable logic controllers. In *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 283–288, 2017.

[55] Siemens. Energy automation – intelligent and future-proof. https://www.siemens.com/global/en/products/energy/energy-automation-and-smart-grid.html, -. Accessed: 2023-09-09.

[56] Siemens. Siemens and esri partner to bring grid planning and operation to a new level. https://press.siemens.com/global/en/pressrelease/siemens-and-esri-partner-bring-grid-planning-and-operation-new-level, 2022. Accessed: 2023-09-09.

[57] Brian Singer, Amritanshu Pandey, Shimiao Li, Lujo Bauer, Craig Miller, Lawrence Pileggi, and Vyas Sekar. Shedding light on inconsistencies in grid cybersecurity: Disconnects and recommendations. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 38–55. IEEE, 2023.

[58] Jonathan Spring, Eric Hatleback, Allen Householder, Art Manion, and Deana Shick. Time to change the cvss? *IEEE Security & Privacy*, 19(2):74–78, 2021.

[59] Jake Styczynski and Nate Beach-Westmoreland (Booz Allen Hamilton). When the lights went out. a comprehensive review of the 2015 attacks on ukrainian critical infrastructure. *Booz Allen Hamilton*, 2019. Accessed: 15-03-2023.

[60] Andy Swales et al. Open modbus/tcp specification. *Schneider Electric*, 29(3):19, 1999.

[61] Symantec. Living off the land: Turning your infrastructure against you. Online: https://www.symantec.com/content/dam/symantec/docs/white-papers/living-off-the-land-turning-your-infrastructure-against-you-en.pdf, 2019. Accessed: 16-03-2024.

[62] DPS Telecom. A rugged remote terminal unit for the smart grid market. https://www.dpstele.com/insights/2020/01/03/smart-grid-market/, 2020. Accessed: 2023-10-09.

[63] Mini S Thomas and John Douglas McDonald. *Power system SCADA and smart grids*. CRC press, 2017.

[64] Trend Micro. Israel's electric authority "hack" caused by ransomware, 2016. Accessed: 29-05-2023.

[65] Darshana Upadhyay and Srinivas Sampalli. Scada (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, 89:101666, 2020.

[66] US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency. People's republic of china state-sponsored cyber actor living off the land to evade detection. Online: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a, 2023. Accessed: 16-03-2024.

[67] US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency. Prc state-sponsored actors compromise and maintain persistent access to u.s. critical infrastructure. Online: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a?utm_source=CISACyber&utm_medium=post&utm_campaign=VT_020724, 2024. Accessed: 16-03-2024.

[68] Muhammad Usama and Muhammad Naveed Aman. Command injection attacks in smart grids: A survey. *IEEE Open Journal of Industry Applications*, pages 1–11, 2024.

[69] Craig Valli, Andrew Woodward, Clinton Carpene, Peter Hannay, Murray Brand, Reino Karvinen, and Christopher Holme. Eavesdropping on the smart grid. 2012.

[70] Jing Xie, Chen-Ching Liu, Marino Sforna, Martin Bilek, and Radek Hamza. Threat assessment and response for physical security of power substations. In *IEEE PES Innovative Smart Grid Technologies, Europe*, pages 1–6, 2014.

[71] Kareem Yusuf. How ibm® and esri are working together to map a more sustainable future. https://www.ibm.com/blog/how-ibm-and-esri-are-working-together-to-map-a-more-sustainable-future/, 2023. Accessed: 2023-09-09.

[72] Daniel Kapellmann Zafra, Raymond Leong, Chris Sistrunk, Ken Proksa, Corey Hildebrandt, Keith Lunden, and Nathan Brubaker. Industroyer.v2: Old malware learns new tricks, 2022. Accessed: 29-07-2023.

[73] Jiapeng Zhang and Yingfei Dong. Cyber attacks on remote relays in smart grid. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9, 2017.

[74] Jixuan Zheng, David Wenzhong Gao, and Li Lin. Smart meters in smart grid: An overview. In *2013 IEEE green technologies conference (GreenTech)*, pages 57–64. IEEE, 2013.

Appendix A.
Ransomware attacks on power grids

Table 5 lists known ransomware incidents that impacted electric utilities or the electric grid, obtained from the CIRA dataset [50]. This data is based on news articles or reports that describe the existence of these ransomware cyberattacks, and there might have been more ransomware cyberattacks against the electricity sector. We observe an increase in the number of ransomware attacks against the electricity industry in recent years. This can be mainly explained by the fact that ransomware attacks have become massively popular during the in the last few years, especially since the COVID-19 pandemic, and the electricity sector consequently also reflects this increase. Most of the ransomware cyberattacks have caused economic impact or data leakage, yet only a minority have caused operational damage. In the cases where the operability is affected, it is mainly by bringing down the web or e-mail services of these companies.

Appendix B.
Vulnerability analysis

In this paper, we modeled adversaries by considering their motivation, goals, knowledge, and capabilities. However, establishing the feasibility of these capabilities has proven to be a intricate task. To avoid merely speculating on potentially unrealistic capabilities, we conducted a study that provides evidence about the practicality of the described threats. This is supported by the identification of vulnerabilities that if properly exploited, give an attacker the mentioned capabilities, validating therefore the realism of our modeled scenario.

This study has been conducted in three phases: selection of devices to be examined, collection of OSINT information about the devices, and analysis of the identified vulnerabilities.

B.1. Device selection

Firstly, we have identified a series of devices present in the electrical network that have been or may be targets of attacks by adversaries with the objectives, knowledge, and capabilities we have modeled. For this selection, we have relied on the study of the attack surface carried out in Section 3.1, especially in the operational domain. Based on this, the selected systems and devices are:

- Supervisory Control And Data Acquisition (SCADA)
- Geographic Information Systems (GIS)
- Advanced Metering Infrastructure (AMI)
- Supervisory Control And Data Acquisition (SCADA)
- Remote Terminal Unit (RTU)
- Programmable Logic Controller (PLC)

B.2. OSINT collection methodology

Once we have identified the main devices to be studied, the next steps is to collect OSINT information for product and manufacturers of these devices and their associated vulnerabilities. For this collection, we leverage two popular catalogs from the NVD, i.e., Common Platform Enumeration (CPE) and Common Vulnerability Exposure (CVE).

B.2.1. Products. To search for specific products, we rely on the CPE system, which is a structured naming scheme for information technology systems, software, and packages, providing a description format for binding text and tests to a name [38]. A key challenge in this step is to identify which are the right IT systems to look for, i.e. those that are used in Smart Grids. However, some of them are not exclusive, e.g. SCADA systems are used in the scope of various ICS. Also, the high market diversity leads to a high amount of products that might be used for Smart Grids, which hardens the analysis. Accordingly, we focus our research on four companies that, according to industry reports [31], [52], have a higher revenue in the market of Smart Grids by September 2023. These companies are IBM, Cisco, Siemens and ABB.

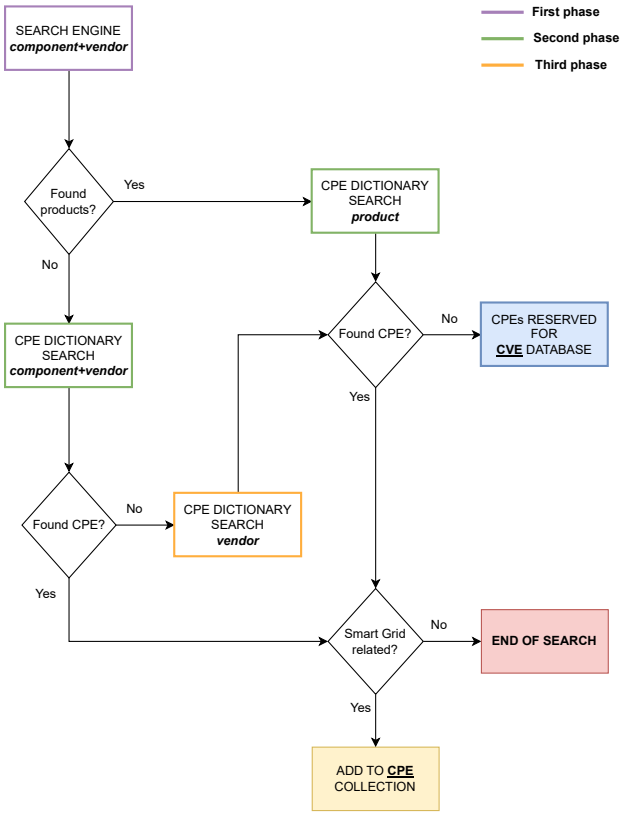

Figure 2. Flowchart of the methodology to collect CPEs

Figure 2 shows the methodology employed to select the CPEs related to the selected devices. As the flowchart presents, the **first phase** consisted on introducing the keywords *component* + *vendor* in a web search engine. Using this approach we found a new vendor (Esri), which was not initially identified. We noted that this company has commercial collaboration with Siemens and IBM for manufacturing GIS products, and thus we include it in our analysis [56] [71].

This search allowed to find a catalog of products related to smart grids offered by Siemens [55] providing names for specific products. This allowed us to make specific searches in the CPE Dictionary, as we explain

Year	Affected Entity	Country	Ransomware Variant	Impact
2017	Iberdrola	Spain	Wannacry	Economic
2020	Reading Municipal Light Department	USA (Massachusetts)	Undisclosed	Economic
2020	LTI Power Systems	USA (Ohio)	Undisclosed	Data Leakage
2020	EDP	Portugal	Ragnar Locker	Economic & Data Leakage
2020	Northwest Territories Power Corporation	Canada	NetWalker	Operability (Web & E-Mail)
2020	Elexon	UK	Revil/Sodinokibi	Economic & Data Leakage
2020	Electricity Generating Authority of Thailand	Thailand	Maze	Data Leakage
2020	Enel Edesur S.A.	Argentina	Snake/EKANS	Economic & Operability
2020	K-Electric	Pakistan	NetWalker	Economic & Data Leakage
2020	Enel Group	Global	NetWalker	Economic & Data Leakage
2021	Carnegie Clean Energy	Belgium	Avaddon	Undisclosed
2021	Centrais Eletricas Brasileiras (Eletrobras)	Brazil	Undisclosed	Operability
2021	Companhia Paranaense de Energia (Copel)	Brazil	Darkside	Data Leakage
2021	Wiregrass Electric Cooperative	USA, Alabama	Undisclosed	Operability (Website)
2021	Delta-Montrose Electric Association (DMEA)	USA, Colorado	Undisclosed	Operability & Data Loss
2021	CS Energy	Australia, Queensland	Conti	Operability
2022	ESKOM Hld SOC Ltd.	South Africa	Everest	Economic & Data Leakage
2022	State Electric Company Limited (STELCO)	Canada	Undisclosed	Operability
2022	Nordex	Global	Conti	Operability
2022	Montenegro government and CI	Montenegro	Cuba	Economic & Data Leakage
2022	Gestore dei Servizi Energetici SpA (GSE)	Italy	BlackCat/ALPHV	Operability & Data Leakage
2022	Tata Power	India	Hive	Economic
2022	Empresas Publicas de Medellin (EPM)	Colombia	BlackCat/ALPHV	Operability & Data Leakage
2022	Entrust Energy	USA, Texas	NetWalker	Economic

TABLE 5. RANSOMWARE ATTACKS WITH IMPACT IN THE POWER SMART GRID

below. Similarly, some of ABB's specific product names were identified in this stage. However, this search did not give any results about the other two vendors (Cisco and IBM). Although we collected general information about their presence in the smart grid market, it did not mention specific products they may offer for these systems.

The **second phase** used the CPE Dictionary. Similar to the previous phase, it uses keywords to find relevant CPEs. In addition to the pair of keywords used in the previous search (*component* + *vendor*), we introduced a new keyword: *product*, to include the specific products found in the first phase.

Finally, we conducted a **third and final phase** where we searched for products related to *Esri* GIS products, obtaining various CPEs of products related to Smart Grids. In this phase, we made an attempt to look for CPEs related to IBM and Cisco. This search, however, resulted in a huge amount of CPEs (more than 40k results), due to the prevalence of these vendors in various IT markets. Since we could not collect specific information for products being specifically used in Smart Grids, we decided to leave out these two vendors from the study. This way, we choose to not err on the side of having False Positives (i.e., not including devices that are not being deployed in Smart Grids) in our study.

To end this process, all the resulting CPEs were manually verified to confirm that they were used in smart grids, adding these to the collection of CPEs. For those products that were not found on the CPE dictionary, they were reserved to later search them in the CVE ("Common Vulnerabilities and Exposures") database.

B.2.2. CVE search. Figure 3 depicts the process to find the vulnerabilities by looking for CVEs associated for each of the CPEs collected previously. The set CPEs contain a direct reference to their associated CVEs, which allowed to conduct the query in an automated way. Still, during this process we also searched on the CVE Database for products that did not have an associated CPE, leading to new vulnerabilities on a product from SIEMENS without an associated CPE.

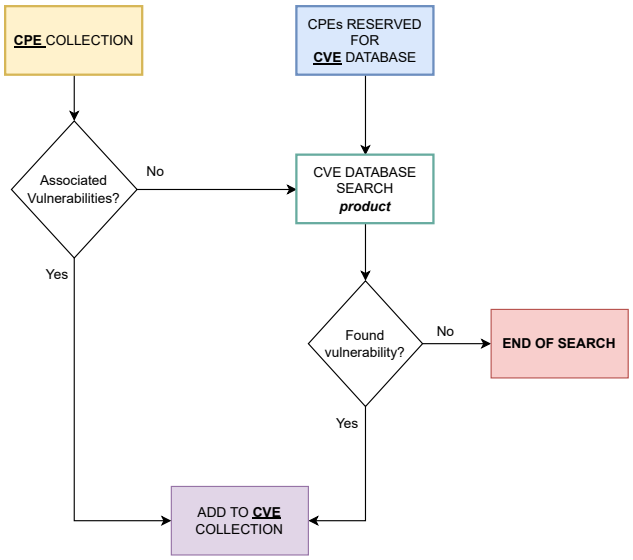

Figure 3. Flowchart of the methodology to gather CVEs

B.3. Analysis

Our collection process resulted on a total of 164 different CPEs, which are then grouped since various of them are different versions for the same product. Accordingly, we finally obtain a set of 50 groups of CPEs (i.e., 50 different products). Table 6 summarizes the products and CPEs found for each component, and the number of CVEs associated to each of them. It is important to point out that the total of number of CVEs pictured is not the direct sum of all the CVEs, since some CPEs share the same associated CVEs. The group 'PLC' refers

to Programmable Logic Controllers (PLC) used in Smart Grids. These are general purpose devices that allow to monitor and control ICS, e.g., collecting information or delivering instructions. They can be categorized in any of the other components, and thus are presented in a separate group for clarity.

Component	#Products	#CPEs	#CVEs
Remote Terminal Unit (RTU)	7	13	11
SCADA	7	8	40
Geographic Info. Sys. (GIS)	16	86	83
Power Automation Sys. (PAS)	9	15	36
Advance Meter. Infras. (AMI)	4 + 1*	14 + 4*	17
Demand Resp. Sys. (DRS)	1	4	2
Program. Logic Contr. (PLC)	5	20	14
Total	**50**	**164**	**203**

TABLE 6. OVERVIEW CPE COLLECTION *CPES THAT ARE ALSO PRESENT IN DRS GROUP

Table 7 shows the amount of CPEs grouped by vendor, including the type of component. It can be observed that the majority of CPEs belong to the vendor Siemens, which manufactures products of all categories. Additionally, only two CPEs belong to the vendor ABB, corresponding to a PAS and an AMI. Finally, as discussed earlier and as it can be observed in both tables, the vendor 'Esri' is exclusively dedicated to the production of GIS products.

Vendor	Number CPEs	Components present
Siemens	32	All
Esri	16	'GIS'
ABB	2	'PAS' and 'AMI'

TABLE 7. DISTRIBUTION OF CPES BY VENDOR

Once we have collected the CPEs, we conduct a qualitative overview of the associated vulnerabilities. To this end, we rely on a third metric from the NVD, i.e., the **"Common Vulnerability Scoring System" (CVSS)**. For each vulnerability, this metric characterizes the exploitation capabilities (e.g., whether physical access is required), and the impact in terms of confidentiality, integrity, and availability losses to the affected systems. We note that this metric is inconsistent and leaves room for ambiguities [58]. Indeed, 32 of the collected CVEs contain two different scores, i.e., one provided by the NIST, and another one provided by the vendor. For instance, in *CVE-2022-30694*, NIST set the score as 3,5 indicating a low criticality where Siemens rated it as 6,5 designating a medium criticality. In this case, not only the score changed, but also the assigned criticality level and impact on the CIA Triad. In our study, for inconsistent cases, we use the score provided by the vendor, as their role as manufacturers could allow them to have a better understanding on the potential impact of a vulnerability over the NIST.

We analyze the total of 203 CVE collected. We next provide a general overview of the main characteristics of said vulnerabilities.

We first analyze the **access vector**, which indicates the context in which the vulnerability can be exploited. As depicted in Figure 4, a vast majority of the vulnerabilities (81.2%) can be exploited remotely (network access). While this risk can be mitigated by establishing proper perimetral cyber-defenses (e.g., firewalls), a wrong configuration or vulnerability in these defenses could allow an attacker to exploit the device from an external location, posing a risk to the operation of the grid.

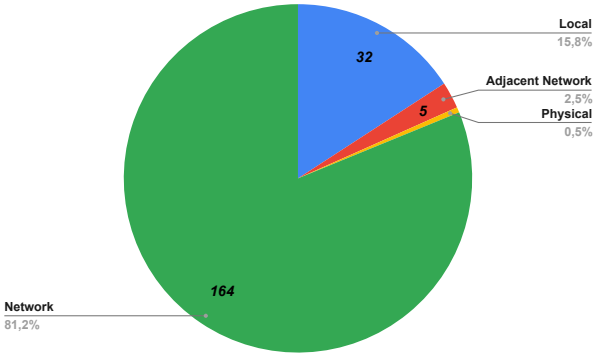

Figure 4. Access vector count of CVE collection

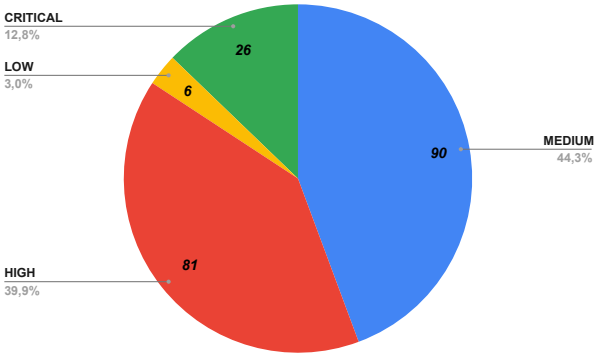

Figure 5. Severity count of CVE collection

The CVSS assigns a score for the **severity** of each CVE, based on the impact and exploitability sub scores, which ranges from None to Critical [41]. While *Medium* and *Low* scores have lower possibility of being exploited, or their impact is lower, vulnerabilities marked a *High* or *Critical* have a higher risk of being exploited and with more severe consequences. Figure 5 overviews the severity of the CVEs identified in this study. Over half of the vulnerabilities have a severity which is high or critical.

The CVSS base score contains a the feature named "User interaction", which can be either 'required' if some sort of user activity is required to trigger the exploitation (which can be enforced by means of Social Engineering techniques, e.g., to download a malicious file), or 'none' if no user interaction is required, in which case it increases the severity of the vulnerability. In our case, 123 CVEs ($\approx$ 60%) did not require user interaction, resulting in higher severity. Among the remaining CVEs, 66 required of user interaction to be exploited while 14 did not have this feature because they were only available in CVSS score version 2, which does not include the user interaction metric. Other CVSS features have a similar impact in the overall score. However, it is important to know that that low severity vulnerabilities are still exploitable, as sophisticated attackers could use them to carry out complex attacks due to the interdependencies

of the different devices for the proper operation of the grid (see §4).

Impact	Confidentiality	Integrity	Availability
None	50 - (24,6%)	63 - (31,2%)	94 - (46,3%)
Low	62 - (30,5%)	64 - (31,7%)	11 - (5,4%)
High	91 - (44,8%)	75 - (37,1%)	98 - (48,3%)

TABLE 8. CIA TRIAD IMPACT OF CVE COLLECTION

Table 8 presents the impact that the vulnerabilities have on the three security domains: confidentiality, integrity and availability. As shown in the table, more than half of the vulnerabilities would have an impact on the **availability** of a product, which could cause it to stop its function. This is particularly worrying due to interdependencies of the devices in the different operational domains. Therefore, if a product (or group of products) were to stop functioning and providing service, it would have an impact on the rest of the domains of the grid. It is important to point out that smart grids are critical infrastructures. Therefore, any impact on the availability of a product is critical as it could disrupt the correct functioning of the grid.

In terms of **integrity**, over two thirds of the vulnerabilities have impact on the integrity of the information provided by the products, with 37% having a high impact. These numbers are concerning as smart grids rely on the data recorded by different products across the grid to determine the best electricity distribution, and tampering with these data could provoke important financial or operational damage. Indeed, a compromise on the integrity of the data could cause the energy flow to be below or over its required level. This could result in insufficient energy for consumers or product damage, and overall, a malfunctioning of the grid.

And in regard to the **confidentiality**, over than 75% of the CVEs have impact on confidentiality where almost 45% of the total are classified as high impact. This raises privacy concerns because as explained earlier in the paper, smart grids receive data from the consumer domain. Consequently, the information of the consumers is also at risk. Additionally, leaked information, such as the consumed or generated electricity, could be used to exploit vulnerabilities with integrity impact, providing better understanding of the flow of electricity across the network.