applied sciences

Review

Microgrid Cyber-Security: Review and Challenges toward Resilience

Bushra Canaan, Bruno Colicchio and Djaffar Ould Abdeslam *

IRIMAS Laboratory, University of Haute Alsace, 61 rue Albert Camus, 68093 Mulhouse, France;
bushra.canaan@uha.fr (B.C.); bruno.colicchio@uha.fr (B.C.)
* Correspondence: djaffar.ould-abdeslam@uha.fr; Tel.: +33-3-8933-6020

Received: 25 July 2020; Accepted: 12 August 2020; Published: 14 August 2020

Abstract: The importance of looking into microgrid security is getting more crucial due to the cyber vulnerabilities introduced by digitalization and the increasing dependency on information and communication technology (ICT) systems. Especially with a current academic unanimity on the incremental significance of the microgrid's role in building the future smart grid, this article addresses the existing approaches attending to cyber-physical security in power systems from a microgrid-oriented perspective. First, we start with a brief descriptive review of the most commonly used terms in the latest relevant literature, followed by a comprehensive presentation of the recent efforts explored in a manner that helps the reader to choose the appropriate future research direction among several fields.

Keywords: cyber-physical security; microgrid; cyber-attacks

1. Introduction

The sustainable flow of energy, or in other words, energy security, in the field of electrical supply systems, does not always rely on the physical availability of resources. Today's technical challenges are extended to include the constant equilibration of demand–supply systems in terms of electricity quality and cyber security.

Upgrading the electrical network has not been as dynamic as it should be. With technology being implemented in almost every area of our modern life and smart applications growing in scope and complexity, the power sector makes its steps towards the smart grid at a pace of an extreme cautiousness.

The bidirectional flow of power and information generated and monitored by highly advanced types of equipment and mechanisms signifies the new generation of the energy networks. Smart grids are expected to deliver tangible progress to our conventional power systems on both aspects of efficiency and reliability, all together with integrating the maximum share of renewable resources reinforced by distributed intelligent and demand-side management techniques [1,2].

Changes will give the consumers and prosumers a wider range of choices and accord them with the possibility to actively participate in the optimizing operation of the system, by means of providing them with detailed instructions on how to better use their supply and act as authorized partners.

Smart grid benefits can also be extended to enrich the coupled economic sector through reducing operational costs and losses, generating new job opportunities, and reformulating the face of the energy market with time-based pricing and a more accurate speculation of demand and response profiles [3], in a time where electricity price forecasts have become a fundamental input and an important tool for decision-making mechanisms of the energy service provider companies.

But yet, the complexity level of the actual power networks and the critical role that it plays in every domain form a double-edged challenge—especially when the introduced technologies might itself be the source of threat.

New types of communication and data-management systems must handle not just the different emerging media trends and smart equipment (e.g., computer-based or microprocessor-based), it also needs to cope with existing legacy systems [4] in a manner that is adjustable to scalability and above all, resistant to cyber intrusion [5]. To this end, smart grids have to come as a complementary solution and not an eliminating or excluding one. These technical uncertainties, plus the additional investment costs, have evoked the political reluctance practiced by energy operators against this shift.

Europe has been working on energy transition and smart grids since 2005, starting by creating the smart grid technology platform which has set the year 2020 as a horizon to complete the process [2]. There were also several initiatives that carried out the development of experimental testbeds for smart grids solutions which aimed to highlight the most critical challenges and potentials accompanied by this evolution and their influence on the European power systems. Nevertheless, a further and more holistic analysis that is based on a profound technical understanding of each individual system architecture and basically includes the impact of both social and economic aspects on such heterogeneous systems, is yet to be accomplished in order to be able to trade-off between the existing approaches and pilot experiences, choosing a unique and valid experience that is suitable to be scaled up and replicated [6].

On the other hand, a very promising approach to overcome the majority of previous issues appears through energy communities, in which current grid problems are managed in a coordinated way such that avoiding costly network reinforcement along with maintaining aspired values of the smart grid. That is why we might be able to envisage the future smart grid as a sort of aggregation of multiple integrated entities or microgrids supervised, monitored, and controlled via a reliable communication-based layer. Accordingly, the increasing interest in microgrid development as the core of the smart grid systems is completely justified [7], although this increasing interdependency between physical and nonphysical power system components, which forms the so-called cyber-physical systems, raises a whole new level of complications.

In this work we closely examine the existing approaches to address the cyber-physical security in power systems with focusing on microgrids.

The structure of the paper is organized as follows; the second section describes the gradient evolution of the concept of the cyber threat, starting from the attacks targeting industrial control down to the electrical grid. Later, the third section elaborates on standardized definitions and terminology choices for the contemporary problematic challenges. In section four, we move on to the actual issues and case studies that occupy the researchers' attention from different viewpoints. Finally, we conclude by providing some insights about the unsettled challenges in addition to realistic recommendations in the light of the presented argument.

2. Industrial Cybersecurity Incidents Emergence

The 21st century witnessed the initiation of various cyber incidents affecting sensitive infrastructures. The discovered complexity of cyber-attacks on Industrial Control Systems (ICS) revealed the dexterity level of the attackers in Industrial Con [8].

The smart grid internet interconnection subjects the grid to different forms of hazards, particularly with regard to Advanced Persistent Threats (APT), Distributed-Denial-of-Service (DDoS), botnets, and zero-days. Stuxnet, Duqu, Red October, or Black Energy are only a few examples of the advent mayhems touching industrial security since 2010 [3].

Stuxnet, the worm that caused the first reported cyber-physical incident, was discovered by a senior researcher at Kaspersky Lab, Roel Schouwenberg, in June 2010. With a purpose that was beyond stealing, erasing or modifying data, Stuxnet endeavored to cause material sabotage in the supervisory control and data acquisition (SCADA) system as a physical industrial control system. It was regarded as the first cyber-warfare weapon to encompass a complex piece of malware that has infected an estimated 50,000 to 100,000 computers mostly found in Iran, Indonesia, India, and Azerbaijan [9].

Duqu and Flame, another two worms intended towards industrial control systems, were observed more than a year after Stuxnet. Despite the similarities in code source with Stuxnet, they had different objectives. Duqu was designed to track and gather useful information that would help to compromise the opted industrial control set. Flame or Flamer was a more sophisticated malware, especially developed for cyber espionage on these networks. Spotted cases were mainly located in Iran and other countries of the Middle East [10].

In December 2015, a cyber attack on Ukraine's power system has procured a wide-area outage, affecting around 225,000 customers. The attack was associated with a new variant of Black Energy Trojan named Disakil [3]. According to reports issued by power companies, the SANS institute and Electricity Information Sharing and the Analysis Center (E-ISAC), the problem started several months before the actual attack by installing the malware through phishing emails. At this period, the hackers only monitored and collected valuable information about the system operation during what is usually called the reconnaissance phase. On the day of the incident, the attackers took control over the Human–Machine Interface (HMI) and cut the power by opening a certain number of breakers. In order to intercept the service restoration, a denial of service (DoS) attack on the communication network, additionally to the classic telephone lines, was employed to prevent the clients from reporting the problem. Even applications that determined the outage extent were blocked by the malware that was able to recognize the system softwares [11,12].

One year earlier, the same threat agents were identified by the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) during an attempt to penetrate the U.S. electric sector. Despite the fact that the attack, in this case, never happened, it definitely attracted attention on the future potentials of the cyber threats on a sector of utmost vitality [9].

3. Definitions and Overview

3.1. *Cyber-Physical Security*

The IEA (International Energy Agency) defines energy security as "the uninterrupted availability of energy sources at an affordable price". Traditionally, security used to be achieved on two fundamental levels; short-term security that deals with the stability of the demand–supply procurers, and the dynamism that enables the energy system to adapt as quickly as possible to sudden changes in the grid loads. Moreover, long-term security focuses on investments that support economic and sustainable development requirements.

Recently, with the arrival of smart grids which are essentially defined according to IEEE 2030-2011 standard, as a composition of three interoperability infrastructures, as set forth in Figure 1. This suggested interdependency has led the security problem to grow in complex imposing supplementary challenges threatening of introducing easier ways of causing damage to the fundamental security concerns, all along with creating new ones.

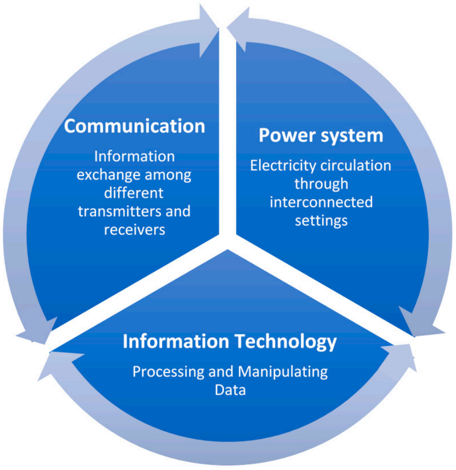
Communication
Information exchange among different transmitters and receivers
Power system
Electricity circulation through interconnected settings
Information Technology
Processing and Manipulating Data

Figure 1. Smart grid architecture in compliance with IEEE 2030.

Consequently, recent security assessment has focused on identifying the potential vulnerabilities introduced by the cyber layer and analyzes the possible impacts on energy systems, which has given birth to a brand new research area called cyber-physical security. A cyber-physical system is co-engineered collaborating domains of physical and computational counterparts, in which the crucial system tasks are basically handled with its physical part, while informatically enhanced processes-normally referred to as cyber- are responsible for maximizing the exploration of intelligent devices and application [13].

The reason why academia recently chosen to add the term "physical" to the equation is to shed light over the emerging threats imposed by connecting these two fundamentally different infrastructures together, which practically may lead to problems that do not particularly belong to a failure of either systems [14]. In light of these assumptions, further investigation is still needed to either confirm or deny the putative relationships [15].

The most indispensable objectives of security requirements considerations of any data transferring communication in the IT network security are known as CIA-triad, which stands for Confidentiality, Integrity, and Availability, respectively. According to The National Institute of Standards and Technology (NIST)'s guide on cybersecurity strategy, architecture, and high-level requirements, Confidentiality refers to "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information . . . " [44, U.S.C., Sec. 3542], and a loss of confidentiality results in unauthorized disclosure of information. Whereas Integrity is "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity . . . " [44, U.S.C., Sec. 3542] in other words, integrity is the unauthorized modification or destruction of transferred information. Availability, on the other hand, means "Ensuring timely and reliable access to and use of information . . . " [44, U.S.C., Sec. 3542] as if altering availability will lead to the disruption of the access to or use of information or an information system.

Smart grid security is also built upon the previous trestles, but with a difference in priority order, where availability comes on top of the requirements, followed by integrity, accountability, and finally confidentiality. Other referencing emphasizes the accountability as additional security criteria [16]. This sequence of importance goes back to the severity of impacts resulting from tampering with these criteria.

Attackers can penetrate the smart grid communication systems using vulnerable entry points in the logical border surrounding a network, known as the Electronic Security Perimeter (ESP). Interventions may occur with the help of numerous mediums, such as the Universal Serial Bus (USB) thumb drive, viruses, and even software patches and updates [17].

Despite the fact that cyber intrusions on cyber-physical systems (CPSs) can be found under different terms, such as bias injection attack, zero dynamics attack, denial of service (DoS) attacks, eavesdropping attack, replay attack, stealthy attack, covert attack, and dynamic false data injection attacks [18]. These attacks can still be classified according to the one or multiple security criteria they are jeopardizing, as set forth in Figure 2.

Intentionally introduced faults or malicious attacks triggered by the cyber layer leaving serious impacts on not only the technical aspects, but also on economic and social correlations in power network operations, are the focus of this research.

Effects range from tampering smart meters data or manipulating the forecasted load profiles up to reaching equipment damage or even complete blackouts [19].

However, achieving such results is never an easy business. Indeed, physical prerequisites and the current state of the power system architecture with contemporary defense mechanisms, such as controllers prepared to re-examine each input parameter against a selection of acceptable values preventing possible physical damages [20], burden the attacker with the mandatory acquisition of a customized knowledge about the physical nature of the system added to the already required computer-related competencies. But then again, this does not mean that the conventional ways of protection, such as the ones adopted to restrain the spread of fault effects by isolating of a malfunctioning entity, are enough to prevent an attacker from achieving an unacceptable condition in the grid [20].

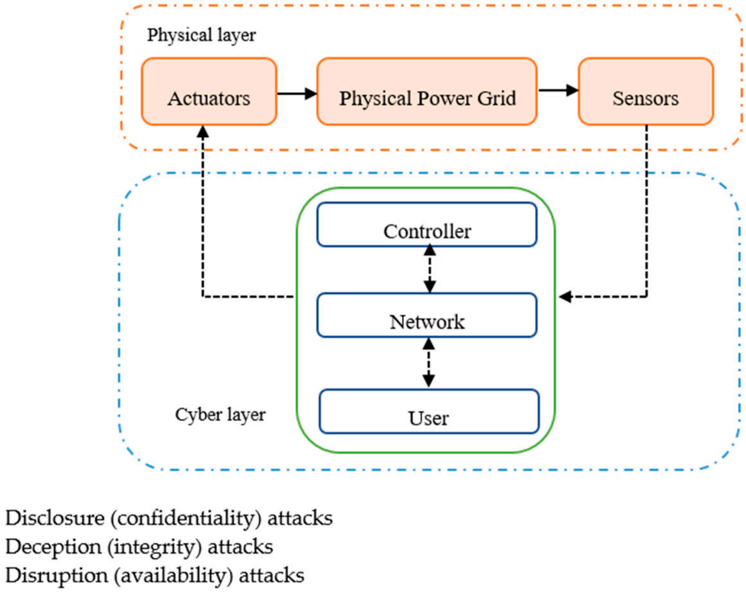
Physical layer
Actuators
Physical Power Grid
Sensors
Controller
Network
User
Cyber layer
Disclosure (confidentiality) attacks
Deception (integrity) attacks
Disruption (availability) attacks

Figure 2. Three types of cyber-attacks.

In that vein, reasonable strategies to fend off such incidence fall into two complementary categories. The first one is about developing measures that tend to detect malicious attacks and tackle down the cause of infection in the system in order to deal with either the compromised unit or entity through isolation or the direct cause from wherein the adversary could have accessed the network. The second important aspect is cyber resiliency, in which we anticipate the behavior of our system under attack and elaborate on what could be done to expeditiously recover from these attacks in a passive protection fashion.

At any rate, we must keep in mind that keeping the system utterly safe, over and above maintaining a level of simplicity allowing the intuitive understanding of the entangled operation, is a paradox that preoccupies the power system researchers and engineers.

3.2. Modern Distribution Network Vulnerabilities

Distribution systems play a major role in the electricity sector value chain linking transmission to consumption and providing direct contact with consumers [6]. Knowing that their systems were originally designed for passive energy delivery (in one direction), Distribution System Operators (DSOs) find themselves nowadays forced to cope up with the tremendous changes pertaining to the electrical networks, on especially on the medium to low voltage scale.

Unlike in transmission systems that have adopted the Energy Management Strategy (EMS) early in the 1970s, the application of proper EMS at the distribution level was not put into action until recently, since it did not have much of added avail [21].

Following the foregoing tendency, measures continue to offer incentives that consolidate the integration of all the flexible distributed resources into the market, side by side, with new demand–response technologies on the demand side [5].

Dispatchable generation units owned by the DSO, which could be turned on and off by the energy operator to match a scheduled output that meets the network requirements, are a very useful avenue that has been widely exploited over the years in peak shaving and declining stress over the network components at times of high demand. Nevertheless, the surplus of the distributed generation (DG), especially the non-dispatchable (renewable) type, can adversely affect the performance of the distribution systems causing power quality issues, augmented fault levels, voltage violation, protection issues, in addition to line overloading or congestion [21].

Certain DSOs have set rules of thumb that determine the adequate segment of DG that should enter the distribution networks depending on the hosting capacity of each of them. In general, an estimated 15% of the network's peak demand could be connected to the distribution network without causing significant problems [22].

The needed elements for DG metering and monitoring change from country to country or even between regions. Hence, more or less data might participate in the decision that determines whether a DG participates in the energy markets or not, in respect to its impact on the local network, keeping in mind that larger DG installations could also have an extended disconcerting impact on the regional or national transmission system [21].

3.3. Microgrids as a Cyber-Physical System (CPS)

Despite the tendency to associate the term microgrid with the power sector, we find that the concept represents itself in a larger context related to the energy community with different means of energy production, transition, and storage, all along with achieving the mutual goals of boosting technical and economic resilience [23].

Through the years, different definitions have been placed in the technical literature to describe the concept of a microgrid. The first one was proposed in [24,25] imagining the microgrid as the ultimate solution for the reliable integration and control of the ensemble of Distributed Energy Resources (DERs), including Energy Storage Systems (ESSs) and controllable loads [26].

Similarly, in [27,28], microgrid paradigm is foreseen as a very appealing strategy to overcome challenges in integrating the massive renewable resources resulting from summing up all community-scale capacities, which is still being kept on hold due to the inflexibility of the current networks. Furthermore, these individual DERs are often too small to enter the electricity market, which is another problem that has been solved thanks to this new topology.

This goes in line perfectly with what is stated by the US Department of Energy, with only one difference stressing the clear barriers with respect to the distribution network, in the way that it permits the microgrid to have the ability to operate not only within grid-connected mode but also in autonomous island mode [29], which in turn was found, in numerous studies, to be considered as a sine qua non to denote a microgrid [9].

With microgrid pushing the power system over the edges of decentralization, a geographically localized distributed power model makes more sense regarding risk-management in terms of regional resilience and preventing cascading failure in the event of weather events, cyber-attacks, etc. [28]. Knowing that the electricity supply for small urban or industrial communities (isolated microgrid) where the main grid connection is inaccessible was never a novel trend in the world of electrical alimentation [27].

There were numerous attempts to create a standardized configuration of the smart grid's building block, namely microgrid. However, its structure is yet considered to be arbitrary and any technically well functioning connection is valid [13,27]. It is important to notice that the microgrid's ability to fit in different configurations and to be customized as a function of the present requirements and constraints is the exact same reason why it is so hard to classify it in a fixed frame. Figure 3 illustrates a generalized structure for modern microgrids.

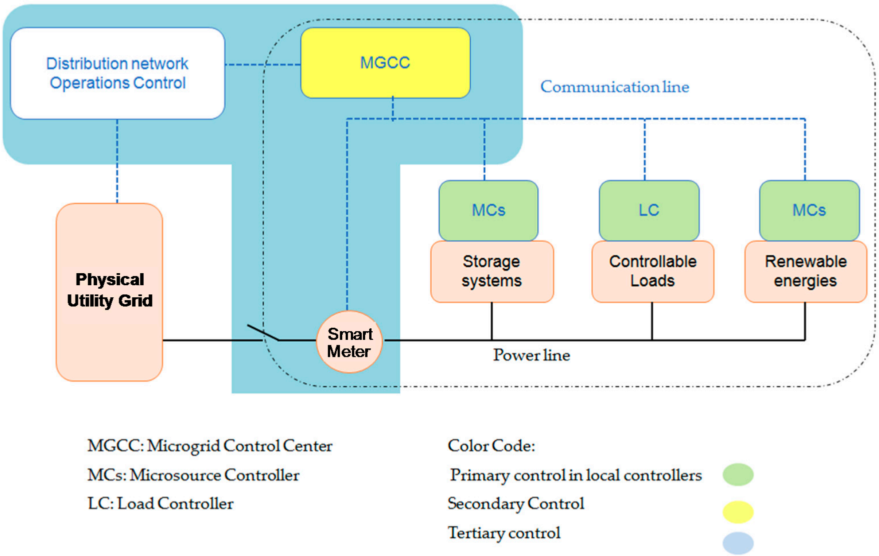

Figure 3. Modern basic structure of a microgrid.

From an operational perspective, there are only two types of microgrids (MGs):

A grid-connected MG, which is built to operate in either islanded or connected mode, might have one or several connection points with the grid. A single point of connection is very common though [8].

An isolated or stand-alone microgrid does not even have a point of common coupling (PCC) with the main grid [19]. Microgrids' implementation into utility does not always have to follow the classical case where a single MG is connected directly. Other alternatives can still exist, such as multiple tie line-based interconnected microgrids and small MGs within larger ones, so as the biggest takes the role of the governor large areas electrical power system [28].

The operational efficiency of microgrids necessitates sophisticated but most importantly secure measurement, communication, and control realized by various controlling methods, sensors, actuators, and field devices [18]. Moreover, microgrids are a highly sensitive cyber-physical system [13], in which the physical part is strongly influenced by the integrity of the cyber part, due to more entry point, very low required latency and the absence of multi-stage security detection. Consequently, attackers have more of a chance to cause serious problems in microgrids, leading to overall catastrophic consequences [30].

Recent papers have gone through securing the cyber-physical structure of the microgrid from different standpoints. Preliminary efforts probing cyber-attacks against the power systems would usually treat these attacks as a sort of noise or disturbance. So they tried their best to eliminate these disturbances using filtration techniques [31,32]. However, these techniques are based on pre-defined statistics which lose their effectiveness when facing slightly more fine tuned attacks [11].

In the following sections, we reviewed the recently proposed approaches from different domains.

4. Perspective-Based Interventions Addressing Cyber Attacks

4.1. Microgrid Communication

Being a cyber-physical system, microgrids inherent equally advantages and disadvantages of the combined systems. Communication network is essential to effectively incorporate many of desired features of the smart grid, such as the distributed automated system, distributed energy resource protection, islanding, and the display of network state and performance.

Standard communication problems also appear in microgrids, as it suffers from incompatibility between different types of heterogeneous communication technologies [13], besides the increasing reliance on Wi-Fi and internet-based communications, which are more susceptible to cyber interference but still essential for ancillary services related to microgrids, such as weather forecast data, fuel prices, peak hours, etc. [13]. Taking into consideration the expanding amount of data transferred between microgrid's components, different connected microgrids, or with an external centralized control and monitoring point, upon the design of the control structure. Satellite data (GPS) might also be a sort of communicated signals under danger in synchronous microgrid with phasor measurement units (PMUs).

On the other side, intrusion detection, firewall, and other selected solutions from the traditional security measures against rudimentary attacks targeting conventional data networks can also be included in smart microgrid applications [33].

While some prefer to leave the power generation control network isolated from the public network as a countermeasure against cyber contingencies, the leverage of open transmission protocols and computers with common operating systems that performed as intelligent electronic devices (IED) cannot be neglected nor eliminated today. Especially with essential improvements on automation efficiency and control system costs [16].

As an attempt to study and simulate the influence of an attacked communication network on electric power systems, earlier efforts went to model the attacks as a time delay to be accounted within the control loop, a subject that has been widely explored even outside the scope of cyber-attacks. For example, in an islanded microgrid, the authors in [34] have examined the communication delay limits beyond which we might risk having instability issues. They proposed an impact mitigation approach that revolves around gain scheduling for PI (proportional–integral) used in the secondary frequency controller that can be adopted in other microgrids as long as they can be modeled in the same small-signal model.

However, these assumptions on the nature of attack impacts are oversimplified and do not fully cover the new debouching aspect of joint cyber-physical models [35,36]. Others argue on the matter of communication latency's impact on microgrid control on the first place, building on an example that puts out shreds of evidence on having an inconspicuous and highly nonlinear relationship of delay rates between the source causing the delay and the resulting delays in the networks [37]. They also state the fact that, except for the simplest of cases, deriving tight bounds between delays, or other relevant metrics such as loss rates, is nearly impossible, especially when the models' analytical accuracy declines as the network size grows from single-hop settings to relay networks.

Taking the communication problem to a larger extent, a Cyber-Physical Power System (CPPS), ref. [38] digs into what might be a better communication configuration in terms of preventing a cascading failure, and in a comparison, based on transmission efficiency threshold values, they find that double-star communication networks perform better than the mesh communication networks.

Preventing cascading failure in cyber-physical power systems (CPPS) through a comprehensive analysis of the mechanisms and dynamical characteristics of interdependent networks was also the focus of the research presented in [2]. The writers have reviewed the different existing approaches and methods of power and communication systems coupling and interconnection and then proposed a novel interdependent model with the "degree–electrical degree" assortative link pattern that has proved its effectiveness in reducing the probability of large-scale blackouts caused by random attacks. Whereas, in the case of malicious attacks, simulation outputs have demonstrated the superiority of the random link model. Results also highlight in a more general manner the importance of coupling strength between the two layers over the choice of the interdependent model. The more dependent the power system is on the communication system, the more fragile it becomes.

Among a very diverse variety of problems discussed in the Information and Communication Technology (ICT) field, the particularity of synchrophasor systems vulnerabilities against cyber-attacks was highlighted due to the growing interest in synchrophasor technology applications [39]. Notably, the absence of built-in security structures in the widely adopted IEEE C37.118 communication framework that sets up the standards for PMUs and Phasor Data Concentrators (PDCs) is making it highly exposed to cyber threats [40].

Experiments involved resiliency examination of the communication system structure based on IEEE C37.118 under different attack scenarios, accompanied by estimation of possible impacts on synchrophasor application that uses this standard [40].

In [41], vulnerability analysis went deeper into the IEEE C37.118 framework structure to its weakest components, which the transport protocol layer, as they discuss the susceptibility of two commonly used protocols in transport layers (i.e., Transmission control Protocol (TCP) and User DatagramProtocol UDP) against DoS and FDI attacks summarizing the requirements to be used for creating a successful cyber intrusion as well as to prevent it.

A comprehensive comparison with ICE 61,850 that took into consideration the security implication of both standards stressing the advantages and disadvantages that encounter the synchrophasor application developers was also performed in [42].

Figure 4 summarizes the proposed approaches explaining the main mechanisms and pathways considered in acting against cyber intervention in the communication domain.

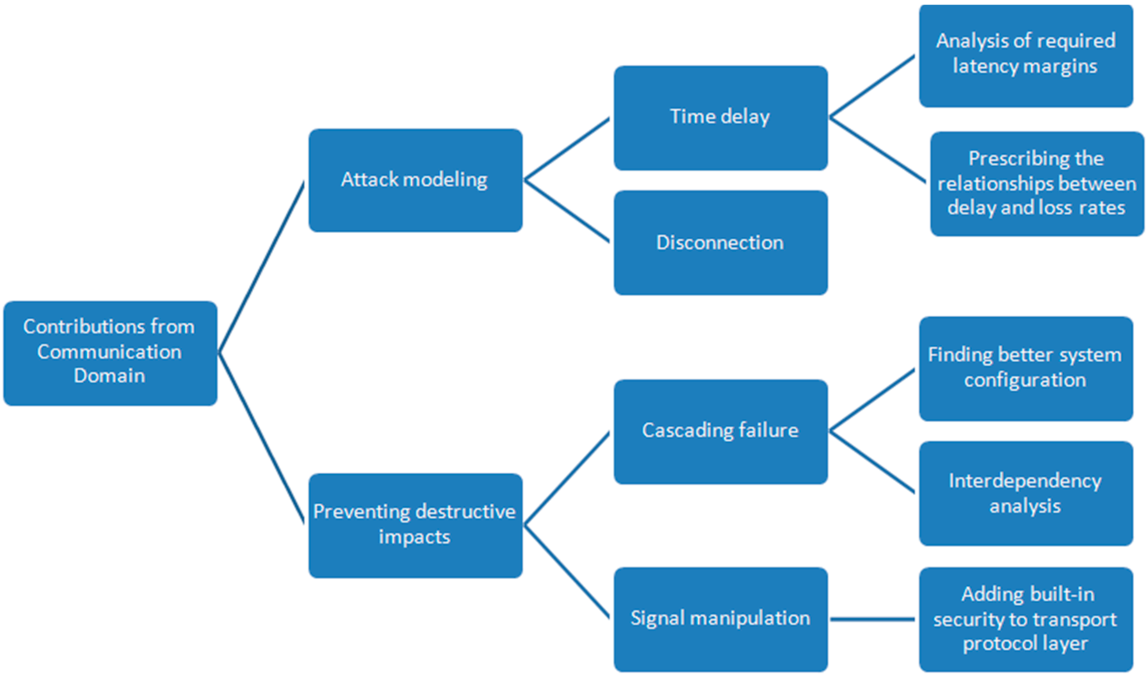
Contributions from Communication Domain
Attack modeling
Time delay
Disconnection
Analysis of required latency margins
Prescribing the relationships between delay and loss rates
Preventing destructive impacts
Cascading failure
Signal manipulation
Finding better system configuration
Interdependency analysis
Adding built-in security to transport protocol layer

Figure 4. Contributions from the communication domain.

4.2. Impact Analysis

Another way of proving that cyber-physical solutions for the power sector are not just a solution waiting for a problem, remarkable efforts in the field of impact estimation and threat modeling were made to dispel the doubts on the capability of cyber-attacks to cause actual physical damage.

The research presented in [20] demonstrates the possibility of authentic corruption caused by two types of cyber-attacks (availability and integrity attacks) jeopardizing the ICT and the GPS systems required for the sane functioning of a microgrid in three different operating modes (connected, islanded and sync-islanded). The severity of the physical impact which may vary between local blackout, the main instability violation of power quality equipment damage and human danger witnessed in the example microgrid is strongly related to its own architecture.

Other researchers were more interested in exploring the effects on a specific area in the microgrid systems, such as secondary frequency control function in [43] and distributed load sharing [44]. But since these studies are limited by the chosen system, more efforts had to go further into developing threat modeling methodology that fits into the purpose of risk characterization in different systems architectures.

As an attempt to fill the gap, ref. [39] explores the possible arising genres of threat in the components of different systems predicted on missing security properties, and how powerful this could be on the system security entirely.

4.3. Microgrid Control

4.3.1. Control Structure

The sound operation of power management strategy (PMS) is more critical in microgrids. Reasons narrow down to the imperative adjustment of multiple interconnected DG units with significant differences in power capacities and generation system characteristics that become more and more Electronically Interfaced (EI-DG), requiring a faster response to keep dynamically changing characteristics (voltage/angle) within the appropriate margins [26].

A microgrid's control systems are a typical target for attackers. Based on the purpose of which they are implemented, microgrid's control structure can be profoundly different and the control features are limited or customized to a desired subset of functions from a larger group of options [45]. In grid-connected mode, for example, frequency and voltage values are regulated by the host grid at the point of common coupling (PCC) whereas tasks like the DER's active and reactive power accommodation, energy management and load sharing, in addition to a safe transition between connected–islanded modes are still elaborated by the microgrid's control systems. During islanded mode or in remote conditions that are completely isolated from the grid, the microgrid's local controllers take full responsibility for all stability measures which also vary depending on the microgrid type (Islanded AC, synchronized islanded AC, naurally islanded DC) [27]. Typically, having one of the DERs operating as the isochronous generator forming the microgrid voltage and frequency is quite common in islanded microgrids. In this case, the rest of the DERs could participate in supporting voltage and frequency if needed [9], whilst the complete absence of a dominant source of energy generation during the autonomous mode of operation adversely amplifies the complexity of the assigned task list.

The majority of prior researches pictures the microgrid's control paradigm in a hierarchical manner, following the successfully adopted structure in the legacy grid [23].

Hierarchical control levels of microgrids are usually anticipated in three layers: primary, secondary, and tertiary. There are no definite technical boundaries between strategies of each level rather than a sort of indication based on relevant considerations, such as response rapidity interval, purpose-oriented control, and central-distributed control.

However, without losing generality, we can say that primary and secondary control strategies are practically associated with operational stability and accordance between microgrid's components, while harmonization with the host grid is applied by tertiary control [27].

Primary control features the fastest response with the smallest decision time step, voltage, and frequency regulation as well as protection executed on this level, which are entirely based on local measurements and droop mechanism with no communication needed [27]. That is why operations on this level are conserved away from cyber incidents.

On the contrary, secondary control operates on a slower time scale, often with a reduced communication bandwidth by using sampled measurements. It collaborates consistently with the other two levels to satisfy the requirements set by the tertiary control. The secondary control measures values across the microgrid, and accordingly, updates the desired setpoints for the primary controllers [46].

Tertiary control on the highest hierarchy collects state information of the energy system through the communication infrastructure and makes decisions to optimize the overall performances of microgrid with the longer decision time step. It may also be responsible on the economic dispatch of controllable resources and coordination with the distribution system operator with Energy Management System (EMS) ensuring power balance constraint, security constraint, and operational constraints [23].

Previous control functions can be achieved through either centralized or distributed implementation of the control architecture. The discussion on privileging one control method over the other is still questioned by several papers focusing on different aspects [7,23,43].

Distributed control was originally proposed as a solution to boost scalability in modern networks by means of facilitating the introduction of supplementary DERs. It splits control tasks between units instead of the substantive upgrading of single excessive computational capacities. Moreover, the sparsity of communication networks utilized in distributed control schemes reduces the infrastructure cost [43]. Not to mention, that is also considered to be more resilient as single-point failure does not lead to cascading failure, unlike centralized or what might be called hierarchical control, in which messages that carry out measurements and instructions from and to all system components should pass by a dedicated central controller. Correspondingly, centralized control schemes have a better understanding of the microgrid functions since it has an embedded version of the system model in the central controller which in turn will trigger an optimal application of EMS objectives including the economic performance simultaneously with satisfying real-time operational constraints.

In [7], authors review basic branches of distributed control optimization and their application with a brief reflection on the cybersecurity consideration, promoting distributed control on the bases of mitigation obstacles relevant to communication risks and stakeholders' resistance to sharing critical data.

Among distributed optimization methods, consensus control has gained more attention in microgrid's control community recently. The initial notion was inspired by biological phenomena that revolve around providing each unit of vision on the overall objective to a limit where different DERs converge to a single value. Here, decisions are built upon local measurements and peer-to-peer communication, offering this model extra flexibility, adding to the already well established feature in the distributed structure. Cooperative control is also a very feasible solution for stability control in terms of voltage and frequency equilibration and economic control with cost consensus for generation units across the network [23].

4.3.2. Automation Control against Cyber-Attacks

Since control systems were conventionally developed to detect, process, and mitigate the systematic and unpredicted errors, there is no wonder it has been the focus of numerous research cases in the field of attack predictability, detection and protection.

Microgrids are prone to the same types of attacks found in the utility grid. DoS events provoke multiple issues without a doubt, but at the same time, they are easily detected by the system operator which will probably recognize in an adequate rapidity that it is under attack. Similarly, the superior severity of the FDI attacks is largely attributed to the detection method's complexity and variability upon the adopted control structure [47].

Broadly, detection and mitigation of conventional attacks are already well explored in the literature. FDI that succeeds in penetrating the network while maintaining discretion without altering the system observability disturbance alarms, also known as stealth attacks [48], are able to cause unpredictable stability issues and the worse is that they are practically impossible to detect [49].

From a defender perspective, recent research attainable choices are perceived into either addressing the fault detection and isolation in control loops (detection based) [50] or working on precaution measures based on threat modeling and security analysis (protection based) [51].

The popular method used to detect bad measurement data in power transmission systems is the Static State Estimator (SSE). It is generally based on a weighted least squared (WLS) solution and it is not immune against attacks itself [52,53].

State estimation is also important to microgrid control functionality and it is usually found in traditional energy management systems derived from steady-state models [18]. However, static state models were no longer able to capture the systems' dynamics accurately with the exacerbated numbers of DERs on the generation side and the debuting retrofits on the demand side.

The research presented in [18] emphasizes the importance of deploying a secure dynamic state estimation on the side of AC-connected microgrids as a portion of the distribution network. Similar to [54] they proposed an estimator algorithm for a standard structure-preserving model that incorporates system dynamics. Method validation illustrates the estimator's ability to give a secure dynamic state estimation when supplied with inaccurate measurements caused by either an attack that manipulates communication between transceivers and the microgrid operator, or attacks that manipulate measurement units themselves, even without considering an attack scenario.

Traces left on the operation of observers turn into an efficient key to be used in attack detection. Distributed state estimation method is used as a way of detecting cyber-attacks of the FDI type. In [55], a consensus-based controlled DC microgrid was investigated where each distributed generation unit had employed the Unknown Input Observer (UIO) to estimate the state of its neighboring units and isolating the fault source consequently.

Another control approach using UIO was proposed in [50]. A fully decentralized load frequency controller was developed and tested with a perspective to be applied to multi-AC and DC microgrids.

Given that the relative simplicity of the cyber-attack detection of the FDI type in distributed control schemes, authors in [49] have decided to raise the bar by firstly introducing a stealth attack that is able to deceive the conventional distributed voltage observer without triggering the detection mechanism. After that, they proposed a general algorithmic-based detection framework for DC microgrids where they added a cooperative vulnerability factor (CVF) to the voltage PI controller. Finally, and under worst-case scenarios, artificial disturbances were added to by coupling the CVF with the secondary current sublayer in order to enhance the chance of capturing the attacks.

Later, the same DC microgrid model was used in another experiment using artificial intelligence in [56]. A Nonlinear Auto-Regressive Exogenous (NARX) neural network was trained over the previously mentioned control method during offline operation, capturing and storing its behavior, only to be used then as an online estimator for DC voltages and output currents of each unit. The FDI attacks detectability of this method was built on the estimation errors making it suitable for a larger spectrum of DC microgrid, in contradiction to the cases presented in [49,57] that only suits those functioning with cooperative consensus-based algorithms.

The FDI problem shaping in terms of determining the aspects that could be altered by such an attack was the subject of [58], in which a detection method was built on the assumption of the attack capability to modify the invariant values required in the secondary distributed control layer.

A new technique for optimal dynamic state estimation, based on a distributed algorithm for multiple connected DC microgrids under FDI attack, was proposed and tested over malicious and normal load disturbance in [47], proving its capability of distinguishing between the two cases. Unlike previous literature that dealt with DC microgrids as quasi-static models, this work employed a dynamic microgrid paradigm where the three DC connected microgrids employed in the study collaborated under a control configuration, that enabled each of them to verify the security status of the other two, making it possible to isolate the potentially infected entity.

4.3.3. Protective Control

Without continuing further into the investigation on the nature of the imperiling data or the way that the attackers may use in order to achieve instability in the system, other research simply focused on adding redundancy security to the existing used control methods. Authors in [30] have proposed increasing the security by coding the signals that carry the information about the state's measurements with an error-correcting code Recursive Systematic Convolutional (RSC) code and then decoding it to enhance the performance of the proposed semidefinite programming based on optimal feedback controller, coupled with Kalman filter estimator by elimination of a portion of noise on an IEEE 4-bus distribution feeder considered as four grid-connected microgrids.

Reachability analyses were frequently employed to determine if an unstable state could be reached due to certain changes in the monitored variable. This was elaborated in [28] by designing a stability monitoring and control comprehensive framework, that guarantees resiliency against attacks through isolating the problematic bus, while covering critical loads compensated from neighboring microgrids.

4.4. Co-Simulation Testbeds

Experimental studies are still economically unfeasible for microgrids, as it is for large-scale smart grids. With only a few reliable platforms around the world capable of performing highly complicated tests, real-time simulation is a powerful alternative solution in this area of research [37].

Models running on this mode of simulation adhere to a very small step size in order to achieve an accurate result. Bypassing the right step size to a larger value produces an erroneous simulation while smaller values do not fit into the simulator constraints. This, in turn, creates a challenge, especially with models with high-speed switching devices [37]. The large number of switching devices is not the only source of trouble in simulating power systems. Broadly, the integrated power electronics devices in the smart grid simulation also tolerate high-frequency pulse width modulation signals, and that what explains the shift from traditional offline simulators that are time-consuming and not adjusted for slow phenomena [59].

Additional complications come to the surface concerning the representation of the cyber-physical components in the same computational environment. The inhomogeneous nature of both power and communication systems plus the obvious differences in components, transmission content, and working mechanisms make it very challenging to accommodate the desired realistic features in one frame. For instance, the time-varying or continuous solvers suit the power systems while communication networks' simulation necessitate a discrete or event-dependent simulation [60]. In other words, the behavior of the grid control is mainly well defined using mathematical formulations, which is not exactly the case in the nearly stochastic, unpredictable data transmission protocol layer that belongs to the accompanying ICT system [61].

Even when ending up finding the perfect tool to simulate each structure separately, interfacing the two simulators in a way that guarantees the integration of the distinct characteristics for both, without restraining the core to either of each is not always evident and often stipulates grappling with synchronization and data exchange.

With all these obstacles, it seemed just right that some works had chosen to probe the different types of taxonomies of the existing testbeds since that discovering the various tools and techniques implemented in the current testbeds, counting also the strong and weak points for each one, is crucial to build and develop new experimental platforms.

In this context, the term "co-simulation" refers to the practical and realistic co-existence of the examined subsystems whereupon they operate hand by hand to reflect smart grid interactions [62].

The co-simulation development can take two directions; the first one primarily focuses on a specific tool that has been familiarly dealt with, in the course of studying individual subsystems. Researchers who seek this approach are usually more concerned in deepening their understanding of the interaction control between the intended subsystems. The second approach is a platform-based one which implies fixing the attention on the development of a comprehensive framework with a standardized interface capable of embracing different tools. This attracts researchers who deal with utterly complicated simulation environments, especially when flexibility in connecting the subsystem is inevitably expected, without intervening in neither layouts [61].

4.5. Smart Meters and Data Security

Energy sector's pathway is clearly heading towards more distributed resources and control. Consumers are becoming more and more ready to invest in distribution-edge devices comprised of residential PV panels, storage devices, electrical vehicles, and their recharging points in addition to smart control tools. Smart Meters (SM) at the endpoint of distribution networks liaise with consumers and lends them an open window to interact with the utility. In an ideal scenario, smart segments must effectively communicate via Advanced Metering Infrastructure (AMI) to reach the perfect balance, as set forth in Figure 5. Since its first appearance in 1872 [63], the concept of electricity meter has remarkably evolved. Conventionally, electricity meters used to provide information only about electricity consumption in terms of total current amplitude, while intelligent meters are supposed to support a wide range of applications rather than just metering [64].

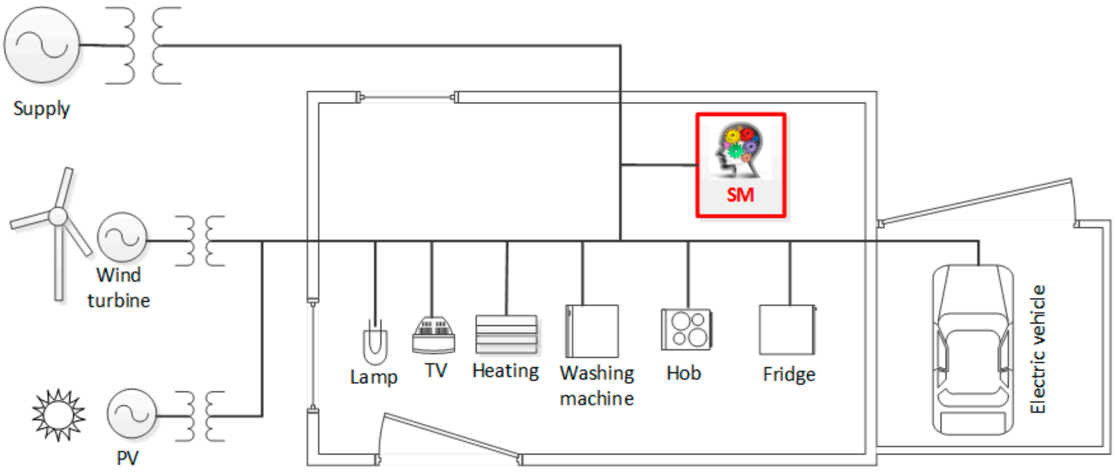

Figure 5. Smart meter role.

As specified in 2012/27/EC directive, Smart meters are "an electronic system that can measure energy consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication" [65].

Once again, smart application functionalities are not clearly framed in official norms that usually define and impose quantifying criteria in terms of technical specifications. This is why working and elaborating on the standardization enclosure, especially for the most affiliated pieces of the smart grid, becomes an urgent need.

However, a good few guidelines were established to help the industry involved in developing the new generation of meters.

The European Smart Meters Industry Group (ESMIG) has fixed characteristics such as remote reading, bidirectional communication, support of advanced tariff systems and ability to run billing applications, and remote energy supply control to be the minimum features required in smart meters [64].

The need to address metering issues arises practically at the same time as the development of distribution electricity grids. Providing measurement, control, communication, power, display, and synchronization capabilities shall be no easy task for smart meters.

Smart meters at the moment are installed and deployed by the utility inside of consumer's facilities. They communicate real-time measurements with data concentrators and control centers that monitor and partially control the meters.

Machine-to-Machine (M2M) communications among appliances in accordance with information provided by service providers enhance demand response functionality, leading to a win–win situation [66]. Besides the aforementioned control and management advantages, collected data can also help the grid operators in an application such load forecasting.

The absence of human interventions is a key feature of advanced metering plug and play mode, is very desirable but unfortunately, at its earliest phases, comes with relatively high expenses.

The exposure to a different kinds of communication systems, including internet, in addition to the needed adaptability to work with different billing applications, that are probably open sourced not to mention the double ownership making smart meters the most vulnerable component of the smart grid.

Pursuing autonomy, future meters are being tested to enlarge their authority margin so the amount of transferred data to and from control centers can be reduced.

Impact on the electrical systems depends on the select functionality assigned to the smart meter. Of course, the availability of the entire service of a smart meter is still considered to leave the worst impact on systems, but data communicated via smart meters which provide considerably detailed information about consumers' consumption behavior or habits are the biggest new concerns. Confidentiality data can be exported in many grievous ways such as optimizing the attacker's understanding of the compromised target so that he can make a more severe attack, extort the service providers, or even sell to unauthorized parties [67].

Energy providers, on the other hand, had their own share of concerns: the manipulation of data at the user end either due to the intentional act by the consumers themselves or cyber-attacks could be used to steal power and billing manipulation, resulting in revenue loss [68]. For this reason, authenticated software should be implemented, not only on inside the meters, but also on the access side for a granted sound operation [66].

The consumer's trust is critical for SMs and AMI expansion: one of the most modern ways to resolve security-related issues is through blockchain or distributed ledgers technology.

Blockchain technology is a very promising solution with great potential to radically change the energy sector from the way we know it. It was firstly introduced in a financial context with cryptocurrency, widely known as "Bitcoin". Blockchain provides a trustworthy platform for peer-to-peer transaction using distributed storage for keeping track of the exchanged data. Smart contracts on top of the blockchain define individually the rules upon which contractors exchange resources (quantity, quality, price), eliminating third-party intermediaries and cutting down extra expenses and accelerating the operations rhythm [69].

Blockchain can contribute to maximizing social welfare for energy delivery through managing tamper-proof energy supply transactions in absolute transparency, providing the metering fundamentals as well as billing and clearing processes. It is also suitable for extended applications such as ownership certificates, asset management, proof of origins, copyrights and emission limits in addition to renewable energy quality standards [69]. All and more are features that also help to empower the role of small renewable generations that belong to prosumers and monetize their assets. Thus, it supports the two essential desired features in the smart grid security and distribution.

The study in [70] provides a systematic classification of the latest blockchain research projects and startups' experiences in the energy sector applications. It also analyzes the opportunities, potential challenges, and limitations of using a number of examples on peer-to-peer (P2P) energy trading in decentralized marketplaces with the latest technological inventions, notably the Internet of Things (IoT) and e-mobility.

Going back to the microgrids, authors in [71] put forward a blockchain-based framework for a microgrid as an aggregated prosumer to optimization-decentralized transactive energy management, and support secure the interactions among different energy sectors.

In practice, existing energy market mechanisms are still a bit far from getting replaced by blockchain models since they do not completely cope with current legal regulatory frames. Furthermore, the technology itself has not reached the desired certain maturity [69].

5. Discussion and Conclusions

In this article, we examined the existing approaches to address cyber-physical security from a microgrid perspective. As explained above, the work on the smart grid application, in general, lacks approach intersections, and is still being dealt with from separate domains in the research world. Although using the microgrid model to carry out experiments on the cyber-physical security has plenty of practical justifications attributed to the important role it plays in paving the way towards smart grids, the microgrid's context was mainly consulted owing to the relative simplicity in capturing and recording interventions, either as an injected attack or control modification. For example, the islanded microgrids broached by a fair number of papers, especially the DC type, have unarguable merits in terms of autonomy. However, this will only leave us with specially tailored methods and solutions that do not necessarily fit all cases.

Cybersecurity measures for energy systems still come as accessories and not as a built-in function. In particular, for most of part, the electricity-related equipment that gets evolved at an exponential rate makes it extremely difficult for cyber defenses' mechanisms to keep pace with this development in the absence of up-to-date standards and common market trends. At least, securing the smart grid requires a multidisciplinary approach, and economic and social development are usually forgotten or neglected aspects in this process. Even the most remarkable technology inventions are useless without being approved by clients.

Author Contributions: Cyber-Physical Security concept, Conceptualization and Writing, B.C. (Bushra Canaan); Supervision and Micro-Grid Concept, B.C. (Bruno Colicchio); Supervision and Validation, D.O.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the INTERREG-V program RES_TMO (Project No. 6.3).

Acknowledgments: This work is supported by the European INTERREG-V program RES_TMO (Project No. 6.3). We thank Barbara Koch (Freiburg University, Germany) project lead of RES_TMO and Upper Rhine Cluster for Sustainability Research.

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

References

1. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
2. Rashid, M.H. Energy Systems in Electrical Engineering. In *Smart Grids and Their Communication Systems*; Kabalci, E., Kabalci, Y., Eds.; Springer: Singapore, 2019; pp. 1–644.
3. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]
4. Hossain, E. Communication Architectures and Models for Smart Grid. In *Smart Grid Communications and Networking*; Hossain, E., Han, Z., Poor, H.V., Eds.; Cambridge University Press: Cambridge, UK, 2012; pp. 1–103.
5. Prettico, M.; Flammini, G.; Andreadou, M.G.; Vitiello, N.; Fulli, S.; Masera, G. *Distribution System Operators Observatory 2018: Overview of the Electricity Distribution System in Europe*; Publications Office of the European Union: Ispra, Italy, 2019; pp. 1–77.
6. Prettico, G.; Gangale, F.; Mengolini, A.; Lucas, A.; Fulli, G. Distribution system operators from european electricity distribution systems to representative distribution networks. *JRC Tech. Rep. Luxemb.* **2018**, *99*, 273–280.
7. Yazdanian, M.; Mehrizi-Sani, A. Distributed control techniques in microgrids. *IEEE Trans. Smart Grid* **2014**. [CrossRef]
8. Sridhar, S.; Govindarasu, M. Model-based attack detection and mitigation for automatic generation control. *IEEE Trans. Smart Grid* **2014**. [CrossRef]
9. Chlela, M. *Cyber Security Enhancement Against Cyber-Attacks on Microgrid Controllers*; McGill University Montréal: Montréal, QC, Canada, 2017; pp. 1–177.
10. Knapp, E.D.; Samani, R. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*, 1st ed.; Syngress: Rockland, MA, USA, 2013.
11. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2017**, *99*, 45–56. [CrossRef]
12. Lee, R.M.; Assante, M.J.; Conway, T. *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.*; E-ISAC: Washington, DC, USA, 2016; pp. 1–23.
13. Rekik, M.; Chtourou, Z.; Gransart, C.; Atieh, A. A cyber-physical threat analysis for microgrids. In Proceedings of the 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Hammamet, Tunisia, 19–22 March 2018. Available online: https://ieeexplore.ieee.org/document/8570411 (accessed on 6 May 2020).

14. Cai, Y.; Huang, T.C. Cascading failure analysis considering interaction between power grids and communication networks. *IEEE Trans. Smart Grid* **2016**, *7*, 530–538. [CrossRef]
15. Zhang, H.; Peng, M.; Guerrero, J.M.; Gao, X.; Liu, Y. Modelling and Vulnerability Analysis of Cyber-Physical Power Systems Based on Interdependent Networks. *Energies* **2019**, *12*, 3439. [CrossRef]
16. Liu, J.; Xiao, Y.; Gao, J. Achieving accountability in smart grid. *IEEE Syst. J.* **2014**, *8*, 493–508. [CrossRef]
17. Srivastava, A.; Morris, T.; Ernster, T.; Vellaithurai, C.; Pan, S.; Adhikari, U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. *IEEE Trans. Smart Grid* **2013**, *4*, 235–244. [CrossRef]
18. Fooladivanda, D.; Hu, Q.; Chang, Y.H.; Sauer, P. Secure State Estimation and Control for Cyber Security of AC Microgrids. *arXiv* **2019**, arXiv:1908.05843.
19. Esmalifalak, M.; Shi, G.; Han, Z.; Song, L. Bad data injection attack and defense in electricity market using game theory study. *IEEE Trans. Smart Grid* **2013**, *4*, 160–169. [CrossRef]
20. Friedberg, I.; Laverty, D.; McLaughlin, F.; Smith, P. A Cyber-Physical Security Analysis of Synchronous-Islanded Microgrid Operation. In Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research 2015, Belfast, Swindon, UK, 17–18 September 2015.
21. Hayes, B.P. Distribution Generation Optimization and Energy Management. In *Distributed Generation Systems*; Gharehpetian, G.B., Agah, S.M.M., Eds.; Elsevier Inc.: Oxford, UK, 2017; pp. 415–451. [CrossRef]
22. Stavros, A.P.; Nikos, D.H.; Pierre, A.; Luiz, M.A.; Bernhard, B.; Clinton, G.C.-B.; Drossos, N.; Bayez, E.; Mingtian, F.; Vincent, G.; et al. Capacity of Distribution Feeders for Hosting Distributed Energy Resources. Papathanassiou 2014 Capacity ODCIGRE 2014. June 2014. Available online: http://cigreaustralia.org.au/assets/ITL-SEPT-2014/3.1-Capacity-of-Distribution-Feeders-for-hosting-Distributed-Energy-Resources-DER-abstract.pdf (accessed on 5 June 2020).
23. Feng, X.; Shekhar, A.; Yang, F.; Hebner, R.E.; Bauer, P. Comparison of hierarchical control and distributed control for microgrid. *Electr. Power Compon. Syst.* **2017**. [CrossRef]
24. Lasseter, B. Microgrids distributed power generation. *Power Eng. Soc. Winter Meet.* **2001**, *1*, 146–149.
25. Lasseter, R. Microgrids. *IEEE Power Eng. Soc. Winter Meet.* **2002**, *1*, 305–308.
26. Katiraei, F.; Iravani, M.R. Power management strategies for a microgrid with multiple distributed generation units. *IEEE Trans. Power Syst.* **2006**, *21*, 1821–1831. [CrossRef]
27. Olivares, D.E. Trends in microgrid control. *IEEE Trans. Smart Grid* **2014**, *5*, 1905–1919. [CrossRef]
28. Buason, P.; Choi, H.; Valdes, A.; Liu, H.J. Cyber-physical systems of microgrids for electrical grid resiliency. *ICPS* **2019**, 492–497. [CrossRef]
29. Ton, D.; Bryan, E.; Marnay, C. Microgrids Program Overview, Power Systems Engineering Research and Development. *Aalb. 2015 Symp. Microgrids.* **2015**, 1–22.
30. Rana, M.M.; Li, L.; Su, S.W. Cyber attack protection and control of microgrids. *IEEE/CAA J. Autom. Sin.* **2018**, *5*, 602–609. [CrossRef]
31. Peach, N.; Basseville, M.; Nikiforov, I.V. Detection of Abrupt Changes: Theory and Applications. *J. R. Statal Soc. Ser. A (Stats in Soc.)* **1993**, *1*, 185. [CrossRef]
32. Jiao, Q.; Modares, H.; Lewis, F.L.; Xu, S.; Xie, L. Distributed $\mathcal{L}_2$-gain output-feedback control of homogeneous and heterogeneous systems. *Automatica* **2016**, *71*, 361–368. [CrossRef]
33. Manandhar, K.; Cao, X.; Hu, F.; Liu, Y. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 370–379. [CrossRef]
34. Liu, S.; Wang, X.; Liu, P.X. Impact of communication delays on secondary frequency control in an islanded microgrid. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2021–2031. [CrossRef]
35. Hammad, E.; Farraj, A.; Kundur, D. Fundamental limits on communication latency for distributed control via electromechanical waves. *IEEE Int. Conf. Commun.* **2017**. [CrossRef]
36. Farraj, A.; Hammad, E.; Kundur, D. A systematic approach to delay: Adaptive control design for smart grids. *IEEE Int. Conf. Smart Grid Commun.* **2015**, 768–773. [CrossRef]
37. Guo, F. Comprehensive real-time simulation of the smart grid. *IEEE Trans. Ind. Appl.* **2013**, *49*, 899–908. [CrossRef]
38. Cai, Y.; Li, Y.; Cao, Y.; Li, W.; Zeng, X. Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. *Int. J. Electr. Power Energy Syst.* **2017**, *89*, 106–114. [CrossRef]
39. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. *IEEE Innov. Smart Grid Technol. Conf. Eur.* **2017**, 1–6. [CrossRef]

40. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. IEEE C37.118-2 synchrophasor communication framework: Overview, cyber vulnerabilities analysis and performance evaluation. *Proc. Int. Conf. Inf. Syst. Secur. Priv.* **2016**, 167–176. [CrossRef]
41. Wang, Y.; Gamage, T.T.; Hauser, C.H. Security implications of transport layer protocols in power grid synchrophasor data communication. *IEEE Trans. Smart Grid* **2016**, *7*, 807–816. [CrossRef]
42. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks. *IEEE Power Energy Soc. Gen. Meet.* **2016**. [CrossRef]
43. Liu, S.; Liu, P.X.; Wang, X. Effects of cyber attacks on islanded microgrid frequency control. *Proc. IEEE Int. Conf. Comput. Support. Coop. Work Des.* **2016**, 461–464. [CrossRef]
44. Zhang, H.; Meng, W.; Qi, J.; Wang, X.; Zheng, W.X. Distributed load sharing under false data injection attack in an inverter-based microgrid. *IEEE Trans. Ind. Electron.* **2019**, *66*, 1543–1551. [CrossRef]
45. Chlela, M.; Joos, G.; Kassouf, M.; Brissette, Y. Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. *IEEE Power Energy Soc. Gen. Meet.* **2016**. [CrossRef]
46. Nasirian, V.; Moayedi, S.; Davoudi, A.; Lewis, F.L. Distributed cooperative control of dc microgrids. *IEEE Trans. Power Electron.* **2015**, *30*, 2288–2303. [CrossRef]
47. Vu, T.V.; Nguyen, B.H.L.; Ngo, T.A.; Steurer, M.; Schoder, K.; Hovsapian, R. Distributed optimal dynamic state estimation for cyber intrusion detection in networked dc microgrids. In Proceedings of the IECON 45th Annual Conference of the IEEE Industrial Electronics Society 2019, Lisbon, Portugal, 14–17 October 2019. Available online: https://ieeexplore.ieee.org/document/8927045 (accessed on 25 June 2020).
48. Zhao, J.; Mili, L.; Wang, M. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures. *IEEE Trans. Power Syst.* **2018**, *33*, 4868–4877. [CrossRef]
49. Sahoo, S.; Mishra, S.; Peng, J.C.H.; Dragicevic, T. A stealth cyber-attack detection strategy for dc microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
50. Alhelou, H.; Golshan, M.E.; Hatziargyriou, N.D. Deterministic dynamic state estimation-based optimal lfc for interconnected power systems using unknown input observer. *IEEE Trans. Smart Grid* **2020**, *11*, 1582–1592. [CrossRef]
51. Chaojun, G.; Jirutitijaroen, P.; Motani, M. Detecting false data injection attacks in ac state estimation. *IEEE Trans. Smart Grid* **2015**, *6*, 2476–2483. [CrossRef]
52. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
53. Dán, G.; Sandberg, H. Stealth attacks and protection schemes for state estimators in power systems. *IEEE Int. Conf. Smart Grid Commun.* **2010**, 1–6. [CrossRef]
54. Hu, Q.; Fooladivanda, D.; Chang, Y.H.; Tomlin, C.J. Secure state estimation and control for cyber security of the nonlinear power systems. *IEEE Trans. Control Netw. Syst.* **2017**, *5*. [CrossRef]
55. Gallo, A.J.; Turan, M.S.; Nahata, P.; Boem, F.; Parisini, T.; Ferrari-Trecate, G. Distributed cyber-attack detection in the secondary control of dc microgrids. In Proceedings of the European Control Conference, Limassol, Cyprus, 12–15 June 2018. Available online: https://zenodo.org/record/2590092#.XzYHZzURXIU (accessed on 3 July 2020).
56. Habibi, M.R.; Baghaee, H.R.; Dragicevic, T.; Blaabjerg, F. Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**. [CrossRef]
57. Sahoo, S.; Peng, J.C.H.; Devakumar, A.; Mishra, S.; Dragičević, T. On detection of false data in cooperative dc microgrids a discordant element approach. *IEEE Trans. Ind. Electron.* **2020**, *67*, 6562–6571. [CrossRef]
58. Beg, O.A.; Johnson, T.T.; Davoudi, A. Detection of false-data injection attacks in cyber-physical DC microgrids. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2693–2703. [CrossRef]
59. Li, W.; Joós, G.; Bélanger, J. Real-time simulation of a wind turbine generator coupled with a battery supercapacitor energy storage system. *IEEE Trans. Ind. Electron.* **2010**, *57*, 1137–1145. [CrossRef]
60. Zhang, J.; Chu, Z.; Sankar, L.; Kosut, O. Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Trans. Power Syst.* **2018**, *33*, 4775–4786. [CrossRef]
61. Hammad, E.; Ezeme, M.; Farraj, A. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. *Int. J. Electr. Power Energy Syst.* **2018**, *104*, 817–826. [CrossRef]

62. Kosek, A.M.; Lünsdorf, O.; Scherfke, S.; Gehrke, O.; Rohjans, S. Evaluation of smart grid control strategies in co-simulation: Integration of IPSYS and mosaic. In Proceedings of the 2014 Power Systems Computation Conference, Wroclaw, Poland, 18–22 August 2014.
63. The History of Making the Grid Smart Engineering and Technology History Wiki. Available online: https://ethw.org/The_History_of_Making_the_Grid_Smart (accessed on 18 June 2020).
64. Uribe-Pérez, N.; Hernández, L.; de la Vega, D.; Angulo, I. State of the art and trends review of smart metering in electricity grids. *Appl. Sci.* **2016**, *6*, 68.
65. European Parliament and Council. Legislative acts, Directive 2012/27/EU of the European Parliament and of the Council of 25 October on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC, 2012/27/EU. *Off. J. Eur. Union* **2012**, *12*, 1–56.
66. Avancini, D.B.; Rodrigues, J.J.P.C.; Martins, S.G.B.; Rabêlo, R.A.L.; Al-Muhtadi, J.; Solic, P. Energy meters evolution in smart grids: A review. *J. Clean. Prod.* **2019**, *217*, 702–715. [CrossRef]
67. Tellbach, D.; Li, Y.F. Cyber-attacks on smart meters in household nanogrid: Modeling, simulation and analysis. *Energies* **2018**, *11*, 316. [CrossRef]
68. Patil, Y.S.; Sankpal, S.V. Multi-Player Attack Detection Model for Smart Meter Security in Smart Grid Systems. *Int. J. Appl. Eng. Res.* **2019**, *7*, 1488–1492.
69. Hasse, F.; Von Perfall, A.; Hillebrand, T.; Smole, E.; Lay, M.; Charlet, L. Blockchain–an Opportunity for Energy Producers and Consumers? Available online: https://asian-power.com/sites/default/files/asianpower/print/AP_Novdec16_p44-45.pdf (accessed on 12 July 2020).
70. Andoni, M.; Valentin, R.; David, F.; Simone, A.; Dale, G.; David, J.; Peter, M.; Andrew, P. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2018**, *100*, 143–174. [CrossRef]
71. Li, Z.; Bahramirad, S.; Paaso, A.; Yan, M.; Shahidehpour, M. Blockchain for decentralized transactive energy management system in networked microgrids. *Electr. J.* **2019**, *32*, 58–72. [CrossRef]