



Review

Advancements and Research Trends in Microgrids Cybersecurity

Giovanni Battista Gaggero , Paola Girdinio and Mario Marchese * 

Department of Electrical, Electronics and Telecommunications Engineering and Naval Architecture—DITEN, University of Genoa, via Opera Pia 11A, 16145 Genoa, Italy; giovanni.gaggero@edu.unige.it (G.B.G.); paola.girdinio@unige.it (P.G.)

* Correspondence: mario.marchese@unige.it; Tel.: +39-010-335-2806

Abstract: Microgrids are growing in importance in the Smart Grid paradigm for power systems. Microgrid security is becoming crucial since these systems increasingly rely on information and communication technologies. Many technologies have been proposed in the last few years for the protection of industrial control systems, ranging from cryptography, network security, security monitoring systems, and innovative control strategies resilient to cyber-attacks. Still, electrical systems and microgrids present their own peculiarities, and some effort has to be put forth to apply cyber-protection technologies in the electrical sector. In the present work, we discuss the latest advancements and research trends in the field of microgrid cybersecurity in a tutorial form.

Keywords: smart microgrids; cybersecurity; software defined networking (SDN); intrusion detection systems (IDS); anomaly detection; resiliency



Citation: Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and Research Trends in Microgrids Cybersecurity. *Appl. Sci.* **2021**, *11*, 7363. <https://doi.org/10.3390/app11167363>

Academic Editors: Gregory Epiphaniou and Carsten R. Maple

Received: 15 July 2021

Accepted: 9 August 2021

Published: 10 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Microgrids can be defined as small-scale, low, or medium voltage power systems with a decentralized group of electricity sources and loads, which can operate connected to or separated (“islanded”) from the main power network. To ensure a proper control, microgrids often make large use of Information and Communication Technologies (ICT). With the term Smart Microgrids (SM), we refer to microgrids that are based on networked control systems. The control network of smart grids cannot, in general, be considered as an isolated network: the control network is commonly connected to outside to receive remote commands or allow remote maintenance. The used network may include wireless channels, and the grid can be geographically dislocated, making some devices physically reachable and prone to attacks. Moreover, the electrical grid is a critical infrastructure, so it can be the target of attackers with huge technical and economical capacities. For these reasons, cybersecurity is a fundamental issue to improve the resilience of microgrids. Several attacks against critical infrastructures have been pursued in the last few years. One of the most dangerous attacks, which gave further visibility to the cybersecurity risks in the industrial sector, has been Stuxnet [1], followed by other complex worms, such as Duqu and Flame [2]. Specifically, in the electrical sector, a severe attack has been the one against the Ukrainian power grid, which caused approximately 225,000 customers to lose power across various areas [3]. Some papers analyze the risks of attacks against Distributed Energy Resources (DER), which may lead to severe outages [4,5]. Researchers all over the world are making efforts to study microgrids and to build testbeds and demonstration sites. A list of microgrid testbeds has been reported in Reference [6], which also provides a classification by distribution network and geographical area. Still, additional efforts have to be provided in order to implement cyber attacks on real microgrid testbeds.

The process of cybersecurity can be broken down into five sub-problems: Deter, Detect, Delay, Respond, and Recover. To deter deals with discouraging attackers from attempting to gain unauthorized access by implementing measures that are perceived as too difficult

to defeat. To detect is a fundamental step of the defense-in-depth paradigm, which tackles the problem of recognizing malicious activities as rapidly as possible before or after the attacker has gained access to the system. Once the attack has been detected, the system should be able to react against the attacker, delaying the activities of the attacker, and allowing to take proper countermeasures to defeat the attack and recover from possible damages. The technologies and techniques that will be discussed in this paper address these issues.

Many papers have analyzed the vulnerabilities of smart grids and, specifically, of microgrids. This paper aims to discuss the main recent advancements and new research trends in the field of cybersecurity of smart microgrids, and the applications in this field of innovative technologies, such as Software Defined Networking, new approaches for intrusion and anomaly detection, and resilient control strategies. The paper is structured as follows. Section 2 discusses the state-of-the-art in the field of cybersecurity of smart microgrids. Section 3 analyzes techniques that can be applied to microgrid communication protocols and highlights possible vulnerabilities and countermeasures, with a particular focus on the role of IEC 62351 to secure microgrids. The rest of the paper focuses on technologies that can provide great benefits to the security of microgrids but that are still a research field. Section 4 discusses the application of the Software-Defined Networking (SDN) paradigm to enhance microgrid resilience and cybersecurity, while Section 5 considers the implementation of Intrusion Detection System (IDS) techniques on electrical devices with a special attention to Host-IDS (HIDS). Section 6 focuses on physics-based anomaly detection algorithms that can be applied to power systems. The main works on control strategies that can be implemented in distributed energy resources in order to improve the resilience to cyber-attacks and the availability of the whole system are summarized in Section 7. Conclusions are drawn in Section 8.

2. Cybersecurity in Smart Microgrids

Smart Grid is the new paradigm for power systems. Even if there is no unique definition, the European Union Commission Task Force for Smart Grids provides the following one: “A Smart Grid is an electricity network that can cost-efficiently integrate the behavior and actions of all users connected to it—generators, consumers, and those that do both—in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. A smart grid employs innovative products and services, together with intelligent monitoring, control, communication, and self-healing technologies”.

It is hard to evaluate the cybersecurity risk of smart grids due to the huge variety of Information and Communication Technologies that can be used to achieve a wide set of tasks. For example, the National Electric Sector Cybersecurity Organization Resource (NESCOR) identifies six scenarios in the power system where main failures related to cybersecurity threats [7] can happen: Advanced Metering Infrastructure, Distributed Energy Resources (DER), Wide Area Monitoring Protection and Control, Electric Transportation, Demand Response, and Distribution Grid Management. Each technology has its own peculiarities impacting differently on the whole power system. Several papers address the issue to survey the main vulnerabilities and threats of the electrical power system: [8–10]. Reference [5] discusses the architecture of power systems with a high penetration of DER and related cybersecurity issues and summarizes attack scenarios against DER also considering attack prevention, detection, and response measures specifically designed for DER.

A Survey on Cyber-Security of Smart Microgrids is proposed in Reference [11], where a sample of recent cybersecurity projects, a review of cybersecurity standards and protocols for power systems, and a classification of attacks with related impact and mitigation strategies are provided. Reference [11] provides a short overview of some technologies that will be further discussed in this paper. Reference [12] addresses the cyber-physical security in power systems by focusing on microgrids and their control structure. Papers including an analysis at a glance of the most promising recent technologies that can improve the

cybersecurity of smart microgrids are still missing at the best knowledge of the authors of this paper.

3. The Action of IEC 62351

Control networks in Supervisory Control And Data Acquisition (SCADA) systems were typically realized by using only proprietary solutions. Several application protocols were developed, each targeting specific communication constraints required by the control systems. The need of remote control and the advances in computer networks led to the blending of traditional control networks with modern Internet. Consequently, control systems inherited security vulnerabilities that threatened the modern internet [13]. In the electrical sector, broadly employed protocols to communicate data and control information are Modbus, DNP3, IEC 60870-5, and IEC 61850. In particular, although developed for substation automation, IEC 61850 suite is exploited for smart microgrids [14]. Abstract data models defined in IEC 61850 can be mapped to different protocols, such as Manufacturing Message Specification (MMS), Generic Object Oriented Substation Event (GOOSE), and Sampled Measured Values (SMV), which can run over TCP/IP networks or over substation LANs by using Ethernet.

As said, severe vulnerabilities affect these protocols. Different papers show possible attacks at these protocols and the related impact. In Reference [15], vulnerabilities of GOOSE are tested by using real-time simulation and industry standard hardware-in-the-loop emulation. Reference [16] shows how an attacker can launch a Man-In-The-Middle attack on the MMS communications of a photovoltaic inverter installation by using ARP spoofing.

Some of these vulnerabilities are currently addressed by IEC 62351, which is a standard developed by WG15 of IEC TC57. The main purpose is to address the problem of security of TC 57 series of protocols including IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, and IEC 61968 series. Currently, the standard is composed of 18 parts listed in Table 1.

Table 1. Summary of IEC 62351 specifications.

| Section | Description |
|------------|--|
| Part 1 | Introduction to security issue |
| Part 2 | Glossary of terms |
| Part 3 | Profiles including TCP/IP |
| Part 4 | Profiles including MMS and derivatives |
| Part 5 | Security for IEC 60870-5 and derivatives |
| Part 6 | Security for IEC 61850 |
| Part 7 | Network and system management (NSM) data object models |
| Part 8 | Role-based access control for power system management |
| Part 9 | Cyber security key management for power system equipment |
| Part 10 | Security architecture guidelines |
| Part 11 | Security for eXtensible markup language (XML) documents |
| Part 12 | Resilience and security recommendations for power systems with DER cyber-physical systems |
| Part 13 | Guidelines on security topics to be covered in standards and specifications |
| Part 90-1 | Guidelines for handling role-based access control in power systems |
| Part 90-2 | Deep packet inspection of encrypted communications |
| Part 90-3 | Guidelines for network and system management |
| Part 100-1 | Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 |
| Part 100-3 | Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP |

IEC 62351 series does not provide only cryptography for common electrical control system protocols. It also defines cybersecurity requirements to implement security technologies in the operational environment, including objects for network and system management, role-based access control, cryptographic key management, and security event logging.

IEC 62351 offers a list of guidelines for protocols security and a framework for secure operations. It is designed to be referenced by other standards, not used directly. For example, IEC 62351-3 specifies how to provide confidentiality, tamper detection, and message level authentication for SCADA and telecontrol protocols, and how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) 1.2 according to RFC 5246. However, its implementation in actual operation scenarios, such as overcurrent relay coordination or DER management systems, is open to interpretation. For example, IEC 62351-6 standard stipulates the use of digital signatures to ensure integrity in IEC 61850 message exchanges, but the digital signature requires a high computational time with consequent problems for practical implementation in GOOSE messages. For these reasons, IEC 62351 cannot offer a strict procedure for the implementation of cryptography techniques.

Reference [17] provides an assessment of the security of IEC 62351 and concludes that, although the standard contains some inaccuracies and unconventional choices, and does not consider new cryptographic algorithms that could provide the same security guarantees at a lower performance cost, the standard provides a significant security improvement, by assuring authenticity, integrity and confidentiality of data. Some recent papers address the issue of IEC 62351 implementation. A complete evaluation of security mechanisms for IEC 61850 message exchanges, including GOOSE, SV, routable-GOOSE (R-GOOSE), routable-SV (R-SV), MMS is presented in Reference [18]. The implementations of IEC 62351-4 Security for IEC 61850 MMS Messages has been discussed in Reference [19]. An analysis of the implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security according to IEC 62351 has been presented in Reference [20]. An analysis and performance evaluation of the implementation of IEC 62351-6 probabilistic signature scheme to secure GOOSE Messages is contained in Reference [21].

For these reasons, the implementation of IEC 62351-based techniques to secure common microgrid protocols will represent a significant improvement. Still, some effort has to be invested in order to apply the standard in different contexts.

4. Software Defined Networking

Software-Defined Networking (SDN) technology is an approach to network management that enables dynamic, resource-efficient, and programmable network configuration in order to improve network performance and monitoring. SDN centralizes the network intelligence in one network component by decoupling the forwarding process of network packets (data plane) from routing process and control actions (control plane). SDN is a useful solution to improve the performance, safety, and security of different types of networks, including smart grid control systems. OpenFlow is the most popular standard/protocol to exchange messages between control and data planes in SDN [22].

A comprehensive survey of SDN-based smart grid communication is presented in Reference [23]. Applications include Substation Automation, Advanced Metering Infrastructures, Phasor Measurement Units, and also microgrids. Many papers focus on the benefit of SDN in isolating different traffic types/applications, prioritizing traffic, assuring resilience and fast failure recovery, and for the implementation of virtual network slices [24].

SDN also has interesting applications for the security of Industrial Control Systems (ICS), especially for incident response. It allows increasing the resiliency of the control system, thanks to the possibility to dynamically re-configure the network after the detection of a fault or of a compromised device, allowing it to operate even in degraded conditions. This is particularly useful for control networks within critical infrastructures, which require extremely high availability. Reference [25] discusses how SDN and Network Function Virtualization (NFV) technologies can help design automatic incident-response mechanisms for ICS and also describes a prototype to show the feasibility in a scenario that uses Programmable Logic Controllers (PLC) managing a classical tank-filling control system. Reference [26] studies the applicability of emerging technologies in the area of IP networks,

including SDN, NFV, and next generation firewalls, to secure ICS. Reference [27] proposes an attack detection and localization algorithm and designs an intervention strategy in the networked robot control field. A software-defined security approach to secure field zones in ICS is shown in Reference [28]: it consists of a hybrid anomaly detection module that inspects anomaly behaviors in network communications and physical process states. It proposes a multi-level security response module that allows isolating any compromised zone.

Microgrids could significantly benefit from self-healing network management, which includes but is not limited to [29]:

- quick reset and reconfiguration of switches in order to isolate suspicious devices in the microgrid;
- establishment of application-specific filtering operations in the switches located close to attack sources; and
- on-demand path establishment for control commands to shrink attacker's operation time window.

SDN allows verifying the entire communication network concerning security policies (e.g., access control) and network situations (e.g., loop-freedom and congestion-freedom). SDN allows also directly implementing a Network Intrusion Detection System (NIDS) within the SDN controller, even if such implementation may introduce a latency time that could be incompatible with the allowed latency in a microgrid environment [30]. The application of the SDN paradigm in microgrids may comprehend both security and control applications, as shown in Figure 1.

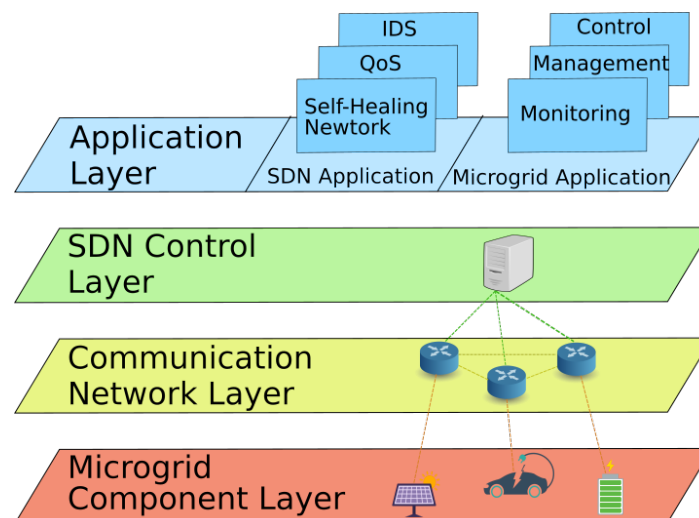


Figure 1. Multi-Layered SDN-enabled Microgrid architecture.

Focusing on security applications, the SDN paradigm has been applied in different scenarios, to address attacks that target different communication layers. Reference [31] proposes an SDN architecture able to switch between wireless and power line communication to keep proper control within a direct current microgrid under a Denial of Service (DoS) attack. Reference [31] proposes an architecture that exploits SDN control plane message exchanges over the power bus, allowing the reconfiguration of the data plane connections. In this way, all generators in the microgrid operate as either voltage regulators (active agents) or current sources (passive agents), with their operating modes being determined by software-defined controls supported by the control plane communication performed over the power bus. An SDN-based attack detection to protect networked microgrids from cyber-attacks based on a botnet that targets inverter controllers of DERs is presented in Reference [32].

Of course, the implementation of such an architecture can further broaden the attack surface [33]. Nonetheless, SDN technologies can improve the overall microgrid resiliency

towards cyber-attacks, faults, or natural events, thanks to the offered customizable network configuration ability. It is a promising research field with immediate practical applications.

5. Intrusion Detection Systems

Intrusion Detection Systems (IDS) are devices or software applications that monitor a portion of the systems and try detecting malicious activities and policy violations. IDS can be classified from different viewpoints. We can identify two big families:

- Network Intrusion Detection Systems (NIDS) that analyze network traffic collected from one or more points of the communication network; and
- Host Intrusion Detection Systems (HIDS) that analyze the activity of a single host (i.e., a terminal) of the network.

Other classifications can be based on the strategy used to detect the malicious activity (signature-based or anomaly-based) or on the action that the system implements after detecting an attack (IDS can be purely passive or block traffic flows/applications, usually referred to as Intrusion Prevention System (IPS)), as shown in Table 2.

Table 2. IDS classification.

| IDS Classification | | |
|----------------------|-----------------|----------------------|
| By monitored element | Network-IDS | Host-IDS |
| By actions | Passive (IDS) | Active (IDS and IPS) |
| By detection methods | Signature-based | Anomaly-based |

Different NIDS solutions specifically designed for ICS protocols have been proposed in the literature and are also available as commercial solutions. NIDS are usually passive elements of the network to avoid them significantly slowing down the responses to attacks. It would be dangerous to implement an active element in a safety-critical control network due to the possible high false positive rate that would affect the whole system safety.

In the IT field, two common HIDS solutions are Open Source HIDS SECURITY (OSSEC) and Tripwire. OSSEC is a free and open-source HIDS that supports a wide range of Operating Systems (OS), while Tripwire is a commercial solution. These solutions combine passive actions performed periodically in order to not affect the system performance, such as the identification of unauthorized file modifications (through, for example, file integrity checking by using checksum databases), of malicious processes, and of log behaviors (for instance by monitoring specific parameters), and active capabilities, similarly to host firewalls that allow blocking unauthorized network communications by adding firewall rules.

A further improvement in the field of HIDS is online intrusion detection (or “real-time” or “in-line” intrusion detection). Real-time HIDS analyze different features of the host, including OS aggregated behavior, such as CPU and memory metrics, shell commands, and system calls; application information, such as loaded modules and libraries, programming code, and processes; user behavior and host network information, such as physical and logical interfaces, and their configuration, as well as network packets [34].

Nevertheless, in order to implement HIDS in ICS devices, further considerations are necessary. Two major challenges have to be faced: the time performance in devices with severe latency requirements and low computational power, and the risk related to the implementation of active HIDS.

Attributes that a HIDS suitable for ICS application should include are [35]:

- **Configurability:** capability to be configured as specified by the requirements of the target system;
- **Configuration and Knowledge Security:** HIDS configuration and used data should be protected against unauthorized access and modifications;
- **Resiliency:** HIDS action cannot affect the availability of the device;
- **Low Performance Overhead:** the execution of the HIDS on the target device should not negatively influence the performance of the underlying system;

- Low Detection Time: detection and response to intrusions should be as fast as possible; and
- Interoperability: the HIDS should be able to interact with other technologies, such as Security Information and Event Management (SIEM).

In general, regarding embedded industrial devices, operational requirements for industrial environments, such as real-time capabilities, and availability must be ensured, even in the context of a cybersecurity action. Domain specific standards, guidelines, and recommendations that can be applied for specific industrial sectors must be considered to address this issue.

In a microgrid environment, the most time-critical devices are PLC, Remote Terminal Units (RTU), and, in particular, electrical protections.

To give a few examples about electrical protections:

- IEC 60834 requires that the latency of the transmission and reception of a control signal related to a protective action has to be lower than 10 ms, while IEC 61850 imposes a latency lower than 3 ms;
- IEEE 1646-2004 requires information on protective actions to be exchanged by the devices inside the same substation in a time lower than a quarter of a period (i.e., 5 or 4 ms depending on the 50 or 60 Hz frequency); and
- less stringent limits (between 8 and 12 ms) are required for the exchange of information on protective actions with devices outside the substation.

Most PLC and RTU are based on Real-Time Operating Systems (RTOS) [36]. The main characteristic of RTOS is the way they handle operations and resources, completing and executing tasks within a defined time frame due to their optimized architecture and features. Multi-tasking is still possible, thanks to task scheduling. RTOS handle priority: each task has a priority, and the task with the highest priority has a preference of execution, even if it is necessary to prevent a lower-priority task from being executed.

Real-Time HIDS are sometimes implemented as a kernel module in Linux-based operating systems. This type of implementation can affect the device performance. For this reason, even if some papers already propose HIDS specifically designed for ICD devices [35], further effort has to be put forth to verify the applicability of these solutions to electrical devices within a smart microgrid.

6. Physics-Based Anomaly Detection

Cyber-attacks against industrial systems aim to modify the physical behavior of the usual system process. In cyber-physical systems, the physical evolution of the system state has to follow immutable laws of nature. For this reason, some papers propose to add a further line of defense in ICS, represented by algorithms able to rapidly notice abnormal physical behaviors based on measures extracted from the industrial process. For example, the physical properties of the process can be used to create models that, in turn, may be exploited to check if information coming from sensors is consistent with the physical laws and the expected physical behavior of the system and if the sent control commands correspond to a real need or if they derive from an artificial modification of the measure. Applications include not only smart microgrids but also water control systems, power grids, chemical process control, and medical devices, among many others.

Monitoring the “physics” of cyber-physical systems to detect attacks is a growing area of research. Reference [37] presents a review of physics-based anomaly detection schemes based on a unified taxonomy. These system can be categorized under different viewpoints. Two possible categories are: algorithms based on pre-defined models and algorithms based on Machine Learning (ML). State estimation models for power systems, which exploit the known equations of power transmissions, belong to the first category. However, for some complex systems, such as DES, to write a closed-form equation that takes into account all the measured parameters can be difficult. In these cases, ML can help develop anomaly detection algorithms, even if the great disproportion between available data of normal and

abnormal behavior typical in cyber-physical systems can limit the application of ML-based schemes. Peculiar anomaly detection techniques are used to address this issue [38].

Physics-based Anomaly Detection Systems find many applications in the smart micro-grid environment. After the development a consensus-based distributed voltage control architecture of isolated DC microgrids, an analytical consistency-based anomaly detection mechanism based on variables associated with the proposed algorithm is presented in Reference [39]. Reference [40] proposes an IDS built on the combination of network data, together with power system and control information. Reference [41] shows a contextual anomaly detection method based on an artificial neural network and its use in the detection of malicious voltage control actions in the low voltage distribution grid. Reference [42] presents a high-dimensional data-driven cyber-physical attack detection and identification based on electric waveform data measured by waveform sensors in the distribution power networks. Reference [43] describes an anomaly detection algorithm to reveal attacks on PhotoVoltaic (PV) systems, such as PV disconnect, power curtailment, Volt-var attack, and reverse power flow in a portion of the distribution grid with a sufficient percentage of DER penetration. This approach exploits semi-supervised ML algorithms, such as Neural network autoencoder, One Class Support Vector Machine (SVM), Isolation Forest, Random Forest with synthetic corruption, Principal Component Analysis (PCA) with convex hulls, and Inverse-PCA techniques. An approach based on a fully-connected neural network autoencoder to detect cyber-attacks within a PV system is proposed in Reference [44]. A deep learning scheme composed of long and short term memory-stacked autoencoders and convolutional neural networks followed by a softmax activation layer is used in Reference [45] for fault detection in a wind turbine.

Physics-based anomaly detection systems represent an interesting field of research, in particular for DERs. Further research studies should include a comparison between the huge variety of anomaly detection techniques and should test the proposed approaches against new malicious activities that can be imposed on distributed electrical generators.

7. Resilient Control Strategies

As already discussed, microgrids can operate in grid-connected or islanded modes. If the microgrid works in the grid-connected mode, the generators inject power by following economical logics, while the frequency and voltage are kept in the correct range by the main electrical grid. On the contrary, if it operates in islanded mode; the generators have to guarantee voltage and frequency regulation. The control of the electrical grid is usually schematized into three levels, as shown in Figure 2:

- Primary Control: aimed at restoring the imbalance between generation and load by changing the frequency of the power system. In inverter-based microgrids, this is achieved through droop equations; it is the fastest among the three levels.
- Secondary Control: aimed at restoring the nominal value of the frequency and the power exchange among the power systems. It acts at longer time.
- Tertiary Control: aimed at optimizing the economical aspects of load sharing, usually through an Energy Management System (EMS).

Both in islanded and grid-connected modes, EMS can periodically send the power setpoints to the generators through the control network by using different protocols. To jeopardize the control of the electrical grid acting in grid-connected mode can cause economic damages or even, in some cases, afflict the stability of the whole grid. In islanded mode, attacking control mechanism is a severe threat to the grid stability.

In inverter-based microgrids, secondary control can be based on communication schemes. In these cases, attacks against the communication infrastructure can have severe consequences on the availability of the whole microgrid. The dynamic of electromagnetic system physics is so fast that the attacks targeting secondary control cannot be recognized in time by an IDS to allow the effective deployment of countermeasures. Moreover, these communication-based schemes are vulnerable to unaddressed cryptography attacks, such

as DoS attacks. On the other hand, the control of electrical grids is essential for the service continuity. Resilience is topical in this field.

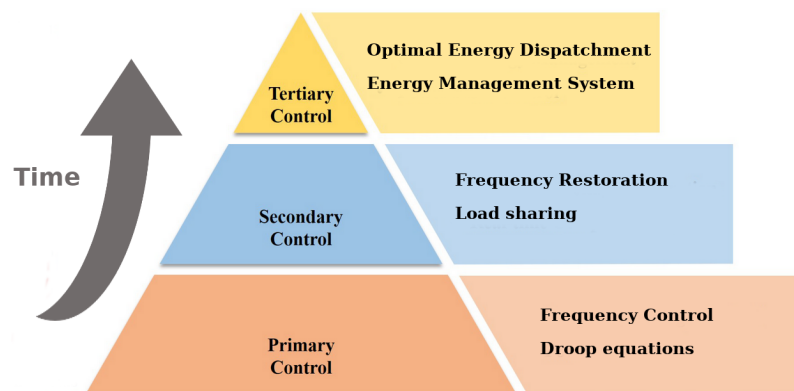


Figure 2. Control levels of the electrical grid.

A cyber-attack resilient control strategy for islanded microgrids is presented in Reference [46]. The proposed control strategy realizes the detection and isolation of corrupted communication links and controllers in a microgrid whose secondary control is based on a distributed control system. A distributed resilient control strategy for frequency/voltage restoration, fair real power sharing, and state-of-charge balancing in microgrids with multiple Energy Storage Systems in abnormal conditions is presented in Reference [47]. Reference [48] studies the impact of various kinds of cyber-attacks, such as false data injection [49], DoS [50], and replay attacks [51], on communication links based on CANBus for secondary control of the distributed generators. Reference [48] also proposes a mitigation strategy based on a reconfigurable secondary control mechanism. Reference [52] introduces a control strategy able to mitigate false data injection and DoS attacks, demonstrating the stability by using the Lyapunov theory under different scenarios, with and without false data injection, and DoS attacks. Reference [53] proposes a distributed optimal frequency control for microgrids resilient against cyber attacks on condition that they are within certain ranges, by introducing an auxiliary networked system interconnecting with the original cooperative control system.

Microgrids can present different DER scenarios, including different types of non-programmable and programmable sources. Non-programmable sources can, anyway, participate to the voltage control by injecting reactive power into the grid. Given the variety of scenarios and the complexity of the interactions of multiple sources participating to frequency control, voltage control, or both, there are still some unaddressed issues in the state of the art to be investigated.

8. Conclusions

In the present work, the application of some of the most promising technology for Industrial Control System to the Smart Microgrid environment has been discussed. These technologies present different maturity levels: while some are addressed by standards, such as in the IEC 62351, others require much more effort for the effective implementation in electrical power systems. SDN decouples the data and control plane and allows controlling an entire data network, thus assuring the action of access control, as well as of congestion avoidance schemes. Having a centralized control also allows implementing a Network Intrusion Detection System (NIDS) directly in the SDN controller and improving microgrid resiliency against cyber attacks and faults. The drawback of using SDN stands in the possible delay introduced by these actions, which could be incompatible with some actions required in an industrial environment. If most NIDS implementation are already commercial tools, Host IDS (HIDS) may represent an improvement, particularly if they act in real-time. Real-time HIDS may use information locally available at the host, such as CPU and memory, system calls, loaded modules and libraries, user behavior, and information

about interfaces, to detect anomalies. The main problem is the time necessary for these algorithms to run and the requested computational power, possibly not available in the industrial terminals where HIDS should act. One of the more interesting research activities concerning the security of smart microgrids and, more generally, of ICS is represented by schemes able to detect abnormal physical behaviors based on measures extracted by the industrial process. Anomaly can be defined as something that deviates from what is standard, normal, or expected. In the context of physics-based anomaly detection, it is an undesired physical working condition of the process, a deviation of the process from a known working condition defined as normal, or as an impossible observation of the state of the process because of an incoherence of the measurements. This definition includes working conditions caused by either faults or malicious manumissions of control devices, actuators, and sensors. In the field of industrial processes, and especially in power systems, typical anomaly detection strategies are based on the dynamic state estimation. Even if efficient, this approach requires the knowledge of the exact behavior of the system. Machine Learning (ML) approaches could be useful to face up this problem. In the field of cyber-physical systems anomaly detection, it is quite common not to have a dataset containing examples of bad physical behavior during a cyber attack. So, it is mandatory to apply algorithms that can “learn” a behavior considered to be normal and classify new examples. The last promising research field discussed in the paper is represented by resilient control strategies. The control of electrical grids is essential for the service continuity. Both in islanded and grid-connected modes, taking control of the electrical grid can cause great damages and also affect the stability of the whole grid. Resilience is essential in this field. Further research is necessary to develop commercial products to be used in the field, but results from simulations and prototypes are really promising.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

| | |
|-------|--|
| ICT | Information and Communication Technology |
| SM | Smart Microgrid |
| DER | Distributed Energy Resources |
| SCADA | Supervisory Control And Data Acquisition |
| MMS | Manufacturing Message Specification |
| GOOSE | Generic Object Oriented Substation Event |
| SVM | Sampled Measured Values |
| SDN | Software Defined Network |
| ICS | Industrial Control Systems |
| NFV | Network Function Virtualization |
| PLC | Programmable Logic Controller |
| IDS | Intrusion Detection System |
| NIDS | Network Intrusion Detection System |
| HIDS | Host Intrusion Detection System |

| | |
|------|-----------------------------|
| DoS | Denial of Service |
| IPS | Intrusion Prevention System |
| RTOS | Real-Time Operating Systems |
| RTU | Remote Terminal Unit |
| EMS | Energy Management System |
| PV | Photovoltaic |

References

- Falliere, N.; Murchu, L.O.; Chien, E. *W32.Stuxnet Dossier*; Symantec Security Response; Symantec Corp.: Tempe, AZ, USA, 2011; Volume 5, p. 29.
- Bencsáth, B.; Pék, G.; Buttyán, L.; Felegyhazi, M. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet* **2012**, *4*, 971–1003. [[CrossRef](#)]
- Case, D.U. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): Washington, DC, USA, 2016; 388p.
- Liu, X.; Shahidepour, M.; Cao, Y.; Wu, L.; Wei, W.; Liu, X. Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1330–1339. [[CrossRef](#)]
- Qi, J.; Hahn, A.; Lu, X.; Wang, J.; Liu, C.C. Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Phys. Syst. Theory Appl.* **2016**, *1*, 28–39. [[CrossRef](#)]
- Hossain, E.; Kabalci, E.; Bayindir, R.; Perez, R. Microgrid testbeds around the world: State of art. *Energy Convers. Manag.* **2014**, *86*, 132–153. [[CrossRef](#)]
- Lee, A. *Electric Sector Failure Scenarios and Impact Analyses*; Electric Power Research Institute: Palo Alto, CA, USA, 2013; Volume 1.
- Wang, W.; Lu, Z. Cyber security in the smart grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [[CrossRef](#)]
- Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [[CrossRef](#)]
- El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [[CrossRef](#)]
- Nejabatkhah, F.; Li, Y.W.; Liang, H.; Ahrabi, R.R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [[CrossRef](#)]
- Canaan, B.; Colicchio, B.; Ould Abdeslam, D. Microgrid cyber-security: Review and challenges toward resilience. *Appl. Sci.* **2020**, *10*, 5649. [[CrossRef](#)]
- Volkova, A.; Niedermeier, M.; Basmadjian, R.; de Meer, H. Security challenges in control network protocols: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 619–639. [[CrossRef](#)]
- Bani-Ahmed, A.; Weber, L.; Nasiri, A.; Hosseini, H. Microgrid communications: State of the art and future trends. In Proceedings of the 2014 International Conference on Renewable Energy Research and Application (ICRERA), Milwaukee, WI, USA, 19–22 October 2014; pp. 780–785.
- Reda, H.T.; Ray, B.; Peidaee, P.; Anwar, A.; Mahmood, A.; Kalam, A.; Islam, N. Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid. *Sensors* **2021**, *21*, 1554. [[CrossRef](#)]
- Kang, B.; Maynard, P.; McLaughlin, K.; Sezer, S.; Andrén, F.; Seitz, C.; Kupzog, F.; Strasser, T. Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–8.
- Schlegel, R.; Obermeier, S.; Schneider, J. A security evaluation of IEC 62351. *J. Inf. Secur. Appl.* **2017**, *34*, 197–204. [[CrossRef](#)]
- Hussain, S.S.; Ustun, T.S.; Kalam, A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. *IEEE Trans. Ind. Inform.* **2019**, *16*, 5643–5654. [[CrossRef](#)]
- Ustun, T.S.; Hussain, S.S. IEC 62351-4 Security Implementations for IEC 61850 MMS Messages. *IEEE Access* **2020**, *8*, 123979–123985. [[CrossRef](#)]
- Hussain, S.S.; Farooq, S.M.; Ustun, T.S. Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security. *IEEE Access* **2019**, *7*, 80980–80984. [[CrossRef](#)]
- Farooq, S.M.; Hussain, S.S.; Ustun, T.S. Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages. *IEEE Access* **2019**, *7*, 32343–32351. [[CrossRef](#)]
- Hu, F.; Hao, Q.; Bao, K. A survey on software-defined network and openflow: From concept to implementation. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 2181–2206. [[CrossRef](#)]
- Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2637–2670. [[CrossRef](#)]
- Ren, L.; Qin, Y.; Wang, B.; Zhang, P.; Luh, P.B.; Jin, R. Enabling resilient microgrid through programmable network. *IEEE Trans. Smart Grid* **2016**, *8*, 2826–2836. [[CrossRef](#)]
- Piedrahita, A.F.M.; Gaur, V.; Giraldo, J.; Cardenas, A.A.; Rueda, S.J. Leveraging software-defined networking for incident response in industrial control systems. *IEEE Softw.* **2017**, *35*, 44–50. [[CrossRef](#)]
- Genge, B.; Graur, F.; Haller, P. Experimental assessment of network design approaches for protecting industrial control systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *11*, 24–38. [[CrossRef](#)]

27. Sándor, H.; Genge, B.; Szántó, Z.; Márton, L.; Haller, P. Cyber attack detection and mitigation: Software defined survivable industrial control systems. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 152–168. [[CrossRef](#)]
28. Yang, J.; Zhou, C.; Tian, Y.C.; Yang, S.H. A software-defined security approach for securing field zones in industrial control systems. *IEEE Access* **2019**, *7*, 87002–87016. [[CrossRef](#)]
29. Jin, D.; Li, Z.; Hannon, C.; Chen, C.; Wang, J.; Shahidehpour, M.; Lee, C.W. Toward a cyber resilient and secure microgrid using software-defined networking. *IEEE Trans. Smart Grid* **2017**, *8*, 2494–2504. [[CrossRef](#)]
30. Fausto, A.; Marchese, M. Implementation details to reduce the latency of an SDN Statistical Fingerprint-Based IDS. In Proceedings of the 2019 International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Rome, Italy, 27–29 November 2019; pp. 1–6.
31. Danzi, P.; Angjelijinoski, M.; Stefanović, Č.; Dragičević, T.; Popovski, P. Software-defined microgrid control for resilience against denial-of-service attacks. *IEEE Trans. Smart Grid* **2018**, *10*, 5258–5268. [[CrossRef](#)]
32. Li, Y.; Qin, Y.; Zhang, P.; Herzberg, A. SDN-enabled cyber-physical security in networked microgrids. *IEEE Trans. Sustain. Energy* **2018**, *10*, 1613–1622. [[CrossRef](#)]
33. Haas, Z.J.; Culver, T.L.; Sarac, K. Vulnerability Challenges of Software Defined Networking. *IEEE Commun. Mag.* **2021**, *59*, 88–93. [[CrossRef](#)]
34. Liu, M.; Xue, Z.; Xu, X.; Zhong, C.; Chen, J. Host-based intrusion detection system with system calls: Review and future trends. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–36. [[CrossRef](#)]
35. Martinez, C.V.; Vogel-Heuser, B. A host intrusion detection system architecture for embedded industrial devices. *J. Frankl. Inst.* **2019**, *358*, 210–236. [[CrossRef](#)]
36. Vargas, C.; Langfinger, M.; Vogel-Heuser, B. A tiered security analysis of industrial control system devices. In Proceedings of the 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, Germany, 24–26 July 2017; pp. 399–404.
37. Giraldo, J.; Urbina, D.; Cardenas, A.; Valente, J.; Faisal, M.; Ruths, J.; Tippenhauer, N.O.; Sandberg, H.; Candell, R. A survey of physics-based attack detection in cyber-physical systems. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–36. [[CrossRef](#)]
38. Pimentel, M.A.; Clifton, D.A.; Clifton, L.; Tarassenko, L. A review of novelty detection. *Signal Process.* **2014**, *99*, 215–249. [[CrossRef](#)]
39. Shi, D.; Lin, P.; Wang, Y.; Chu, C.C.; Xu, Y.; Wang, P. Deception Attack Detection of Isolated DC Microgrids under Consensus-Based Distributed Voltage Control Architecture. *IEEE J. Emerg. Sel. Top. Circ. Syst.* **2021**, *11*, 155–167. [[CrossRef](#)]
40. Chavez, A.; Lai, C.; Jacobs, N.; Hossain-McKenzie, S.; Jones, C.B.; Johnson, J.; Summers, A. Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems. In Proceedings of the 2019 IEEE CyberPELS (CyberPELS), Knoxville, TN, USA, 29 April–1 May 2019; pp. 1–6.
41. Kosek, A.M. Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model. In Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), Vienna, Austria, 12 April 2016; pp. 1–6.
42. Li, F.; Xie, R.; Yang, B.; Guo, L.; Ma, P.; Shi, J.; Ye, J.; Song, W. Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach. *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**, doi:10.1109/JESTPE.2019.2943449. [[CrossRef](#)]
43. Shilay, D.M.; Lorey, K.G.; Weiz, T.; Lovetty, T.; Cheng, Y. Catching Anomalous Distributed Photovoltaics: An Edge-based Multi-modal Anomaly Detection. *arXiv* **2017**, arXiv:1709.08830.
44. Gaggero, G.B.; Rossi, M.; Girdinio, P.; Marchese, M. Detecting System Fault/Cyberattack within a Photovoltaic System Connected to the Grid: A Neural Network-Based Solution. *J. Sens. Actuator Netw.* **2020**, *9*, 20. [[CrossRef](#)]
45. Fotiadou, K.; Velivassaki, T.H.; Voulkidis, A.; Skias, D.; De Santis, C.; Zahariadis, T. Proactive Critical Energy Infrastructure Protection via Deep Feature Learning. *Energies* **2020**, *13*, 2622. [[CrossRef](#)]
46. Zhou, Q.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. A cyber-attack resilient distributed control strategy in islanded microgrids. *IEEE Trans. Smart Grid* **2020**, *11*, 3690–3701. [[CrossRef](#)]
47. Deng, C.; Wang, Y.; Wen, C.; Xu, Y.; Lin, P. Distributed resilient control for energy storage systems in cyber—Physical microgrids. *IEEE Trans. Ind. Inform.* **2020**, *17*, 1331–1341. [[CrossRef](#)]
48. Rath, S.; Pal, D.; Sharma, P.S.; Panigrahi, B.K. A Cyber-Secure Distributed Control Architecture for Autonomous AC Microgrid. *IEEE Syst. J.* **2020**, doi:10.1109/JSYST.2020.3020968. [[CrossRef](#)]
49. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2011**, *14*, 1–33. [[CrossRef](#)]
50. Hussain, A.; Heidemann, J.; Papadopoulos, C. A framework for classifying denial of service attacks. In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Karlsruhe, Germany, 25–29 August 2003; pp. 99–110.
51. Hosseinzadeh, M.; Sinopoli, B.; Garone, E. Feasibility and detection of replay attack in networked constrained cyber-physical systems. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 24–27 September 2019; pp. 712–717.
52. Zhou, Q.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A.; Che, L.; Liu, X. Cross-Layer Distributed Control Strategy for Cyber Resilient Microgrids. *IEEE Trans. Smart Grid* **2021**, doi:10.1109/TSG.2021.3069331. [[CrossRef](#)]
53. Liu, Y.; Li, Y.; Wang, Y.; Zhang, X.; Gooi, H.B.; Xin, H. Robust and Resilient Distributed Optimal Frequency Control for Microgrids Against Cyber Attacks. *IEEE Trans. Ind. Inform.* **2021**, doi:10.1109/TII.2021.3071753. [[CrossRef](#)]