

**On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids**

Gupta, Kirti; Sahoo, Subham; Panigrahi, Bijaya Ketan; Blaabjerg, Frede; Popovski, Petar

*Published in:*  
Energies

*DOI (link to publication from Publisher):*  
[10.3390/en14164941](https://doi.org/10.3390/en14164941)

*Creative Commons License*  
CC BY 4.0

*Publication date:*  
2021

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University](#)

*Citation for published version (APA):*

Gupta, K., Sahoo, S., Panigrahi, B. K., Blaabjerg, F., & Popovski, P. (2021). On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids. *Energies*, 14(16), Article 4941. <https://doi.org/10.3390/en14164941>

**General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -



**Take down policy**

If you believe that this document breaches copyright please contact us at [vbn@aub.aau.dk](mailto:vbn@aub.aau.dk) providing details, and we will remove access to the work immediately and investigate your claim.



## Article

# On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids

Kirti Gupta <sup>1</sup>, Subham Sahoo <sup>2,\*</sup> , Bijaya Ketan Panigrahi <sup>1</sup>, Frede Blaabjerg <sup>2,\*</sup>  and Petar Popovski <sup>3</sup>

<sup>1</sup> Department of Electrical Engineering, Indian Institute of Technology, Delhi 110016, India; Kirti.Gupta@ee.iitd.ac.in (K.G.); Bijaya.Ketan.Panigrahi@ee.iitd.ac.in (B.K.P.)

<sup>2</sup> Department of Energy, Aalborg University, 9220 Aalborg, Denmark; ssa@energy.aau.dk

<sup>3</sup> Department of Electronic Systems, Aalborg University, 9220 Aalborg, Denmark; petarp@es.aau.dk

\* Correspondence: fbl@energy.aau.dk

**Abstract:** The integration of variable distributed generations (DGs) and loads in microgrids (MGs) has made the reliance on communication systems inevitable for information exchange in both control and protection architectures to enhance the overall system reliability, resiliency and sustainability. This communication backbone in turn also exposes MGs to potential malicious cyber attacks. To study these vulnerabilities and impacts of various cyber attacks, testbeds play a crucial role in managing their complexity. This research work presents a detailed study of the development of a real-time co-simulation testbed for inverter-based MGs. It consists of a OP5700 real-time simulator, which is used to emulate both the physical and cyber layer of an AC MG in real time through HYPERSIM software; and SEL-3530 Real-Time Automation Controller (RTAC) hardware configured with ACSELERATOR RTAC SEL-5033 software. A human-machine interface (HMI) is used for local/remote monitoring and control. The creation and management of HMI is carried out in ACSELERATOR Diagram Builder SEL-5035 software. Furthermore, communication protocols such as Modbus, sampled measured values (SMVs), generic object-oriented substation event (GOOSE) and distributed network protocol 3 (DNP3) on an Ethernet-based interface were established, which map the interaction among the corresponding nodes of cyber-physical layers and also synchronizes data transmission between the systems. The testbed not only provides a real-time co-simulation environment for the validation of the control and protection algorithms but also extends to the verification of various detection and mitigation algorithms. Moreover, an attack scenario is also presented to demonstrate the ability of the testbed. Finally, challenges and future research directions are recognized and discussed.

**Keywords:** cyber-physical system (CPS); microgrids; distributed secondary control (DSC); cybersecurity; Modbus; SMV; GOOSE; DNP3; vulnerabilities



**Citation:** Gupta, K.; Sahoo, S.; Panigrahi, B.K.; Blaabjerg, F.; Popovski, P. On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids. *Energies* **2021**, *14*, 4941. <https://doi.org/10.3390/en14164941>

Academic Editor: Alberto-Jesus Perea-Moreno

Received: 3 July 2021

Accepted: 11 August 2021

Published: 12 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

According to the IEEE Grid Vision 2050, smart grid is anticipated to comprise of an automation and control framework over entire power grids for efficient and reliable bidirectional power flow [1]. The tight integration of critical power and underlying cyber infrastructure in addition to the progress in sensors, communication technologies and renewable energy sources aid in accomplishing a complex paradigm of cyber-physical systems [2,3]. In recent years, cybersecurity has become a notable threat to modern-day power systems due to the extensive integration of communication technologies. Moreover, any infiltration in the cyber domain can also impede on the physical security of the power systems due to the deep integration of physical and cyber domains [4–6]. Consequently, evaluating and developing cyber-physical system security is therefore of utmost importance to the future electricity grid.

In recent decades, numerous cyber attacks have been revealed in the energy sector with diverse impacts at various levels [7,8]. While some attacks could not be located at all, others were devastating both economically and to human life. The first major attack occurred in 1982 when a gigantic gas pipeline blast took place [9]. The Stuxnet attack in Iran revealed the threat that cyber attacks represented to power utility control systems [10]. On 23 December 2015, a wide blackout in Kyiv, Ukraine, occurred for several hours via a cyber attack, which impaired three major distribution companies and more than 225,000 customers [11]. One year later, another Kyiv-based cyber attack took place in 2016, during which the hackers shut off 20% of the city's electrical energy consumption [12]. The rapid rise of these incidents represents a real threat. The massive impacts of these incidents have led governments worldwide to diagnose these emerging threats. In 2010, the National Institute of Standards and Technology Internal Reports (NISTIR) 7628 published guidelines for smart grid cybersecurity [13] principles, in which microgrid cybersecurity was considered as a major threat scenario.

A microgrid is a cyber-physical infrastructure whose physical layer (which should not be confused with the one used in communication systems) consists of the power infrastructure (such as DGs, including power electronics devices, transformers, loads and circuit breakers), sensors (responsible for sensing information on the current state of the system), actuators (to implement control decisions) and controllers. Moreover, the cyber layer consists of devices such as switches, routers as well as wired and wireless communication links (CLs) [14], which are responsible for delivering information to relevant layers. The controllers at the intersection of the physical and cyber layers have identified a common subset layer, which is called the control layer. This layer is comprised of control devices (the local controller (LC), secondary controller (SC), master controller (MC)) and human operators. This layer receives data from the sensor layers and decides on a control action to be executed, which is carried through the communication infrastructure if necessary [15]. The utilized communication networks may expose MG components (i.e., communication links, the LC, SC and MC) to potential cyber attacks [16]. Similarly, physical security boundaries can also be violated by physical breaches affecting all layers. It is essential that the operation of the microgrid should not be affected by failures in either the physical or the information and communication technology (ICT) infrastructure [17]. Therefore, it is of prime importance that the impacts of cyber attacks are assessed as well as identified, and that effective countermeasures for enhancing the cybersecurity measures are developed. To carry out the validation of these approaches, a testbed can provide an effective platform.

Several smart grid testbeds have been developed, some of which are listed in Table 1. Every testbed has its own unique features and functions. The features a testbed can provide depend on the devices and communication protocols integrated. As one moves from the fully simulated system to the integration of actual hardware devices and communication protocols, there is an enhancement of the realistic environment provided by the testbed. In this paper, the interaction of two devices (OP-5700 and RTAC) provides a co-simulation environment with the physical layer and partial cyber layer emulated in OP-5700 and the partial cyber layer in RTAC with actual network devices such as switches, routers and an Ethernet interface. The testbed integrates standard communication protocols such as SMV, GOOSE, Modbus and DNP3 at various levels of the microgrid system. The execution architecture defines the span and flexibility of the testbed. The centralized mechanism [18] concentrates all devices in a system and locally performs data acquisition, whereas the distributed mechanism integrates multiple devices working harmoniously and can be accessed both locally and remotely. The centralized mechanism, on the one hand, is easy to use, but lacks in terms of flexibility and expansion. In this regard, most testbeds have a distributed execution mechanism [19–22]. In addition, each testbed has its own objective which might include security, control, system performance and multiple objectives. Security-oriented testbeds focus on cybersecurity, communication security, physical security and mitigating the impacts of various attacks on the system.

**Table 1.** Taxonomy of cyber-physical smart grid testbeds.

Year: Testbed (Platform)	Targeted Objective	Distinctive Features	Communication Protocols	Tools
2013: [23] PowerCyber Testbed (Real-Time (RT) Co-Simulation)	Wide-area situational awareness, cybersecurity	Impact on voltage stability	IEC 61850, C37.118, Modbus, DNP3, OPC UA	RTDS, DigSilent
2013: [24] Florida State University (Controller Hardware in Loop)	Distribution grid management, demand response	Impact study on distributed control	TCP/IP	RTDS
2014: [25] Greenbench (RT Co-Simulation)	Cybersecurity	Impact study on power system dynamics	TCP/UDP	PSCAD, OMNeT++
2015: [18] Physical Co-Simulation Testbed (RT Co-Simulation)	Cybersecurity	Impact on wide-area voltage stability control	C37.118-2005, C37.118-2011	RTDS, RSCAD, DeterLab, NS-3
2016: [19] Microgrids Testbed (RT Co-Simulation)	System performance	Impact study on controllers	Modbus	Simulink, OPAL-RT, OMNeT++
2016: [20] Communication-Based Remote Access Testbed (Hardware)	Remote control, cybersecurity, wide-area situational awareness	Cloud communication for central controller with SCADA and relays	OPC UA, C37.118.1, C37.118.2, IEC 61850, Modbus	SkkyNet, Kepware, ReLab
2017: [21] Multifunctional CPS Testbed (RT Co-Simulation)	Cybersecurity	Impact study on multi-level control centres	DNP3.0, IEC 60870-5-104	RTDS, WANE
2017: [22] South Dakota State University (Hardware in Loop)	Cybersecurity and stability control of power system	Power system protection and control	DNP3.0, SEL-C662	OPAL-RT, RT-lab
2018: [26] (Real-Time Testbed)	Hierarchical microgrid control	Multi-agent control and protection	IEC61850, DDS	FIPAs, DDS Middleware
2019: [27] (Offline Co-Simulation)	Power systems cybersecurity and control verification	Economical as offline	TCP/IP	EMTDC/PSCAD, OMNeT++, MATLAB
2020: [28] (RT Co-Simulation)	Cybersecurity	Resource management study	IEEE 1815	NS-3, QEMU, HELICS, Opendnp3, GridLAB-D
2021: [29] (Controller Hardware in Loop Co-Simulation)	Cooperative control	Impact study on controllers with TCP/IP	TCP/IP	RT-LAB, OPNET
<b>2021: Testbed in this paper (RT Co-Simulation)</b>	<b>Cybersecurity, remote control, cooperative control and protection of microgrid</b>	<b>Impact study on standard protocols for cooperative control and protection with local/web-based HMI</b>	<b>SMV, GOOSE, Modbus, DNP3.0</b>	<b>OPAL-RT, Hypersim, RTAC, ACSELERATOR RTAC SEL-5033 software, ACSELERATOR Diagram Builder SEL-503</b>

The control-oriented testbed guarantees the correctness of the control logic developed for cyber-physical systems. The performance-oriented testbed evaluates the impact of network delay on the performance of the system as these smart grid testbeds are time-critical and may have devastating consequences with the introduction of delays. In addition to the sole objective mentioned above, a testbed may have multiple objectives. The proposed testbed focusses on cybersecurity in the control (local/remote) and protection architectures of a microgrid. It can be used to quantify the impact of various cyber-physical vulnerabili-

ties. The different physical and cyber vulnerabilities associated with the various devices in an electrical system are briefly discussed in the following section.

The key contributions of this paper can be summarized as:

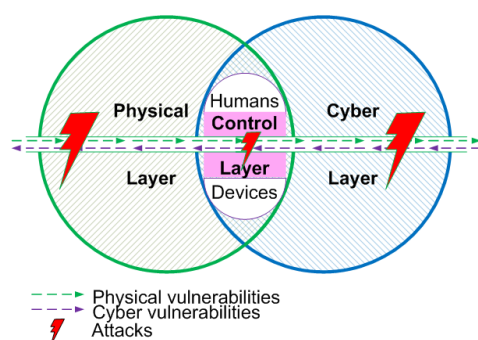
- We studied the usage of ICTs and their intermittency using tailored protocols in the testbed for both the cooperative control and protection architectures of microgrids;
- We validated the modeling of physical and cyber infrastructures of the test microgrid, which provides a real-time feasibility study of cyber attacks using different vulnerable points;
- We provided both local and fully web-based remote HMI access;
- We integrated actual switches and routers which aid in studying attack impacts on real network traffic;
- We assessed vulnerability—specifically in relation to the control and protection architectures of a microgrid system;
- We presented the basic modeling of some of the attacks which can penetrate system security and affect the control and protection architectures of a microgrid;
- We demonstrated the effect of a smart attack on the test microgrid.

The remainder of this paper is organized as follows. In Section 2, various cyber-physical vulnerable points and types of attacks are addressed. Furthermore, the cyber-physical infrastructure modeling of a test MG in OP-5700 and RTAC, in addition to switches, routers and an Ethernet interface is presented. Additionally, the integration of various recommended communication protocols (Modbus, SMV, GOOSE and DNP3), attack scenarios and their impacts on the control and protection architectures is demonstrated in the testbed. In Section 3, the effectiveness of the proposed control architecture with the communication interface is validated in a test islanded MG with four DGs, which can be extended to the required test case. Furthermore, the network packets and message exchanges are also demonstrated with the help of Wireshark (a network monitoring tool). The HMI available to the control user, serving as remote control, is further presented with the real-time results. In continuation, smart attack on  $\omega_{ref}$  is also demonstrated as an example. Section 4 articulates the features of the proposed testbed-like scalability; the inclusion of variants of a communication medium and protocols other than inbuilt in the simulation tools; capability to model various attack scenarios and extend to a more realistic environment by integrating various real devices in the loop, the platform for vulnerability assessment and the validation of the detection, mitigation and resilient algorithms against attack scenarios. Finally, concluding remarks and future research directions are presented in Section 5.

## 2. Testbed Development and Vulnerability Assessment

Advancements in electronic and communication technologies have led to an increase in the attack surface, thereby creating more vulnerable nodes in the smart grid architecture. Each device in the system has its own vulnerability and with the integration of each device or communication interface, the attack surface is further increased. As shown in Figure 1, the attackers can infiltrate via any of these paths to cause devastating impact on all layers. Some of the cyber and physical vulnerabilities and attacks in different layers of the electrical system are pictorially depicted in Figure 2, followed by a detailed description. They compromise the security and reliability with rising concerns over the stability and economic issues. Several recent works have conducted investigations into the vulnerable points, attack categorization, impact analysis and proposition of solutions in cyber-physical domains. This research work presents a detailed real-time co-simulation environment to provide a platform for the identification of various attack surfaces and studying the impact of various attacks.





**Figure 1.** Interaction between physical and cyber layer vulnerabilities.

In Figure 2, the physical layer is comprised of conventional energy sources (such as alternator), modern energy sources (such as solar and wind), a diesel generator, transformers, a circuit breaker (CB), transmission lines, cables, loads (such as industrial and residential), sensors (such as the hall effect sensor for current), measurement devices (such as a current transformer (CT), potential transformer (PT) and phasor measurement unit (PMU)) and actuators. The sensors, measurement devices and actuators are hard-wired to the remote terminal unit (RTU). The RTU is an interface between sensors/transducers and communication systems. The cyber layer consists of a communication medium (wired or wireless), different devices (such as the switch, router and gateway). A switch connects devices in a network (such as the local area network (LAN)), while the router connects devices across multiple networks, such as LAN and wide-area network (WAN). The virtual private network (VPN) is used to securely connect the network outside LAN, however, they are still susceptible to attacks. The gateway, on the other hand, as the name suggests, is a passage to connect two networks together that may work upon different networking models. The information provided by RTUs (a key element of supervisory control and data acquisition (SCADA)) to system operators in the control/maintenance center (for state estimation, economic dispatch) is asynchronous and relatively slow to capture many short-duration disturbances on the grid. Alternatively, PMUs are regarded as the key element of a wide-area monitoring system (WAMS), capturing voltage and current with a rate up to 200/240 frames per second. Furthermore, they provide time-stamps of each sample accurately with high-speed and coherent real-time information of the power system, which is not available from legacy SCADA systems. The WAMS architecture includes the time server, Ethernet clock, global positioning system (GPS) antenna and GPS satellite, as shown in Figure 2. However, this article will only focus on the SCADA system. In SCADA architecture, the control layer consists of devices such as programmable logic controllers (PLCs) for controlling, relays for protection, HMI to locally monitor (with a limited controlling option) the status of the network. Furthermore, the different physical and cyber vulnerabilities of this architecture and its potential attacks are illustrated in Figure 2.

Cyber-physical attacks either include physical breaches into the system and damaging the devices; or compromising them without touching any equipment, e.g., by causing electromagnetic damage such as overvoltage or an electromagnetic pulse. Emission security (EmSec) physical attacks are attacks which depend on the heat, light, sound, or the electromagnetic radiation emissions coming out of the system [30]. Intrusion into the hardware supply chain in this category can manipulate the physical processes and cause the failure of costly equipment. Unauthorized physical access can have destructive consequences on any of the layers. Similar to physical attacks, attacks on the cyber layer may be accomplished with actual physical communication links or virtual network access. The first category includes either breaking down the communication channel (channel jamming), delivering falsified messages known as false data injection attacks (FDIA), (e.g., GPS spoofing), as well as replaying and relaying messages. For the second category, the attacker may manipulate the code to change the firmware or the software. They can exhaust the devices by making them constantly carry out the actions without allowing them to enter power saving mode—also known as sleep deprivation. Moreover, the network can be made inaccessible

by forcing a large number of unnecessary packets in the path, commonly termed as denial of service (DoS) attacks [30,31]. These also include command manipulation, malware injection, man-in-the-middle, packet sniffing and VPN attacks. As shown in Figure 2, cyber attackers can infiltrate locally (by a malicious laptop or storage device in the substation) or remotely, by infiltrating the network and gaining unauthorized access from the control layer affecting the remaining layers all the way down to the physical layer. However, these are only a few and do not represent all the vulnerabilities of a smart grid architecture. With the further development of technologies, more attack surfaces will come and hence vulnerabilities will increase.

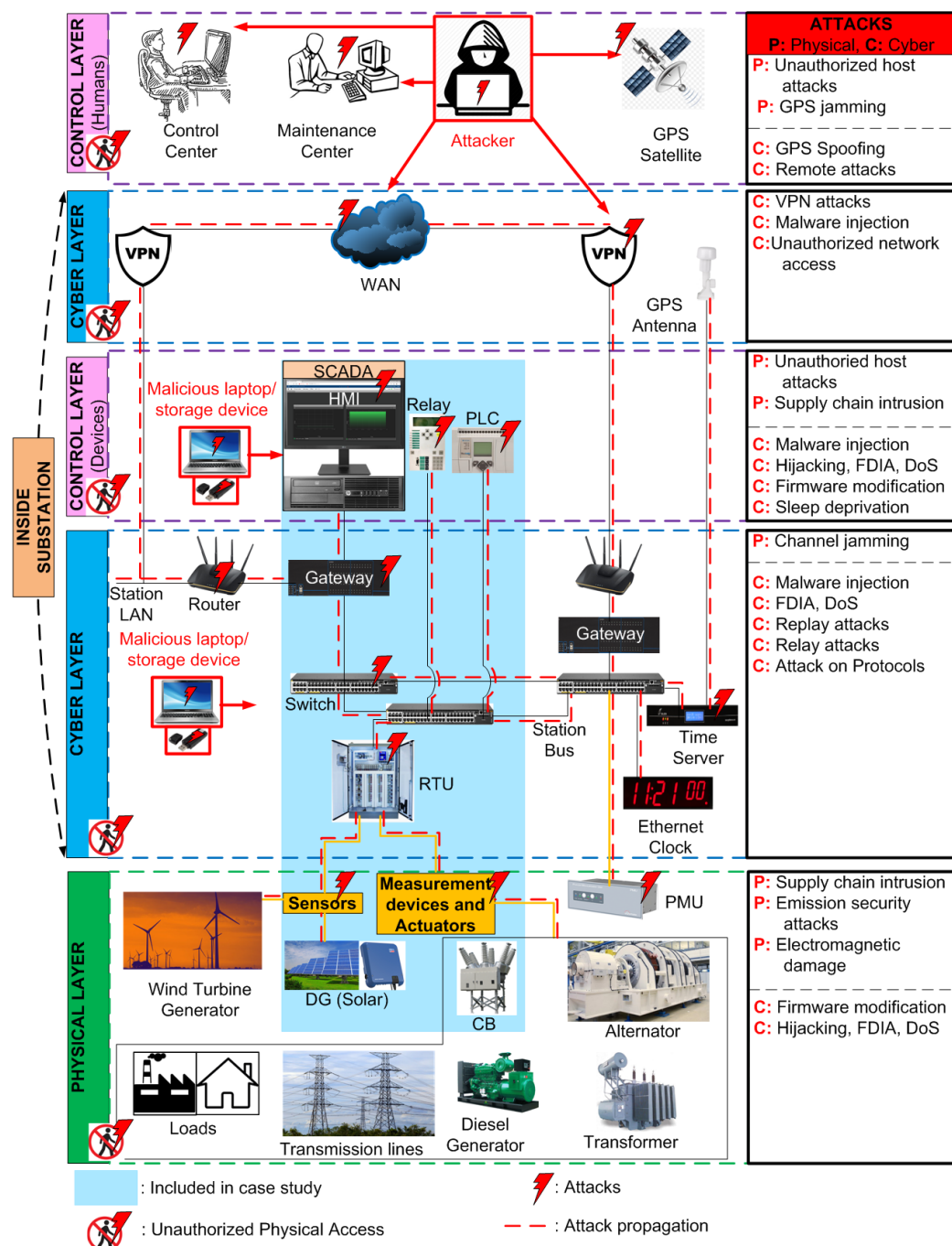


Figure 2. Bird-eye view of vulnerabilities in microgrids.



In this paper, we primarily focus on a cyber-physical AC microgrid, as shown in Figure 3, which can be extended to a grid-connected microgrid, and a networked AC/DC microgrid. As shown in Figure 2, we will discuss the shaded blue portion in further sections.

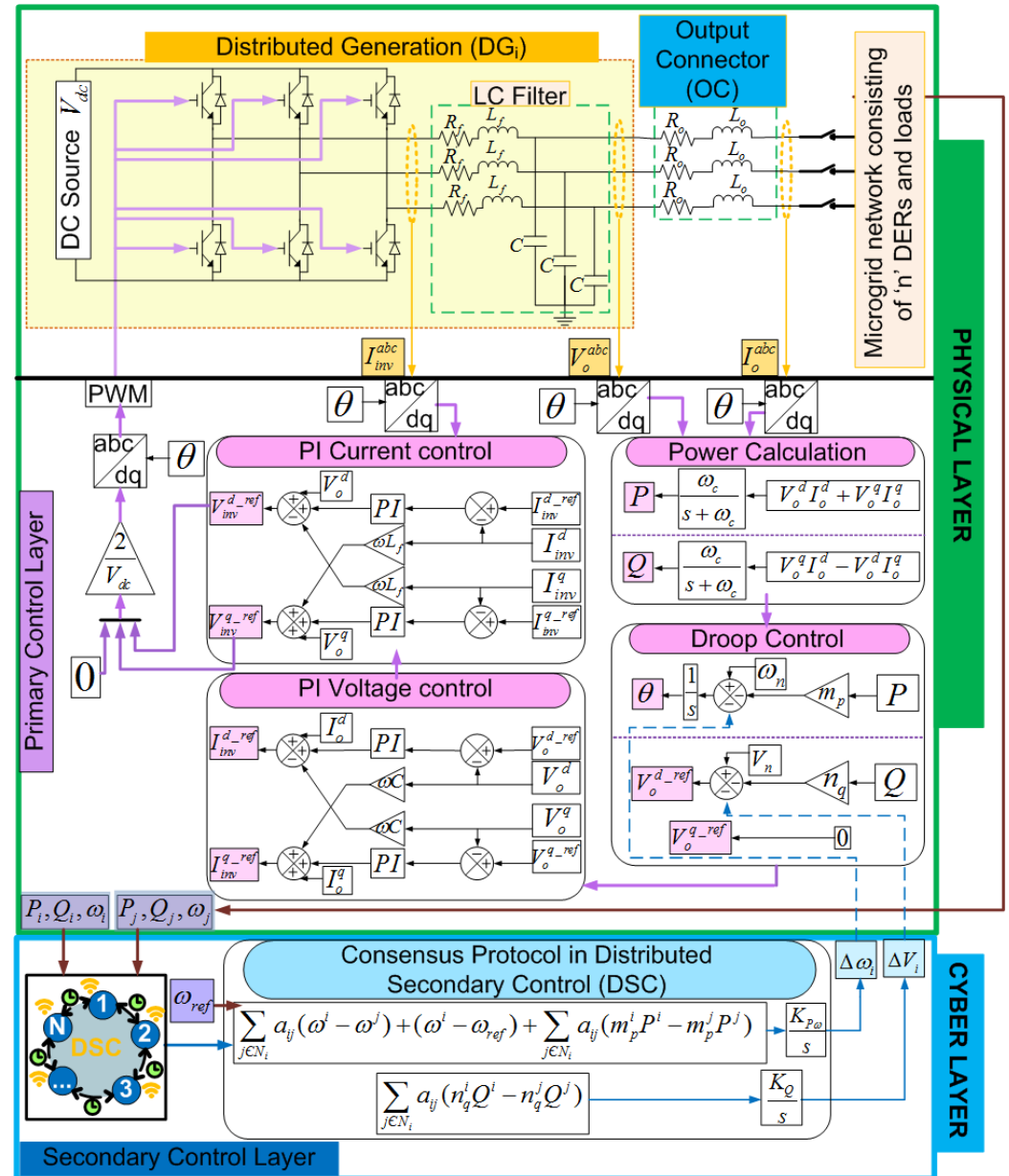


Figure 3. Overall control architecture for an AC microgrid in a cyber-physical model.

For the development of a real-time co-simulation testbed and the vulnerability study of such a system, a three-fold approach was carried out. It comprises of physical layer modeling, cyber layer integration with communication protocols to interact with physical model and vulnerability assessment. Moreover, they have been extended to attack categorization, impact analysis for different attacks scenarios on the islanded AC microgrid test model. As stated above, a microgrid provides a promising solution to integrate and manage heterogeneous energy sources to autonomously run in an efficient manner [32]. This distinctive feature of microgrids is a prominent factor in enhancing their resiliency under extreme events owing to their hierarchical control architecture. This architecture has recently become an operational standard for microgrids, consisting of the primary, secondary and tertiary control levels.

In the control layer, the primary control (PC) level consists of inner voltage, current control loops and droop control. The secondary control level is responsible for frequency restoration as well as voltage regulation and aids in proportional active and reactive power sharing. The tertiary control level manages the flow of active and reactive power between the microgrid and the upstream grid in grid-connected mode [33]. The primary and secondary controls are shown in Figure 3. When comparing Figure 3 with Figure 2, it can be observed that the DG, sensors and primary controller all reside in the physical layer. These measurements were further carried by RTUs for secondary controller (PLC in this case), residing in the control layer linked by the cyber layer through protocols in a communication medium. Similar to one DG shown in Figure 2, 'N' DGs can be connected with these controllers interacting through a distributed secondary control (DSC) architecture with the  $\omega_{ref}$  signal generated by the master controller.

This paper more specifically considers the secondary control level, as it plays a vital role in guaranteeing the reliable operation of a microgrid to critical customers at the nominal voltage and frequency values after the microgrid loses support from the main grid, making it operate in an off-grid mode from grid-connected mode. The secondary control level can either adopt centralized or distributed communication architectures. Compared to conventional centralized secondary control architecture, distributed secondary control is relieved from a reliability bottleneck related to a single point of failure. Moreover, it offers more flexibility, plug-and-play ability, scalability [34], as well as less communication overhead with improved transient performance, as demonstrated in [3]. The distributed control architecture is presented in Figure 3 with the objectives of:

1. Frequency restoration:

$$\lim_{t \rightarrow \infty} \omega_i(t) = \omega_{ref} \quad (1)$$

2. Proportional active power sharing:

$$\lim_{t \rightarrow \infty} [m_p^j P^j(t) - m_p^i P^i(t)] = 0 \quad (2)$$

3. Proportional reactive power sharing:

$$\lim_{t \rightarrow \infty} [n_q^j Q^j(t) - n_q^i Q^i(t)] = 0 \quad (3)$$

where  $j \in N_i$ , i.e., all the immediate neighbors of  $i$ th DG.

As presented in the above equations, a secondary controller removes the steady state error introduced by the primary controller and maintains the frequency of the network at the reference value provided by the MC. Similarly, active and reactive power are proportionally shared among all DGs to the network. As illustrated in [35], the objective of proportional reactive power sharing does not guarantee voltage regulation, and hence may lead to poor bus voltage profiles in a microgrid in many cases. The accuracy of reactive power sharing depends on both the line reactances and the allowable bounds of voltage in a microgrid. Furthermore, a tunable compromise between reactive power sharing and voltage regulation can ensure satisfactory operation. However, in this case, only proportional reactive power sharing is considered.

The cyber-physical layout of the islanded MG topology with the secondary controllers under consideration is presented in Figure 4, where the internal modeling of DGs is the same as that presented in Figure 3. The line and load data with DG parameters (common to all four DGs) are tabulated in Table 2 and the control parameters of the secondary controller are listed in Table 3. As shown in Figure 4, after sensing the information from sensors, the primary controller transmits the control signal to its respective DG. This is a local controller which has no network access. Furthermore, to improve steady-state performance, a secondary controller is incorporated, which interacts with neighboring secondary controllers through distributed secondary control architecture and generates a control signal for its respective primary controller. The reference signal (frequency in this case) is given by the

MC. These control signals travel through communication links (wired/wireless). The information for a particular protocol travels through these communication links with specified operational delays (selected depending on the particular application).

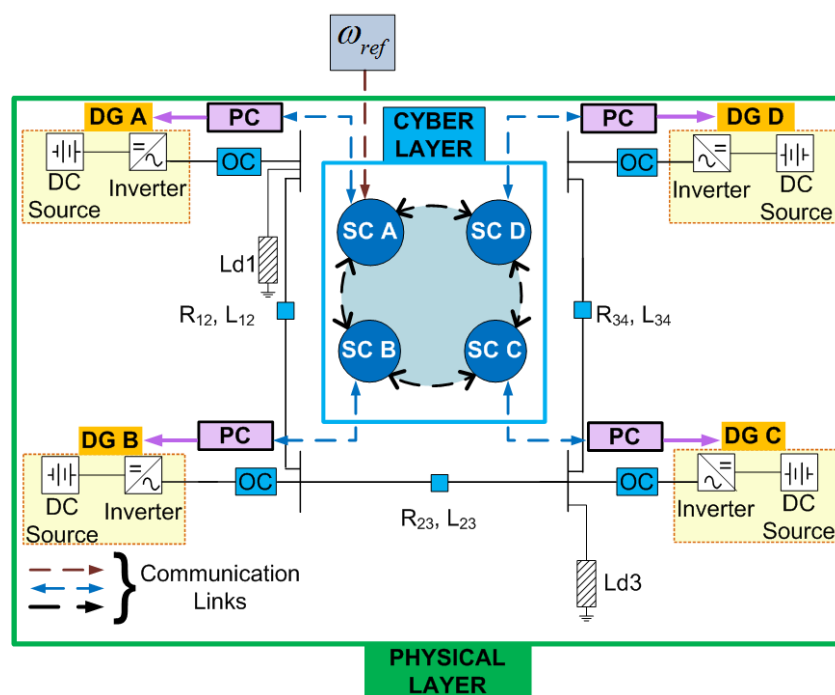


Figure 4. The control network of an islanded AC microgrid testbed.

Table 2. Parameters of the microgrid test system in Figure 4.

Active power droop coefficient	$m_p$	$9.4 \times 10^{-5}$	
Reactive power droop coefficient	$n_q$	$1.3 \times 10^{-3}$	
Voltage controller proportional gain	$K_{pv}$	0.2	
Voltage controller integral gain	$K_{iv}$	1	
Current controller proportional gain	$K_{pc}$	50	
Current controller integral gain	$K_{ic}$	100	
Line parameters	$Line_{12}$	$R_{12} = 0.23 \, \Omega$	$L_{12} = 318 \, \mu H$
	$Line_{23}$	$R_{23} = 0.35 \, \Omega$	$L_{23} = 1847 \, \mu H$
	$Line_{34}$	$R_{34} = 0.23 \, \Omega$	$L_{34} = 318 \, \mu H$
Load parameters	$Load_1 (Ld1)$	$P_1 = 36 \, kW$	$Q_1 = 36 \, kVAr$
	$Load_3 (Ld3)$	$P_3 = 45.9 \, kW$	$Q_3 = 22.8 \, kVAr$

Table 3. Control parameters of secondary controller in Figure 4.

Gains	$K_{p\omega}$	40
	$K_Q$	1.5
Reference frequency	$\omega_{ref}$	$2\pi \cdot 50$

In addition to the previously presented external physical and cyber vulnerabilities, the microgrid control and protection system is also affected by the inherent time delays in the network; hence, the selection of a proper standard communication protocol is of the utmost importance to the communication interface. Various authors have presented several communication protocols for data exchange between each level of devices in this regard. The authors in [36] present the operation of a small-scale microgrid using IEC 61850. Moreover, the authors in [26] have proposed a hybrid agent framework combining the foundation for intelligent physical agents (FIPAs), IEC 61850, and data distribution service

(DDS) standards. As proposed in [37], the information exchange between the primary controller and secondary controller is over Modbus protocol. Furthermore, SIWG [38], CA Rule 21, and CSIP [39] recommend the Modbus protocol for the internal communications of a DER client and converter controller, similar to interface applied herein. In [40], the OPC-UA protocol was used to implement consensus-based distributed control, whilst Ref. [41] uses CAN bus. Since the distributed secondary control is based on peer-to-peer communication, the publish–subscribe architecture suits this framework where the data of one agent (frequency, active/reactive power in this case) are published over the network and are subscribed to by the assigned agents to generate their control decisions after computation through the consensus protocol, as shown in Figure 3. Many recent works have applied several of these protocols such as DDS, MQTT, AMQP, GSE [42], ZeroMQ [37]. As interoperability standards are needed to address the heterogeneous nature of smart grid data, the IEC 61850 has emerged as a widespread interoperability standard which can be used for communication in a distributed control architecture. The SMV protocol is used here to transmit and receive the consensus variables at a 4 kHz sampling rate. To monitor and control the microgrid, HMI is used. It interacts with the microgrid system with DNP3 protocol as also recommended in [38].

The real-time co-simulation testbed setup, presented in Figure 5, provides an environment to interface the detailed model of a microgrid with real communication protocols over an Ethernet-based network, with actual network devices (switches, communication channel, etc.). Here, the physical and cyber network of the test microgrid are emulated in OP5700 through HYPERSIM software; and SEL-3530 RTAC hardware with HMI is used for local/remote monitoring and control. The creation and management of HMI is carried out in the ACSELERATOR Diagram Builder SEL-5035 software. The signals (active/reactive power, frequency, voltage) are monitored over HMI. With the HMI being a fully web-based platform, no additional software is needed other than a web browser. It can be viewed through a web browser on a remote computer with the features of providing role-based access, logging data, enabling alarms. The signals can also be monitored on digital storage oscilloscope (DSO).

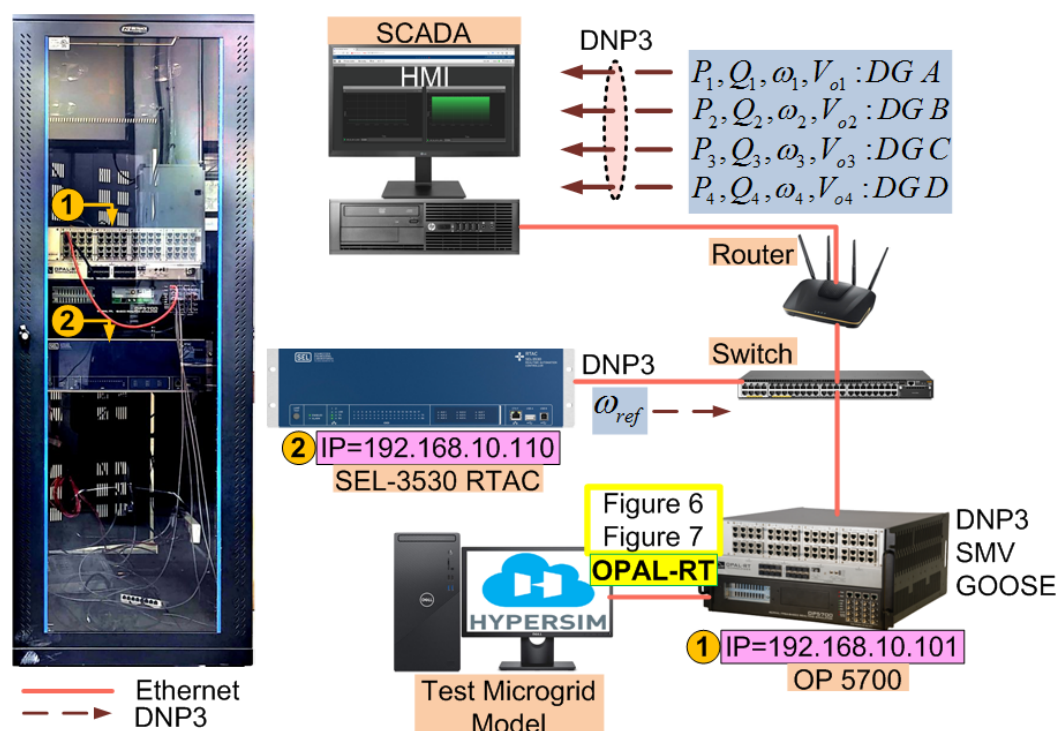


Figure 5. Testbed setup.

The setup for the test microgrid with the various attack surfaces to study the impact of various attacks in this testbed is presented in Figure 6. To name a few, these attacks can be DoS, FDIA and message replays.

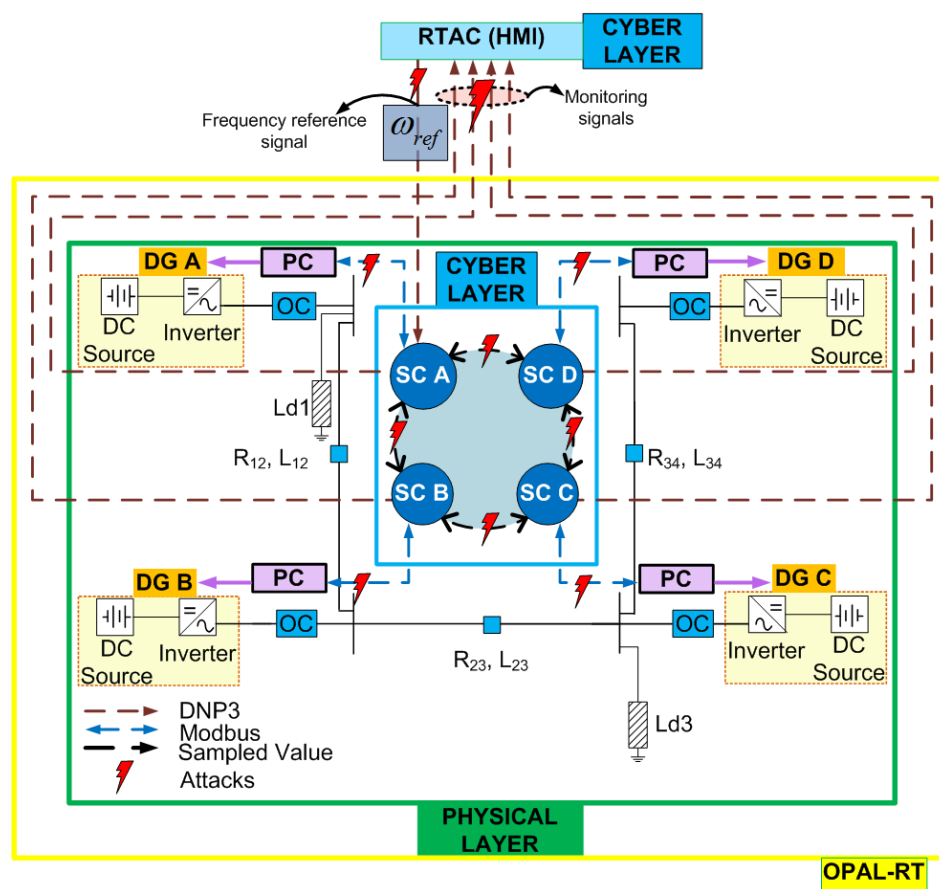


Figure 6. Control architecture of a test microgrid in the testbed.

Similarly to secondary controllers, communication between relays is also crucial for sensing the updated current, voltage and frequency to rigorously perform the fault detection and isolation process by sending updated control signals to circuit breakers. Many authors have presented the compatibility of centralized protection schemes with the IEC 61850 protocol in microgrid applications [43]. However, as stated previously, centralized schemes may have catastrophic impacts on even a single point failure. In addition, centralized approaches rely on huge amounts of data exchanges, requiring high communication infrastructure capabilities and exhaustive computation powers to accomplish the required task of system protection and power restoration. In contrast, distributed or agent-based protection schemes require only local and neighboring information exchanges for the decision, hence providing an effective real-time communication architecture. Moreover, IEC 61850 with the logical node definition offers fast data exchanges with a peer-to-peer communication capability among two or more devices [44–46].

Since microgrids have complex cyber-physical interdependencies, extensive efforts have been made to develop data communication standards for protection in the International Electrotechnical Commission (IEC) 61850 international standard, with strict constraints on communicating fault-related messages, such as the 4 ms time limitation levied on SMV and GOOSE messages [45]. SV messages are used to transmit voltage and current signals from merging units (MUs) to the protective devices. The prime objectives of the GOOSE message is to send a trip signal to the CB to isolate the faulty section from the system and for peer-to-peer relay communications [47]. A switched Ethernet network is used for the communication of both these messages. Therefore, designing control algorithms for a protection system is a delicate and complex procedure. This complexity is



further escalated for example when dealing with an adaptive protection algorithm design in which the association between multiple agents, namely intelligent electronic devices (IEDs), for identifying and isolating faults, is time-critical. This communication standard can be implemented in the test microgrid, as shown in Figure 6. The vulnerable points to generate attack scenarios in this testbed architecture are also presented in Figure 6.

Given the well-established merits of distributed control schemes over centralized control methodologies, the transition from current central controllers to future distributed schemes is inevitable. Despite its significant advantages, the distributed cooperative control framework, similarly to other cyber-physical systems, is vulnerable to cyber attacks as it relies on the local sensing of current/voltage variables and a communication network to exchange local variables, and there is no central entity to monitor the overall cyber scenario. Clearly, the robustness and availability of the communication infrastructure is an important prerequisite for the success of microgrid control and contemporary adaptive protection algorithms [48].

Considering the typical cooperative control system of a microgrid, each component with associated vulnerability and attacks based on Figures 6 and 7 is summarized below:

#### 1. CYBER VULNERABILITIES:

- **Secondary controller:** Distributed cooperative controllers can be implemented on PLCs with communication networks [40], making the secondary controllers as well as data transmission vulnerable to cyber threats, as investigated in many recent works [49,50].
- **HMI:** Through this interface, the operator can monitor the dynamic changes in the network and send the command signals (if enabled). The attackers can infiltrate HMI by exploiting its software vulnerabilities from a remote site or through malware injections and disrupt the signals observed, presenting a false state of the system.
- **Communication links:** It can be wired or wireless and could be manipulated by attackers or distorted by the environment.
- **The routers and gateways:** DoS, packet mistreating attacks (PMAs), routing table poisoning (RTP), hit and run (HAR), persistent attacks (PAs) are some of the common possible attacks on routers, which either disrupt the system or inject harmful packets, helping the attackers gain access to the network. Since the gateway is a crucial link in the flow of information between different sensors, interfaces and equipment are among the main targets of attackers. DoS attacks and gaining access to the I/O mapping table to manipulate the process in order to cause disruption are among the attacks preventing operators from viewing and taking correct actions.
- **Protocols:** The popularity of the IEC 61850 protocol is attributed to its ease of connection via the Ethernet (rather than traditional hard wired systems and the standard structure of message offering interoperability). These features prove advantageous to attackers as Ethernet-based networks are easily accessible, and as it is a standard protocol, attackers can know its structure and hence its vulnerability. A similar argument also applies to other protocols such as Modbus and DNP3 [51]. To cope up with attacks, various encryption algorithms are been used to produce variants of protocols. However, it should be noted that the computation time for these checks must adhere to the required time and must not impede upon performance. The control and protection systems require real-time signals to take decisions and any delay in this loop could result in losses as well as environmental disasters. An example can be seen in the smart grid concept where the communication infrastructure has eminent significance, especially when matching energy generation and consumption schemes. If energy demand and response balance is not met, the stability of the grid may be compromised and lead to brown- and blackouts. Therefore,



decisions for controlling various resources can have a drastic impact on the overall system behavior [52–54].

2. **PHYSICAL VULNERABILITIES:** The devices in the physical layer may include sensors, relays, circuit breakers, primary controllers and secondary controllers. Primary controllers realized on digital signal processors (DSPs) are operated locally and they are thus not vulnerable to cyber attacks, as typically they do not have network access, but may be damaged physically [40]. Similarly, infiltration in the hardware supply chain can degrade and damage the equipment and devices.

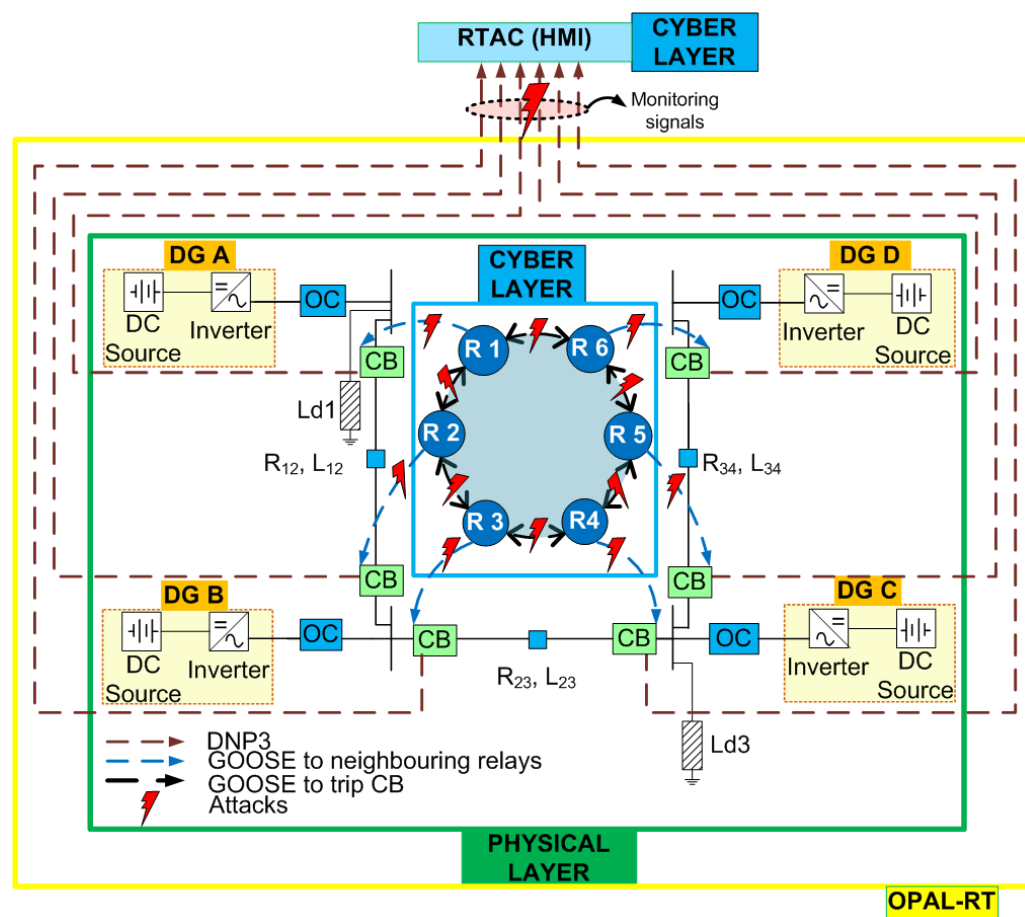


Figure 7. Protection network with communication protocols.

Figure 8 depicts physical devices constituting the components of the microgrid, sensors, control center and actuators. The microgrid includes the DG (in addition to power electronics devices), primary controllers (local to the DG), circuit breakers for the protection of the system, loads and network. The sensors include devices to measure the power, frequency, voltages and currents of the microgrid. These measured signals were then acquired by the controllers through a communication medium. These controllers can be locally present or can remotely access and control the system through SCADA. The control architecture comprises the secondary controllers and the protection architecture of relays. The figure represents 'N' agents (secondary controllers or relays) connected in distributed architecture through a communication medium. Furthermore, these control signals are transmitted to the actuators to perform the control action. In this regard, primary controllers receive the signal from secondary controllers and circuit breakers from relays. The communication medium presented can be wired or wireless and always work on a specified communication protocol. These protocols have been addressed in detail previously. These devices and protocols have individual vulnerabilities and the situation is aggravated when these are integrated. The attacker could exploit these vulnerabilities and enter the physical

and communication network to initiate attacks to have devastating effects on the system. The physical attacks may be on the physical devices such as the jamming communication channel intended for information exchange; intruding in the supply chain and damaging the equipment, including controllers and relays. The cyber attacks may be on the sensors, communication medium, controllers and actuators. These can be categorized as disclosure, deception, disruption attacks [55] depending on their impact on the system, compromising the confidentiality, integrity, and availability of information in smart grids. Confidentiality refers to the protection of information from unauthorized access and disclosure. Integrity ensures that the information is authentic and protected from unintended modifications. Availability guarantees that the information is available to all the intended users.

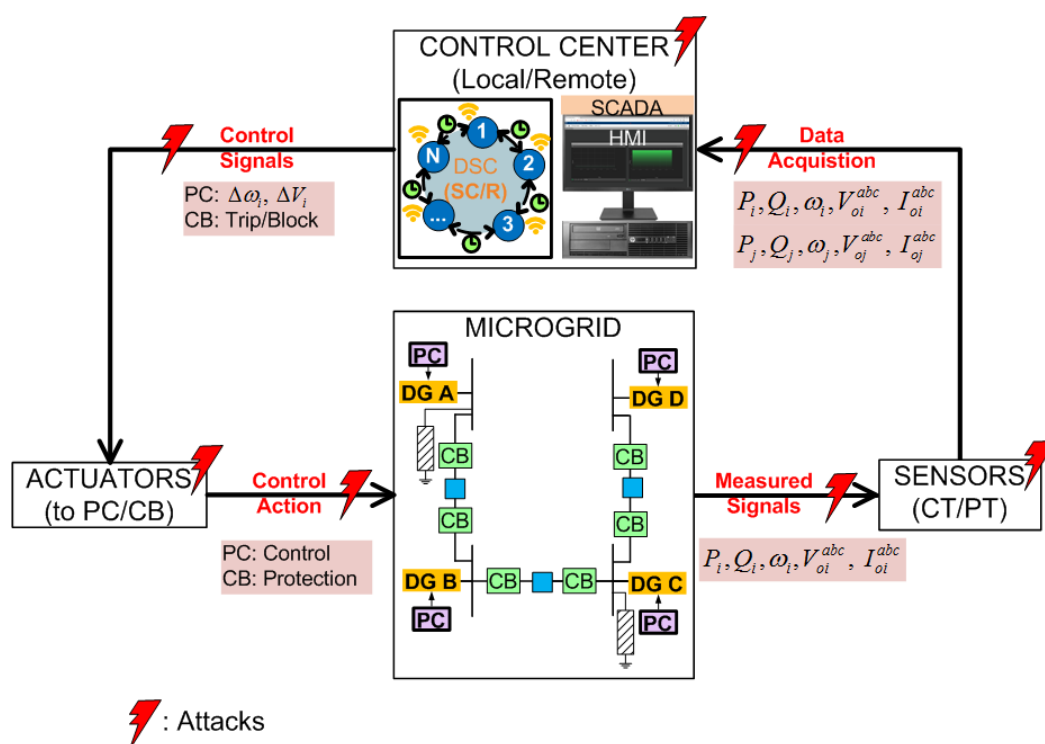


Figure 8. Attack surface view on the microgrid.

DoS is directed against the communication network, and either floods it with data packets or compromises specific devices to disrupt the data transfer [56]. These endanger the availability of communication system services [57], preventing the authorized user of a service to access that service [58]. The adversary may initiate an FDIA by spoofing a signal, either in the sensors, controllers or the communication network [59], which compromises the integrity of microgrid data. These can be launched on an individual node, which can be easily detected, or on many nodes in a coordinated manner in order to achieve a particular objective in a stealthy manner. By modifying information exchanging through communication networks, FDIA could cause the disruption of microgrid control functions, such as state estimation [60], voltage control [61], active power control [62], and load sharing [63]. These in turn (i) cause power outage for microgrid customers; (ii) delay the responses of DER to control and protection systems; (iii) synchronize DG to frequency reference values other than actual; and (iv) overload DERs or disregard the equipment thermal thresholds [50]. Hijacking the attack disrupts the update process of the consensus algorithm by completely substituting the existing signal with an external input [64]. The consequence of such attacks, alternatively referred to as random attacks, can impede the optimal performance of the microgrid, ultimately resulting in inevitable power imbalance [65].

It must be noted that a hybrid attack is also a prospect where multiple attacks are combined together to further intensify the attacking mechanism. An example to illustrate such a scenario can be a combination of DoS and FDIA. This will, on the one hand, modify the transmitted/received signals through FDIA, which propagates in the network to cause alarming situations. On the other hand, DoS would disrupt the communication and authorized access which would prevent the operators returning the system to its normal state. These attacks, with their influence on the control objectives of a microgrid, are tabulated in Table 4. The protection objective, intended to measure signals such as voltages, current and frequencies through sensors; compute the system state; and—if any deviation from normal operation is found—take the corrective action; is accordingly also hampered with the attack on the protection architecture.

**Table 4.** Outcomes of various attacks.

Types of Attacks		Objectives Fulfilled in Equations		Consequences
		Frequency Restoration (1)	Proportional Ac- tive and Reac- tive Power Shar- ing (2), (3)	
DoS		No	No	Prevents authorized access to data/service
FDI	Individual node attack	No	No	Disrupts network stability and control
	Coordinated node attack			
	CASE: I	Yes	No	Alters original active power sharing to gain additional profits
	CASE: II	No	Yes	Deviates system frequency affecting stability
	CASE: III	Yes	Yes	Remains stealth initially, later disorients the system operation
Hijacking		No	No	Deters optimal performance
DoS + FDI		No	No	Affects both accessibility and optimal operation

The attackers may be a disgruntled employee (ICS/IT), vendors, security guards or outsiders (cyber criminals, hacktivists, terrorists, cyber fighters) [66]. In any case, these attackers may damage CPS security and stability, as well as affect communication between protective devices. The challenge is that in a closely interconnected cyber-physical system, such as in a microgrid with adaptive protection, minor malfunctions in the cyber domain can have catastrophic impacts in the physical domain [67].

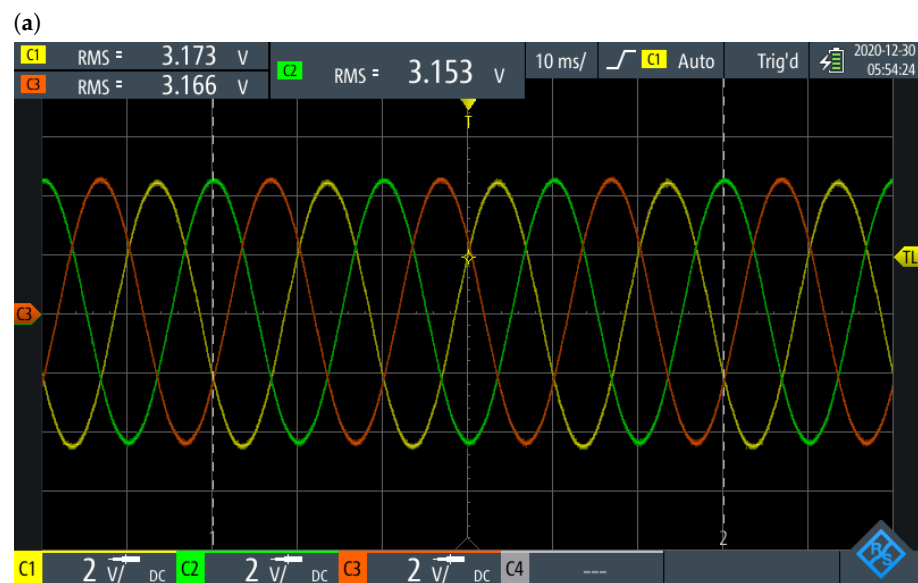
To enhance the security of CPSs under various cyber attacks of any AC, DC, networked or hybrid microgrid, suitable countermeasures need to be designed. These can generally be segregated into three tasks [55,68], namely (i) **prevention**: to safeguard the system from an attack [69]; (ii) **resilient operation**: to bear with the maximum influence of the attack and operate as close to the normal state as possible without causing serious harm to hardware assets, financial reparations or productivity costs [70–76]; and (iii) **detection and isolation**: to identify the origin of the attack, alienate the corrupted subsystems and return to the normal state as quickly as possible [77–82]. All these vulnerabilities and impacts of

attacks can be studied in the testbed so that relevant and effective countermeasures can be developed and validated.

### 3. Results on the Testbed

#### 3.1. Real-Time Simulation Results

After the modeling of physical and cyber layers in OP5700 through the HYPERSIM software, various signals of the MG test case are monitored on DSO (Figure 9) and in scopeview of HYPERSIM (Figure 10).

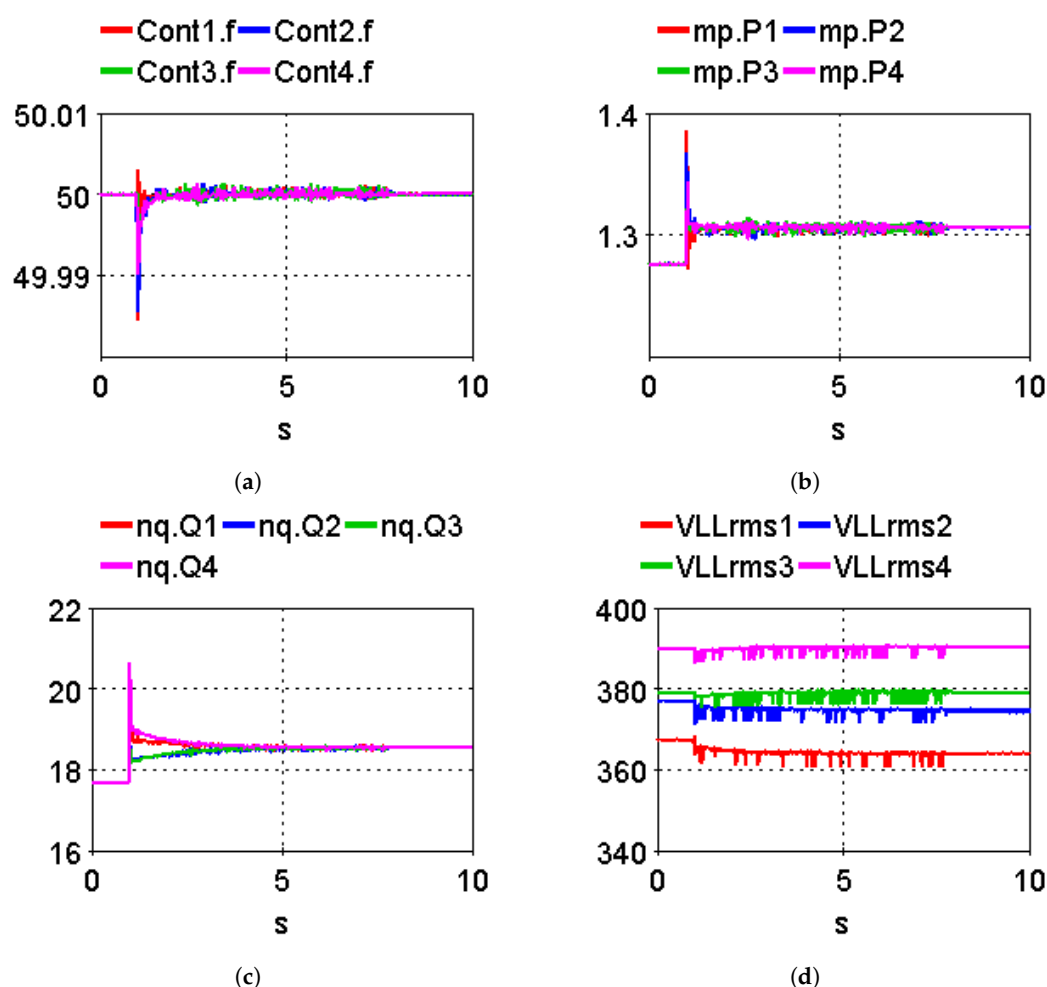


(b)

**Figure 9.** Real-time simulation results on DSO with respect to time (s) (a)  $V_o^{abc}$  (scaled down by 100); and (b)  $I_o^{abc}$  (scaled down by 10 A/V).

The captured three-phase voltage  $V_o^{abc}$  and current signals  $I_o^{abc}$  (Figure 3) at the bus of DG A (Figure 6) are presented in Figure 9a,b. As the maximum analog output from the OPAL-RT simulator is confined to  $\pm 16$ V, these signals must be scaled down to obtain the signals which would otherwise be saturated. The voltage signal is scaled down by 100 and the current signal by 10 A/V to obtain the corresponding voltage signals in DSO. The effectiveness of the control strategy is validated through the frequency of the power signals in the scopeview of HYPERSIM. Here, the objectives in Equations (1)–(3)

are satisfied, as seen in Figure 10a–c, maintaining the frequency at the nominal value of 50 Hz and accomplishing the proportional active and reactive power flow, even with a load increment of 4 kW at Ld1 at 1 second with constant DC sources. As mentioned earlier, the developed testbed only has three major objectives, namely frequency restoration as well as proportional active and reactive power sharing; however, the voltage of different buses is also within the operational range represented by line–line rms voltages (in V) in Figure 10d.



**Figure 10.** Real-time simulation results with constant DC sources on HYPERSIM with respect to time (s) with a 4 kW load (Ld1) increment at 1 s: (a) frequency restoration (frequency (Hz)); (b) proportional active power sharing; (c) proportional reactive power sharing; and (d) RMS values of  $V_o^{abc}$  (V).

### 3.2. Communication Protocols Established

In the testbed, as shown in Figures 6 and 7, the Modbus, SV and GOOSE protocols with both publisher and subscriber modules are established in OPAL-RT through the HYPERSIM simulation platform over the Ethernet interface, whereas the DNP3 master is established in RTAC whilst the slave resides in OPAL-RT. The network analysis tool Wireshark is installed on desktop on the same network to capture the packet and visualize the message exchanges. It can be observed in Figure 11 under the ‘Protocol’ column that the respective protocols are established in the testbed.

After the successful setting up of the DNP3 protocol between RTAC and OPAL-RT, the following controller message shown in Figure 12 with the number of successful and dropped packets can be seen.

Source	Destination	Protocol
192.168.10.110	192.168.10.101	DNP 3.0
192.168.10.101	192.168.10.110	DNP 3.0
192.168.10.110	192.168.10.101	TCP
192.168.10.110	192.168.10.101	DNP 3.0
192.168.10.101	192.168.10.110	DNP 3.0
Source	Destination	Protocol
SuperMic_78:21:90	Iec-Tc57_01:28:50	GOOSE
SuperMic_78:21:90	Iec-Tc57_04:01:00	IEC61850 Sampled Values
SuperMic_78:21:90	Iec-Tc57_04:01:01	IEC61850 Sampled Values
SuperMic_78:21:90	Iec-Tc57_04:01:02	IEC61850 Sampled Values
SuperMic_78:21:90	Iec-Tc57_04:01:03	IEC61850 Sampled Values

Figure 11. Packets over Wireshark.

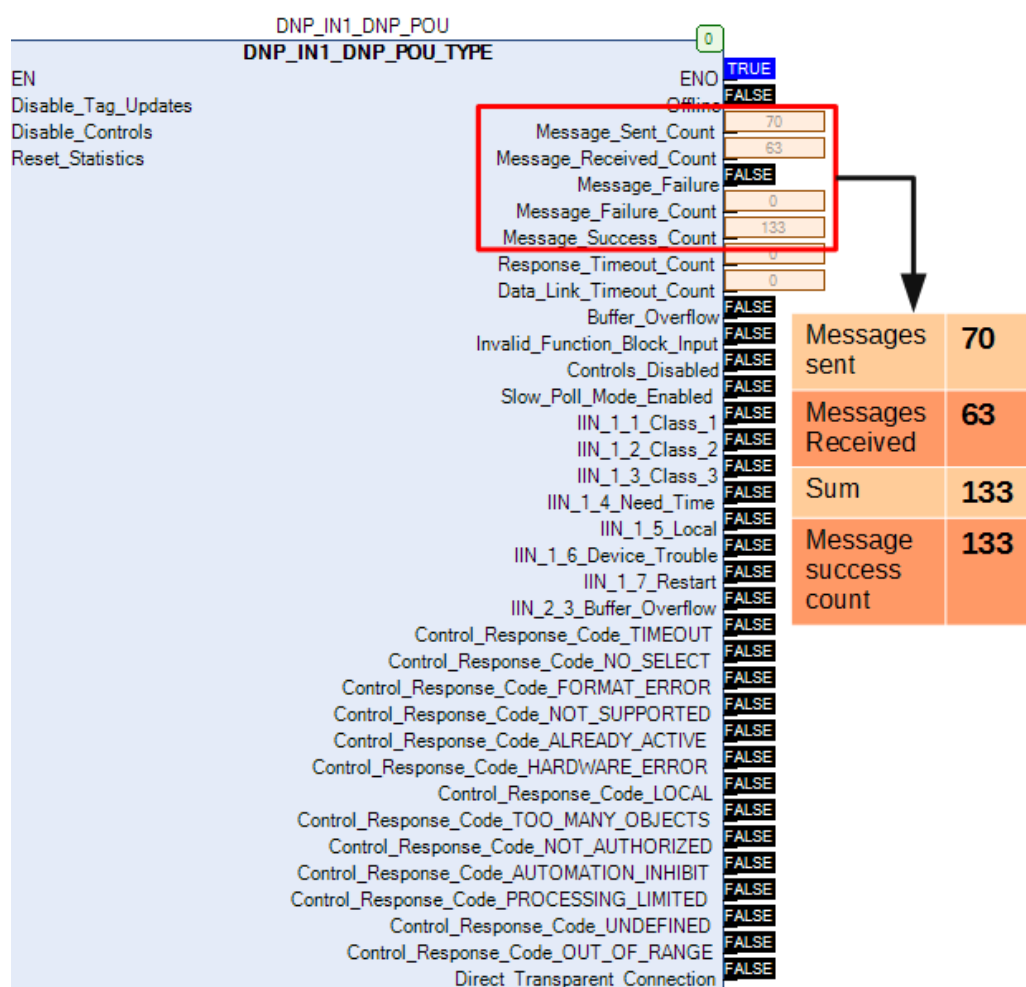


Figure 12. Data communicated over DNP3 on RTAC.

Here, the total messages sent are 70 and the total messages received are 63, which equals a total of 133 messages. As can be seen, the total message success count is 133 and the message failure count is 0, denoting reliable communication between the devices. Moreover, the data sent over the DNP3 channel are depicted in Figure 13, where the frequency (in Hz), the rms value of the voltages (in V), the active powers (in W), and the reactive powers (in VAR) are shown, respectively.



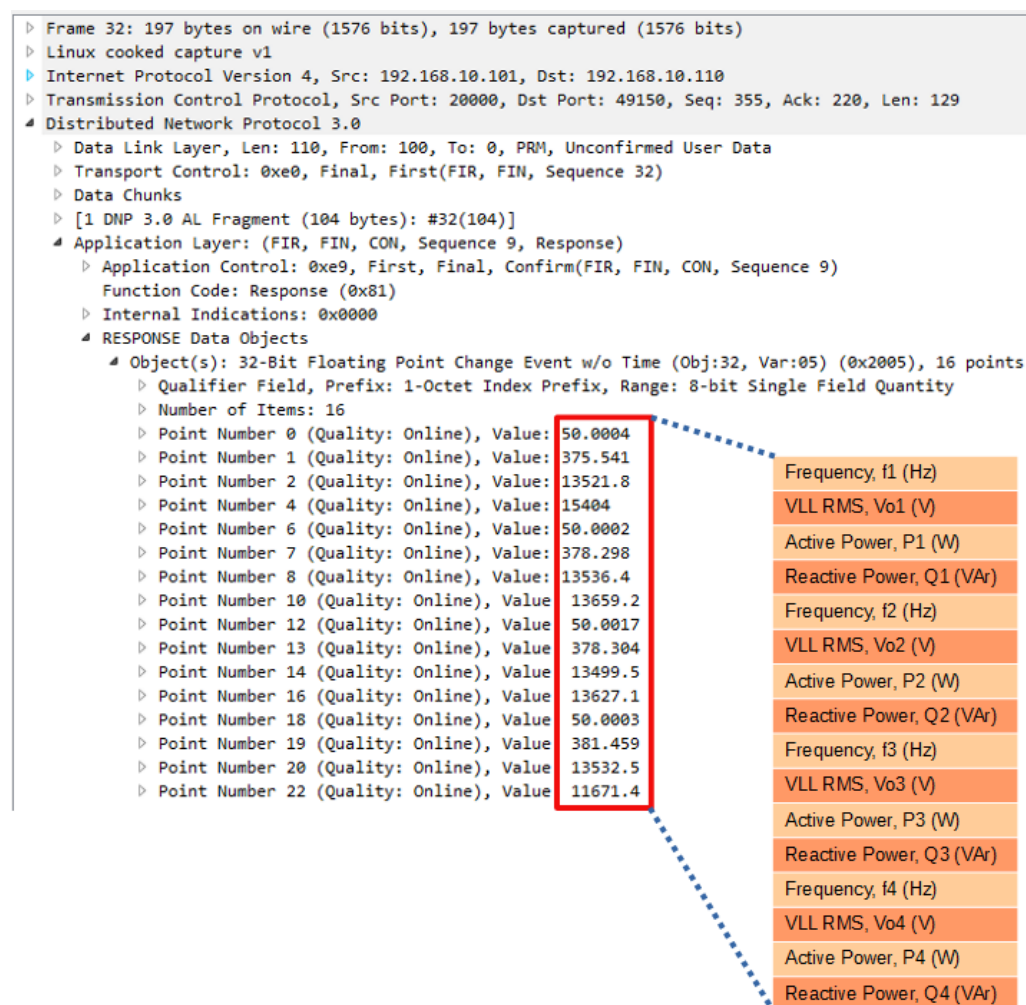


Figure 13. Data communicated over DNP3 on Wireshark.

To summarize, in the control network of the test microgrid, the following protocols are established, namely the Modbus protocol for information exchange between the primary and secondary controller; the sampled message values protocol for data exchanges by a secondary controller agent within its neighboring secondary controllers to set up a distributed control architecture; and the DNP3 protocol for monitoring and the reference signal generation from HMI. Similarly, in the protection network, the GOOSE protocol was established for the trip signal-to-circuit breakers and for peer-to-peer communication between the relay agents to set up the distributed protection architecture. Similarly to the control architecture, HMI is also integrated with the DNP3 protocol to observe the variations in the network.

### 3.3. HMI

The human-machine interface is the software part of the SCADA system, which is useful for controlling and logging data, alarm initiation as well as monitoring applications. It provides a graphical user interface to the operator which gives an overall view of the network under consideration, enabling (in many cases) to regulate its parameters for efficient, stable and reliable performance. However, in the testbed discussed, only monitoring signals and frequency reference signal information is exchanged. The ACSELERATOR Diagram Builder SEL-5035 software was used to create the interaction window for the user, as shown in Figure 14. This window can be locally or remotely accessed by any personnel through the web interface with proper login credentials. This platform was developed to monitor the signals. The signals being communicated can be observed in

Figures 15 and 16, which is according to the data communicated as shown in Figure 13, which are continuously updated with any dynamic changes in the network.

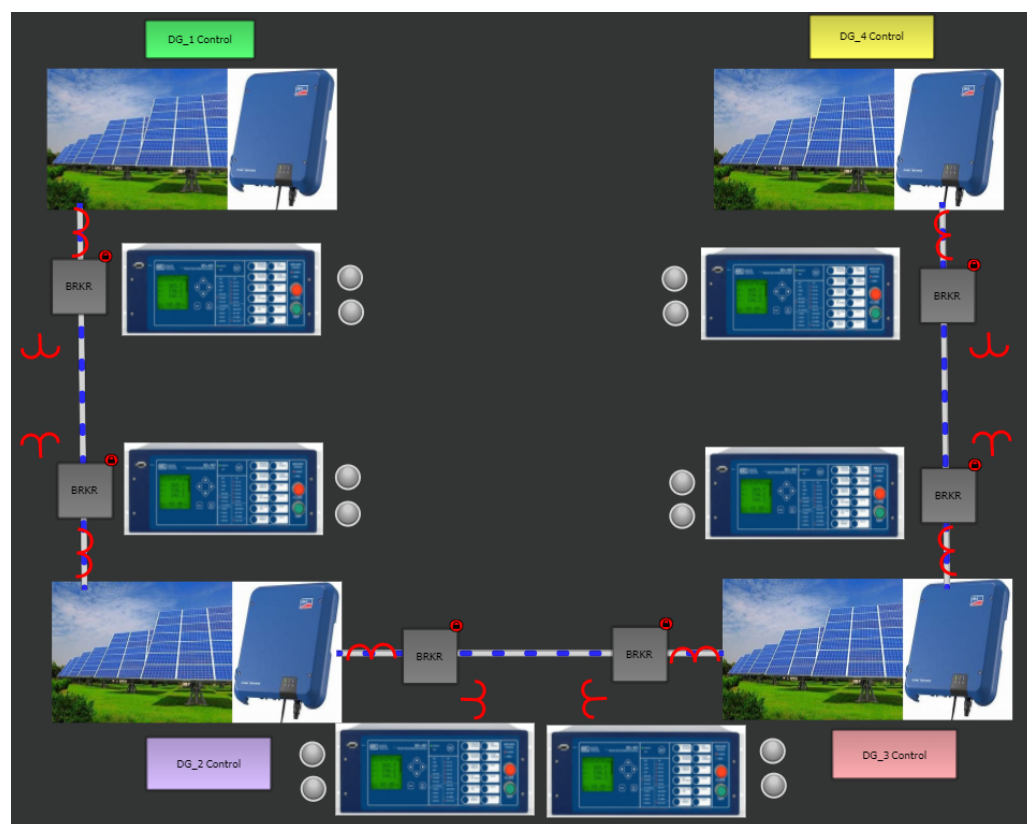


Figure 14. Human-machine interface (HMI) for the user.



Figure 15. Real-time values of frequency (Hz) in HMI.

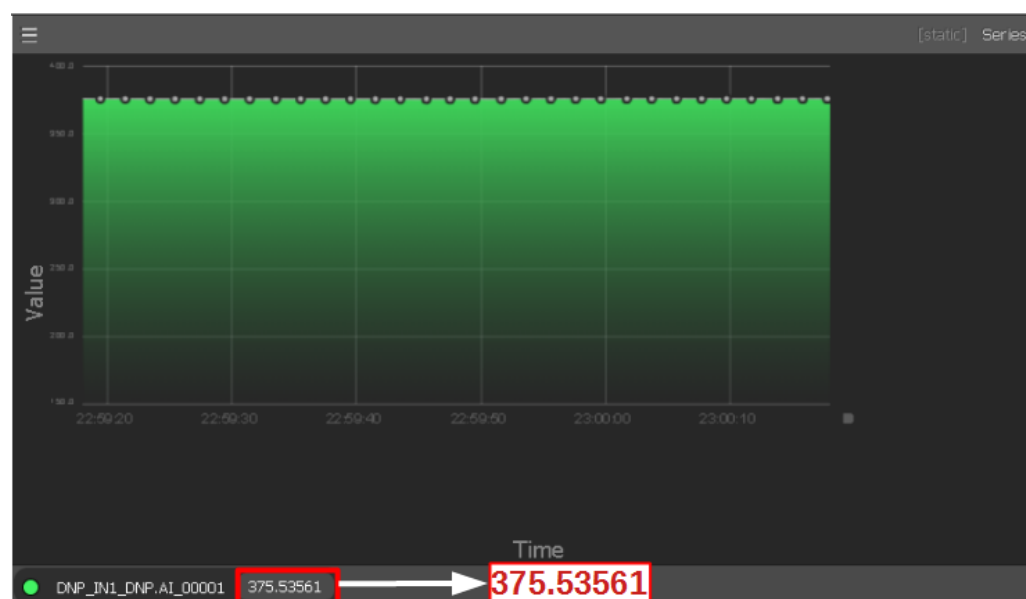


Figure 16. Real-time values of line–line Vrms (V) in HMI.

### 3.4. Attack Scenarios

While all the attacks mentioned are equally hazardous, FDIA poses greater danger due to the difficulty in its identification, as suggested by NIST [83]. Unlike other attack types, the system may appear to be functioning normally without noticing the existence of the FDIA and later on destabilize the system by the injection of unfair data. This type of attack is tabulated as CASE: III in Table 4, which is also termed as a smart attack. Figure 17a,b show a smart attack on  $\omega_{ref}$  where the system initially behaves normally (converges to the reference frequency signal with a smaller attack value) and is followed by disorienting the system with a higher attack value. More details about constructing these attacks can be found in [84,85]. Similarly, the impact analysis of various attacks can be observed in the testbed and respective countermeasures can be developed and validated.

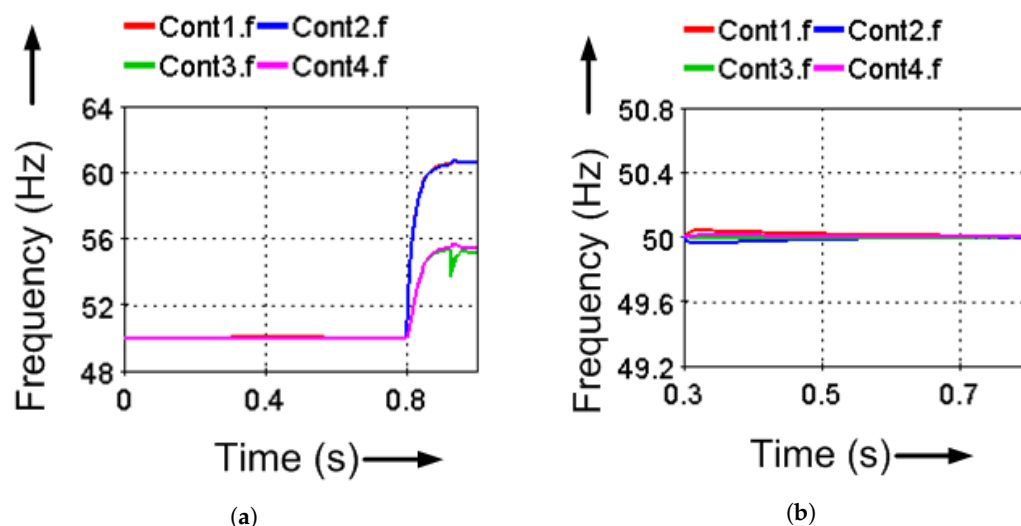


Figure 17. (a) Smart attack on  $\omega_{ref}$  initiated at 0.3 s; and (b) zoomed graph from 0.3 to 0.8 s of (a).

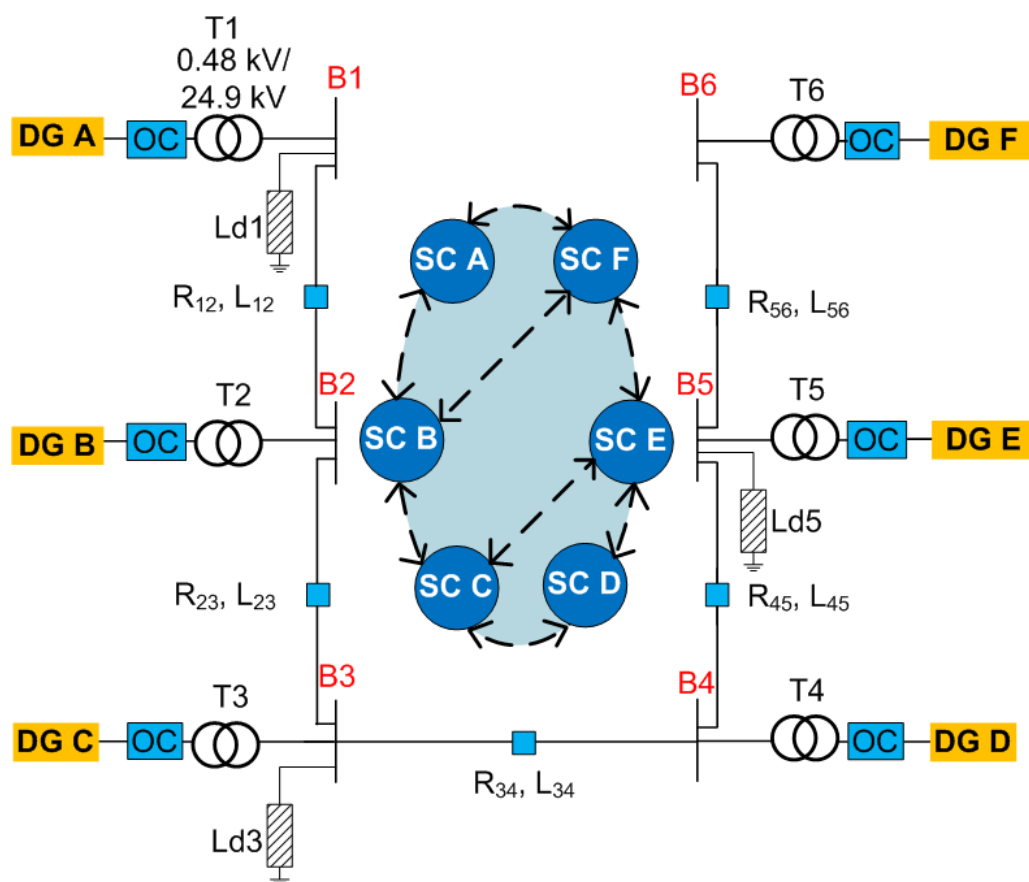
## 4. Features of Testbed

Cyber-physical system modeling and testing constitute a challenging research field with the integration of heterogeneous elements, complex architectures and communication protocols involved at different levels. This paper presents a real-time co-simulation testbed for cybersecurity applications in a microgrid. The testbed provides scalability to different

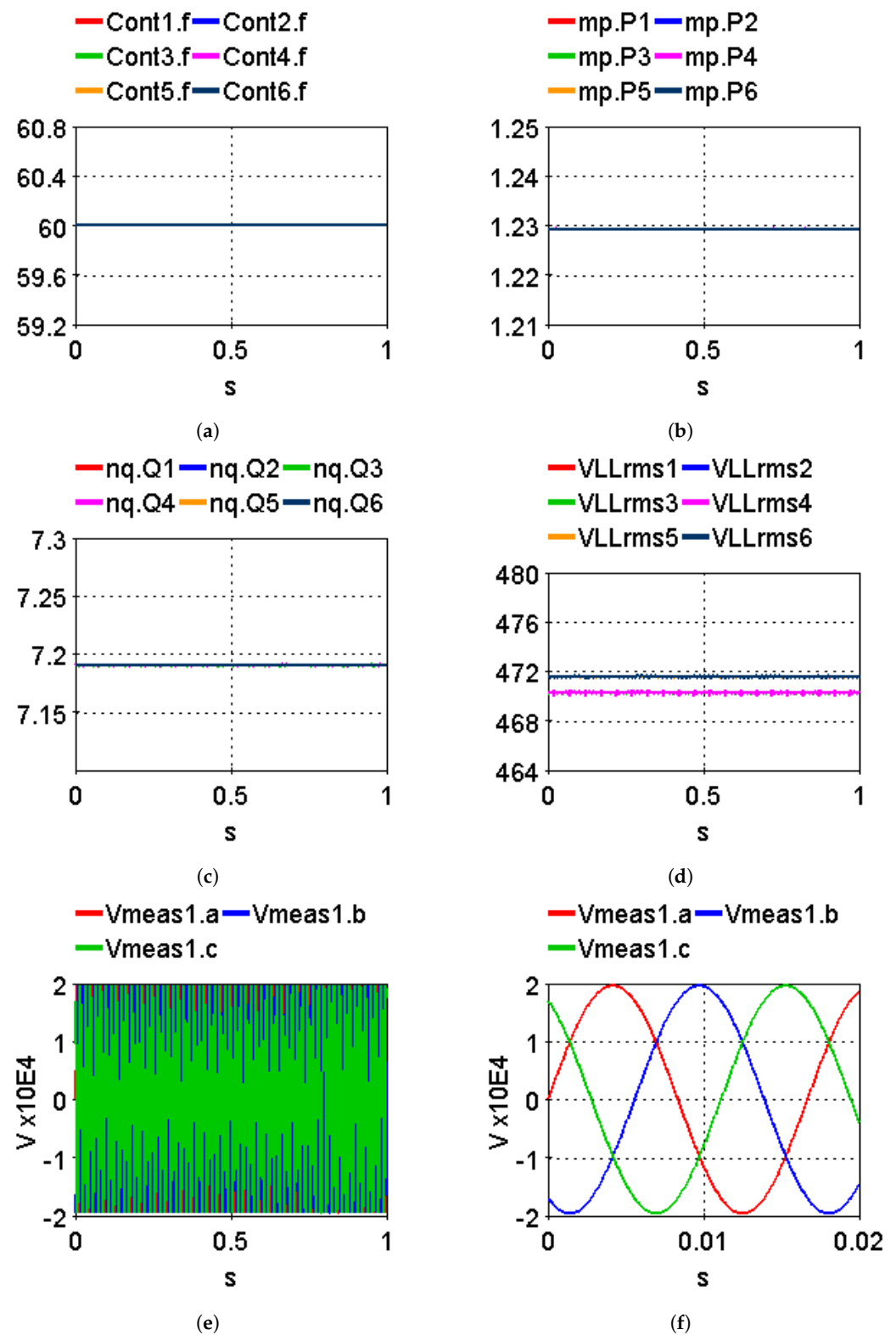
user-defined test cases; facilitates the integration of several standard and non-standard communication protocols; aids in the modeling of different attack scenarios; eases the extension to realistic scenarios; and provides a platform for vulnerability assessment and the validation of countermeasures against attacks. These salient features of the developed testbed are briefly discussed in this section.

#### 4.1. Scalability

The modeling of an islanded AC microgrid test case with four DGs was presented. Similarly, different architectures can be modeled. These may include AC grid-connected microgrids, DC microgrids, cooperative microgrids and hybrid microgrids. Furthermore, the comparison of different cyber layer graphs on the same physical microgrid architecture can be studied. In a similar manner, the performance of a cyber graph on different microgrid architectures can be studied. To demonstrate this feature, Figure 18 shows an islanded AC microgrid with six DGs. It has a radial network architecture and meshed cyber graph. The operating frequency of the microgrid is 60 Hz. Each DG is connected to the feeder through a wye–wye transformer with a voltage rating of 0.48/24.9 kV. Figure 19 shows the objectives fulfilled by this microgrid consisting of six DGs with transformers in a radial network with a meshed cyber graph. Figure 19a–f represent the frequency restoration, proportional active power sharing, proportional reactive power sharing, voltage across DGs, voltages at bus B1 and the zoomed version of bus B1. This clearly indicates that the objectives are satisfied in this microgrid. This can be further extended to propose and compare different control and protection algorithms.



**Figure 18.** Islanded radial AC microgrid with six DGs in addition to transformers and a meshed cyber graph.



**Figure 19.** Real-time simulation results in HYPERSIM with respect to time (s): (a) frequency restoration (frequency (Hz)); (b) proportional active power sharing; (c) proportional reactive power sharing; (d) RMS values of  $V_0^{abc}$  (V); (e) voltage at B1 (V); and (f) zoomed version of (e).

#### 4.2. Communication Protocol Variants

The testbed offers many inbuilt communication protocols which include C37.118, DNP3, IEC61850 and Modbus, as presented in Figure 20. In addition, a graphical user

interface (GUI) for the SMV publisher and subscriber modules with a sampling frequency (fs) of 4 kHz is represented in Figure 21. This shows the variables accessed by the user to establish this communication protocol. Similarly, the user can set up other standard protocols as well. Furthermore, the testbed is not only limited to these inbuilt protocols, as other communication protocols can also be established externally and integrated with the testbed, as presented in [41], where the CAN devices have been integrated in the simulator.

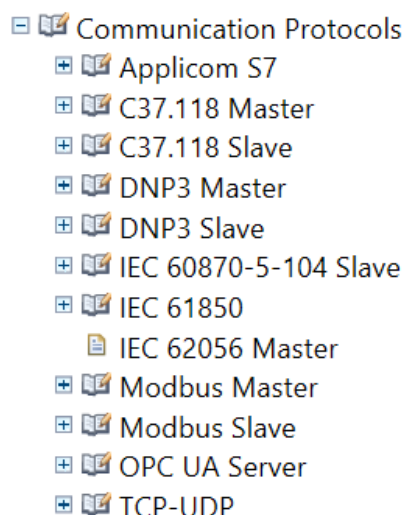


Figure 20. Inbuilt communication protocols.

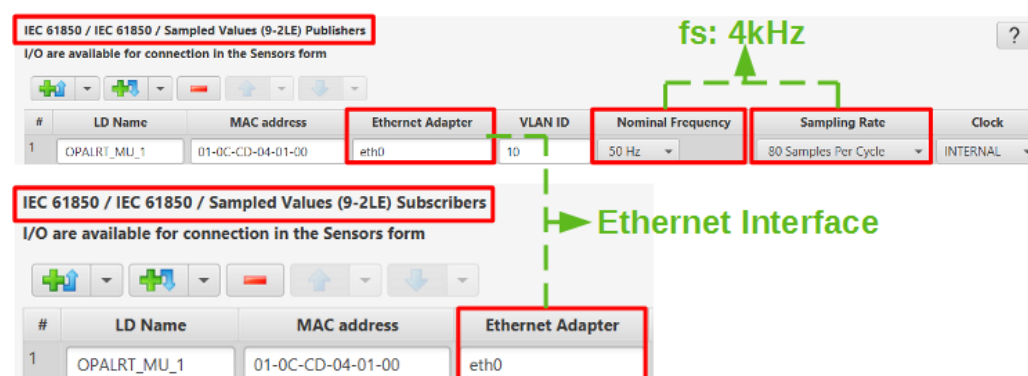


Figure 21. GUI for SV publishers and subscribers.

#### 4.3. Attack Modeling

As described previously, various attacks can be modeled and their impacts can be studied on the system. Some of these attacks with their locations and consequences are listed below in Table 5. Equation (4) specifies the data communicated by various devices such as the master controller, local controller and communication links:

Table 5. Attack variants.

Type of Attack	Attack Location	Consequences
DoS	CL	Stops the data stream
Time delay	LC, MC, CL	Delays the data exchanges
FDI	LC, MC, CL	Manipulates the data



$$\varepsilon = \begin{cases} \omega_{ref} & : MC \text{ data} \\ \omega^i, P^i, Q^i & : LC \text{ data} \\ \omega^j, P^j, Q^j & : CL \text{ data} \end{cases} \quad (4)$$

Equation (5) presents the modeling of the denial of service, time delay and false data injection attacks. These attacks are modeled over the communicated data, as represented in Equation (4):

$$\varepsilon^a(t) = \begin{cases} \eta \cdot \varepsilon(t) & ; \eta = 0 : DoS \text{ attack} \\ \varepsilon(t - \tau) & ; \tau > 0 : Time \text{ delay attack} \\ \alpha \cdot \varepsilon(t) + \beta & ; \alpha \neq 1 \text{ and } \beta \neq 0 : FDI \text{ attack} \end{cases} \quad (5)$$

where  $\varepsilon$  : variables to be attacked on;

$\varepsilon^a$  : Variables during attack;

$\eta$  : DoS attack variable;

$\tau$  : Time delay attack value;

$\alpha$  : FDI attack scaling value;

$\beta$  : FDI attack value; and

$\varepsilon, \eta, \tau, \alpha, \beta$  can be time-invariant or time-variant.

#### 4.4. Extension to More Realistic Scenarios

Different types of testbeds such as simulation-based, controller hardware in loop (C-HIL), power hardware in loop (P-HIL), power testbed and full system are presented in Table 6. There is a trade-off for these testbeds on the grounds of cost, fidelity and coverage. The cost refers to the expenditure required to build, develop and maintain it; test fidelity defines the closeness to a real-world system with the inclusion of hardware devices and a communication interface (with latencies); and test coverage represents the list of test conditions that can be performed safely on the developed testbed.

**Table 6.** Validation platform variants.

Testbed	Characteristic		Testbed Cost	Test Fidelity	Test Coverage
	Actual Devices	Simulated Devices			
Simulation	None	All	Low	Low	High
C-HIL	Controller	Rest	Moderate	Moderate (less)	High
P-HIL	Controller and one power equipment	Rest	High	Moderate (more)	Moderate
Power testbed	Scaled down DER equipment	None	High	Moderate (more)	Low
Full system	All	None	High	High	Low

The developed testbed is comprised of simulated physical and cyber layers on different systems coupled to each other with actual communication devices (switches, routers) and real communication protocols. This can be further extended by integrating actual controllers and relays in the testbed to enhance the closeness to realistic scenarios.

#### 4.5. Assessment Platform

The shaded area of Figure 2 is included in the testbed. It is comprised of DGs, sensors, measurement devices, a primary controller, a secondary controller in OP-5700, and an HMI in RTAC with real communication devices (switches, routers) and standard communication protocols—as further represented in Figure 6. The vulnerabilities in devices (switches, routers) and communication protocols can be explored. Furthermore, the whole architecture of Figure 2 can be modeled with actual devices in the loop to extend it to other validation platforms, as mentioned in Table 6, increasing the attack surface area. The newer vulnerabilities with the integration of these several devices and communication protocols with different communication media can be further investigated. Furthermore, with the modeling of attacks, different attack scenarios can be generated and their impact on the system can be investigated and the countermeasures developed can be validated on the testbed.

#### 5. Conclusions

This paper developed a real-time co-simulation testbed and provides an overview of the vulnerability of the AC microgrid in islanded mode. It presents the possible cyber and physical breaches to exploit the security breaches of the microgrid test system. It also developed basic attack models and demonstrates the impact of smart attacks on the test microgrid.

To summarize, the implementation and validation of the testbed will help researchers in planning the installation of modern infrastructures, label vulnerabilities across different operational layers and understand interoperability issues such as control, protection, stability, etc. The security of the protocols implemented is a next challenge which will be studied in the future.

**Author Contributions:** Conceptualization, K.G. and B.K.P.; methodology, K.G. and B.K.P.; software, K.G. and B.K.P.; validation, K.G. and B.K.P.; investigation, B.K.P., S.S., F.B. and P.P.; resources, B.K.P. and S.S.; writing—original draft preparation, K.G. and S.S.; writing—review and editing, K.G., B.K.P., S.S., F.B. and P.P.; visualization, B.K.P., S.S., F.B. and P.P.; supervision, B.K.P., S.S., F.B. and P.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

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

#### Abbreviations

The following abbreviations are used in this manuscript:

AMQP	Advanced Message Queuing Protocol
CAN	Controller Area Network
CA Rule 21	California Rule 21
CBs	Circuit Breakers
C-HIL	Controller Hardware in Loop
CL	Communication Link
CPS	Cyber-Physical System
CSIP	Common Smart Inverter Profile
CT	Current Transformer
DDS	Data Distribution Service
DERs	Distributed Energy Resources
DGs	Distributed Generations
DNP3	Distributed Network Protocol
DoS	Denial of Service
DSC	Distributed Secondary Control
DSO	Digital Storage Oscilloscope

DSP	Digital Signal Processor
EmSec	Emission Security
FDIA	False Data Injection Attack
FIPAs	Foundation for Intelligent Physical Agents
GOOSE	Generic Object-Oriented Substation Event
GPS	Global Positioning System
GSE	Generic Stream Encapsulation
GUI	Graphical User Interface
HAR	Hit and Run
HMI	Human–Machine Interface
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEDs	Intelligent Electronic Devices
I/O	Input/Output
IT	Information Technology
LAN	Local Area Network
LCs	Local Controllers
MC	Master Controller
MGs	Microgrids
MQTT	Message Queuing Telemetry Transport
MUs	Merging Units
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal Reports
OC	Output Connector
OPC UA	Open Platform Communications Unified Architecture Unified Architecture
PA	Persistent Attacks
PC	Primary Controller
P-HIL	Power Hardware In Loop
PI	Proportional Integral
PLC	Programmable Logic Controllers
PMA	Packet Mistreating Attacks
PMUs	Phasor Measurement Units
PT	Potential Transformer
RT	Real Time
RTAC	Real-Time Automation Controller
RTP	Routing Table Poisoning
RTU	Remote Terminal Unit
SC	Secondary Controller
SCADA	Supervisory Control and Data Acquisition
SIWG	Smart Inverter Working Group
SMV	Sampled Measured Values
SV	Sampled Value
VPN	Virtual Private Network
WAMS	Wide-Area Monitoring System
WAN	Wide-Area Network

## References

1. Simard, G. *Smart Grid Research: Power-IEEE Grid Vision 2050*; IEEE: Piscataway, NJ, USA, 2013. [\[CrossRef\]](#)
2. Faheem, M.; Shah, S.B.H.; Butt, R.A.; Raza, B.; Anwar, M.; Ashraf, M.W.; Ngadi, M.A.; Gungor, V.C. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* **2018**, *30*, 1–30. [\[CrossRef\]](#)
3. Duan, J.; Wang, C.; Xu, H.; Liu, W.; Xue, Y.; Peng, J.-C.; Jiang, H. Distributed control of inverter-interfaced microgrids based on consensus algorithm with improved transient performance. *IEEE Trans. Smart Grid* **2017**, *10*, 1303–1312. [\[CrossRef\]](#)
4. Sorebo, G.N.; Echols, M.C. *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid*. Available online: <https://www.routledge.com/Smart-Grid-Security-An-End-to-End-View-of-Security-in-the-New-Electrical/Sorebo-Echols/p/book/9781439855874> (accessed on 11 August 2021).

5. Teixeira, A.; Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S. Cyber security analysis of state estimators in electric power systems. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5991–5998.
6. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [CrossRef]
7. Loukas, G. Cyber-Physical Attacks: A gRowing Invisible Threat. Available online: <https://www.elsevier.com/books/cyber-physical-attacks/loukas/978-0-12-801290-1> (accessed on 11 August 2021).
8. Liu, C.-C.; Stefanov, A.; Hong, J.; Panciatici, P. Intruders in the grid. *IEEE Power Energy Mag.* **2011**, *10*, 58–66. [CrossRef]
9. Reed, T.C. At the Abyss: An Insider's History of the Cold War. Available online: <https://lightsailed.com/catalog/book/at-the-abyss-an-insiders-history-of-the-cold-war-thomas-reed/9780307414625/> (accessed on 11 August 2021).
10. Stuxnet. June 2015. Available online: <https://en.wikipedia.org/wiki/Stuxnet> (accessed on 11 August 2021).
11. 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; Volume 388.
12. Condliffe, J. *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for iNfrastructure Attacks*; MIT Technology Review: 2016. Available online: <https://www.technologyreview.com/2016/12/22/5969/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/> (accessed on 11 August 2021).
13. Introduction to NISTIR 7628 Guidelines for Smart GRID Cyber Security. Available online: [https://www.nist.gov/system/files/documents/smartgrid/nistir-7628\\_total-2.pdf](https://www.nist.gov/system/files/documents/smartgrid/nistir-7628_total-2.pdf) (accessed on 11 August 2021)
14. El Shafie, A.; Niyato, D.; Hamila, R.; Al-Dhahir, N. Impact of the wireless network's PHY security and reliability on demand-side management cost in the smart grid. *IEEE Access* **2017**, *5*, 5678–5689. [CrossRef]
15. Venkataramanan, V.; Hahn, A.; Srivastava, A. CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency. *IEEE Trans. Smart Grid* **2019**, *11*, 1055–1065. [CrossRef]
16. Mazumder, S.K.; Kulkarni, A.; Sahoo, S.; Blaabjerg, F.; Mantooth, A.; Balda, J.; Zhao, Y.; Ramos-Ruiz, J.; Enjeti, P.; Kumar, P.R.; et al. A review of current research trends in power-electronic innovations in cyber-physical systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**. [CrossRef]
17. He, D.; Chan, S.; Zhang, Y.; Wu, C.; Wang, B. How effective are the prevailing attack-defense models for cybersecurity anyway? *IEEE Intell. Syst.* **2013**, *29*, 14–21. [CrossRef]
18. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [CrossRef]
19. Nelson, A.; Chakraborty, S.; Wang, D.; Singh, P.; Cui, Q.; Yang, L.; Suryanarayanan, S. Cyber-physical test platform for microgrids: Combining hardware, hardware-in-the-loop, and network-simulator-in-the-loop. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5.
20. Cintuglu, M.H.; Mohammed, O.A. Cloud communication for remote access smart grid testbeds. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5.
21. Zhang, H.; Ge, D.; Liu, J.; Zhang, Y. Multifunctional cyber-physical system testbed based on a source-grid combined scheduling control simulation system. *IET Gener. Transm. Distrib.* **2017**, *11*, 3144–3151. [CrossRef]
22. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [CrossRef]
23. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
24. Stanovich, M.J.; Leonard, I.; Sanjeev, K.; Steurer, M.; Roth, T.P.; Jackson, S.; Bruce, M. Development of a smart-grid cyber-physical systems testbed. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.
25. Wei, M.; Wang, W. Greenbench: A benchmark for observing power grid vulnerability under data-centric threats. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 2625–2633.
26. Cintuglu, M.H.; Youssef, T.; Mohammed, O.A. Development and application of a real-time testbed for multiagent system interoperability: A case study on hierarchical microgrid control. *IEEE Trans. Smart Grid* **2016**, *9*, 1759–1768. [CrossRef]
27. 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.* **2019**, *104*, 817–826. [CrossRef]
28. Duan, N.; Yee, N.; Salazar, B.; Joo, J.-Y.; Stewart, E.; Cortez, E. Cybersecurity analysis of distribution grid operation with distributed energy resources via co-simulation. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020; pp. 1–5.
29. Wang, Z.; Qi, D.; Mei, J.; Li, Z.; Wan, K.; Zhang, J. Real-time controller hardware-in-the-loop co-simulation testbed for cooperative control strategy for cyber-physical power system. *Glob. Energy Interconnect.* **2021**, *4*, 214–224. [CrossRef]
30. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
31. Chawla, A.; Agrawal, P.; Singh, A.; Panigrahi, B.K.; Paul, K.; Bhalja, B. Denial-of-service resilient frameworks for synchrophasor-based wide area monitoring systems. *Computer* **2020**, *53*, 14–24. [CrossRef]

32. Khodaei, A. Microgrid optimal scheduling with multi-period islanding constraints. *IEEE Trans. Power Syst.* **2013**, *29*, 1383–1392. [CrossRef]
33. Bidram, A.; Davoudi, A. Hierarchical structure of microgrids control system. *IEEE Trans. Smart Grid* **2012**, *3*, 1963–1976. [CrossRef]
34. Bidram, A.; Davoudi, A.; Lewis, F.L.; Qu, Z. Secondary control of microgrids based on distributed cooperative control of multi-agent systems. *IET Gener. Transm. Distrib.* **2013**, *7*, 822–831. [CrossRef]
35. Simpson-Porco, J.W.; Shafiee, Q.; Dörfler, F.; Vasquez, J.C.; Guerrero, J.M.; Bullo, F. Secondary frequency and voltage control of islanded microgrids via distributed averaging. *IEEE Trans. Ind. Electron.* **2015**, *62*, 7025–7038. [CrossRef]
36. Burbano, R.A.G.; Gutierrez, M.L.O.; Restrepo, J.A.; Guerrero, F.G. IED Design for a Small-Scale Microgrid Using IEC 61850. *IEEE Trans. Ind. Appl.* **2019**, *55*, 7113–7121. [CrossRef]
37. Du, Y.; Tu, H.; Lukic, S. Distributed control strategy to achieve synchronized operation of an islanded MG. *IEEE Trans. Smart Grid* **2018**, *10*, 4487–4496. [CrossRef]
38. Commission, C.E.; Commission, C.P.U. *Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters*; SIWG Phase 2: Sacramento, CA, USA, 2015.
39. Obert, J.; Cordeiro, P.; Johnson, J.; Lum, G.; Tansy, T.; Pala, M.; Ih, R. *Recommendations for Trust and Encryption in der Interoperability Standards*; Technical Report; SAND2019–1490; Sandia National Laboratories: Albuquerque, NM, USA, 2019.
40. Wang, Y.; Mondal, S.; Deng, C.; Satpathi, K.; Xu, Y.; Dasgupta, S. Cyber-Resilient Cooperative Control of Bidirectional Interlinking Converters in Networked AC/DC Microgrids. *IEEE Trans. Ind. Electron.* **2020**, *68*, 9707–9718. [CrossRef]
41. Rath, S.; Pal, D.; Sharma, P.S.; Panigrahi, B.K. A Cyber-Secure Distributed Control Architecture for Autonomous AC Microgrid. *IEEE Syst. J.* **2020**, 1–12. [CrossRef]
42. Starke, M.; Herron, A.; King, D.; Xue, Y. Implementation of a publish-subscribe protocol in microgrid islanding and resynchronization with self-discovery. *IEEE Trans. Smart Grid* **2017**, *10*, 361–370 [CrossRef]
43. Mohanty, R.; Sahoo, S.; Pradhan, A.K.; Blaabjerg, F. A Cosine Similarity Based Centralized Protection Scheme for DC Microgrids. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**. [CrossRef]
44. Habib, H.F.; Youssef, T.; Cintuglu, M.H.; Mohammed, O. A multi-agent based technique for fault location, isolation and service restoration. In Proceedings of the 2016 IEEE Industry Applications Society Annual Meeting, Portland, OR, USA, 2–6 October 2016; pp. 1–8.
45. Cintuglu, M.H.; Ma, T.; Mohammed, O.A. Protection of autonomous microgrids using agent-based distributed communication. *IEEE Trans. Power Deliv.* **2016**, *32*, 351–360. [CrossRef]
46. Rahman, M.S.; Mahmud, M.A.; Oo, A.M.T.; Pota, H.R. Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems. *IEEE Trans. Ind. Inform.* **2016**, *13*, 436–447. [CrossRef]
47. Kimura, S.; Rotta, A.; Abboud, R.; Moraes, R.; Zanirato, E.; Bahia, J. Applying IEC 61850 to real life: Modernization project for 30 electrical substations. In Proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, USA, 21–23 April 2008.
48. Habib, H.F.; Mohamed, A.; El Hariri, M.; Mohammed, O.A. Utilizing supercapacitors for resiliency enhancements and adaptive microgrid protection against communication failures. *Electr. Power Syst. Res.* **2017**, *145*, 223–233. [CrossRef]
49. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Cyber Security in Control of Grid-Tied Power Electronic Converters—Challenges and Vulnerabilities *IEEE J. Emerg. Sel. Top. Power Electron.* **2019**. [CrossRef]
50. Bidram, A.; Poudel, B.; Damodaran, L.; Fierro, R.; Guerrero, J.M. Resilient and cybersecure distributed control of inverter-based islanded microgrids. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3881–3894. [CrossRef]
51. 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]
52. 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]
53. Hussain, S.S.; Farooq, S.M.; Ustun, T.S. A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages. *IEEE Trans. Power Deliv.* **2020**, *35*, 2565–2567. [CrossRef]
54. Hoyos, J.; Dehus, M.; Brown, T.X. Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure. In Proceedings of the 2012 IEEE Globecom Workshops, Anaheim, CA, USA, 3–7 December 2012; pp. 1508–1513.
55. Sánchez, H.S.; Rotondo, D.; Escobet, T.; Puig, V.; Quevedo, J. Bibliographical review on cyber attacks from a control oriented perspective. *Annu. Rev. Control* **2019**, *48*, 103–128. [CrossRef]
56. Zhang, H.; Qi, Y.; Wu, J.; Fu, L.; He, L. DoS attack energy management against remote state estimation. *IEEE Trans. Control. Netw. Syst.* **2016**, *5*, 383–394. [CrossRef]
57. Chlela, M.; Mascarella, D.; Joos, G.; Kassouf, M. Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks. *IEEE Trans. Smart Grid* **2017**, *9*, 4702–4711. [CrossRef]
58. Understanding Denial-of-Service Attacks | US-CERT. 6 February 2013. Available online: <https://www.us-cert.gov/ncas/tips/ST04-015> (accessed on 8 March 2017).
59. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [CrossRef]
60. Liu, X.; Li, Z. False data attacks against AC state estimation with incomplete network information. *IEEE Trans. Smart Grid* **2016**, *8*, 2239–2248. [CrossRef]



61. Saha, S.; Roy, T.; Mahmud, M.; Haque, M.; Islam, S. Sensor fault and cyber attack resilient operation of DC microgrids. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 540–554. [\[CrossRef\]](#)
62. Chlela, M.; Joos, G.; Kassouf, M.; Brissette, Y. Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5.
63. 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.* **2018**, *66*, 1543–1551. [\[CrossRef\]](#)
64. Torre, G.D.L.; Yucelen, T. Adaptive architectures for resilient control of networked multiagent systems in the presence of misbehaving agents. *Int. J. Control* **2018**, *91*, 495–507. [\[CrossRef\]](#)
65. Sahoo, S.; Peng, J.C.-H.; Mishra, S.; Dragičević, T. Distributed screening of hijacking attacks in DC microgrids. *IEEE Trans. Power Electron.* **2019**, *35*, 7574–7582. [\[CrossRef\]](#)
66. 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), Yasmine Hammamet, Tunisia, 19–22 March 2018; pp. 731–737.
67. Akella, R.; Tang, H.; McMillin, B.M. Analysis of information flow security in cyber—Physical systems. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 157–173. [\[CrossRef\]](#)
68. Dibaji, S.M.; Pirani, M.; Flamholz, D.B.; Annaswamy, A.M.; Johansson, K.H.; Chakraborty, A. A systems and control perspective of CPS security. *Annu. Rev. Control* **2019**, *47*, 394–411. [\[CrossRef\]](#)
69. Brugman, J.; Khan, M.; Kasera, S.; Parvania, M. Cloud based intrusion detection and prevention system for industrial control systems using software defined networking. In Proceedings of the 2019 Resilience Week (RWS), San Antonio, TX, USA, 4–7 November 2019; pp. 98–104.
70. Sahoo, S.; Dragičević, T.; Blaabjerg, F. An event-driven resilient control strategy for dc microgrids. *IEEE Trans. Power Electron.* **2020**, *35*, 13714–13724. [\[CrossRef\]](#)
71. Sahoo, S.; Peng, J.C.-H. A localized event-driven resilient mechanism for cooperative microgrid against data integrity attacks. *IEEE Trans. Cybern.* **2020**, *51*, 3687–3698. [\[CrossRef\]](#)
72. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Resilient operation of heterogeneous sources in cooperative DC microgrids. *IEEE Trans. Power Electron.* **2020**, *35*, 12601–12605. [\[CrossRef\]](#)
73. Sahoo, S.; Dragičević, T.; Blaabjerg, F. Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids. *IEEE Trans. Power Electron.* **2020**, *36*, 2522–2532. [\[CrossRef\]](#)
74. Danzi, P.; Angelichinoski, 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. [\[CrossRef\]](#)
75. Danzi, P.; Angelichinoski, M.; Stefanović, Č.; Popovski, P. Anti-jamming strategy for distributed microgrid control based on power talk communication. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017; pp. 911–917.
76. Lu, Z.; Wang, W.; Wang, C. Camouflage traffic: Minimizing message delay for smart grid applications under jamming. *IEEE Trans. Dependable Secur. Comput.* **2014**, *12*, 31–44. [\[CrossRef\]](#)
77. 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. [\[CrossRef\]](#)
78. Zhao, J.; Zhang, G.; La Scala, M.; Dong, Z.Y.; Chen, C.; Wang, J. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. *IEEE Trans. Smart Grid* **2015**, *8*, 1580–1590. [\[CrossRef\]](#)
79. Sahoo, S.; Mishra, S.; Peng, J.C.-H.; Dragičević, T. A stealth cyber-attack detection strategy for DC microgrids. *IEEE Trans. Power Electron.* **2018**, *34*, 8162–8174. [\[CrossRef\]](#)
80. 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.* **2019**, *67*, 6562–6571. [\[CrossRef\]](#)
81. Cecilia, A.; Sahoo, S.; Dragičević, T.; Costa-Castelló, R.; Blaabjerg, F. Detection and Mitigation of False Data in Cooperative DC Microgrids With Unknown Constant Power Loads. *IEEE Trans. Power Electron.* **2021**, *36*, 9565–9577. [\[CrossRef\]](#)
82. Zhang, J.; Sahoo, S.; Peng, J.C.-H.; Blaabjerg, F. Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids. *IEEE Trans. Power Electron.* **2021**, *36*, 9637–9647. [\[CrossRef\]](#)
83. Pillitteri, V.Y.; Brewer, T.L. *Guidelines for Smart Grid Cybersecurity*; NIST Interagency/Internal Report (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. [\[CrossRef\]](#)
84. Sahoo, S.; Yang, Y.; Blaabjerg, F. Resilient synchronization strategy for ac microgrids under cyber attacks. *IEEE Trans. Power Electron.* **2020**, *36*, 73–77. [\[CrossRef\]](#)
85. Sadabadi, M. S.; Sahoo, S.; Blaabjerg, F. A Fully Resilient Cyber-Secure Synchronization Strategy for AC Microgrids. *IEEE Trans. Power Electron.* **2021**. [\[CrossRef\]](#)