energies

Article

Cost and Cybersecurity Challenges in the Commissioning of Microgrids in Critical Infrastructure: COGE Case Study

Rodrigo Antonio Sbardeloto Kraemer [1,*], Douglas Pereira Dias [1], Alisson Carlos da Silva [1], Marcos Aurelio Izumida Martins [1] and Mathias Arno Ludwig [2]

[1] Sustainable Energy Center, CERTI Foundation, Florianópolis 88040-970, SC, Brazil; dpd@certi.org.br (D.P.D.); ava@certi.org.br (A.C.d.S.); mlz@certi.org.br (M.A.I.M.)

[2] R&D and Innovation, AES Brasil, São Paulo 04578-000, SP, Brazil; mathias.ludwig@aes.com

* Correspondence: rsk@certi.org.br

Abstract: The application of microgrids in critical infrastructures has grown considerably due to the power supply reliability and resilience, and the island operation possibility of providing independence from the main grid. However, the necessity of intense information exchange between the devices that compose the microgrid to their proper operation, and the communication infrastructure required to realize that, makes the system vulnerable to cybersecurity threats. In this context, the case study presented in this paper raises two important subjects of discussion in the Brazilian electrical sector context, which are microgrids and cybersecurity in critical infrastructures of the electrical sector. Therefore, this paper presents the practical challenges related to these two subjects by reporting the development, implementation, and commissioning of a new microgrid controller, and the solutions found to accelerate the development by reducing costs, mitigating risks, and optimizing the commissioning time.

Keywords: hardware-in-the-loop; microgrid modeling; risk mitigation; dispatched generation; real-time simulation; cybersecurity

check for updates

Citation: Kraemer, R.A.S.; Dias, D.P.; da Silva, A.C.; Martins, M.A.I.; Ludwig, M.A. Cost and Cybersecurity Challenges in the Commissioning of Microgrids in Critical Infrastructure: COGE Case Study. *Energies* **2022**, *15*, 2860. https://doi.org/10.3390/en15082860

Academic Editors: Hannu Laaksonen and Omid Palizban

Received: 18 March 2022
Accepted: 10 April 2022
Published: 14 April 2022

1. Introduction

The main grid has become more dynamic and complex with the digitalization and decentralization of the electricity sector [1,2]. The insertion of new elements in the network such as bidirectional energy sources, power electronic devices, digital sensors, control and management systems, and renewable energy resources (RER) is the main cause of this change. Despite technological advances, the large penetration of distributed energy resources (DER) in the main grid makes the system susceptible to reliability and stability problems [2].

Due to instability problems in the main grid such as degradation of the electrical power quality, periods of high load demand, and island occurrences, among others, microgrids (MG) have emerged as a fundamental complement to ensure the resilience and reliability in the power supply to the consumers [3,4]. Besides the power supply, MGs can offer ancillary services to the main grid such as voltage and frequency regulation, provide on- or off-grid operation, allow practical integration of DER, and help to reduce peak load demands through smart management of the available energy resources [2].

In Brazil, despite the advances in regulatory terms to standardization and encourage the distributed generation that contributed to the MG insertion still have a lack of specific laws to promote the MG implementation in order to achieve financial benefits. Those financial benefits can be obtained through regulation changes such as allowing charging of the MG Energy Storage Systems (ESS) with energy from the utility grid, specifying ancillary services that MG can provide, and standardizing the interconnection procedures applied to MGs, among others [5,6]. Currently, the economic benefit of MG implementation in Brazil is restricted to providing energy to remote and isolated communities that have no access to the distribution network and to critical infrastructures that need an uninterrupted power supply [5,7].

Besides that, due to the vast territorial extension of Brazil and its diverse biomes, there are several renewable power sources that are viable technically and economically to use in MGs such as solar, wind, hydro, biogas, and biomass [7]. Due to this diversity of power sources, challenges arise related to the design, integration, and management of those RERs in an MG, mainly in the commissioning stage. In this way, some works in the literature focus on the adversities of Brazilian MG management observing the technical, economical, and regulatory aspects.

In [8], the authors present an MG Energy Management System (EMS) with RER based on a Hybrid Model Predictive Control (HMPC) strategy, while considering the particularities of the Brazilian energy market that must be respected. The proposal takes into consideration the different energy tariffs of the market and the compensation energy rules that occur when the MG injects energy into the main grid. In the same way, the authors in [9] present an EMS based on Mixed-Integer Linear Programming (MILP), also considering the costs involving the Battery Energy Storage System (BESS) operation costs.

Regarding energy quality in MGs, there is a need to monitor all devices that compose it, which requires several measurement instruments and an adequate communication network. Legacy devices that do not present the same efficiency as the current ones and the integration of several DERs in an MG may interfere with the energy quality of the MG presenting problems such as active–reactive power variation, voltage, frequency deviation, harmonic insertion, and poor power factor, among others [10]. In this way, since MGs require an intense information exchange between their devices to properly operate, there is a demand for the use of sophisticated communication technologies. Therefore, technological advances led to integration between the power electronics of MG devices and the communication and network functionalities that transform them into cyberphysical systems; consequently, they have become exposed to current cybersecurity threats [10–13].

The Brazilian Electrical Energy Regulator (ANEEL), through its Research and Development (R&D) program, encourages the development of new technologies and business models as a way to create and modify regulations as well as benefiting society. In this way, due to technical, economic, and environmental benefits that a MG can provide, several Brazilian energy companies have mobilized to promote projects with the incentives of this R&D program that seek to validate technical and economical concepts in order to take advantage of new opportunities that are financially attractive.

The aforementioned project—the Intelligent Microgrid Control and Optimization System—has the goal to develop a solution to monitor, manage, control, and optimize MGs and validate through proof of concepts (PoCs). The PoCs were selected according to the consumer's profiles with the purpose of incorporating the technical and economical particularities of each consumer in the solution, making it more robust and efficient to the Brazilian scenario.

In this context, one of the selected consumers was the AES Brasil Generation Operation Center (COGE), which is considered a critical infrastructure due to the nature of its operations, concentrating the operation of all power plant generation managed by AES Brasil. The COGE operates 24-h a day and 7 days per week and has redundant power sources to maintain the continuous power supply to the critical loads, even in main grid contingency scenarios or the unavailability of a backup power source [12,14,15].

Due to these reasons, the commissioning stage of a new MG solution in critical infrastructure that considerably limits the possibility of MG operation tests requires a detailed plan so that the commissioning is executed in a short period of time without consequences to MG operation. In [16,17], MG tests using real-time simulation are analyzed. Through Hardware-in-the-Loop (HIL), these works apply different scenarios and strategies in the approached MGs under a lower cost and risk, and with greater flexibility and safety. Thus, it is possible to test and analyze the proposed solutions such as voltage regulation, energy quality, power management, controls, and minimize the development time. Therefore, a test setup was built where the MG was modeled and implemented in a HIL system, allowing the execution of a wider number of tests such as tests related to the control, system stress, and cybersecurity. Besides that, the use of the HIL system contributed to reducing the costs and security risks of failed tests.

Thus, the main contribution of this paper is to present the challenges raised during installation and commissioning of this MG, describe the solutions adopted, and discuss the subjects pertinent to cybersecurity and MGs. It is worth mentioning that the controller design details will not be discussed, the focus will be on the COGE MG case study and how the challenges encountered and the solutions adopted can contribute to the evolution of discussions about MGs.

The paper structure is presented as follows: Section 2 presents the scope of the current R&D project that conceived a new MG control and management solution; Section 3 shows the COGE microgrid infrastructure; the adopted cybersecurity strategies and the tests executed are presented in Section 4; the solution to accelerate development and MG commissioning and to reduce the costs related to human resources mobilization is shown in Section 5; finally, Section 6 discusses the challenges, presents possible solutions, and points out some subjects that can be developed further considering the scope of the paper.

2. Microgrid Project—Case AES Brasil

The R&D project named Intelligent Microgrid Control and Optimization System is divided into two phases. The first one sought to develop and implement a Microgrid Centralized Controller (MGCC) to supply the COGE of the AES Brasil company, allied to a SCADA (Supervisory Control And Data Acquisition) system to monitor, control, and schedule several operations. The second phase, which is presented in this paper, focused on improving the developed solution of phase one to obtain a product that could be used by the AES Brasil customers. In this way, the E+BOX was developed—a MG controller and data aggregation gateway—as shown in Figure 1.

For the proper operation of the E+BOX, a connection with the server is necessary, as it runs the optimizer that is responsible for calculating the MG setpoints (e.g., power reference, state) considering economical aspects and consumer requirements, the photovoltaic and load forecast algorithms, the database, and the MG management platform. If E+BOX loses communication with the internet, the system assumes new control rules to supply power to the loads, considering the priority of each one registered by the consumer.

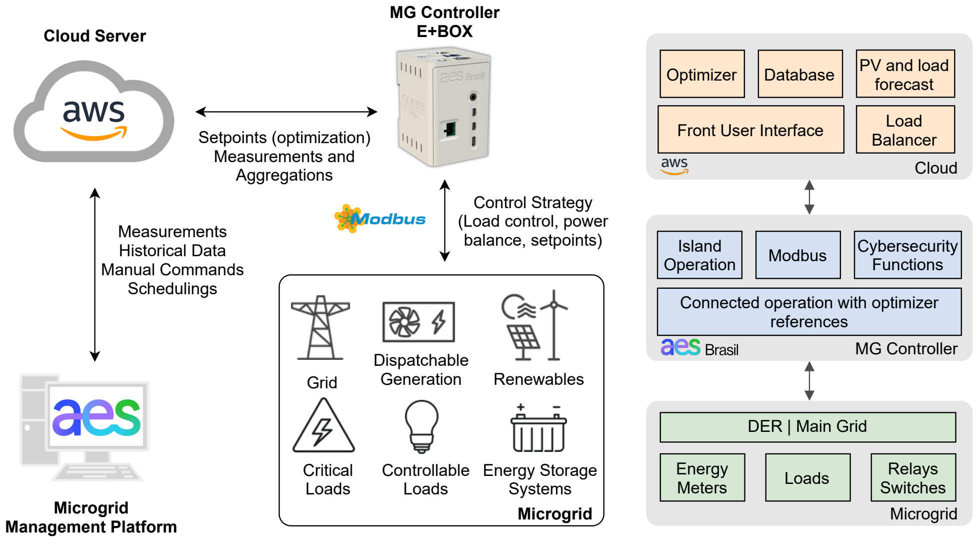

Figure 1. Product solution diagram for MG control and management.

2.1. MG Management Platform

The MG management platform is a SCADA system developed in the R&D project that allows the customer to have access to the real-time MG operation through its interface presented in Figure 2. During MG commissioning, the customer registers all devices that compose the MG (main grid energy meter, photovoltaic system, controllable loads, etc.) with their respective Modbus memory maps, and technical and economic specifications such as acquisition and maintenance costs, nominal power, among others. Besides that, the platform has other functionalities such as an energy tariff register, scheduling of operations, key performance indicators, access to historical data, remote manual operation, and registration of new devices in order to allow the system to follow the MG improvements and modifications.

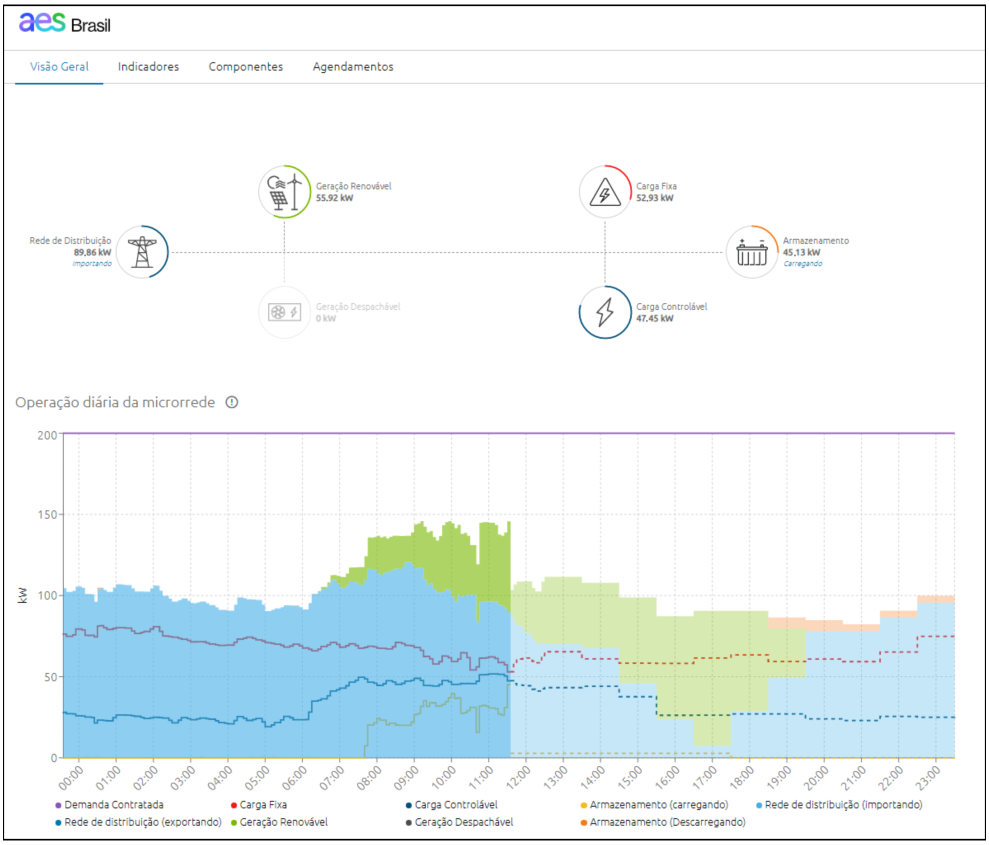

Figure 2. MG platform interface—Overview tab.

2.2. Cloud Server

The solution has a cloud server where the MG management platform, optimizer, database, and forecast algorithms are hosted. The implementation of the forecast algorithm and the optimizer in the cloud server allow the reduction of E+BOX in terms of computer processing power, cost, and size, besides the possibility of offering a management platform that provides access to the user to historical data and key performance indicators (KPI) of the MG.

2.2.1. Optimizer

The optimizer developed in phase one of the project, and presented in [18], was designed to operate as an MGCC that can operate as a generic controller for different MG configurations. The MGCC optimizer is based on MILP optimization technique [19] and considers the various possibilities of RERs available in Brazil; it was developed in order to enable the control of MGs with multiple DERs, such as dispatchable generators, photovoltaic and wind systems, ESS, and multiple control loads, in addition to allowing it to operate connected to the grid or in islanded mode.

The MGCC received further improvements through the insertion of a priority load model with the objective of minimizing the MG operation cost, without compromising the fulfillment requirements of power quality and security operation of the MG [20]. Moreover, the MGCC has incorporated a new battery model that allows the optimizer to be more selective in BESS usage in order to prolong the battery lifespan [21].

Below are presented the parameters that impact the optimization problem and, consequently, the MG operation related to economical aspects.

- Energy market information: energy tariff, taxes, tariff modality.
- Dispatchable generation information: diesel and natural gas price.
- ESS information: acquisition cost, maintenance cost, lifetime, C-rate, battery type.
- DER (photovoltaic or wind) information: lifetime, acquisition cost, maintenance cost.
- Loads information: priority based on customer profile, costs of turn-off the load.
- DER and load forecast: forecast inputs are provided to the optimizer through data measured in the field, weather conditions, and historical data.

The MG setpoints, calculated by the optimizer, are sent every 15 min to the E+BOX with a forecast horizon of 24 h. In case of a lost connection to the internet, the E+BOX will still have setpoints to be followed by the MG controller; therefore, every 15 min, the E+BOX receives new setpoints that overwrite the oldest forecasts.

2.2.2. Forecasting

The load and photovoltaic generation forecast algorithm is based on Machine Learning using the unsupervised learning method. For forecasts, the measured data in the field are used and sent to the server by the E+BOX, in addition to having access to the historical database. Besides that, the predictor has access to weather conditions to predict the photovoltaic generation. The forecast algorithm provides a 24-h horizon, where the first hour is discretized in 5 min and, after that, it is 1 h.

2.3. E+BOX

The E+BOX is a piece of hardware based on Raspberry Pi 4, which has an auxiliary shield that provides additional communication ports and a power supply input with a wide range of acceptable voltage. The hardware has two ethernet ports, one serial port, a power supply input that can vary between 8 and 36 Vdc, and an expandable external memory through an SD card, allowing larger data and log storage.

2.3.1. Communication

The E+BOX establishes communication with the MG devices such as energy meters, photovoltaic inverters, controllable loads, ESS, or dispatchable generators through Modbus communication RTU/RS485 or TCP/IP. Besides that, the data measured by E+BOX are sent to the server through HTTPS secure connection. The way that the data inputs and outputs are managed to provide security to the system will be described in detail in Section 4.

2.3.2. Operational Data Flow

According to Figure 1, the E+BOX is the link between the MG and the server. Every 10 s, the controller requests MG devices' measurements such as power (active, reactive, and apparent), voltage, current, energy, total harmonic distortion (THD), and power factor. Moreover, the server sends the setpoints for the power and state of the devices as dispatchable power sources or ESS. Each device has a set of mandatory measurements (or commands) to allow the proper operation of the controller. Furthermore, every 15 min, the E+BOX receives from the server the setpoints of power and state calculated by the optimizer. The controller, in turn, sends the aggregations (mean values) of the measurements at intervals of 5, 15, and 30 min to the cloud database.

2.3.3. Control System

There are two macro operation conditions of E+BOX, related to grid connection and internet connection. The E+BOX can operate with the MG in grid-connected or island mode, with or without an internet connection. The control strategy implemented in the E+BOX is tertiary level, where every 15 min, the server sends the MG setpoints to the controller. The controller, in turn, sends the setpoints to the MG devices with the purpose of ensuring the power balance of the MG according to the calculation of the optimizer. This control action occurs every 10 s and is called "short-term loop".

In the case that the E+BOX loses internet connection, the short-term loop considers the last setpoints sent by the optimizer for the maximum of 24 h (prediction horizon); after that, the setpoints are overwritten in order to prioritize the power supply to the critical loads, disregarding economic aspects.

3. Critical Microgrid Structure

One of the selected PoCs to validate the developed product was the COGE of AES Brasil, which is considered a critical infrastructure, as mentioned earlier. Located in the city of Bauru, São Paulo, Figure 3 shows the simplified diagram of the COGE MG. The MG has a photovoltaic system (PV), a battery energy storage system (BESS), a diesel generator (DG), controllable loads, and critical loads, where most of the critical loads are IT (Information Technology) devices.

The MG switch (Figure 3) has fault detection and anti-islanding detection algorithms to ensure the disconnection of the MG from the main grid when the parameters such as voltage and frequency are out of the specifications of the standards PRODIST [22] and IEEE Std. 1547 [23]. Thus, when the MG switch disconnects the MG from the grid at the point of common coupling (PCC), the DG forms the grid by regulating the voltage and frequency of the AC bus. The MG parameters are specified in Table 1.

Table 1. COGE MG Parameters.

Parameter	Value	Parameter	Value
Main grid line voltage	13.8 kV	MG transformer power	500 kVA
Grid frequency	60 Hz	Diesel GenSet power	500 kVA
MG line voltage	220 V	Critical Loads power	132 kVA
BESS power	180 kVA	Controllable Load 1 power	24 kVA
BESS nominal capacity	200 Ah	Controllable Load 2 power	22 kVA
PV power	99 kW	Controllable Load 3 power	14 kVA

All devices of COGE MG (Figure 3), whether they are loads or generation sources, are monitored through energy meters or integrated controllers. The critical and controllable loads, with exception of the PCC measurement, are monitored through energy meters (M) integrated to the E+BOX via RS485 bus over the Modbus RTU protocol. This RS485 bus is connected to a gateway that converts the Modbus RTU to Modbus TCP/IP. The DG, BESS, and PV have their own local controllers that allow direct integration with the E+BOX via Modbus TCP/IP.

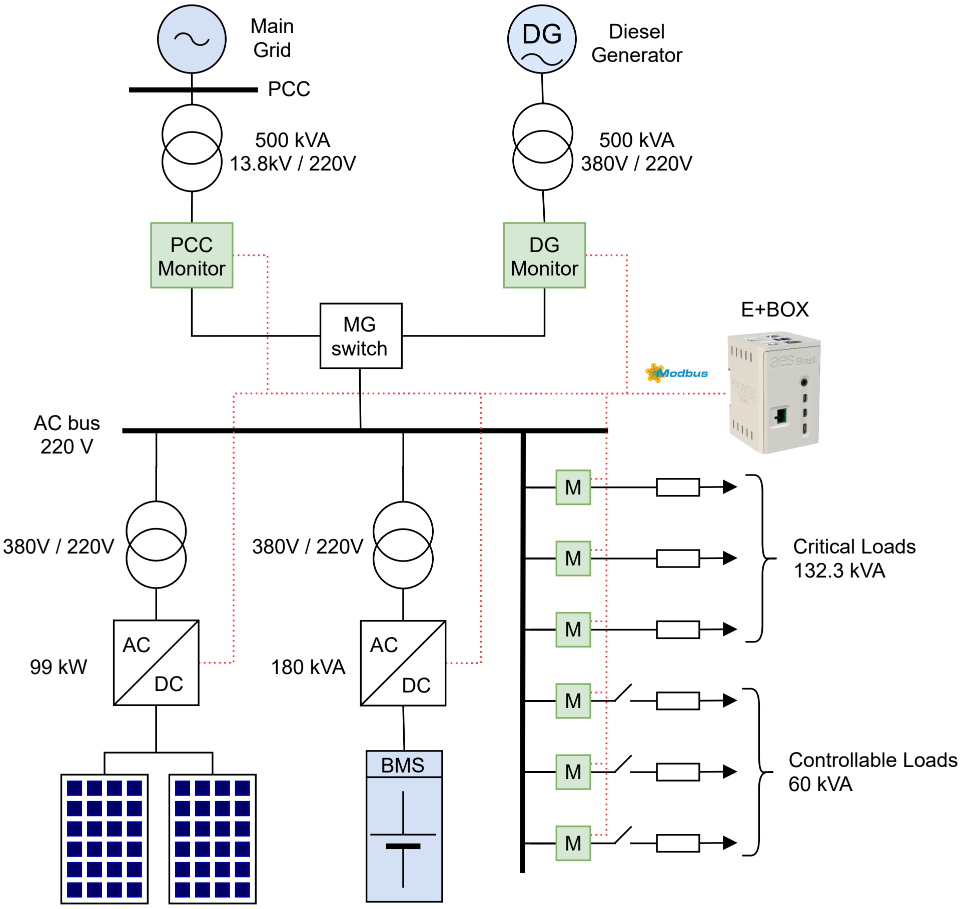

Figure 3. Simplified diagram of the COGE MG.

4. Network Structure and Cybersecurity

Infrastructures of the electrical sector, such as power plants and operation centers, among others, have the characteristic of being designed to operate for several years (above 25 years). Due to this characteristic, and allied with the rapid technology evolution, it is common to find old systems and equipment that no longer have manufacturer support or updated firmware, or even lack functions that allow easy and proper integration with the communication network of the company. Consequently, this type of scenario exposes the infrastructure to cybersecurity vulnerabilities. An example of this is found in [12], where a DER can introduce additional cybersecurity risks due to the communication resources of the device.

In this context, there is a current convergence between the IT systems with OT (Operational Technology) systems. Consequently, many security strategies adopted in IT infrastructures are replicated in OT infrastructures when possible because OT systems have many particularities, such as the possibility of limited internet connection, considerable electromagnetic interference, proprietary communication protocols, among others.

From a regulatory point of view of cybersecurity in the Brazilian electricity sector, the National Electrical System Operator (ONS) submitted a proposal to ANEEL regarding the safe operation of the National Interconnected Electrical System (SIN), establishing requisites of cybersecurity in 2019. After two years of debates, ANEEL published the Normative Resolution n° 964 (REN 964) on 22 December 2021 that deals with the cybersecurity guidelines for the electrical sector agents [24]. The project presented in this paper follows international strategies and good practices regarding cybersecurity, as also recommended by REN 964, even though these guidelines were released late in the development.

Regarding the communication protocols in MGs, the IEC 61850 is highly recommended due to the communication speed, reliability, and high-security levels against cyberattacks [25]. However, since the E+BOX has the intent to attend minor MGs at the first moment, and observing the Brazilian stage of MG developments, the Modbus protocols were adopted. Further, the Modbus will be a good option once the majority of the legacy devices in Brazilian electric infrastructures are compatible with it.

Despite the Modbus protocol presenting a low level of security against cyberattacks and presenting delays in communication when having the need to transmit a large amount of data in the RS485 network [25], the resulting system of the E+BOX is highly integrable with the customers' infrastructures.

To solve the delay problem communication in customers with a considerable quantity of monitored and controlled devices over the RS485 network (e.g., greater than 32), the adopted strategy was to segment the devices through a gateway that converts the Modbus RTU over RS485 to Modbus TCP/IP over ethernet. The device segmentation was realized according to their location in the MG. The formation of RS485 networks between closer equipment is prioritized to allow the communication bus to reach higher baud rates since the distance of the RS485 bus between the devices affect directly the maximum possible baud rate. From that, a local gateway is applied that communicates with the E+BOX through ethernet cable with Modbus TCP/IP protocol, which minimizes the communication delay.

Regarding the low level of security that the Modbus protocol presents, below is described the proposed network structure, segmented according to the Purdue model [26–28], which segments the network in levels according to the device roles in the infrastructure. Further, each level has a different configuration of firewall rules to prevent cyberattacks and unauthorized access. Below is described the network structure adopted in this project.

Due to the strategic role that the COGE plays in the generation power plants (hydroelectric, solar, and wind), in addition to the cybersecurity strategies, a secure network structure was developed, establishing a secure connection between the devices installed at the field and the cloud server. Figure 4 presents the simplified diagram of the MG network. This diagram shows the user link with the system, the cloud server, the energy meter, field devices, the E+BOX, and other communication devices that may exist at other consumers. This is how the exchange of information between the field devices, the cloud server, and the user is realized.

As observed in Figure 4, the communication is structured based on a 4G modem, local internet, security router, switch, E+BOX, gateways, and field devices. Therefore, in order to allow the equipment to communicate with other parts of the network, it is necessary to define several communication and cybersecurity settings to apply OT segmentation strategies aiming at a functional, secure, and reliable system.

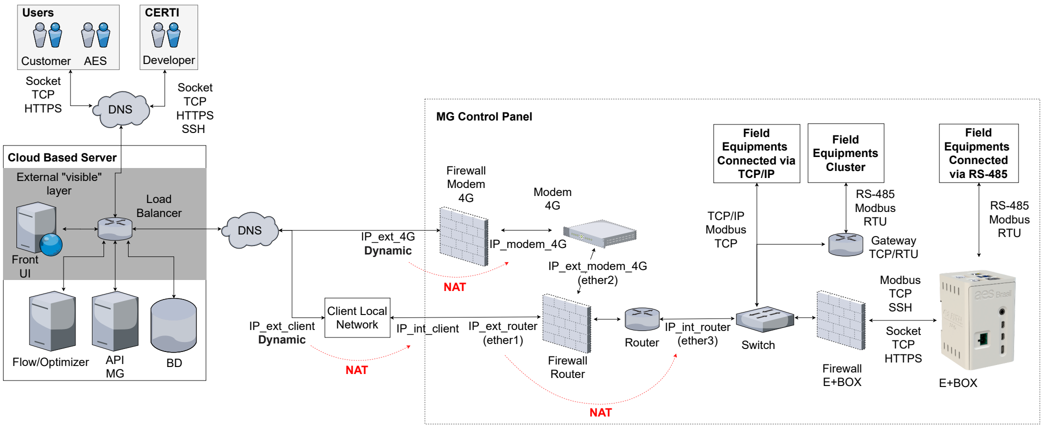

Figure 4. MG network diagram.

The system integration between the cloud and the field devices is realized through an internet connection. The block "Client Local Network" represents the consumer local internet point of connection and is the main source of internet access. To provide reliability to the system, a redundant internet connection through the 4G modem is foreseen, represented by the group of elements in the diagram named "Firewall 4G modem" and "4G modem". This group of elements represents an industrial device that allows the implementation of firewall rules to limit, control, and block unwanted access.

After the security layer mentioned above, the system has a security router that corresponds to the group of elements in Figure 4 named "Firewall router" and "Router". This device allows the management of all data traffic of the internal MG network providing an additional security layer. It should be noted that the security router is also responsible for the redundancy internet connection between the local client network and the 4G modem.

After passing through the router security layer, the system is connected to the MG controller. Thus, as found in the network diagram by the block "Firewall RPI", the controller enables the implementation of firewall rules establishing a filtering layer of data traffic.

Given the necessity of centralizing the read and write procedures of the energy meter and integrated controllers, the E+BOX must be connected to all devices that compose the MG, becoming a MGCC. The network structure (Figure 4) shows the connection between the controller and all other devices either by Modbus TCP through a switch, or by Modbus RTU through the serial port available in the E+BOX. Another possibility to allow the interconnection of devices is the use of a gateway to convert Modbus RTU to Modbus TCP/IP. In this case, it is possible to connect several RS485 devices to a gateway and replicate this setup, connecting the gateways to a switch.

4.1. Security Strategies

Given the proposed network structure presented in Figure 4, the adopted strategies against the main cybersecurity threats to MGs are analyzed [10].

4.1.1. Unauthorized Access and Sensitive Information Disclosure

The proposed network structure prevents unauthorized access and data interception. The Transport Security Layer (TLS) 1.2 protocol is used between the E+BOX and the cloud server, which is an encrypted end-to-end communication protocol that guarantees data integrity and privacy. Further, the security header HTTPS is used to add an additional security layer to the TLS protocol. Additionally, the authentication process of a new E+BOX by the cloud server is through a private key certificate.

The other filed devices such as the security router, the E+BOX itself, and gateways are configured to request authentication credentials from any unidentified user. Moreover, those devices are configured to allow communication traffic only for registered IPs.

4.1.2. DDoS Attack

The Distributed Denial of Service (DDoS) attacks are managed by the cloud server and the MG devices, security router, and 4G modem. Those field devices are configured to identify DDoS attacks and filter the origin addresses of those attacks by blocking the connection of the respective IPs. To the cloud server, the cookie feature available in TLS 1.2 is used; this mechanism forces the attacker to prove their reachability and, consequently, prevent DDoS attacks [13].

4.1.3. Repudiation Attack

The repudiation attack is prevented by using the private key certificate to authenticate an E+BOX by the cloud server. In the field, the MG devices are configured to authorize only registered IP's traffic through specific ports.

5. Microgrid Test Setup

Some aspects such as cybersecurity and the indispensability of continuous operation of the critical facilities, as is the case at the COGE, motivate the use of hardware-in-the-loop (HIL) devices to allow a wide variety of tests before commissioning [12,14]. Other benefits are the time and cost optimization due to preliminary testing, as well as decreased health and safety risks for the field team. These benefits stand out as essential factors that motivate the use of HIL technology, accelerating the MG development process while mitigating important risks. Furthermore, the HIL approach provides greater control and diversity over the tests.

Figure 5 presents the test setup used to validate the developed applications and to consolidate and improve the cybersecurity aspects. The tests are based on the real-time emulation of the COGE MG modeled in the HIL and integrated with the E+BOX. Thus, the MG devices such as DERs, loads, and BESS are modeled using the Typhoon HIL software, which is linked to the hardware Typhoon HIL 602+. As in the real application, the communication between the E+BOX controller and Typhoon HIL 602+ is achieved through Modbus TCP/IP.

On the other hand, it can be observed that the integration between the controller and the cloud server is preserved as in the field, based on the data transfer through HTTPS and at the socket TCP level. Further, for redundancy and real-time data validation purposes, the tests can be monitored in the developed management platform or at the Typhoon HIL SCADA.

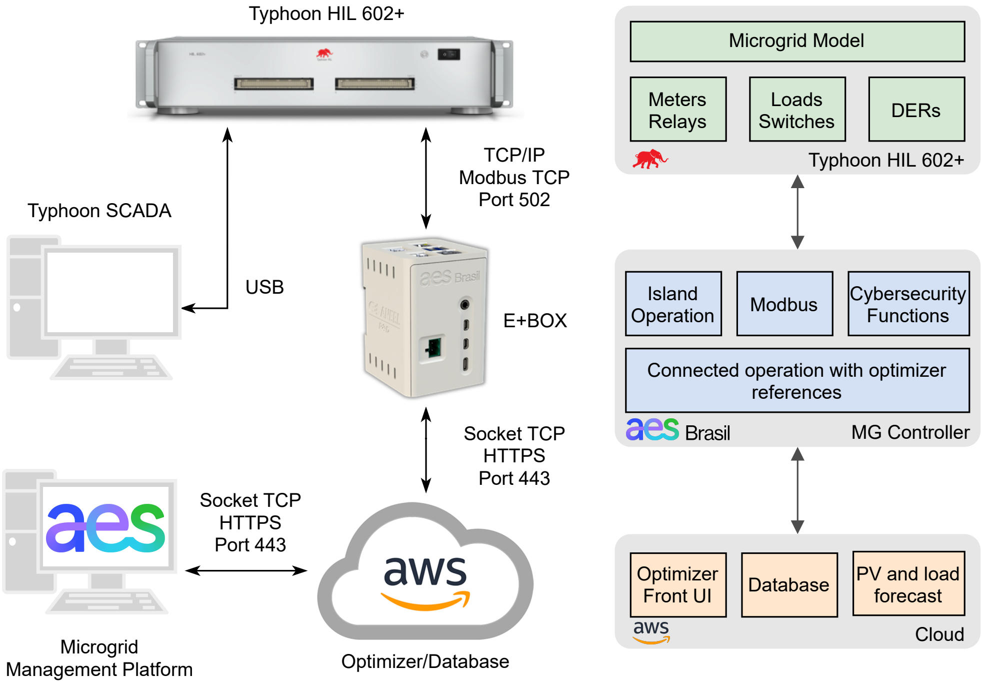

Figure 5. COGE MG setup configuration.

5.1. Reducing Costs

In order to present a fair comparison related to the reduced costs achieved in this project using the MG test setup presented in Figure 5, the data of another MG project developed by the CERTI Foundation will be used, but without the use of a MG test setup.

The project named Development of Pilot Application of Power Distribution Microgrid with Distributed Generation and Commercial Operation Model (COELCE MG) was developed by CERTI Foundation in 2019 [29]. The solution proposed by the COELCE MG project was very similar to the E+BOX in terms of control strategy and MG size (number of devices and installed power). Unlike the project presented in this paper, the COELCE MG project used the local MG implementation to validate and test the majority of the functionalities. Due to the distance between the CERTI Foundation (Floranópolis, Santa Catarina, Brazil) and the COELCE MG (Fortaleza, Ceará, Brazil), the development team needed to travel several times to certify the proposed solution and finish the commissioning stage.

In order to exemplify and compare the costs of each project, Table 2 presents information about the amount of travel needed in each project and the costs involved.

Table 2. Comparison of costs between E+BOX project and COELCE MG project.

Field Team	Number of Travels	Total Costs
6 members	8	R$93,265.17
3 members	2	R$21,147.28
Difference		R$72,117.89

5.2. Result Analysis

With the purpose of presenting a comparison of the COGE MG operation with and without the E+BOX, the simulations were realized considering two different approaches: (1) the MG operates without any controller, except the MG switch (Figure 6a–c); (2) the microgrid operates with the E+BOX and under the setpoints given by the optimizer and the forecast algorithm (Figure 6d–f).

In order to have an equal comparison between the operation scenarios, the simulation of the COGE MG with the E+BOX was performed under a real operation profile of COGE without any controller, as presented in Figure 6. Thus, a period of time was selected from the measurements that represented a dynamic and diversified scenario for the behavior of the MG's elements, in order to reproduce different levels of photovoltaic generation, critical overload, and also the main grid fault. In terms of the time simulation, the profile used has a period of three days.

Due to the need for effective control to carry out the power dispatch and the charging operation of the BESS properly and efficiently, the scenario where the MG is operated by the E+BOX can be pointed out as one of the most notable differences between the results, as can be seen in Figure 6.

Thus, it can be verified that the BESS charging process occurs significantly in periods of low demand or high photovoltaic generation. Therefore, the main grid impacts are minimized, as is verified when the curves for both scenarios are compared.

Another aspect that can be analyzed concerns the control of infringing the limit of contracted demand of the main grid. As can be observed on the second day, power exceeds the contracted demand (200 kW), with an approximated duration of three and a half hours, if the grid fault and the start of the diesel generator are disregarded. The demand predictor identified this infringement; thus, the optimizer dispatched the BESS with lower power for a longer period of time, rather than with higher power for a shorter period of time. Hence, the demand infringement was lower, resulting in reduced payment of exceeded demand. Such results can be explained since the optimizer considers the economic aspects as well as electrical ones.

Finally, it stands out that the objective of this result analysis is not to discuss the details of the optimizer and the model, motivating this more superficial approach.

The HIL test setup allowed the team to perform some tests that would not be possible at COGE. The analyzed Figure 6 allowed testing of the E+BOX under the following scenarios:

- High photovoltaic power generation (first and third day): the surplus power was used to charge the BESS.
- Reduce the energy bill (first and third day): use the BESS power to supply the load demand in the times that the energy tariff is higher, between 6 p.m. and 9 p.m.

- Grid fault (second day): use the BESS to supply the load demand during a grid fault and turn off some controllable loads to reduce the load demand.

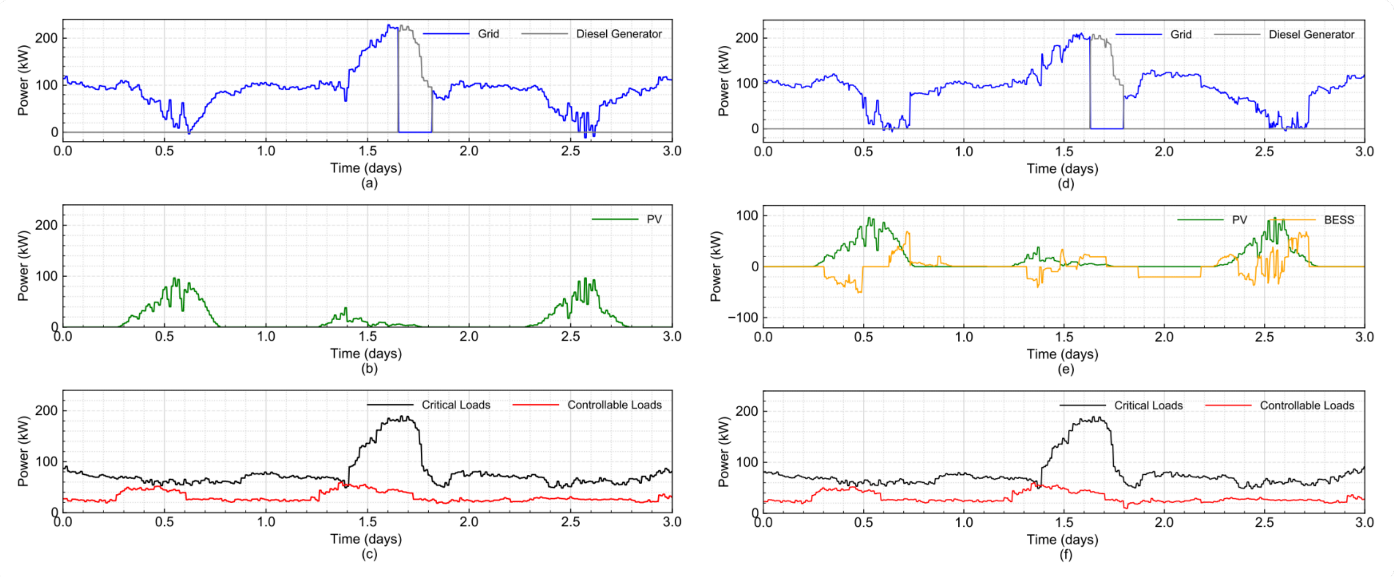

Figure 6. COGE MG operation: (**a**–**c**) without E+BOX and (**d**–**f**) with E+BOX and setpoints defined by the optimizer in the HIL.

6. Conclusions

The MG control and management solution named E+BOX presented in this paper sought to contribute with the development of the MG environment in order to point out technical and regulatory challenges with the purpose of promoting the discussion and evolution of the electrical sector. The selection of COGE MG as a case study for this paper reveals technical and economical challenges, such as the need to optimize the time of commissioning so as to not affect the operation of critical infrastructure, and improve the tests of system functionalities, while meeting cybersecurity requisites and reducing the team mobilization costs.

The Typhoon HIL was used to model and simulate the MG in real-time, to validate the product, as well as to execute continuous functionality and cybersecurity tests. Consequently, there was a total cost reduction and an increase in worker safety during the tests; as the result of postcommissioning, a digital twin model of the COGE can be made available to the client. With the digital twin model, it is possible for the client to test out previous modifications in a digital environment to verify the MG behavior and generate MG improvement scenarios with economic studies to verify investment returns, among other possibilities.

In addition, the proposed solution allows the customer to segment the MG devices in a safe way that allows monitoring all devices, identifying possible problems with energy quality, and analyzing KPIs in an easy way. This facilitates the customer to adopt measures to improve the MG performance and mitigate problems related to maintenance of equipment due to poor energy quality and reduce energy bills.

At the end of the project, the customers who received the installation of the PoC, in addition to the COGE, will receive training and continuous support, so that they can make the best use of the management tool and obtain financial return with the E+BOX.

The paper presented the challenges encountered in the MG implementation in a critical infrastructure and pointed out the advances of the proposed solution over the existing Brazilian regulations about MGs and cybersecurity in the electric sector.

Author Contributions: The authors contributed equally in the research: Conceptualization, data curation, and investigation: R.A.S.K., D.P.D. and A.C.d.S.; formal analysis: M.A.I.M. and M.A.L.; project administration: M.A.I.M. and M.A.L.; resources, R.A.S.K.; supervision: R.A.S.K. and M.A.I.M.; supervision: M.A.I.M.; validation: M.A.I.M.; writing—original draft: R.A.S.K.; writing—review and editing: R.A.S.K., D.P.D., A.C.d.S., M.A.I.M. and M.A.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Research and Development project PD PD-00064-1054-2019, granted by the Brazilian Electricity Regulatory Agency (ANEEL) and AES Brasil.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the Research Program and Technological Development of the electricity sector regulated by ANEEL and AES Brasil for their financial support. This paper is related to the project PD-00064-1054-2019, which is cooperated between CERTI Foundation in association with the AES Brasil.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; nor in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ANEEL	Brazilian Electricity Regulatory Agency
BESS	Battery Energy Storage System
COGE	Generation Operation Center
DER	Distributed Energy Resources
DG	Diesel Generator
EMS	Energy Management System
ESS	Energy Storage System
HIL	Hardware in the Loop
HMPC	Hybrid Model Preditive Control
KPI	Key Performance Indicators
MG	Microgrid
MGCC	Microgrid Centralized Controller
MILP	Mixed-Integer Linear Programming
PCC	Point of Common Coupling
PoC	Proof of Concept
RER	Renewable Energy Resources
R&D	Research and Development
SCADA	Supervisory Control And Data Acquisition
THD	Total Harmonic Distortion
TLS	Transport Security Layer

References

1. Lan, Y.; Guan, X.; Wu, J. Online Decentralized and Cooperative Dispatch for Multi-Microgrids. *IEEE Trans. Autom. Sci. Eng.* **2020**, *17*, 450–462. [CrossRef]
2. Saeed, M.H.; Fangzong, W.; Kalwar, B.A.; Iqbal, S. A Review on Microgrids' Challenges amp; Perspectives. *IEEE Access* **2021**, *9*, 166502–166517. [CrossRef]
3. Wan, W.; Bragin, M.A.; Yan, B.; Qin, Y.; Philhower, J.; Zhang, P.; Luh, P.B. Distributed and Asynchronous Active Fault Management for Networked Microgrids. *IEEE Trans. Power Syst.* **2020**, *35*, 3857–3868. [CrossRef]
4. Jampeethong, P.; Khomfoi, S. Coordinated Control of Electric Vehicles and Renewable Energy Sources for Frequency Regulation in Microgrids. *IEEE Access* **2020**, *8*, 141967–141976. [CrossRef]
5. Martins, M.A.I.; Fernandes, R.; Heldwein, M.L. Proposals for Regulatory Framework Modifications for Microgrid Insertion–The Brazil Use Case. *IEEE Access* **2020**, *8*, 94852–94870. [CrossRef]

6. Bellido, M.H.; Rosa, L.P.; Pereira, A.O.; Falcão, D.M.; Ribeiro, S.K. Barriers, challenges and opportunities for microgrid implementation: The case of Federal University of Rio de Janeiro. *J. Clean. Prod.* **2018**, *188*, 203–216. [CrossRef]
7. Santos, A.Q.O.; da Silva, A.R.; Ledesma, J.J.G.; de Almeida, A.B.; Cavallari, M.R.; Junior, O.H.A. Electricity Market in Brazil: A Critical Review on the Ongoing Reform. *Energies* **2021**, *14*, 2873. [CrossRef]
8. Conte, E.; Mendes, P.R.C.; Normey-Rico, J.E. Economic Management Based on Hybrid MPC for Microgrids: A Brazilian Energy Market Solution. *Energies* **2020**, *13*, 3508. [CrossRef]
9. Roesler, P.H.; López-Salamanca, H.L.; Medeiros, L.D.; Pedretti, A.; Tortelli, O.L. Load Management Optimization for Islanded Microgrids under Brazilian Regulatory Normative. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Conference—Latin America (ISGT Latin America), Gramado, Brazil, 15–18 September 2019; pp. 1–6. [CrossRef]
10. Marchand, S.; Monsalve, C.; Reimann, T.; Heckmann, W.; Ungerland, J.; Lauer, H.; Ruhe, S.; Krauß, C. Microgrid Systems: Towards a Technical Performance Assessment Frame. *Energies* **2021**, *14*, 2161. [CrossRef]
11. Li, Z.; Shahidehpour, M.; Aminifar, F. Cybersecurity in Distributed Power Systems. *Proc. IEEE* **2017**, *105*, 1367–1388. [CrossRef]
12. Sarker, P.S.; Venkataramanan, V.; Cardenas, D.S.; Srivastava, A.; Hahn, A.; Miller, B. Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5. In Proceedings of the 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Sydney, Australia, 21 April 2020; pp. 1–6. [CrossRef]
13. Kondoro, A.; Dhaou, I.B.; Tenhunen, H.; Mvungi, N. A Low Latency Secure Communication Architecture for Microgrid Control. *Energies* **2021**, *14*, 6262. [CrossRef]
14. Ghenea, I.; Gaiceanu, M. Microgrid Power Infrastructure for Critical Operations. In Proceedings of the 2019 6th International Symposium on Electrical and Electronics Engineering (ISEEE), Galati, Romania, 18–20 October 2019; pp. 1–6. [CrossRef]
15. Wang, J.; Cisse, B.M.; Brown, D.; Crabb, A. Development of a microgrid control system for a solar-plus-battery microgrid to support a critical facility. In Proceedings of the 2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 23–26 April 2017; pp. 1–5. [CrossRef]
16. Huo, Y.; Gruosso, G. Hardware-in-the-Loop Framework for Validation of Ancillary Service in Microgrids: Feasibility, Problems and Improvement. *IEEE Access* **2019**, *7*, 58104–58112. [CrossRef]
17. Yang, P.; Yu, M.; Wu, Q.; Wang, P.; Xia, Y.; Wei, W. Decentralized Economic Operation Control for Hybrid AC/DC Microgrid. *IEEE Trans. Sustain. Energy* **2020**, *11*, 1898–1910. [CrossRef]
18. Makohin, D.G.; Gloria, L.L.; Zeni, V.S.; Pica, C.Q.; Neto, E.P.A.; Arend, F.G.; Asami, D.Y.; Heraldo, E. Design and Implementation of a Flexible Microgrid Controller through Mixed Integer Linear Programming Optimization. In Proceedings of the 2018 9th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Charlotte, NC, USA, 25–28 June 2018; pp. 1–7. [CrossRef]
19. Gutiérrez-Oliva, D.; Colmenar-Santos, A.; Rosales-Asensio, E. A Review of the State of the Art of Industrial Microgrids Based on Renewable Energy. *Electronics* **2022**, *11*, 1002. [CrossRef]
20. Glória, L.L.; Costa, G.H.S.; Oliveira, D.B.S.; de Bona, J.C.; Oliva, N.A.; Pica, C.Q.; Ludwig, M.A. A Load Prioritization Model for a Microgrid Operation in the Islanded Mode. In Proceedings of the 2020 IEEE PES Transmission Distribution Conference and Exhibition—Latin America (TDLA), Montevideo, Uruguay, 28 September–2 October 2020; pp. 1–6. [CrossRef]
21. Izumida Martins, M.A.; Rhode, L.B.; Almeida, A.B.D. A Novel Battery Wear Model for Energy Management in Microgrids. *IEEE Access* **2022**, *10*, 30405–30413. [CrossRef]
22. ANEEL—Agência Nacional de Energia Elétrica. Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional. PRODIST. Available online: https://www.gov.br/aneel/pt-br/centrais-de-conteudos/procedimentos-regulatorios/prodist (accessed on 18 February 2022).
23. *IEEE Std 1547-2018; Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–138. [CrossRef]
24. ANEEL—Agência Nacional de Energia Elétrica. Política de Segurança Cibernética Para Agentes do Setor de Energia eléTrica. Resolução Normativa n° 964. Available online: https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-de-2021-369359262 (accessed on 18 February 2022).
25. Cagnano, A.; De Tuglie, E.; Mancarella, P. Microgrids: Overview and guidelines for practical implementations and operation. *Appl. Energy* **2020**, *258*, 114039. [CrossRef]
26. *ANSI/ISA-95; Enterprise-Control System Integration*; ISA—International Society of Automation: Research Triangle, NC, USA, 2020.
27. *NIST SP 800-82 Rev. 2; Guide to Industrial Control Systems (ICS) Security*; NIST—National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.
28. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2021**, *14*, 27. [CrossRef]
29. Bianchini, I.L.; Izumida Martins, M.A.; Pica, C.Q.; Zeni, V.S.; Rodrigues, N. Microgrid test setup and procedures implemented on a real pilot project. In Proceedings of the 2017 IEEE 8th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Florianopolis, Brazil, 17–20 April 2017; pp. 1–4. [CrossRef]