

Article

Integrating Smart Grid Devices into the Traditional Protection of Distribution Networks

Bruno Silva Torres ^{1,2,*} , Luiz Eduardo Borges da Silva ^{1,2}, Camila Paes Salomon ¹ 
and Carlos Henrique Valério de Moraes ¹

¹ Electrical Engineering Graduate Program, Itajuba Federal University, Itajuba 37500-903, Brazil; leborgess@gmail.com (L.E.B.d.S.); camilapsalomon@unifei.edu.br (C.P.S.); carloshvmoraes@gmail.com (C.H.V.d.M.)

² R&D Department, Gnarus Institute University, Itajuba 37500-052, Brazil

* Correspondence: bs_torres@hotmail.com

Abstract: Smart grids are a reality in distribution systems. They have assisted in the operation, control, and most of all, the protection of urban networks, significantly solving the contingencies of these networks. This paper treats the initial stage of implementing smart grid switching devices in distribution networks. In this stage, smart grid technologies need to operate with the traditional protection elements (such as fuses, reclosers, and sectionalizers). This fact can create trouble in the protection schemes because there are two distinctive philosophies. In some companies, especially those without substantial capital, these two protection philosophies can run together for many years. The most popular intelligent electronic devices (IEDs) available in the market are studied to verify their features and the possibility to incorporate techniques to allow the two philosophies to work together. After that, the proposed approach shows how the existing IEDs can interact with the traditional devices. Special functions can also be incorporated to inform the control center of an operational problem, increasing the observability of the network. With the proposed approach, the IEDs are transformed into intelligent agents. Practical examples using real distribution systems are presented and discussed, proving the efficacy of the proposed methodology.

Keywords: smart grids; power distribution; traditional urban protection; contingencies; IED; intelligent agents; rule-based system; multiagent systems



Citation: Torres, B.S.; Borges da Silva, L.E.; Salomon, C.P.; de Moraes, C.H.V. Integrating Smart Grid Devices into the Traditional Protection of Distribution Networks. *Energies* **2022**, *15*, 2518. <https://doi.org/10.3390/en15072518>

Academic Editor: Ahmed F. Zobaa

Received: 9 March 2022

Accepted: 25 March 2022

Published: 29 March 2022

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



Copyright: © 2022 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

Electrical distribution networks have been structured and operated since their inception to meet the needs of their loads, which are constantly evolving and presenting new demands and operational problems [1]. Distribution systems have become increasingly more important due to the increasing number of branches and growing complexity. New challenges stand in the way of delivering quality energy, which more and more consumers demand.

In traditional distribution networks, the protection system has played a significant role in preventing problems at one point in the network from spreading and causing disturbances in other parts of the circuit [2]. In addition, they create a necessary operational guarantee because they act autonomously, aiming at the security of the network and the people who are close to it.

With the advent of the new devices and philosophies of smart grids, there has been a gradual exchange of traditional devices for smart devices in all distribution systems. Two types of devices and philosophies exist at the moment. Depending on the power distribution company's investment capacity and operational needs, deployment of new technology can take a few months to several years. Moreover, the growing presence of distributed energy resources (DERs) is increasing the challenges of the protection philosophies and the integration of different devices. Thus, in this context, one should notice that several recent

works in the literature have presented innovative protection philosophies for distribution systems. The traditional protection schemes and operations are not dealt with in most of these works.

1.1. Overview of the Smart Grid Strategies

The main idea of this section is not to present a complete and systematic overview of all smart grid strategies, but only to show that the previous works do not deal with traditional protection. They contribute with new control and protection strategies using smart grid devices only. They do not deal with the integration of the traditional protection elements (such as fuses, reclosers, and sectionalizers). This paper uses the terms “smart grid device” and “smart device” interchangeably. They refer to switches existing in the network that have some degree of automatism or intelligence.

In [3], a new strategy for adaptive overcurrent protection was prepared for short-circuit currents when distribution generation exists. This proposed strategy is based on intelligent electronic devices (IEDs) only, establishing procedures for islanded circuits. In [4], active network management is presented, defining operational and network structure changes according to the load and areas without energy. IEDs work together, without other information, to determine the best performance according to data from the overcurrent relays. In [5], a new strategy for optimal protection coordination using dual-setting, directional over-current relays was installed in switches connected in IEDs. There was communication among the IEDs. The reference [6] proposes a meta-heuristic approach for feeder reconfiguration after a short-circuit. The process is based on a discrete particle swarm optimization technique. It considers the load of each branch, the branch capacities, and the IED switch positions to define the best new reconfiguration of the distribution network. In reference [7], fast islanding detection after a protection scheme operation is studied in many different situations with several points of view. Microgrid protection, operating in a grid-connected or an island situation, is also studied. Any single line is devoted to traditional protection elements in all these references. The proposed strategies are established for IEDs only. Equipment such as reclosers and sectionalizers without IEDs features and fuses are not dealt with in those papers.

Some papers related to distribution protection in smart grids follow. In [8], many analyses about protection devices, including distribution generation, are studied with control methodologies to change power flow in protection operation and reconfiguration schemes. In [9], some relay protection strategies are also examined, and the traditional relay protection tuning technology is incorporated in the proposed approach, aiming for wide-area protection. Additionally, in [10], an adaptive instantaneous overcurrent protection scheme is proposed, which sets parameters of IEDs using a real-time Thevenin equivalent circuit. Non-linear equations and Gauss solutions are involved in the IED settings. Only IEDs are implicated in the problem’s resolution, and no traditional protection is mentioned.

Recently, more papers have been published on smart grid devices’ implementations and their acting in the contingency problems in distribution networks. In [11], an interesting approach is introduced using two layers, one for power and another for communication. Several catastrophic contingencies are studied, and the smart grid device features and acting are studied. Experiments were carried out. In [12], several operational conditions and contingencies are studied to locate distributed generation units and shunt capacitors in the distribution network. Those studies took into consideration the actuation of smart devices only. In [13], the system reconfiguration strategy is based on smart devices and external energy sources to supply the critical load of the network. Mixed-integer linear programming runs a stochastic model to create reconfiguration solutions for the network. In [14], a new strategy for forming microgrids in the reconfiguration problem is described. The issue of reverse power flow, the frequency/voltage regulation provided by inverters, and grid support capabilities are studied. The contingency is isolated by the smart grid devices only. Finally, reference [15] presents an interesting complete overview of the smart

grid computational methods. In those methods, only smart devices are used to solve protection and contingency problems. Traditional protection is not mentioned.

Therefore, there is a research gap in the integration of smart grid devices into the traditional protection devices presented in distribution networks, which neglects the reality of these systems in many places around the world. Thus, there is a need to study the implementations of the functions in IEDs and in the traditional protection schemes. It is crucial to notice that the term “intelligent” in “intelligent electronic devices” is not appropriate. The reason for that is presented in a section of this paper.

This paper deals with the integration of smart grid devices into the traditional protection devices of distribution networks more practically. Our main contribution is to present a proposal for precisely integrating a rule-based system into IEDs, transforming them into “real” intelligent devices (named intelligent agents) interacting with the existing devices in the protection systems of current distribution networks.

1.2. Operation in an Incomplete Smart Grid

This consideration is crucial, because these two operational philosophies can remain simultaneously active for months or years. It depends on the power distribution company’s financial capacity and the network’s necessities. In fact, in most developing countries, this incomplete integration will remain for years without a deadline. For example, in Brazil [16], as in many developing countries, such as India, Russia, China, Thailand, Mexico, and South Africa, the most critical aspect to accelerating the substitution of one structure for another is the consumers’ power supply continuity indexes.

The integration analysis for the two philosophies presented in this paper is fundamental mainly for crowded cities with millions of inhabitants. These cities in developing countries have distribution systems in several stages of evolution. For instance, a city with two million inhabitants has around twenty substations spread throughout. Each substation has 5 to 10 circuits, and each circuit is 50 to 70 km and has 500 transformers for low voltage supply. Usually, the distribution protection system is using reclosers in some critical points of the circuit (around 10 per circuit), sectionalizers (approximately 2 to 4 per reclosers), and fuses at each branch of the circuit and in all transformers.

Table 1 shows an aerial photo of a region supplied by two substations (SS1 and SS2), and only three 13.8 kV circuits are represented. SS1 and SS2 have 8 and 10 circuits, respectively. In these three circuits, there are 283 transformers, more than 5000 consumers, 79 branches, and 18 km of extensions, supplying approximately 15 MVA [17–19]. The red squares represent the locations of nine existing reclosers (three per circuit with three sectionalizers each), and the green squares are the three tie switches (Figure 1).

Table 1. Typical load values for branches before 6 pm on a Friday.

S8–S9	S9–S10	S10–S11	S11–X
15A	15A	15A	5A

Regarding these circuits in a smart grid implementation process, the first switches that would be transformed in IEDs are some of the nine reclosers and twenty-seven sectionalizers, and primarily the three tie switches [17]. A significant number of the circuits would continue with the traditional protection (the reclosers and sectionalizers not transformed in IEDs, and the fuses, would be around 350). Thus, it is clear that the implemented IEDs need to interact with the fuses and the other traditional devices (not transformed into IEDs) to seek collaboration in the network trying to integrate the two protection philosophies.



Figure 1. Example of a real distribution network [17].

This paper offers a step in this direction, presenting how simple rules can be incorporated into the IEDs to integrate operations of the traditional devices. It starts with an overview of the main concepts of the traditional protection elements for urban and rural networks and the main elements of the smart grid and intelligent systems. After that, the general structure of an IED is shown, and the most popular devices used in the automation distribution systems are presented along with an analysis of their features and a comparison among them. Then, possible integration of IEDs with fuses is proposed, after introducing the concept of load partitioning each branch. Then, the integration of intelligent agents with reclosers and sectionalizers is presented. Finally, case studies using an existing distribution network are presented, and the computational implementation results prove the efficacy of the proposed methodology.

2. Presentation of Important Concepts

2.1. Main Concepts of the Traditional Protection for Distribution Networks

When protection structures in urban and rural distribution networks are observed, it is possible to verify that they have some switches to open short-circuits along with their circuits, such as fuses, reclosers, and sectionalizers.

A fuse is an element that interrupts the short-circuit current by burning its filament, which then has to be physically replaced by a utility maintenance team. This repair can sometimes take hours (between fault detection and travelling to the location), although the exchange can be done in just a few minutes.

Reclosers are devices that can eliminate short-circuits, including the entire reconnection procedure, by the verification of non-permanent short-circuits.

The sectionalizers act in conjunction with the reclosers, but cannot eliminate short-circuits. Suppose a sectionalizer observes a short-circuit current at one of the reconnection openings. In that case, it opens and remains open by isolating the power from the short-circuit and allowing the rest of the circuit to continue to operate.

Other topics in the protection of traditional urban networks are their coordination and selectivity. These two concepts are fundamental [20]. Coordination is the act of disposing of two or more pieces of protective equipment in series, according to a specific order. Selectivity is the ability of protective devices to act before their backup devices. For example, only one protection device should work as close as possible to the short-circuit when a short-circuit occurs. When this happens, it is said that there was coordination between the protection devices and that there was selectivity between them. Another example of this situation is when some (or all) protective devices that have seen the short-circuit current act. In this case, it is said that there was no selectivity, but that coordination occurred. Finally, neither selectivity nor coordination happened when both the nearest protective device (or devices) did not act, and Figure 2 shows these situations.

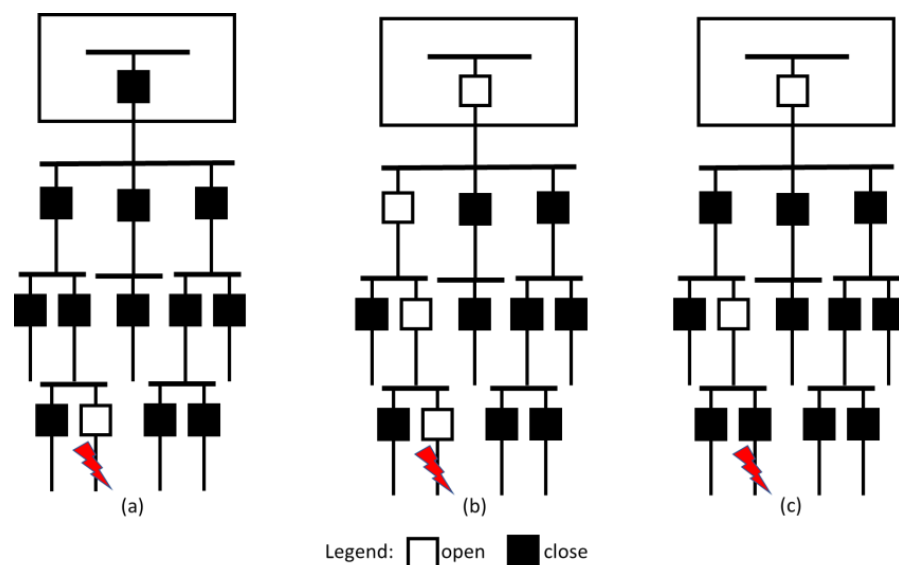


Figure 2. Situations of protective action: (a) with coordination and selectivity, (b) with coordination but without selectivity, and (c) without coordination and selectivity.

2.2. Differences between Smart Grids and Intelligent Systems Concepts

The aim of writing this section was not to present a complete overview of the smart grid concepts and their structures, but only to show some points related to the proposed developments. Firstly, it is important to distinguish between two concepts: smart grids and intelligent systems. Some smart grids can be intelligent systems, but not every smart grid is intelligent; they only are if intelligent techniques are applied to solve a problem. Thus, it is fundamental not to confuse systems with automatisms with intelligent systems. Many manufacturers often falsely sell their products as intelligent products, but they do not include intelligent techniques. Example of these types of devices which have in their names the word intelligent are the IEDs (intelligent electronic devices). They each have a set of structures (analyzed in the next section) to produce an answer automatically, but they are not intelligent devices.

Figure 3 presents a Venn diagram, showing that smart grids do not always include intelligent systems and that intelligent systems are not always applied in smart grids. The important point for this work is the elements that can be present in both: the intelligent elements of the smart grids.

In the region of interest, there are devices with intelligent techniques to solve certain problems. These devices have communication systems to exchange information with other devices or a central system for the most part. If they do, they have all the features necessary to make them “intelligent agents” [21].

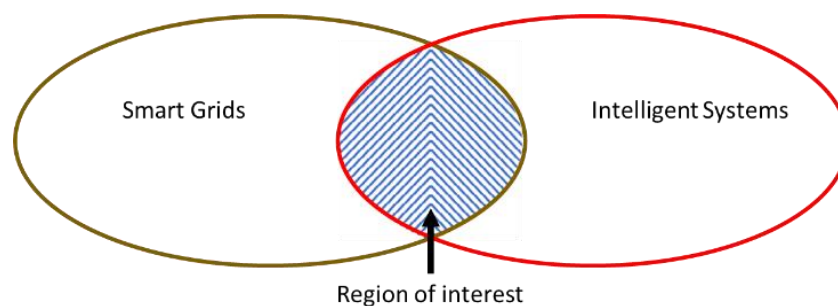


Figure 3. Venn diagram showing smart grids and intelligent systems worlds.

Other important differences introduced by smart grid technology compared with traditional protection are two-way communication, self-monitoring, self-healing, and pervasive control. In traditional protection systems, there is no communication, manual monitoring, manual restoration, and limited control [22]. Additionally, a smart grid has sensors throughout the network, increasing the observability, and the communication allows interactive activity among devices and with multiple stakeholders [23].

3. Overview of IEDs

The term intelligent electronic device refers to an extensive range of electronic devices that automate a system, be it a power plant, a substation, or a distribution system. Several functions can be incorporated into IEDs, such as protection, monitoring, and local control. The main aims of this section are to address whether there is any mention in the literature about the interactions of these IEDs and traditional protection elements and to verify if the IEDs have features to support the proposed approach. This section initially discusses the structure of an IED, showing its features and how an external program can be incorporated into it. Then, the most popular IEDs used currently in distribution system automation are shown. Finally, we show how a set of IEDs can be transformed into a multi-agent system (MAS), producing an intelligent multi-agent system.

3.1. General Structure of an IED

A typical IED architecture consists of microprocessors, local memory, digital and analog inputs, outputs, a communication system, and a power supply. The functions of the microprocessors include the execution of the protection algorithms. Most software used in IEDs works through a set of pre-programmed tasks, which only require adjustments to their parameters. These functions include displaying voltage and current values and limits, data recording, local database control, switch status, interlocking, self-reconnection, and adjusting groups of protections. Within this set of tasks, an essential component is the real-time operating system (RTOS), whose role is to ensure that all other tasks are performed appropriately and in the established priority order [24].

Concerning the software's logic, it is usually made by a human-machine interface or a dedicated communication port. These logics can be written in simple languages, such as Ladder, or directly in more elaborate programming languages, such as C.

Nowadays, for communication, IEDs use IEC 61850 [25], which is a standard for communication networks and systems in substations. Additionally, the IEC TC57 [26] standard has been developed for distribution network automation, and it is based on IEC 61850 guidelines. These standards allow all IEDs from different manufacturers to communicate, exchanging data and messages. The GOOSE protocol [27] provides an efficient way for IEDs to send and receive messages.

3.2. Overview of the Most Popular IEDs Systems Used in Distribution Systems

This section includes the analysis of some of the technological solutions of IEDs systems used in distribution systems available in the market, which are: Schneider Electric's Intelligent Loop Automation, S&C Electric Company's IntelliTeam SG, Eaton's Yukon

Feeder Automation, NovaTech's Distribution Automation, SEL's DAC, Hitachi Energy's Distribution Feeder Automation, and the Siemens Self-Optimizing Grid. The intention is to show the possibility of incorporating functions in all these systems, especially those proposed later in this article, and to map these devices' functional characteristics, applications, and strengths.

3.2.1. Schneider Electric's Intelligent Loop Automation (ILA)

ILA [28] uses a distributed architecture based on logical schemes embedded in the ADVC reclosers' controllers and the disconnecter switches' controllers. Depending on the mode of operation, each IED has one of three possible pre-programmed functions: feeder, tie, or mid-point. A feeder IED usually is closed and opens when it detects an overcurrent in its terminals. The tie IED is the point of the normally open scheme that closes when it catches a loss of voltage in the source terminal or the load terminal. The mid-point IED is located along the feeder, anywhere between a feeder IED and a tie IED. The mid-point IED changes protection group and enters before the tie device closes to maintain the radiality of the circuit.

The loop automation schema can contain two feeder IEDs, multiple mid-point IEDs, and one tie IED. It is necessary to integrate the various LA schemes configured within a distribution system to use a remote terminal unit (RTU) to control the hybrid system. The most current versions of firmware support overload control, which allows the system to avoid transferring load to a feeder that cannot support it. ILA still has an editor to create and supervise the network architecture, in which some additional rules can be incorporated.

3.2.2. S&C Electric Company's IntelliTeam SG

IntelliTeam SG [29] uses a decentralized architecture with an RTU (called IntelliNode) installed at the top of each participating IED (relays, reclosers, circuit breakers, and disconnecter switches) or directly on S&C's reclosers. IntelliTeam SG monitors voltages and currents in real-time using sensors built into fault-sectioning devices. Each IED is configured to know its normal function in the system and other essential parameters, such as the amount of load the device is authorized to receive, the role of the device in the set, and the priority of the source.

The system divides the network topology into groups called teams, hence the system's name. The manufacturer states that there is no limit to the size of the system. S&C offers a topology configurator that also acts as a SCADA to edit and supervise what IntelliTEAM does. It can edit the topology almost freely by inserting the IEDs and connecting them within the schema. This tool also has a replay option, allowing one to visualize in a graphic diagram what happened before, during, and after self-recovery procedures. The S&C system can prioritize sources, handle multiple short-circuits, and avoid feeder overloading. Additionally, it is possible to restore the system to its normal configuration state or decide on a new normal configuration state after the self-healing process has been completed.

3.2.3. NovaTech's Distribution Automation

The Orion DA-Master is a NovaTech Orion system [30] with specialized software that functions as an independent master controller in a single or multi-feeder, single or multi-substation distribution automation system. The DA-Master scans measurements, analyzes the data, and initiates the opening and closing commands in the various IEDs installed in the distribution system to perform user-defined system reconfiguration in response to abnormal system conditions. The DA-Master supports several communication protocol options that are available in the various IEDs currently found on the market.

If remote monitoring or control is required, the DA-Master can also communicate with an existing SCADA master system in the distribution system. NovaTech Communications Director (NCD) is the logical configurator and has a vast library and protocol profiles of the various modern IEDs. A computational package called DA-Simulator is also available that allows the user to model the distribution system, simulate different short-circuit conditions

in each participating IED, and predict the actions of the self-healing algorithm before the equipment is installed in the field.

3.2.4. Eaton's Yukon Feeder Automation (YFA)

YFA [31] uses a centralized architecture with a self-healing algorithm configured in an RTU, usually installed in the substation. A dynamic system integrates real-time data from the distribution system to detect disturbances and automatically reconfigure the system to isolate the short-circuit, minimizing the total number of affected customers. Several IEDs can be integrated, such as relays, disconnecter switches, capacitor bank controllers, voltage regulators, and short-circuit indicators.

YFA scans the participating IEDs of the self-healing system with various communication protocols, managing all automation functionalities of the distribution system, and can also be integrated into existing SCADA systems. The YFA editing program is a dynamic and configurable platform that uses object-oriented programming. It has a topology editor and a simulator, offering the user the possibility to test the configured programming and its response under normal and abnormal conditions in the distribution system.

3.2.5. SEL's Distribution Automation Controller (DAC)

The DAC [32] uses a hybrid architecture with a self-healing algorithm configured in an RTU, usually installed in a substation. The RTU responsible for data concentration, execution of logical schematics of self-healing, and data communication processing is a real-time automation controller. The system has a primary real-time automation controller that communicates with other substations and the IEDs participating in the distribution network. In this controller, the computer program responsible for the automatism of the network exists. The controller performs algorithms automating isolation and power restoration procedures during short-circuit situations, while additional algorithms optimize network's performance through voltage control and reactive power control. Overload reduction techniques are also used in cases of abnormal electrical system operation.

The system is independent of the IED manufacturer. It can also be integrated into the existing SCADA system, and the configuration is based on libraries and protocol profiles of the various IEDs available on the market. The various IEDs, such as relays, disconnecter switches, capacitor bank controllers, voltage regulators, and short-circuit indicators, can be integrated.

3.2.6. Hitachi's Distribution Feeder Automation

Hitachi's Distribution Feeder Automation [33] uses a decentralized solution installed in the field. The RTU500 series are controllers with an integrated predefined algorithm that allows integrations in medium and low-voltage grids. Sensors and functions work using motorized switches to quickly identify a faulty cable, isolate the fault, and restore the supply. This application uses an Automatic Transfer System (ATS) for simple reconfiguration functionality and includes a high-level solution with peer-to-peer communication. The trigger happens by a failure detection in the primary active source.

This system contains all necessary applications connected to a distribution system to small-scale or mobile power stations. This RTU-based application includes a communication link, automatic speed, power factor, and voltage control. The system registers long-term or periodic overload stresses, and the asset's maintenance plan algorithm can support them.

3.2.7. Siemens Self-Optimizing Grid

The Siemens Self-Optimizing Grid system [34] is based on a regional controller on the substation level, ensuring automatic fault localization, isolation, and restoration. Special controllers make the interface with the control center. They measure data through the distribution network and host the grid's regional and centralized applications. Self-Optimizing

Grid solutions integrate the different grid levels, and depending on integration level, can be: centralized, hybrid, or decentralized.

The Self-Optimized Grid solution comprises the most relevant applications for hybrid solutions. These applications accurately monitor the grid and remotely control stations to ensure high supply reliability and improve system performance. The solution integrates these intelligent automation functions: self-healing, load management, automatic source transfer, overload reduction, and area voltage control.

3.2.8. Comparative Analysis of the Described Technologies

It is known that the structure of a smart grid must be elaborated so that its equipment allows interoperability with different systems. Thus, different algorithms can be deployed for system optimization. The seven systems offered have applications in distribution networks with different evolutionary levels of automation. Altogether, they cover each level of automation and every available network. It is important to note that the evolutionary level of each system is not linked to the technical capacity of the company that owns it, nor the ability of its technical development team. This evolutionary level is related to a company's market strategy, aiming to target one type of system more than another.

The usefulness of the described systems is easily verified by their automation of the identification, isolation, and restoration operations in response to the short-circuits. However, none of them confirmed the existence of functions that deal with traditional protection systems. They would need functions to interact with reclosers, sectionalizers, and fuses. Nevertheless, all shown IEDs have a way to write and manage these functions and analyze the data coming from the network. It is essential to note that traditional devices do not communicate with IEDs. Still, the current that passes through an IED makes it possible to make inferences, as shown later in this article.

3.3. Transforming a Set of IEDs into a Multi-Agent System

The shown IEDs can also be called agents [35] because they have all the main features of them: autonomy, adaptivity, contextuality, and sociability. They have a degree of autonomy which can be chosen based on the system they are to be used in. They also have a certain level of adaptivity to choose the best actions to take. They can contextualize their activities to define if an action must be taken. Finally, they have the ability to interact with others IEDs (sociability). The main elements of the agent are represented in Figure 4. In this figure, the intelligent controller is in a recloser; however, it can be put in another distribution network switch. The intelligent controller receives the data (such as current and voltage measurements and the status of the switch, among others) through its sensors. These data are given to the processing unit of the control, which contains algorithmic, numerical, and intelligent parts. Each part has a specific mission. The algorithm controls the entire process of the IED. The intelligent part provides inferences for each operational state of the network and the controlled switch. It uses the data from the sensors and the data saved in the local memory to choose an action for the controlled switch and to communicate information with other IEDs. The intelligent part usually triggers the numerical part, but the algorithmic part also uses the numerical part a few times. The local memory contains data of the observed part of the network observed by the agent. Finally, the communication system is the way to send and receive messages from and to the other agents.

An agent can be of two types: a common agent or an intelligent agent. The common agent is the one that reacts (or acts) according to a certain logic but without the basis of techniques of an intelligent system. In the world of artificial intelligence (AI), an intelligent agent is a computational system that is able to perform independent actions for the benefit of itself or its controller. Agents are expected to act rationally, operate autonomously, perceive their environment, adapt to changes, and achieve their goals. When uncertain, a rational agent obtains the best or expected outcome.

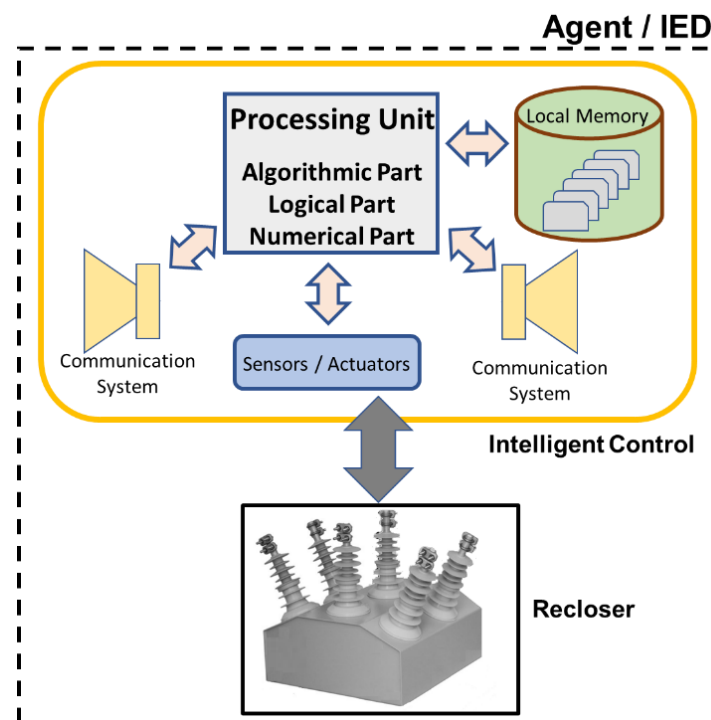


Figure 4. Intelligent agent structure.

Agents can interact among them to find a better solution to a problem, creating a multi-agent system (MAS) [36]. The MAS may have one more qualifier, the word “intelligent.” There are two situations in which an intelligent multiagent system can be found. The first is when the system has intelligent agents that interact and perform functions capable of accomplishing the objective proposed by the system in which they are inserted. The second type is one in which there are only “common” agents (which do not use AI techniques), but that “intelligence” emerges from their interaction. In this work, the intelligent multiagent system is composed of intelligent agents; however, the acronym MAS is maintained.

In a MAS, all intelligent agents should be able to communicate. Each must have the knowledge and skills to perform a particular task and may or may not cooperate to achieve a global goal. It is noteworthy that each agent in a MAS has incomplete information, and agents form a system with sufficient knowledge and ability to solve the problem. Nowadays, MAS is the most important technique to operate distribution networks [37], helping especially during the contingencies, such as short-circuits. In a complete MAS, all actions to eliminate a short-circuit, isolate the branch in which it occurred, and restore the branches without energy, are done by the intelligent agents distributed along with the electrical distribution network [38].

The MAS can be classified into three main types: centralized, decentralized, and hybrid. In the centralized MAS, there is a central process control that maintains communications with all agents, performs the main operation strategies of the network, and sends which actions each agent must produce. Only a few inferences are made locally, and the most part is done in the central unit. Examples of this type of MAS are presented in [39–41].

There is no central unit in the decentralized MAS, which means the agents must make all performances and inferences locally. The agents communicate with other agents to provide a solution for a problem. There is no global system control, decentralized data, and asynchronous computation. Examples of the decentralized MAS are presented in [42–44]. In this work, the MAS considered is of this type, and all the processing is done locally in the agents.

There is a balance between the central and local inference in the hybrid MAS. Central control performs the computation linking all data from the network, such as numerical programs (like load flows) or main strategies (like load shedding). In contrast, the local

control performs by the agent taking care of the switching strategies and local verification of the overload, over (or under) voltage, or short-circuit detections. Examples of the hybrid MAS are presented in [45–47].

4. Proposed Methodology

This section presents the proposed methodology for integrating smart grid devices into the traditional protection of distribution networks. The section presents functions to work with fuses, reclosers, and sectionalizers, and then a summary of the intelligent agent rules.

4.1. Functions to Work with Fuses

In a decentralized MAS, all functions must be in the agents to be performed through inference processes. This section presents a function that incorporates the intelligent agent that allows interactions with fuses. The inclusion of this function allows a more gradual introduction of smart grid elements next to traditional urban networks. Over time and with financial availability, one could replace fuses with intelligent agents.

Implementing this function in the smart agent is not enough to detect the time to break the fuse links before it acts. The intelligent agent should monitor this loss of load and have a supervisory function; i.e., it should inform the operating plant about the fuse link disruption and the consequent loss of load. This allows the utility to send the maintenance team to change the fuse before receiving calls from consumers without power, reducing the durations of power outages and improving the reliability of the System Average Interruption Duration Index (SAIDI). This is one of the advantages of a smart grid.

Agents always supervise fuses downstream and monitor a load loss resulting from opening one of these fuses. The strategy is easy to understand, but its implementation needs a set of calculations that to be performed, depending on the current reduction view by the agent, involving daily load behavior and load forecasting. The load reduction perception function detects “abnormal” variations in the current and places the agent at the attention level.

The system shown in Figure 5 can be helpful to illustrate how this function performs. This figure contains a hybrid protection system merging intelligent agents, fuses, reclosers, and sectionalizers. Each switch S is one protection device. For instance, the elements S7 and S8 are intelligent agents; and S9, S10, S11, S12, and S13 are fuses. Agent S7 supervises fuses S12 and S13, while agent S8 supervises fuses S9, S10, and S11.

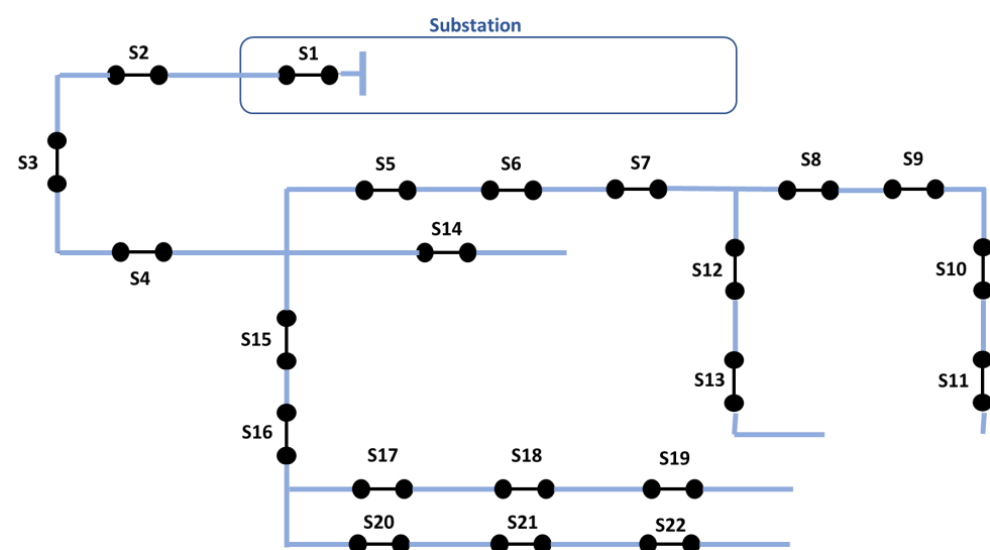


Figure 5. Typical distribution network with hybrid protection devices.

Thus, when the S11 fuse opens, S7 and S8 check the load reduction. They must communicate to determine if this occurred in the fuses supervised by S7 or S8. If both noticed, the loss is on agent S8's line, but if only S7 realized, it was one of the fuses it supervises. Again, if both detected the load reduction, then it is one of the fuses supervised by S8, and it should start an analysis process to know if it was the fuse of S9, S10, or S11 that broke.

4.1.1. Verifying Which Fuse Has a Problem

Once an agent has established that it is likely responsible for the fuse that acted, this verification procedure is initiated. The intelligent agent infers whether the abrupt load reduction occurred due to the opening of a fuse or the simple removal of a large load block (for example, a factory). This check is done through a procedure that investigates whether a short-circuit current occurred immediately before the reduction of a large load block. If this happened, there is a strong chance that the fuse link would have broken; otherwise, there must have been a load reduction. However, the question remains: are these statements entirely factual? The answer to this question is no, because the short-circuit may have occurred within a factory, and in this case, its main circuit breaker has removed the factory without burning the fuse link. In the second hypothesis, the fuse link has been burned due to an overload in the circuit.

It should be remembered that the fuse link has a "memory" of the events that passed through it. This memory exists because it does not necessarily merge at once. It is degraded whenever an overload or a short-circuit current passes through (which is not primarily responsible for opening). Remember that this degradation process is thermal and irreversible.

Although this procedure is not foolproof, it increases the observability of the electrical network, because an agent closer to the event will have greater sensitivity to direct network maintenance efforts than the total lack of observability that occurs in networks with traditional protections.

After checking for a short-circuit current, the agent calculates the load drop, in percentage, by the difference between the pre-fault current and the current divided by the pre-fault current value. The result is used in the next steps of this procedure.

The agent verifies whether the value of the percentage load drop was higher than a pre-established Δ value: if yes, the continuous inference process moves to the next step; if not, the process is completed, and the agent returns to normal. This Δ value allows minor typical load variations to not be confused with load dropouts.

With the process continuing, the next step is to check the memory of the intelligent agent for the load partitioning of each branch. It is placed there when the agent is the initial setup.

This load partitioning is done through the expected workload in the branches, and it represents the typical workload of the branch for one week. Usually, purely residential branches have similar load profiles, only vertically moving the data curve. In contrast, other load profiles (industrial or commercial, or composed of various load types) have different profiles. Power utilities have this data because they carry out measurement campaigns for other purposes.

Thus, when the inference is being made (or during an event, which is the same), it searches for the nearest whole time, and calculates the load of each switch for this time and the partitioning values in percentages. Hence, these partitioning values are compared with the percentage value of load drop, checking the nearest. The nearest value defines the fuse that acted.

Then, the agent must send information to the substation informing it of the broken fuse link to expedite the maintenance process and return energy to the branch (or branches).

4.1.2. Example of Integration of Fuses with Smart Grid Devices

Consider Figure 5, where, as reported above, agent S7 supervises fuses S12 and S13; and agent S8 supervises fuses S9, S10, and S11. Suppose a short-circuit occurs in branch S10–S11. By the coordination criteria, the proper response is the fuse of S10 interrupting the power supply of branch S10–S11 and the branch after S11.

As the short-circuit occurred on the S10–S11 branch, the intelligent agents S7 and S8 observed the short-circuit current. Other agents may also have seen the short-circuit current. Still, due to the simplicity of the explanation, the inferences are reported only by agents S7 and S8, since the other agents will verify that they should not take any action, as would occur in the case of agent S7.

Agent S7 notes that at least one of the agents of each team also observed the short-circuit current, and for this reason infers that it should not take any action because the short-circuit did not occur in its observation area.

Agent S8, on the contrary, alone in its team received this information, and hence infers that the short occurred in its observation area. Hence, this agent differentiates between the pre-fault current and the actual current. Assuming that these values are 45 and 32A, respectively, the percentage value of load drop is calculated: 29% $(= (45 - 32) / 45 \times 100\%)$.

Assuming that the Δ value is 4%, the agent infers that one of the fuse links it oversees has been opened. Thus, its rules observe the current hours and take the nearest whole hour. Adopting in this example 17:42 h on a Friday, the typical load data of 18:00 h of each branch are accessed. For example, consider the data shown in Table 1. Table 2 shows the percentage value of the load drop of 29%, showing that the S10 fuse link broke.

Table 2. Typical loads on agent S8 and the fuses S9, S10, and S11 at 6 pm on a Friday.

S8	S9	S10	S11
50A	35A	20A	5A
-	70%	40%	5%

4.2. Functions to Work with Reclosers and Sectionalizers

Other devices that have been used in the traditional protection of urban networks are reclosers and sectionalizers. The function of the reclosers, as stated above, is similar to that of circuit breakers in substations. They can also eliminate a short-circuit and are provided with automatism that allows the timed interruption of the short-circuit current with two main objectives: to verify if the short-circuit is transient and enable the operation of the other protection devices closer to the fault. The sectionalizers also observe the short-circuit current but cannot interrupt it. This opening only occurs in one of the interruptions caused by the recloser. There can be multiple sectionalizers together with a recloser. For example, consider the network of Figure 5, where the S15 protection device is a reconstructor, and the S17 and S20 devices are sectionalizers. The main idea behind this configuration is that faults in the branches after S17 (or S20) are interrupted by the sectionalizer responsible for the branch (not by S15). It causes the faults to be restricted to a minor portion of the network.

It is essential to mention that these two devices may not be simultaneous. Still, the number of times the reconstructor takes action can be counted by the sectionalizer agent.

4.2.1. Integration Function Procedure with Reclosers and Sectionalizers

To exemplify the integration function with reclosers and sectionalizers, consider the network of Figure 5, where the protection device S15 is a recloser; devices S17 and S20 are sectionalizers; S4, S5, S14, S16, and S18 are switches for intelligent agents; and S19, S21, and S22 are fuse switches. It is important to note that S15, S17, S19, S20, S21, and S22 are traditional devices without intelligent agents. Thus, the communication happens in the following teams (formed in the area of interest of the example): S4–S5–S14–S16, S16–S18.

The procedure of this function is similar to that presented in the previous section. It uses the concept of load block loss. This loss occurs with the opening of the fuse (breaking

of its link); this loss is caused by the opening of the recloser or a sectionalizer. Thus, it is essential to know which agent monitors which device.

In this example, agent S4 supervises S15; agent S16 supervises S17, S20, S21, and S22; and agent S18 supervises S19. There is no difference between monitoring a fuse (S21 or S22) and a device (S17 or S20—sectionalizers) to the agent. What matters is simply knowing the load partition on each branch so that the calculation described above can be performed by the agent that monitors these protection devices (which is S16).

Three illustrative cases are studied in this section, with short branches between S17 and S18, between S21 and S22, and between S16, S17, and S20.

In the first case, the short-circuit occurs on branch S17–S18. Hence, the protection acts as follows: S15 verifies whether the short-circuit is temporary or permanent, and if it is permanent, in one of its openings, the S17 sectionalizer opens. Then, after eliminating the short, the agents begin their verification process and possible restoration of the branches. Agents S4 and S16 observed the short-circuit current, and S18 continued.

Thus, agent S4 concluded that nothing should be done because the short-circuit is not in its team's area (S16 also observed the short-circuit current). Agent S18 did not notice anything, then continued right away. Agent S16, which also noticed the short-circuit current, contacts agent S18 and verifies that the short ran through it and is not beyond agent S18.

As agent S16 monitors S17, S20, S21, and S22 protection devices, it should verify which device acted. This is done by the same load partitioning process shown earlier. Thus, it is determined that S17 was the device that acted.

One could also have an additional rule that would indicate whether there are protective devices between S16 and S18 (which ran out of power), and if this second agent ran out of energy, it is because a protective device activated between them. This rule verifies the veracity of completion performed by agent S16. Moreover, when the agent infers that a device has acted, it sends a signal towards the substation informing it of the fact (in this case, device S17).

In the second case, the short-circuit occurs on branch S21–S22. Hence, the protection acts analogously: S15 verifies the type of short-circuit, and being permanent, in one of its openings, the fuse link S21 opens. Then, after eliminating the short, the agents begin their verification process and possible restoration of the branches. Agents S4 and S16 observed the short-circuit current, and S18 did not observe it. Thus, agent S16 infers that the short ran through it and that it happened no further than agent S18.

Agent S16 contacts agent S18, informing it of its actual current. In this way, the agent, as it has the protection devices S17, S20, S21, and S22 under it, performs the calculation of the load loss with the load partition process and checks which device is closer to the load loss, which in this case should be S21. It will send this information to the substation.

In the middle of this process, the verification of the veracity of conclusion is performed, using the rule, which confirms that if S18 also observes the current, it is because S17 did not act.

These two cases involve similar actions and are based only on the partitioning of loads between the branches. The following case is a little different.

In the third case, the short-circuit occurs on branch S16–S17–S20. Hence, the protection acts similarly to the past: S15 checks whether the short-circuit is permanent; it opens, as no other device acted. Then, after eliminating the short-circuit, the agents begin their inference process. Agents S4 and S16 observed the short-circuit current, and S18 did not maintain it. Thus, agent S16 infers that the short ran from after it and was from no further than agent S18. It also verifies that it is out of charge current and that the short-circuit insulation process should begin.

Then, agent S16 starts this process by opening, locking, and sending a message so that S18 also opens and locks. If there were relief circuits, the restoration process would continue in the same way as this document presented.

When opening, S16 sends a signal, in this case, to S4, stating that the circuit breaker can close. As there is a load current in S4 and it monitors a traditional protection device, it turns this message into an acting message for the S15 protection device. There is a problem with the branch after S16 and before S18 (branches S16–S17–S20, S17–S18, S20–S21, S21–S22, and S22–X). When the S15 recloser reaches its standby time, it automatically closes, and there is no longer a short-circuited power supply, and the branch S15–S16 powers back up.

4.2.2. Incorporation of an Intelligent Agent in Reclosers and Sectionalizers

The proposed agent is structured to act on any type of switch, with or without the ability to eliminate the short-circuit current. Until this point in this work, the agent has been used in two ways: in the switches of the substations (circuit breakers—which open short-circuit current) and in the branch switches (disconnectors—which do not open short-circuit current). However, it is important to remember that the agent's structure is the same for each of these switches, regardless of their type.

Thus, the inclusion of the proposed agent, reclosers, and sectionalizers does not bring about any problem, because reclosers are similar (in their performance) to circuit breakers. At the same time, sectionalizers are identical (in their performance) to disconnectors. The philosophies of coordination and selectivity should be kept from the traditional protection structure.

With the agents placed over the protection devices S15, S17, and S20 of Figure 5, the new teams formed in the area of interest are: S4–S5–S14–S15, S15–S16, S16–S17–S20, and S17–S18.

4.3. Intelligent Agent Rules for Integration with Traditional Protection Devices

This section summarizes the key actions (rules) of the intelligent agent (IEDs plus knowledge-based system—KBS) for integration with traditional protection devices. All inference processes start when the IED notes a short-circuit current. After the short-circuit area's elimination, the KBS starts to be executed. It can be divided into two main parts: verifying the performance of a traditional protection device and validation of the integrity of the conclusion, and the KBS is shown here through production rules.

4.3.1. Verification of the Integrity of the Supervised Switches

This rule is used to confirm (or change) the checklist of devices that have provided the loss of a load block. This occurs when these devices are between two intelligent agents. There are two possible situations for using these rules, which are always activated after setting the short location by the agent on one of its sides.

The first case is when the agent has load current and the adjacent agent does not. The second case is when both have load current after the short's elimination. With this, in the first case, it turns out that the device that operated is between the two agents and that all the devices between the two are the ones that make up the list of devices to be checked. In the second case, it was concluded that neither device between the two agents put up with it, so neither device should be on the list to be checked.

Notwithstanding these facts, all devices must be present in the composition of the load partition calculation. The rules for this check of the completion veracity are as follows:

Check the load currents of the agents if both are nonzero. Action: Delete devices between these agents from the solution list.

If I of the agent $\neq 0$ and I of the adjacent agent $\neq 0$, then delete the devices between these agents from the solution list.

Check the load currents of the agents, and one of them is zero. Action: The solution list consists of the devices between these agents.

If I of the agent $\neq 0$ and I of the adjacent agent $= 0$, then the solution list comprises the devices between these agents.

4.3.2. Verification of the Performance of a Traditional Protection Device

The first part of the ruleset is to verify that the intelligent agent is responsible for searching for the possible action of a traditional protection device (fuse, recloser, or sectionalizer). The IED must communicate with the adjacent agents (adjacent IEDs) and verify that they have also recognized the short-circuit current (I_{SC}). If at least one of the agents on each side recognized this short-circuit current, it is not the agent responsible for doing this check. However, suppose neither of the agents adjacent to it observed the short-circuit current. In that case, it is responsible for searching for a possible action by a traditional device supervised by it. The rules for this are:

Check the short-circuit current, verify that at least one adjacent agent observed the short current, and verify that no agent on the other side noted the short-circuit current. Action: Search for the device that acted.

If I_{SC} was recorded, if one of the teams did not observe I_{SC} , then seek action for the device.

If I_{SC} was recorded by any of the agents of the two teams who observed I_{SC} , then return to the normal state of operation.

The second part of the rule, which is applied only to the agent who went through the first part, is to verify if the traditional protection device has been active, with a consequent loss of a load block. Thus, when the current returns to “normal,” it should be verified whether the difference between the pre-fault current (I_{PF}) and the actual current (I) is greater than the Δ value (pre-fixed, which is smaller than the load partition of the branches). If yes, it should be assumed that one of the devices supervised by the agent operated; if not, it is taken that there was no operation of supervised protection, and the agent returns to a normal state. The rules for this are:

Check if the difference between the pre-fault current and the actual current was greater than Δ . Action: continue the search for the device that acted.

If $I_{PF} - I > \Delta$, then continue searching for the device that acted.

The third part of the rule is the search for the device that operated, and this is related to the loss of a load block (difference between the pre-fault current and the actual current in the agent) and the time of day. There is a pre-registered form in the agent’s memory that supervises the load partitioning among the traditional devices. This load partitioning is registered on an hourly basis. Thus, the agent should approximate the current time to the nearest hour and compare the percentage of load block with the partitions at this time, and infer that the traditional protection that acted was the one with the most immediate partition. The rules for this third part are:

Transform the difference between the pre-fault current and the actual current to a percentage value and check the current time (assuming the nearest whole time). Action: Search for the closest percentage value.

If $d = I_{PF} - I$, assuming H:00 time, then check the partition closest to d to H.

4.3.3. Application of the Proposed Approach

This section shows the entire proposed approach where the intelligent agents handle the traditional protection operations. Figure 6 presents all necessary steps of this approach. At the start, the agent assumes all the required data from the observed (traditional) switches: the switch loads for each hour during the week. Additionally, the agent measures its actual current. The algorithm starts with validating the traditional switches observed by the agent. The process continues when a short-circuit current (I_{SC}) is detected. Initially, the agent needs to verify if it should take part in the process or not. If any adjacent agents did not observe the short-circuit current, the agent takes part in the process. Otherwise, if at least one adjacent agent on either side observed the short-circuit, it ends the process. This is performed using the first part of the rule presented above.

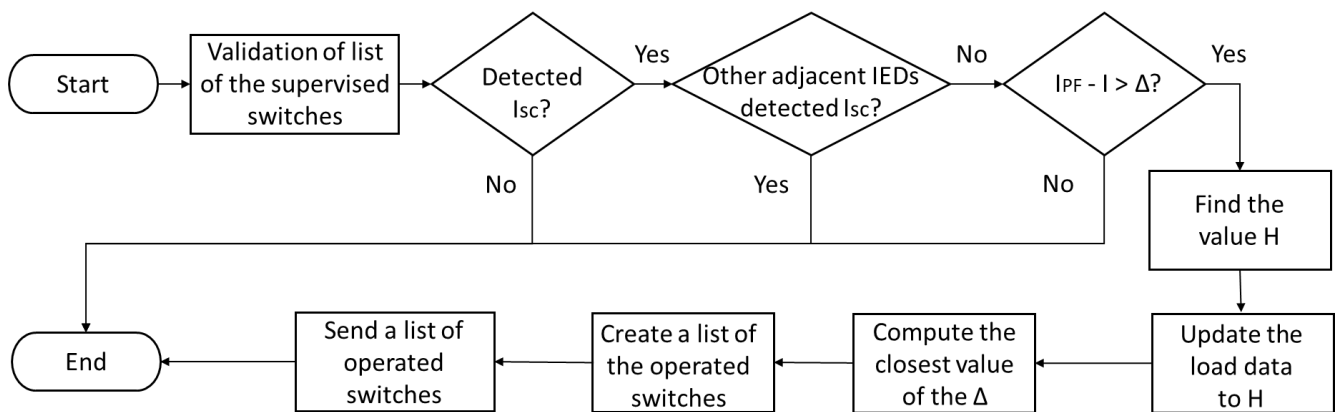


Figure 6. Flowchart of the proposed approach.

The next step is to verify the value of Δ , a pre-fixed value, and compute the difference between the pre-fault current (I_{PF}) and the actual current (I). This value must be smaller than the small load of the observed switch. If this difference value is bigger than Δ , the process continues; otherwise, the process ends. This step starts only after the system operation returns because the agent needs to know the (post-fault) current (I , named here actual current). The focus of this step is performance and is addressed by using the second part of the ruleset presented above.

After these previous steps are performed, the agent is ready to determine a list of possible operated switches. The first step of this part is to determine the value of H —the integer value of the time. For the time between T hours and zero minutes and T hours and twenty-nine minutes, the assumed value of H is T ; and between T hours and thirty minutes until T hours and fifty-nine minutes, the implied value of H is $T + 1$. This part of the approach uses the third part of the ruleset.

In the next step, the updating of the load data occurs. The pre-saved hourly load of each switch for the H value must be updated using a proportionality between the pre-saved value of agent load (I_0) for H and pre-fault current (I_{PF}). Then, for each switch, the pre-saved load value (I_{SWx}) must be updated to a new load value ($I_{SWx-new}$) for the following relation: $I_{SWx-new} = I_{SWx} \times I_{PF}/I_0$. This step's main idea is to promote an update of the values as if it were a system of forecasting load in the very short term.

The next step is the computation to determine a list of the closest values to the difference between the pre-fault current (I_{PF}) and the actual current (I). This list can contain a pre-defined number of switches or selected switches by a given criterium, like a pre-defined interval or percentage of the difference value. It is essential to notice the values used for this computation, the $I_{SWx-new}$ values.

Finally, the message with a list of possible operated switches is sent to the distribution control center, ending the process.

4.3.4. Final Remarks

It is worth mentioning that other characteristics than coordination and selectivity, such as characteristic curves, coordination issues, and other concepts of the traditional protection schemes, are not necessary to understand the proposed approach and are out of the scope of this paper. Moreover, in the proposed approach, the protection studies and the protection element settings continue unchanged. They are not modified by the introduction of smart devices to the network.

5. Application of the Proposed Strategy for Intelligent Agents

This section presents the proposed approach applied in case studies to illustrate the use of the proposed methodology in a didactic way. For that, the network shown in Figure 7 was used. It shows a single-line diagram of a real network of a Brazilian distribution company, which is described in [1,48]. Each bus has a protection device: fuse, recloser,

sectionalizer, or intelligent agent. This network's data contains one-hour load curves divided into working days, Saturdays, and Sundays/holidays. This network is a smart metering pilot project with more than 7000 residential/commercial low-voltage consumers.

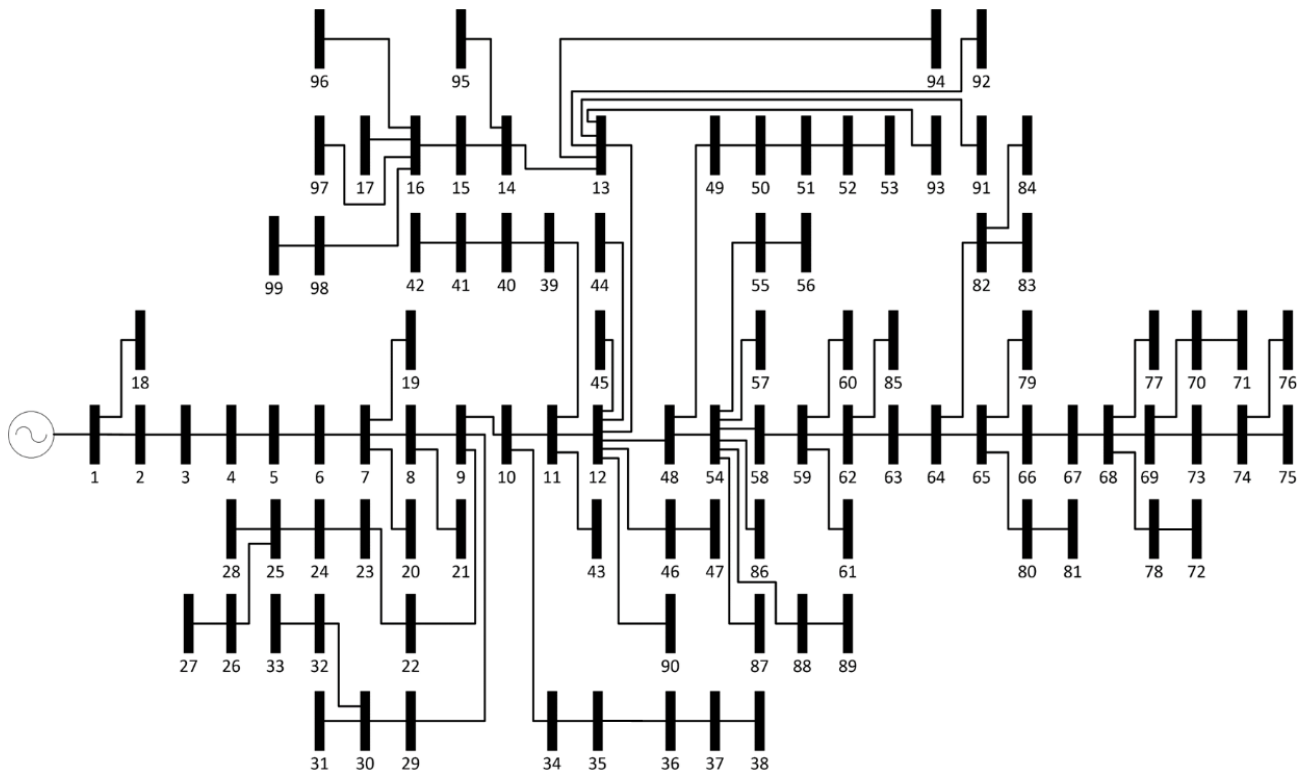


Figure 7. A diagram of a real network of a Brazilian distribution company [1,48].

In this case study, the part of the interest of this network is located from switch 64 onward, i.e., switches 64–84. These switches can be classified as intelligent agents (64, 68), a recloser (64), and sectionalizers (69, 70, 78). For switch 64, the agent was built in the recloser. All other devices are fuses (65, 66, 67, 69, 71, 72, 73, 74, 75, 76, 77, 79, 80, 81, 82, 83, 84). According to the configuration of Figure 7, agent 64 supervises the devices 65, 66, 67, 79, 80, 81, 82, and 83; and agent 68 supervises the following devices: 69, 70, 71, 72, 73, 74, 75, 76, 77, and 78. Notice that the terminal branches are not represented in this figure; however, they exist. For instance, after switch 76, there is a branch with consumers and a load.

Three case studies were created by causing short-circuits in branches 82–83, 70–71, and 74–76 to evaluate the performance of the proposed approach. A fourth case study is presented wherein the protection did not occur correctly.

5.1. Case Study 1: Short-Circuit in Branch 82–83

In this case study, the short-circuit happened in branch 82–83. First, the traditional protection eliminated the short-circuit, and the fuse 82 broke. As agent 64 found the short-circuit current, it established communication with agent 68 and verified this agent did not see this current. Agent 64 inferred the short-circuit happened in its supervised area. Then, it started the computation of the load partitioning of each branch under its supervision. These branches are 64–65, 65–66, 66–67, 67–68, 64–82, 82–83, 82–84, 65–79, 65–80, 80–81, 79–X, 81–X, 83–X, and 84–X.

The agent measured the actual current, computed the difference between the pre-fault current and the actual current, and computed the percentage value of load drop. In this data-driven solution, the current time was verified, and the data were extracted from the agent memory (computed by a previous computation). The entire database used in this example can be found in [19,49].

The load in each bus was transformed into percentual values using the data extracted from the memory. The agent, comparing the percentage value of load drop and the percentual values of each bus, detected the operation of switch 82. Immediately, it sent a message to the substation informing it that switch 82 was broken.

5.2. Case Study 2: Short-Circuit in Branch 70–71

In this second case study, the short-circuit happened in branch 70–71. The traditional protection eliminated the short-circuit using recloser 65 and sectionalizer 70. Then, after three attempts to close the circuit by recloser 64, sectionalizer 70 opened, interrupting the energy in branches 70–71 and 71–X. If the sectionalizer 70 had a problem opening, in the fourth attempt to close the circuit, sectionalizer 69 (the backup protection of 70) could open, but this was not the case.

Then, agents 64 and 68 noticed the short-circuit current. They established communication among them. Agent 64, as agent 68 noticed the short-circuit current, inferred that the short-circuit was not located in its supervised area. Agent 68 inferred the short-circuit happened in its supervised area. Thus, it was one of the branches 69–70, 70–71, 69–73, 73–74, 74–75, 74–76, 71–X, 75–X, and 76–X.

Agent 68 followed the same strategy presented in the previous case study, measuring the actual current, computing the difference between pre-fault and actual current, and computing the percentage value of load drop. After that, data were searched for in the memory (according to the current time), and the load in each bus was composed and transformed into a percentual value. By comparing the percentage value of load drop with the percentual values of each bus, agent 68 inferred the operation was of switch 70, so it sent a message with this information to the substation.

5.3. Case Study 3: Short-Circuit in Branch 74–76

This case study presents a short-circuit in branch 74–76, and via traditional protection, the fuse 74 acted, interrupting the short-circuit. The inference processes in agents 64 and 68 were similar to those in case study 2. Agent 64 inferred the short-circuit happened out of its supervised area. Then, agent 68 started the load partitioning of each branch, concluding, in the end, that fuse 74 acted, so it sent this information to the substation.

5.4. Case Study 4: Wrong Actuation of the Traditional Protection

Suppose that fuse 74 did not act in the previous case study and its backup protection (fuse 73) broke. This fact is not a problem for the inference process of intelligent agents, and the agents would promote the inference process in the same way. Agent 64 would do nothing because the short-circuit is not in its supervised area. In contrast, agent 68 would compute the load partitioning of each branch, conclude that fuse 73 acted, and send this information to the substation.

The answer is correct because fuse 73 acted, but only the maintenance team will verify the malfunction of the protection system in this part of the network.

6. Computational Validation of the Proposed Approach

Computational programs were prepared to validate the proposed approach. This section presents the results of the developed computational programs after many tests were performed.

The first sub-section below presents the structure of the computational program developed to test the validity of the proposed approach. In the second sub-section, we describe how the developed program with the proposed algorithm was executed once to determine a list of operated switches, creating a separate single short-circuit for each branch. The third sub-section shows validation of the proposed approach; thousands of tests were executed, and the quality of the answer is analyzed therein.

6.1. Presentation of the Validating Computer Program

The developed computational program was written to be run thousand times to validate the proposed approach. This section describes what happens when the program is run once. Figure 8 shows the flowchart of the computer program. At the start, the agent is provided with the structure of the monitored network, the positions of the switches, and the positions of the adjacent agents. It starts with a random set of loads (expressed in current) for each branch. The next step is to compute the initial current (I_0) through the agent using the random load of each branch. The agent will use these loads in the following steps. This part of the algorithm is equivalent to the proposed approach when the agent knows each branch's hourly load registered in the local memory.

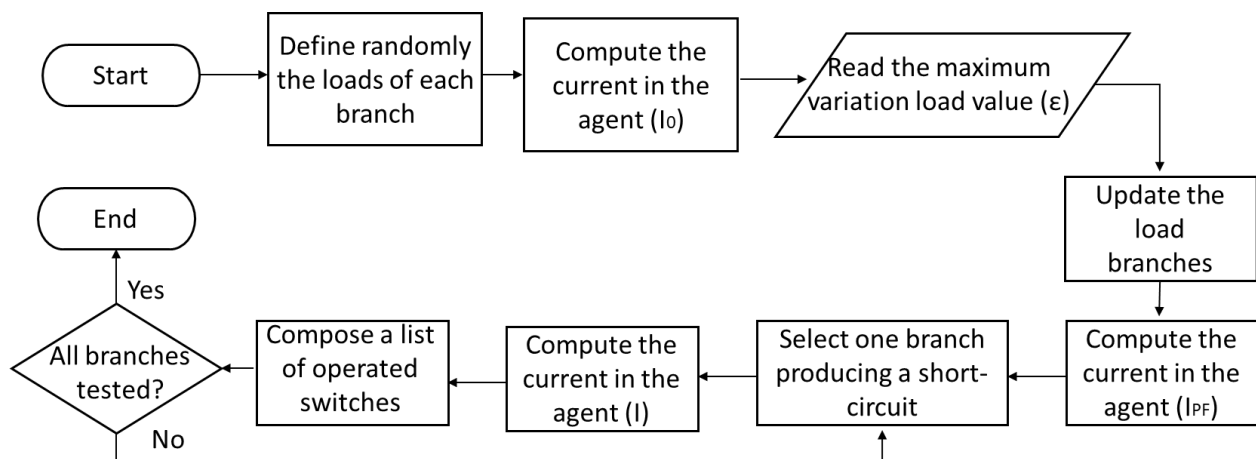


Figure 8. Flowchart of the computer program developed for validating the proposed approach.

After that, the program reads a value of ε (a percentage), the maximum variation, to modify the load branches. In the next step, each load branch is modified using random values between $-\varepsilon$ and $+\varepsilon$ drawn individually for each branch. It is equivalent to the load variation during regular operation. Then, the current in the agent is computed using these new loads. This current is the pre-fault current (I_{PF}) at the proposed approach. Notice that these new loads are used to determine the operated switch, but only to compute the pre-fault current, and in some steps ahead, the actual current (I).

The algorithm starts the test in each branch, simulating a short-circuit and the consequent operation of the switch responsible for eliminating it. This process is performed individually for all observed branches of the agent. After selecting one branch, the actual current (I) is computed without a switching operation, eliminating the load branches.

The list of operated switches is then composed following these actions: (1) update values of the initial values of branch load with the relation I_{PF}/I_0 ; (2) using the initial configuration of the system, determine the current in each switch; (3) compute the difference between $I_{PF} - I$, determining of the loss of a load block; and (4) compose a list with the possible switches, observing the closest values of the load switch. All these actions are represented in the flowchart in a single box.

The next step verifies if all branches were tested or not. If no, the process continues in the next branch; if yes, the process is ended.

This flowchart presents a single execution of the validation algorithm. However, in practice, the algorithm is run a thousand times, and for each execution, a new set of branch loads is chosen, but the value of ε is not modified. Maintaining a ε constant is done to know the algorithm's performance for a given load variation. Notice that changing the load individually for each branch continues to occur.

6.2. Executing the Computational Program Once

In this example, part of the circuit presented in Figure 7 is used, as shown in Figure 9. In this section, two examples are shown. In the first one, the agent is located in switch 64; in the second example, two agents are situated in switches 64 and 68.

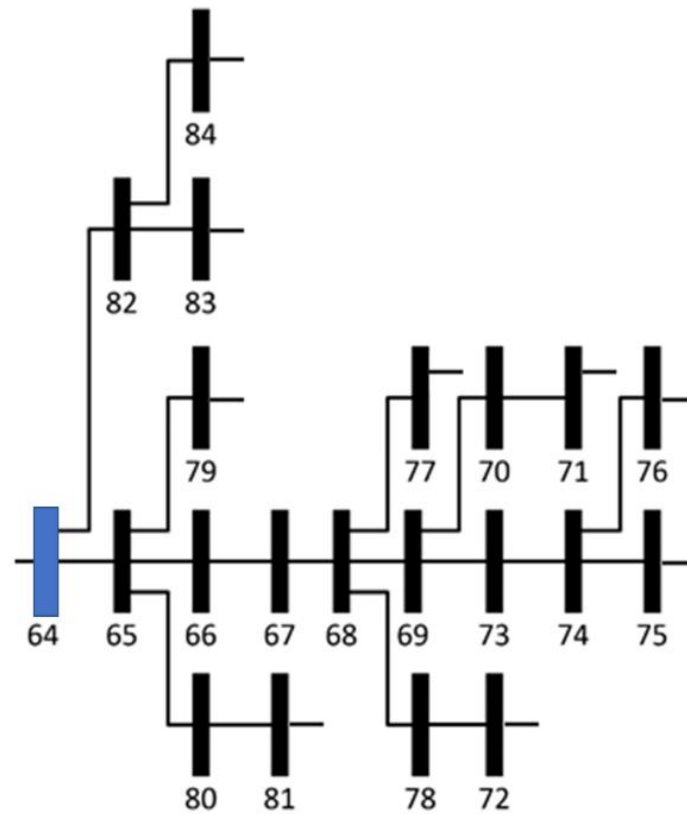


Figure 9. Part of the single diagram of an existing network in Figure 7.

In the first example, suppose the agent has been assembled in the recloser (switch 64). This switch is responsible for observing the switches numbered between 65 to 81.

In this situation, the program is executed, providing a random load for each branch, including the branches after the last switches (as 84, 83, 79, and so on). These branches are also included in the list of branches with single short-circuits.

A single operation of the algorithm randomly generates the values presented in these examples, and they are shown to offer a complete illustrative example.

In the initial step, the network structure after switch 64 is introduced to the program. After that, the program randomly creates loads (I_0 , in pu) for each branch, as shown below in the second column in Table 3.

Table 3. Loads of the example: Initial Load (I_0), Pre-fault Load (I_{PF}), and Up-date Initial Load.

Bus	Registrated Load (I_{0SWx})	Load (I_{PF})	Up-Date Registrated Load ($I_{SWx-new}$)
64	5.067	5.168	5.062
65	1.259	1.239	1.258
66	2.836	2.738	2.833
67	2.522	2.637	2.519
68	5.786	5.691	5.780
69	5.421	5.199	5.415
70	6.796	6.521	6.789

Table 3. Cont.

Bus	Registered Load (I_{0SWx})	Load (I_{PF})	Up-Date Registered Load ($I_{SWx-new}$)
71	1.675	1.733	1.674
72	3.798	3.837	3.794
73	1.312	1.352	1.310
74	2.515	2.573	2.512
75	4.342	4.358	4.338
76	1.292	1.353	1.291
77	2.379	2.350	2.377
78	5.242	5.269	5.237
79	4.511	4.660	4.506
80	2.483	2.512	2.480
81	4.792	4.966	4.787
82	6.132	6.179	6.125
83	1.138	1.161	1.135
84	6.114	5.836	6.098

Using the network structure and the branch loads, the program computes the agent's initial current (I_0), 77.414 pu.

In this example, the value (ε) was defined as 5%. This value is related to the load forecasting error, and this one is classified as enormous. Usually, this value is below 1% in one-hour forecasting. Next, the branch loads are randomly modified with values between -5% and $+5\%$.

Then, using the network structure and these new branch loads, the program computes the pre-fault current (I_{PF}) in the agent, 77.332 pu. Then, the initial load value (I_{0SWx}) is updated using the value 0.9989 ($=I_{PF}/I_0 = 77.332/77.414$), generating a new set of load branch values ($I_{SWx-new}$), as shown in the fourth column in Table 3. In this case, this load update computation is not relevant, but sometimes it is.

Following that, the switches for all branches start to be tested individually. The actual current (I) is defined by the new structure of the network and the modified loads. The loss of a load block difference is obtained from $I_{PF} - I$. The loss of load block is compared with the current of each modified initial load to compose the list of possible operated switches. Table 4 shows the results for short-circuits applied in all studied branches. It presents the operated switch, the list of possible operated switches, and the true operated switch's rank.

Table 4. Examples of short-circuits in all branches, with one agent located in switch 64.

Operated Switch	Complete Ordered List	Rank of Correct Switch
64	[64, 65, 66, 67, 68, 69, 82, 73, 78, 70, 74, 80, 84, 81, 79, 75, 72, 77, 71, 76, 83]	1
65	[65, 66, 67, 64, 68, 69, 82, 73, 78, 70, 74, 80, 84, 81, 79, 75, 72, 77, 71, 76, 83]	1
66	[66, 67, 68, 65, 69, 64, 82, 73, 78, 70, 74, 80, 84, 81, 79, 75, 72, 77, 71, 76, 83]	1
67	[67, 68, 66, 65, 69, 82, 73, 78, 64, 70, 74, 80, 84, 81, 79, 75, 72, 77, 71, 76, 83]	1
68	[68, 67, 66, 69, 65, 82, 73, 78, 70, 74, 80, 84, 81, 79, 75, 72, 64, 77, 71, 76, 83]	1
69	[69, 82, 73, 78, 70, 74, 80, 68, 84, 81, 79, 75, 72, 67, 77, 71, 76, 83, 66, 65, 64]	1
70	[74, 70, 78, 80, 73, 84, 81, 79, 75, 72, 82, 77, 71, 76, 83, 69, 68, 67, 66, 65, 64]	2
71	[71, 76, 83, 77, 72, 75, 79, 81, 84, 80, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1
72	[72, 75, 79, 81, 77, 84, 71, 76, 83, 80, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1

Table 4. Cont.

Operated Switch	Complete Ordered List	Rank of Correct Switch
73	[73, 78, 70, 74, 80, 82, 84, 81, 79, 75, 72, 77, 71, 76, 83, 69, 68, 67, 66, 65, 64]	1
74	[74, 70, 78, 80, 73, 84, 81, 79, 75, 72, 82, 77, 71, 76, 83, 69, 68, 67, 66, 65, 64]	1
75	[75, 79, 81, 72, 84, 77, 71, 80, 76, 83, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1
76	[76, 83, 71, 77, 72, 75, 79, 81, 84, 80, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1
77	[77, 71, 76, 83, 72, 75, 79, 81, 84, 80, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1
78	[78, 73, 70, 74, 80, 84, 82, 81, 79, 75, 72, 77, 71, 76, 83, 69, 68, 67, 66, 65, 64]	1
79	[81, 79, 75, 72, 84, 77, 80, 71, 76, 83, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	2
80	[80, 74, 70, 84, 78, 73, 81, 79, 75, 72, 77, 71, 82, 76, 83, 69, 68, 67, 66, 65, 64]	1
81	[81, 79, 75, 84, 72, 80, 77, 71, 74, 70, 76, 83, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1
82	[82, 73, 78, 70, 74, 80, 84, 81, 79, 75, 72, 69, 77, 71, 76, 83, 68, 67, 66, 65, 64]	1
83	[83, 76, 71, 77, 72, 75, 79, 81, 84, 80, 74, 70, 78, 73, 82, 69, 68, 67, 66, 65, 64]	1
84	[84, 81, 79, 75, 80, 72, 74, 70, 78, 77, 73, 71, 76, 83, 82, 69, 68, 67, 66, 65, 64]	1

By observing the results of Table 4, it is possible to verify that the proposed approach hit the target in most tests. For instance, in the first example, the short-circuit was applied in branch 64–65 with the operation of switch 64; notice that this switch is in the first place on the possible operating switch list. The correct solution was found in second place when switches 70 and 79 were operated.

In the second example, two agents are located in switches 64 and 68 of Figure 9, dividing the observability of this part of the network. The same data in Table 3 were used, and the results are shown in Table 5.

Table 5. Examples of short-circuits in all branches, with two agents located in switches 64 and 68.

Operated Switch	Complete Ordered List	Rank of Correct Switch
64	[64, 69, 65, 73, 74, 70, 66, 75, 67, 78, 76, 77, 68, 72, 71, 82, 79, 80, 83, 84, 81]	1
65	[65, 69, 66, 67, 68, 64, 73, 74, 70, 75, 78, 76, 77, 72, 71, 82, 79, 80, 83, 84, 81]	1
66	[66, 67, 68, 69, 65, 73, 74, 82, 70, 64, 75, 78, 76, 77, 72, 71, 79, 80, 83, 84, 81]	1
67	[67, 66, 68, 69, 65, 73, 74, 82, 70, 75, 64, 78, 76, 77, 72, 71, 79, 80, 83, 84, 81]	1
68	[68, 67, 66, 69, 65, 73, 82, 74, 70, 75, 78, 79, 80, 76, 77, 83, 84, 64, 72, 71, 81]	1
69	[69, 73, 82, 68, 74, 67, 66, 70, 75, 78, 79, 80, 76, 77, 83, 84, 72, 71, 81, 65, 64]	1
70	[70, 75, 78, 79, 80, 76, 77, 83, 84, 72, 71, 81, 74, 82, 73, 69, 68, 67, 66, 65, 64]	1
71	[81, 71, 72, 84, 77, 83, 76, 80, 79, 78, 75, 70, 74, 82, 73, 69, 68, 67, 66, 65, 64]	2
72	[72, 71, 81, 84, 77, 83, 76, 80, 79, 78, 75, 70, 74, 82, 73, 69, 68, 67, 66, 65, 64]	1
73	[73, 82, 74, 70, 75, 69, 78, 79, 80, 76, 77, 83, 84, 72, 71, 81, 68, 67, 66, 65, 64]	1
74	[74, 82, 73, 70, 75, 78, 79, 80, 76, 77, 83, 84, 72, 71, 81, 69, 68, 67, 66, 65, 64]	1
75	[75, 70, 78, 79, 80, 76, 77, 83, 84, 72, 71, 81, 74, 82, 73, 69, 68, 67, 66, 65, 64]	1
76	[76, 83, 77, 80, 79, 78, 84, 72, 71, 81, 75, 70, 74, 82, 73, 69, 68, 67, 66, 65, 64]	1
77	[76, 83, 77, 80, 79, 78, 84, 72, 71, 81, 75, 70, 74, 82, 73, 69, 68, 67, 66, 65, 64]	3
78	[78, 79, 80, 76, 77, 83, 75, 84, 72, 71, 81, 70, 74, 82, 73, 69, 68, 67, 66, 65, 64]	1
79	[80, 79, 83, 84, 81, 71, 72, 77, 76, 78, 75, 70, 82, 74, 73, 69, 68, 67, 66, 65, 64]	2
80	[80, 79, 83, 84, 81, 71, 72, 77, 76, 78, 75, 70, 82, 74, 73, 69, 68, 67, 66, 65, 64]	1

Table 5. Cont.

Operated Switch	Complete Ordered List	Rank of Correct Switch
81	[81, 84, 83, 80, 79, 71, 72, 77, 76, 78, 75, 70, 82, 74, 73, 69, 68, 67, 66, 65, 64]	1
82	[82, 71, 72, 77, 76, 78, 75, 70, 79, 80, 83, 84, 81, 74, 73, 68, 67, 66, 69, 65, 64]	1
83	[83, 80, 84, 79, 81, 71, 72, 77, 76, 78, 75, 70, 82, 74, 73, 69, 68, 67, 66, 65, 64]	1
84	[84, 83, 80, 79, 81, 71, 72, 77, 76, 78, 75, 70, 82, 74, 73, 69, 68, 67, 66, 65, 64]	1

Most of these attempts also hit the correct target. Only faults 71 and 79 are ranked in second place, and 77 in the third place.

Note that the program uses random load values, and each time the program is executed, one result appears. The program must be run hundreds of times to validate the proposed approach and create substantiated statistical results.

This computational program can be run at the repository in [50].

6.3. Validating Test of the Proposed Approach

The computational program uses drawn and random processes, so it is necessary to validate the proposed approach with a thousand tests. It includes different branch loads and different values of ϵ for the same network structure.

In the first validation test, the structure shown in Figure 9 was used, and the agent was also located in recloser 64. One thousand executions of the program were run for each value of ϵ , and the values of ϵ chosen were 1%, 2%, 5%, and 10%, so 4000 executions were performed. Table 6 shows these results.

Table 6. Results of the correct switches in the list (in percentages).

ϵ	Position in the List				Error	Hits	Error	Hits
	1st	2nd	3rd	4th	Total	Total	1st	1st + 2nd
1%	96.19%	3.81%	0.00%	0.00%	0.00%	100.00%	3.81%	0.00%
2%	95.24%	4.29%	0.48%	0.00%	0.00%	100.00%	4.76%	0.48%
5%	92.00%	4.67%	3.33%	0.00%	0.00%	100.00%	8.00%	3.33%
10%	74.29%	18.57%	6.19%	0.48%	0.48%	99.52%	25.71%	7.14%

By observing the results above table, it is possible to verify that the number of hits which are first place in the list is higher when the value of ϵ is small. This fact is expected, because the difference between the modified loads and the modified initial loads increases with the value of ϵ . The worst outcome occurred when ϵ was equal to 10%. This value in practice does not exist because, as mentioned before, the value of ϵ is related to load forecasting. This size of load change is not common in a distribution operation. This example was included to verify the quality of detection of the proposed approach even in extreme situations.

Other values of Table 6 show the expected error level when the list sent to the operator contains only one element (one switch) or two elements (two switches). For instance, when the value of ϵ is 2%, the maximum value hit in most situations is under 8% in the one-element list and 3% in the two-element list. These values are 4.76% and 0.48% in the table, respectively.

Now two examples can be presented from this validation process, using intelligent agents located in switches 64 and 68. In this situation, this part of the circuit is divided into two parts: one observed by switch 64 (monitoring switches 65–67 and 79–84) and another observed by switch 68 (monitoring switches 69–78). The same tests as described above were performed for these switches, and the results are shown in Table 7.

Table 7. Results of the correct switches in the list (in percentages)—tests using switches 64 and 68.

ϵ	Position in the List					Hits
	1st	2nd	3rd	4th	Error	
1%	99.52%	0.48%	0.00%	0.00%	0.00%	100.00%
2%	95.71%	3.81%	0.48%	0.00%	0.00%	100.00%
5%	92.86%	6.67%	0.48%	0.00%	0.00%	100.00%
10%	79.05%	14.29%	3.33%	2.38%	0.95%	99.05%

6.4. Discussions

Other real and simulated distribution circuits have been tested similarly, and the results have been similar. The proposed approach indeed merges smart grid devices and traditional protection elements, increasing the network's observability.

Regarding the results of the two previous tables, we verified that the level of hit degree is increased. This was also expected because the test was for a network of almost the same size, and two observed agents divided the monitoring of the switches. After running the program thousands of times, the error was continuously below 3%, which validates the proposed approach in the worst cases. This computational program can be run at the repository in [51].

An error above 10% would be accepted because the system operator has no observability in traditional distribution networks. Thus, any contribution is very welcome during the operation, even partly unreliable ones. The proposed approach can hit this level of error (around 10%) when an intelligent agent monitors the protection of hundreds of branches. However, this case occurs only when the number of intelligent agents is few compared with the number of supervised protection branches.

7. Conclusions

This study aimed to make smart grid agents compatible with traditional protection devices of urban distribution electrical networks. This study of compatibilization is necessary because protection devices are being changed step-by-step. For a reasonable period of time, they will act together, mainly in concessionaires without significant financial resources. Thus, if agents can, from the beginning of their operations in networks, interact with the protection devices (even indirectly), increasing the observability of the network, it would be helpful.

Unlike traditional articles, this article discussed a more practical implementation of installing a smart grid. This topic had not yet been addressed in scientific papers, but it is of fundamental importance for companies in this phase of technological development. Many of them will still be at this stage of their smart grids for many years, and with the techniques presented in this article, they will be able to use the benefits of some (really) intelligent devices in their networks.

It is noticed that most articles deal with more advanced smart grids by proposing operational and troubleshooting techniques. Thus, a critical review of the main articles was not performed because they do not present strategies involving traditional protection. In addition, and for an analogous reason, no comparisons were made with other methods.

The proposed agent had precisely these purposes: to increase the observability of the network for the operation centers, reduce the response time for interventions in the network, and assist in lowering the reliability indexes (CAIDI and SAIDI). The operation team can focus on other essential tasks, such as sending maintenance teams to the site to repair problems in the faulty section of the feeder, optimizing resources, and reducing service outage time.

The first function analyzed provides the interactions with fuse switches: verifying which fuse supervised by the agent had its link broken by a short-circuit current. It uses the comparative load proportionality metric. When the agent supervises fewer fuses, its

accuracy is greater. The proposed method is not always foolproof because it acts with typical proportional loads. However, it is preferable to present a false positive to the operating center than wait for a consumer complaint to be taken.

The second function, for interacting with reclosers and sectionalizers, was then analyzed. Those devices are monitored analogously to the fuses. Despite having completely different roles, they are treated similarly in their integration to intelligent agents; and the comparative metric of load proportionality is used in the same way.

Thus, in the end, the urban protection devices continue to act traditionally. Different treatment only occurs in the analysis of loss of a load block.

This paper also presented the possibility of integrating intelligent agents into the reclosers and sectionalizers existing in the distribution networks. It can be done without any additional action, because the reclosers open short-circuit currents like the circuit breakers, and the sectionalizers, which do not open short-circuit currents, resemble the disconnectors. Both circuit breakers and disconnectors are switches receiving the intelligent agent in the papers available in the literature. Thus, this embedding was done without the inclusion of any extra elements.

The integration proposal in this paper was tested in an existing distribution system, using random data and producing a list of the operated switches. The degree of correct hits in thousands of tests was higher than 97% in various situations, proving the quality of the proposed approach.

Finally, the proposed approach opens many possibilities for new analyses, such as studies about the optimal locations for smart devices, interactive network observability, and innovative protection schemes using smart grid devices and traditional devices. Even in a transitory situation between the traditional protection and smart grid world, this initial phase of smart grid device implementation creates many possibilities with the proposed interaction of the two philosophies.

Author Contributions: B.S.T., C.P.S. and C.H.V.d.M. conceived and designed the experiments; B.S.T., C.H.V.d.M. and C.P.S. performed the experiments; B.S.T., C.P.S. and L.E.B.d.S. analyzed the case studies; B.S.T. and L.E.B.d.S. developed the methodology; and B.S.T., C.P.S. and C.H.V.d.M. analyzed the results of the proposed approach; and B.S.T., C.P.S. and L.E.B.d.S. wrote the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the National Council for Scientific and Technological Development (CNPq), the Coordination for the Improvement of Higher Education Personnel (CAPES), and the Brazilian Electricity Regulatory Agency Research and Development (ANEEL R&D) for supporting this project.

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

References

1. Siebert, L.C.; Aoki, A.R.; Lambert-Torres, G.; Lambert-de-Andrade, N.; Paterakis, N.G. An Agent-Based Approach for the Planning of Distribution Grids as a Socio-Technical System. *Energies* **2020**, *13*, 4837. [\[CrossRef\]](#)
2. Barreto, N.E.M.; Rodrigues, R.; Schumacher, R.; Aoki, A.R.; Lambert-Torres, G. Artificial Neural Network Approach for Fault Detection and Identification in Power Systems with Wide Area Measurement Systems. *J. Control Autom. Electr. Syst.* **2021**, *32*, 1617–1626. [\[CrossRef\]](#)
3. Mahat, P.; Chen, Z.; Bak-Jensen, B.; Bak, C.L. A Simple Adaptive Overcurrent Protection of Distribution Systems with Distributed Generation. *IEEE Trans. Smart Grid* **2011**, *2*, 428–437. [\[CrossRef\]](#)
4. Fletcher, S.D.A.; Norman, P.J.; Fong, K.; Galloway, S.J.; Burt, G.M. High-Speed Differential Protection for Smart DC Distribution Systems. *IEEE Trans. Smart Grid* **2014**, *5*, 2610–2617. [\[CrossRef\]](#)

5. Zeineldin, H.H.; Sharaf, H.M.; Ibrahim, D.K.; El-Zahab, E.E.-D.A. Optimal Protection Coordination for Meshed Distribution Systems With DG Using Dual Setting Directional Over-Current Relays. *IEEE Trans. Smart Grid* **2015**, *6*, 115–123. [CrossRef]
6. Noudjiej Djiepkop, G.F.; Krishnamurthy, S. Multi-Objective Feeder Reconfiguration Using Discrete Particle Swarm Optimization. *Mathematics* **2022**, *10*, 531. [CrossRef]
7. Kim, M.-S.; Haider, R.; Cho, G.-J.; Kim, C.-H.; Won, C.-Y.; Chai, J.-S. Comprehensive Review of Islanding Detection Methods for Distributed Generation Systems. *Energies* **2019**, *12*, 837. [CrossRef]
8. Ates, Y.; Uzunoglu, M.; Karakas, A.; Boynuegri, A.R. The case study based protection analysis for smart distribution grids including distributed generation units. In Proceedings of the 12th IET International Conference on Developments in Power System Protection (DPSP 2014), Copenhagen, Denmark, 31 March–3 April 2014; pp. 1–5. [CrossRef]
9. Wei, L.; Qi, Y.; Qi, H. Research on design and implementation of relay protection in smart grid. In Proceedings of the 2018 Chinese Control and Decision Conference (CCDC), Shenyang, China, 9–11 June 2018; pp. 1439–1443. [CrossRef]
10. Jimenez, S.; Vázquez, E.; Gonzalez-Longatt, F. Methodology of Adaptive Instantaneous Overcurrent Protection Setting. *Electronics* **2021**, *10*, 2754. [CrossRef]
11. Liu, X.; Zhang, B.; Chen, B.; Aved, A.; Jin, D. Towards Optimal and Executable Distribution Grid Restoration Planning with a Fine-Grained Power-Communication Interdependency Model. *IEEE Trans. Smart Grid* **2022**, *11*, 9973. [CrossRef]
12. Sayed, M.M.; Mahdy, M.Y.; Abdel Aleem, S.H.E.; Youssef, H.K.M.; Boghdady, T.A. Simultaneous Distribution Network Reconfiguration and Optimal Allocation of Renewable-Based Distributed Generators and Shunt Capacitors under Uncertain Conditions. *Energies* **2022**, *15*, 2299. [CrossRef]
13. Erenoglu, A.K.; Sancar, S.; Terzi, I.S.; Erdinc, O.; Shafie-khah, M.; Catalão, J.P.S. Resiliency-Driven Multi-Step Critical Load Restoration Strategy Integrating On-Call Electric Vehicle Fleet Management Services. *IEEE Trans. Smart Grid* **2022**, *11*, 5438. [CrossRef]
14. Singhal, A.; Vu, T.L.; Du, W. Consensus Control for Coordinating Grid-Forming and Grid-Following Inverters in Microgrids. *IEEE Trans. Smart Grid* **2022**, *9*, 254. [CrossRef]
15. Assad, U.; Hassan, M.A.S.; Farooq, U.; Kabir, A.; Khan, M.Z.; Bukhari, S.S.H.; Jaffri, Z.U.A.; Oláh, J.; Popp, J. Smart Grid, Demand Response and Optimization: A Critical Review of Computational Methods. *Energies* **2022**, *15*, 2003. [CrossRef]
16. ANEEL—Brazilian Electricity Regulatory Agency, “Module 8—Quality of Electric Energy—Electric Power Distribution Procedures in the National Electrical System—PRODIST. 2021. p. 88. Available online: https://www.aneel.gov.br/documents/656827/14866914/Módulo_8-Revis~ao_12/342ff02a-8eab-2480-a135-e31ed2d7db47 (accessed on 8 June 2021). (In Portuguese)
17. Ferreira, L.R.; Aoki, A.R.; Lambert-Torres, G. A Reinforcement Learning Approach to Solve Service Restoration and Load Management Simultaneously for Distribution Networks. *IEEE Access* **2019**, *7*, 145978–145987. [CrossRef]
18. Ferreira, L.R. Hybrid Intelligent Control for Smart Grid Functionalities Integration. Ph.D. Thesis, Federal University of Paraná, Curitiba, Brazil, 2020. Available online: <https://hdl.handle.net/1884/70724> (accessed on 10 September 2021).
19. Siebert, L.C. Demand Response Optimization System for Intelligent Power Grids. Ph.D. Thesis, Federal University of Paraná, Curitiba, Brazil, 2013. Available online: <http://hdl.handle.net/1884/35731> (accessed on 18 October 2021). (In Portuguese).
20. Sallam, A.A.; Malik, O.P. *Electric Distribution Systems*; Wiley-IEEE Press: Piscataway, NJ, USA, 2019; p. 624. ISBN 9781119509332.
21. Russell, S.J.; Norvig, P. *Artificial Intelligence: A Modern Approach*, 4th ed.; Prentice-Hall: Hoboken, NJ, USA, 2020; p. 2579. ISBN 9780134610993.
22. Ramesh Babu, N. *Smart Grid Systems: Modeling and Control*; Apple Academic Press: Waretown, NJ, USA, 2018; p. 290. ISBN 9781771886253.
23. Belu, R. *Smart Grid Fundamentals: Energy Generation, Transmission and Distribution*; CRC Press: Boca Raton, FL, USA, 2022; p. 568. ISBN 978-1482256673.
24. Tanenbaum, A. *Modern Operating Systems*; Pearson/Prentice Hall: Hoboken, NJ, USA, 2008; p. 160. ISBN 9780136006633.
25. Falk, H. *IEC 61850 Demystified*; Artech House Publishers: Norwood, MA, USA, 2019; p. 332. ISBN 9781630813291.
26. Cleveland, F. IEC TC57 Security Standards for the Power System's Information Infrastructure—Beyond Simple Encryption. In Proceedings of the 2005/2006 IEEE/PES Transmission and Distribution Conference and Exhibition, Chicago, IL, USA, 4–7 May 2006; pp. 1079–1087. [CrossRef]
27. Reda, H.T.; Ray, B.; Peidaee, P.; Anwar, A.; Mahmood, A.; Kalam, A.; Islam, N. Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid. *Sensors* **2021**, *21*, 1554. [CrossRef]
28. Schneider Electric. Intelligent Loop Automation. 2013. p. 84. Available online: https://www.se.com/library/SCHNEIDER_ELECTRIC/SE_LOCAL/APS/213039_E57A/SEAU26709_Loop_Automation_Manual_WEB.pdf (accessed on 21 December 2021).
29. S&C Electric Company. IntelliTeam®SG Automatic Restoration System. 2022. p. 113. Available online: <https://www.sandc.com/globalassets/sac-electric/documents/sharepoint/documents---all-documents/instruction-sheet-1044-570.pdf> (accessed on 28 November 2021).
30. Eaton. Yukon Feeder Automation (YFA)I. 2021, p. 16. Available online: <https://www.eaton.com/content/dam/eaton/products/utility-and-grid-solutions/grid-automation-systems/yukon-feeder-automation/yukon-feeder-automation-ps818001en.docx> (accessed on 28 December 2021).
31. NovaTech. Distribution Automation Controller. 2019. p. 6. Available online: https://back.novatechautomation.com/wp-content/uploads/2020/10/DS_DAMaster_111210.pdf (accessed on 28 October 2021).

32. Schweitzer Engineering Laboratories. Distribution Automation Controller. Available online: <https://selinc.com/engineering-services/distribution-network-automation/> (accessed on 16 February 2022).
33. Hitachi Energy. Self-Healing Distribution Grid. Available online: <https://www.hitachienergy.com/rtu> (accessed on 28 February 2022).
34. Siemens, A.G. *Self-Optimizing Grid—Intelligent Grid Automation*. 2018, p. 12. Available online: <https://assets.new.siemens.com/siemens/assets/api/uuid:28ae65dd-359c-4b96-85bd-280facec62ea/self-optimizing-grid.pdf> (accessed on 18 November 2021).
35. Railsback, S.; Grimm, V. *Agent-Based and Individual-Based Modeling: A Practical Introduction*, 2nd ed.; Princeton University Press: Princeton, NJ, USA, 2019; 360p, ISBN 9780691190839.
36. McArthur, S.D.J.; Davidson, E.M.; Catterson, V.M.; Dimeas, A.L.; Hatziaargyriou, N.D.; Ponci, F.; Funabashi, T. Multi-Agent Systems for Power Engineering Applications—Part I: Concepts, Approaches, and Technical Challenges. *IEEE Trans. Power Syst.* **2007**, *22*, 1743–1752. [[CrossRef](#)]
37. Sharma, A.; Srinivasan, D.; Trivedi, A. A Decentralized Multiagent System Approach for Service Restoration using DG Islanding. *IEEE Trans. Smart Grid* **2015**, *6*, 2784–2793. [[CrossRef](#)]
38. Torres, B.S.; Ferreira, L.R.; Aoki, A.R. Distributed Intelligent System for Self-Healing in Smart Grids. *IEEE Trans. Power Deliv.* **2018**, *33*, 2394–2403. [[CrossRef](#)]
39. Kezunovic, M. Smart Fault Location for Smart Grids. *IEEE Trans. Smart Grid* **2011**, *2*, 11–22. [[CrossRef](#)]
40. Zidan, A.; El-Saadany, E.F. A Cooperative Multiagent Framework for Self-healing Mechanisms in Distribution Systems. *IEEE Trans. Smart Grid* **2012**, *3*, 1525–1539. [[CrossRef](#)]
41. Ibrahim, A.M.; Yau, K.-L.A.; Chong, Y.-W.; Wu, C. Applications of Multi-Agent Deep Reinforcement Learning: Models and Algorithms. *Appl. Sci.* **2021**, *11*, 10870. [[CrossRef](#)]
42. Xu, Y.; Liu, W. Novel Multiagent Based Load Restoration Algorithm for Microgrids. *IEEE Trans. Smart Grid* **2011**, *2*, 152–161. [[CrossRef](#)]
43. Nikkhah, S.; Allahham, A.; Bialek, J.W.; Walker, S.L.; Giaouris, D.; Papadopoulou, S. Active Participation of Buildings in the Energy Networks: Dynamic/Operational Models and Control Challenges. *Energies* **2021**, *14*, 7220. [[CrossRef](#)]
44. Jamal, S.; Tan, N.M.L.; Pasupuleti, J. A Review of Energy Management and Power Management Systems for Microgrid and Nanogrid Applications. *Sustainability* **2021**, *13*, 10331. [[CrossRef](#)]
45. Lim, I.-H.; Sidhu, T.S.; Choi, M.S.; Lee, S.J.; Hong, S.; Lim, S.I.; Lee, S.W. Design and Implementation of Multiagent-Based Distributed Restoration System in DAS. *IEEE Trans. Power Deliv.* **2013**, *28*, 585–593. [[CrossRef](#)]
46. Karavas, C.-S.; Kyriakarakos, G.; Arvanitis, K.G.; Papadakis, G. A multiagent decentralized energy management system based on distributed intelligence for the design and control of autonomous polygeneration microgrids. *Energy Convers. Manag.* **2015**, *103*, 166–179. [[CrossRef](#)]
47. Siebert, L.C.; Aoki, A.R.; Fernandes, T.S.P.; Lambert-Torres, G. Customer Targeting Optimization System for Price-Based Demand Response Programs. *Int. Trans. Electr. Energy Syst.* **2018**, *29*, e2709. [[CrossRef](#)]
48. Frederiks, E.R.; Stenner, K.; Hobman, E.V. The Socio-Demographic and Psychological Predictors of Residential Energy Consumption: A Comprehensive Review. *Energies* **2015**, *8*, 573–609. [[CrossRef](#)]
49. Siebert, L.C.; Sbicca, A.; Aoki, A.R.; Lambert-Torres, G. A Behavioral Economics Approach to Residential Electricity Consumption. *Energies* **2017**, *10*, 768. [[CrossRef](#)]
50. Integrating Smart Grid Devices into the Traditional Protection of Distribution Networks. Available online: https://colab.research.google.com/github/carloshvmoraes/ISGDTPDN/blob/main/ISGD_basic.ipynb (accessed on 18 November 2021).
51. Integrating Smart Grid Devices into the Traditional Protection of Distribution Networks. Available online: https://colab.research.google.com/github/carloshvmoraes/ISGDTPDN/blob/main/ISGD_benchmark.ipynb (accessed on 18 November 2021).