Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

STRAYER: A Smart Grid adapted automation architecture against cyberattacks

Alexandro de O. Paula [a,*], Rodolfo I. Meneguette [b], Felipe T. Giuntini [c], Maycon L.M. Peixoto [d], Vinícius P. Gonçalves [a], Geraldo P. Rocha Filho [e]

[a] *Department of Electrical Engineering, University of Brasília, Brasília, Distrito Federal, Brazil*
[b] *Institute of Mathematical and Computer Sciences, University of São Paulo, São Carlos, Brazil*
[c] *Computer Science Institute, Federal University of Amazonas, Manaus, Brazil*
[d] *Computer Science Department, Federal University of Bahia, Salvador, Bahia, Brazil*
[e] *Department of Computer Science, University of Brasília, Brasília, Distrito Federal, Brazil*

ARTICLE INFO

MSC:
28-11
91B74
93C85
20F10

Keywords:
Smart grid security
Substation automation system
Cybersecurity

ABSTRACT

Even with advances in Smart Grids and their cybersecurity recommendations, recent attacks on automation and protection systems of these structures show that it is still necessary to investigate this research problem. With that in mind, this work proposes STRAYER: a **S**mar**T** a**R**chitecture **A**gainst c**Y**b**ER**attacks to reduce the vulnerability of automation equipment in Smart Grids. STRAYER integrates cybersecurity for monitoring and shielding access, interoperability for maintaining communication between equipment/devices, and risk management for maintaining reliability and preventing real-time cyberattacks on Smart Grids. To validate the STRAYER, we built a prototype commonly used in smart grids. The results showed that STRAYER increases the security efficiency compared to the traditional architecture, reducing the amount of infected equipment and the undue access time to Smart Grids. In addition to the reductions in the amount of IED's affected by invasions, it was also possible to notice that STRAYER avoided the collapse of a Smart Grid, having only minimal and reversible losses, unlike the traditional architecture.

1. Introduction

Smart Grids allow better efficiency in the operation and maintenance of electric power substations assets to manage loads better, reducing costs and enhancing responses to possible problems in these structures [1]. The most current model devised by the National Institute of Standards and Technology (NIST) consists of a communication system to interconnect all areas inherent to the processes of electric energy (*i.e.* generation, transmission, distribution), in addition to the inclusion of the sub-areas of operation and market. The intention is to maintain an intelligent management domain in the electricity sector [2]. Furthermore, all areas have their technological resources improved to maintain automation in state-of-the-art, including cybersecurity precepts [3].

Technological progress in Smart Grids, which aims to digitalize the existing electrical substations, has also brought cyberattack problems to the communication means and protocols of the Substation Automation System (SAS), conceptualized by the IEC 61850 standard. These attacks commonly occur through the computing networks of energy companies, such as the Information Technology (IT), Operating Technology (OT) networks, and even remote access [4]. These problems have been reported in the history of invasions in these structures. On the most recent events, there are those in 2017 and 2020 at Ukraine [5,6], in 2010 and 2015 on Iran, and 2020 in Brazil [7].

Several solutions for Smart Grids have been proposed to solve cyberattack problems [8–11]. Recently, ways to mitigate the problem were demonstrated, such as improvements in the telecommunications system [8], use of standard IT security solutions [9] and even the standardization of monitoring and automation in Smart Grids [10], without mentioning adaptations in the SAS architecture. Another [11] worked on the physical design of a fully digital electrical substation to monitor communication and automation, but the data presented does not aim at effective structure security. About the robustness of the works mentioned, it is clear that there is a lack of the dynamic factor in the solutions above, due precisely to the diversity of types of attacks.

This work proposes STRAYER, a new architecture to mitigate cyberattack problems in Smart Grids regarding the protection of SAS and its equipment. STRAYER integrates cybersecurity for monitoring

* Corresponding author.
E-mail addresses: alexandro.paula@neoenergia.com (A.d.O. Paula), meneguette@icmc.usp.br (R.I. Meneguette), felipegiuntini@icomp.ufam.edu.br (F.T. Giuntini), maycon.leone@ufba.br (M.L.M. Peixoto), vpgvinicius@unb.br (V.P. Gonçalves), geraldof@unb.br (G.P.R. Filho).

https://doi.org/10.1016/j.jisa.2022.103195

Available online 18 May 2022

and shielding access, interoperability for maintaining communication between equipment/devices, and risk management for maintaining reliability and preventing real-time cyberattacks on Smart Grids. For modeling the STRAYER, we used adaptations in communication networks and automation architecture proposed by IEC 61850 standards, redundancy, and separation of operation networks. Therefore, our architecture maintains the integrity of the automation and communication system for Smart Grids and, consequently, the continuity of these structures and full functioning essential services to a particular region's population.

As a proof of concept, a prototype commonly used in smart grids was built to validate the STRAYER designed to operate in a SAS. When compared to traditional architecture, STRAYER performs better in four aspects:

- reduction by 87.5% of IED's affected by attacks by remote access and through IT network;
- decrease of attacks on circuit breakers by 88.9% from remote access;
- delay in the invasion time to the Smart Grid supervisory system by remote access in *16min27sec* compared to the traditional architecture, and;
- increase of *01h11min23sec* in the maximum time of intrusion to an IED through remote access.

The remainder of this work is organized as follows. Section 2 shows the theoretical concepts of the parameters that STRAYER will use to understand the proposal. Section 3 presents the related works and their limitations that this research explores. Section 4 defines how the STRAYER was modeled and its main contribution. Section 5 reveals the validation of STRAYER compared to a traditional architecture. Finally, Section 6 shows the conclusions and the future guidelines.

2. United parameters — about cybersecurity, interoperability and risk management

The STRAYER is conceptualized on meeting three essential parameters for SAS data analysis: Cybersecurity, Interoperability, and Risk Management.

To better understand these parameters, it is necessary to know the basic concepts of them, according to their original definition and focused on the electricity sector:

- **Cybersecurity**. Focused on the commercial electric energy sector, the NIST 8183 standard [12] defines cybersecurity as a data protection methodology that detects and responds to virtual attacks. Even more, the standard reveals that the absence of cybersecurity in an organization with substantially expensive assets can generate the so-called CyberRisk. The CyberRisk is defined as a generalized, administrative and operational, loss related to the failures of technologies applied to a given system, by virtual or physical means, from the unauthorized use of these means, causing modification, misdirection or data loss [12].
- **Interoperability**. Common not only to the work of the IEC 61850 standard but in several segments of the industry and business sector, interoperability has been widely used in the electric energy sector, specifically in Smart Grid equipment with asset and risk management by electric companies administrators. It is the interaction between operating systems, organizations, and even people, through the passage/exchange of information, through infrastructure distributed or adHoc solutions system. There are Interoperability Dimensions [13] aimed at each organizational segment (Organizational, Semantic, among others). With more affinity with this architecture, the Technical Interoperability Dimension approaches STRAYER. For interoperability, the technologies used in the mechanisms must be known. In this way, less effort is required in creating interoperation interfaces, and communication takes place faster and more agile [14].
- **Risk Management**. Following the example of interoperability, it is also being widely used, especially in organizations that have costly assets. The risk analysis and management are very present in the electric energy sector, whether in distribution, transmission, or generation. The most significant application in this area is in Smart Grid Maintenance management. The use of maintenance plans for its equipment, linked to the segments inherent to it, is an example of risk management method. The closest definition of risk management in STRAYER is control activities to direct and control an organization concerning risks. Besides, an iterative technique that assists in establishing strategies, achieving goals, and making decisions [15].

  For our purpose, risk management will serve to (i) make decisions to apply the analyzed data; (ii) establish and achieve security and interoperability objectives; (iii) improve the performance of automation. The risk predictability and cost analysis are prerogatives of the Risk Analysis and Information Security study, determined by ISO 31010 standard [16].

These concepts will be applied in Smart Grids, which are digital substation with high electrical power that contains equipment to raise or reduce a specific range of electrical voltage, depending on the use. Automation Equipment (switches, routers, gateways, GPS's, computers, fiber optic cables), Protection (protection relays, circuit breakers, electrical controls), Telecommunications (communication towers, radios, antennas, multiplexers), Measurement (Current or potential transformers — CT and PT) and Transformation (Power or auxiliary services transformers) are used in Smart Grid. Many of these devices are entirely digital and interconnected, facilitating electrical installation.

To turn an analog electric substation into a digital Smart Grid, requires one of two paths: (i) swap all analog components for digital or optical equipment (which takes a lot of time and is relatively expensive), or; (ii) insert Analog/Digital conversion mechanisms (A/D) between the equipment and the communication (operation of the substation). It was thinking about the latter, more accessible option, that manufacturers created digitizing devices, such as IED's (Intelligent Electronic Device) and SAMU's (Stand Alone Merging Units), whose functioning will be seen in later sections.

3. Related work

In the literature, there are some works related to increasing the security performance of networks in Smart Grids due to many attacks, both locally and remotely. These researches used several techniques to try to reach a robust solution against intrusions in electrical power and automation systems.

Lazaro et al. [8] shows a series of solutions aimed at securing communication between Smart Grids, meeting the requirements set out in IEC 62351-6 with an emphasis on messages between all equipment. Even with the robustness of the work, the survey does not present solutions aimed at SAS security.

Faquir et al. [9] uses several existing solutions to protect IT networks using IoT (Internet of Things), such as firewalls, IDS/IPS, remote access via VPN, among others. Although it is still a very robust practice for protecting the electricity company's network, it was not possible to see an improvement in the OT network security system or even for the IED's protection system.

Yang et al. [10] presented the electrical substations monitoring system's main problems, emphasizing communication and cybersecurity. The work consisted of standardizing, in a static way, the monitoring solutions. The solution is based on maintaining data upgrades in Smart Grids, only with the security feature (without risk management or interoperability), maintaining only a basic automation architecture. As cyberattacks are constantly evolving and more dynamic, maintaining a static method would open loopholes for future problems.

Vardhan et al. [11] designed a Smart Grid, following the state of the art concept. The project consisted of the creation of a pilot digital electric substation, with communication between devices on the process bus through Sampled Values messages (SV) [17], with the purpose of comparing data from this structure with traditional energy power plants. Although promising, the concept created had the implementation of high-cost digital equipment and sensors in the few analog switching equipment. The project also uses a basic architecture, without adaptations in the automation and communication topology, and it is not possible to perceive efficient cybersecurity implementations.

Fontes [18] presented a prototype of a test platform, called LabProtec, to design an infrastructure for various tests in digital electric substations with the IEC 61850 standard application. The tests are intended to facilitate the commissioning process of digital substations through bench tests of configurations and adjustments for protection and automation. Several modifications of architectures and equipment from different manufacturers were used, resulting in interoperability and cybersecurity parameters. As the work presented a platform prototype, it was impossible to verify the design results of a real physical platform or mention risk management strategies. However, the work left the way for conceptualizing the information integration project (security + interoperability).

Heinisch et al. [19] presented an innovative proposal regarding the monitoring of external threats in Smart Grid. In the form of a pilot project, the work carried out by an electricity distribution administrator consisted of developing an application to record real-time safety parameters in a virtual digital Smart Grid. However, it was not presented in work, practical use of these records in possible real attacks, or risk management data. The work application has not yet reached the stage of a controlled environment in a real Smart Grid or presentation of a digital architecture.

Lellys et al. [20] focused on the interoperability solution between equipment from different manufacturers. Presented results from cases around the world and simplified architecture based on IEC 61850, from the Process Bus, through the use of SAMU devices (Stand Alone Merging Units), thus digitizing an electric substation. Even though the results presentation is promising, no practical solutions have been reported on SAS logic tests (about interoperability interest) or identifying ways to address the risk of vulnerabilities to cyberattacks inherent in high data traffic SAMU devices.

Other studies have shown results in pilot projects, as demonstrated by Kimura et al. [21] in Brazil. Ge Li-Qing et al. [22], suggested the integration of the monitoring, error, and decision systems of Smart Grids in their platform. Vicente [23] proposed a comprehensive view of interoperability in his work, focusing on the exchange of information on protection relays from different electric substations and universalization of horizontal communication through GOOSE messages (Generic Object Oriented Substation Events). Although promising, they do not present a correlation or similarity with STRAYER's proposal in terms of risk management in their platforms or, presentation of validation data in common with the proposed in this work. The work of Pandey [24] describes a series of possible problems in Smart Grid structures related to cyberattacks and other problems and suggests a more efficient solution.

Unlike the previously mentioned researches, the proposed architecture uses the concept of an integrated solution, joining parameters that solve cyberattack problems with risk management and, at the same time, interoperability so that the architecture becomes complete. Also, the STRAYER requires minimum configuration requirements in SAS architecture, thus tying a standard Smart Grid situation with necessary parameters of safety and operability, regardless of the plant size or Smart Grid electric load.

4. Proposed architecture

This section introduces STRAYER, a new architecture to mitigate cyberattack problems in Smart Grids concerning the SAS and protection of its equipment. For modeling the STRAYER, we used adaptations in communication networks and architecture automation proposed by IEC 61850 standards in addition of more safety devices, redundancy, and separation of operation networks in Smart Grids. STRAYER's main objective is to maintain the integrity of the automation and communication system for these structures and, therefore, the continuity of then and full functioning essential services to a particular region's population.

To facilitate the understanding of the STRAYER and the research gap that this work explores, it is necessary to present the traditional automation architectural model and their loopholes so that later on, it will cover these gaps through the proposed STRAYER solution.

4.1. SAS traditional architecture

Even after the conception of the IEC 61850 in 2004 [25], it took a long time for the electric power industry to notice the importance of cybersecurity in electric substations. The theme was only substantially implemented after the attacks on plants around the world, after 2015. Several researches were carried out for the development of architectures for this purpose. It was a big step, but the architectures were only aimed at the interoperability tests of equipment from different manufacturers and logic tests that make up the SAS.

The IEC 61850 standard presents a basic traditional architecture to turn an analog electric substation into a digital Smart Grid, as presented in Fig. 1. The concepts of Smart Grids, as a rule, has three tiers: (i) Station tier; (ii) Bay tier; and (iii) Process tier. This model is a traditional architecture currently used in several semi-digital structures to apply the standard's basic concepts.

In Smart Grid, there are IED's (Label A, Fig. 1). These devices are responsible for the commands of Smart Grid's Process Level equipment, such as Power/Instrument Transformers and Circuit Breakers (Label B). As such, they become the main targets of cyberattacks.

In traditional SAS architecture, IED's communicate with only one concentrator (Label C), without any redundancy with other switches of the same or another Smart Grid. Each switch interconnects with several IED's through only one port per device. Depending on the frame size, there may be more switches for the same purpose. The IEC 61850 standard indicates that these various layer two elements (switches) are interconnected so that a communication ring is created between them. This communication is done via optical fiber, commonly with Fast Ethernet speed and using GOOSE messages. Furthermore, at least one of these switches communicates with the main switch (Label D), which will take the information to the IOC (Integrated Operations Center).

The most used communication protocols in traditional Smart Grids are GOOSE or GSSE (Generic Substation State Events), disposed in clause 6.4 of the IEC 61850-8-1 standard [26]. Both are used as horizontal and vertical communication, particularly in horizontal communication between switches, as shown in Label E of Fig. 1. It is common for strictly vertical communication to use Modbus, DNP (Distributed Network Protocol), or even ML7870. Moreover, for timestamp synchronism, the IRIG-B protocol (Inter-Range Instrumentation Group — code B) is the most used on a specific bus for this purpose. Although the IEC 61850 standards indicate the use of GOOSE and SV messages, they do so in a standard way, without the possibility of redundant use of these same protocols.

The simple application of the IEC 61850 standards in traditional architecture already brings several benefits to Smart Grid SAS. The main one is a line of switches interconnected in a ring to create a concentrator. This facilitates communication between IED's and time stamp configuration equipment, like GPS. The problem with this traditional architecture, even if applying the pure standard, is that there are several situations of vulnerability:

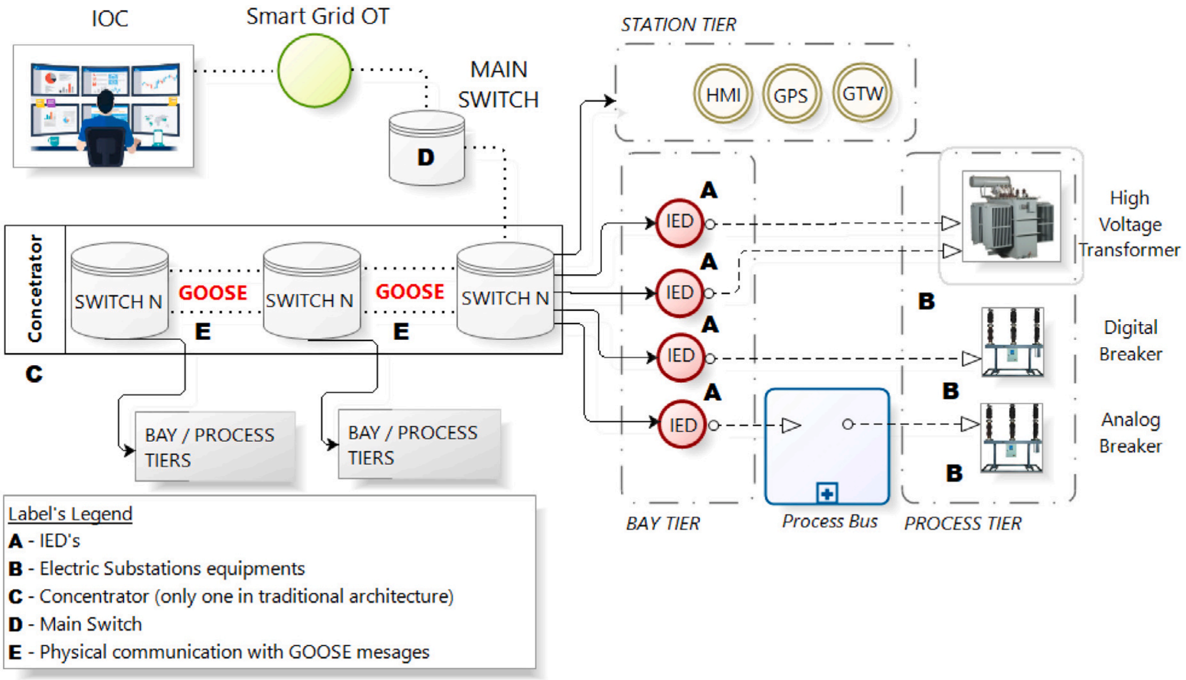


Fig. 1. An example of a IEC 61850 Smart Grid SAS traditional architecture.

- The loss of one of the ports of the edge switch;
- The loss/burning of the communication port with the IED on the switch, or;
- The lack of full integration between IED's.

Such problems can culminate in partial or total loss of the supervisory's operability and leave many security holes, such as the fragility of access to the operational network, opening for interception of messages, and server vulnerability. These can cause the exposure of the IED's, and consequently, of the Smart Grid field equipment. The challenge of the proposed research is to mitigate the problems mentioned above, demonstrating a new architecture presented below.

4.2. STRAYER adapted architecture

STRAYER was developed on an advanced and safer adaptation of the basic SAS architectural model of the IEC 61850 standard, performing the appropriate adjustments for application in Smart Grids. To maintain the recommendations that the standard requires, such as (i) interconnection between the Smart Grid's Process buses; (ii) the use of GOOSE messages and; (iii) use of a three-level SAS model (Station, Bay, and Process). STRAYER integrates security elements, with the purpose to identify ways to mitigate vulnerabilities and risks related to high data traffic in emergency situations in exchanging information between the various Smart Grids equipment like the IED's, high and low voltage busways and protection settings, and the systems involved, like other Smart Grids, the IOC and IT/OT company networks. Therefore, STRAYER presents a design of dynamic variations with more redundancies than the traditional SAS architecture.

Fig. 2 shows STRAYER's operational logic flow. The Risk Management factor is basically in the entire STRAYER process, however, emphasizing the Data Input, Analysis Processes, and Risk Feedback. The Data Analysis is performed on the data provided. With this, the data undergoes a new risk analysis process and is then feedback into the Integrator, making it possible to merge the parameters in question.

The Integrator process reveals where two of the three parameters are joined. There is a great computational effort in this point, which requires equipment with a high technological and processing factor. In practice, the simple union between Interoperability and Cybersecurity factors happens. At the end of the flow, the data is adjusted and ready to be inserted into the Smart Grid. It should be noted that the STRAYER must be at the Smart Grid communication input.

All the processes of the STRAYER logical flow present in Fig. 2 are explained in detail below.

- **Data and Adjustment Input**. These are the original automation, protection, and communication data settings for the Smart Grid IED's. It is common in a commissioning situation that these adjustments are inserted in their original study in the IED's, without proper treatment of security, interoperability or risk management. Packages can be corrupted, damaged, and settings wrong. They are the raw material of the STRAYER.
- **Data processor and the Risk Analysis**. It is the preliminary process of the STRAYER. It comprises the first inspection of the settings data, with simple verification and detection of variations in network communication. It plays the role of an Intrusion Detection/Prevention System (IDS/IPS). In the same way as IDS and IPS devices, they protect STRAYER servers. The standard ICMP Snort signature is used in the process (alert icmp command). The time taken for detection is the same as the TTL (Time to Live) of ICMP type 8 messages (TTL = 64).
- **Integrator**. Its role is to receive the pre-analyzed automation, protection, and communication settings and perform two functions simultaneously: Vulnerability Analysis (VA) and verifying the presence of socket 61850 in the manufacturer's protocol. In the latter, it is possible to perform this action through the IED Capability Description file (ICD) and the Substation Configuration Description file (SCD), present on the inspected adjustments. It can be seen then that the Integrator is able to combine a security function with protocol analysis for interoperability. For this process, STRAYER used the renowned NESSUS CLIENT program for the Kali Linux x86 OS in Command Line mode (CLI).
- **Data Analysis**. The data analysis process is a complement to the Integrator, with regard to the cybersecurity parameter. While the integrator takes care of vulnerability analysis, the Data Analysis handles other network security functions, namely: (i) *Authenticity* - avoiding brute force attacks, using proactiveness (dynamic password modification); (ii) *Confidentiality and Data Integrity* - analyzing package modifications, and; (iii) *Reliability* -

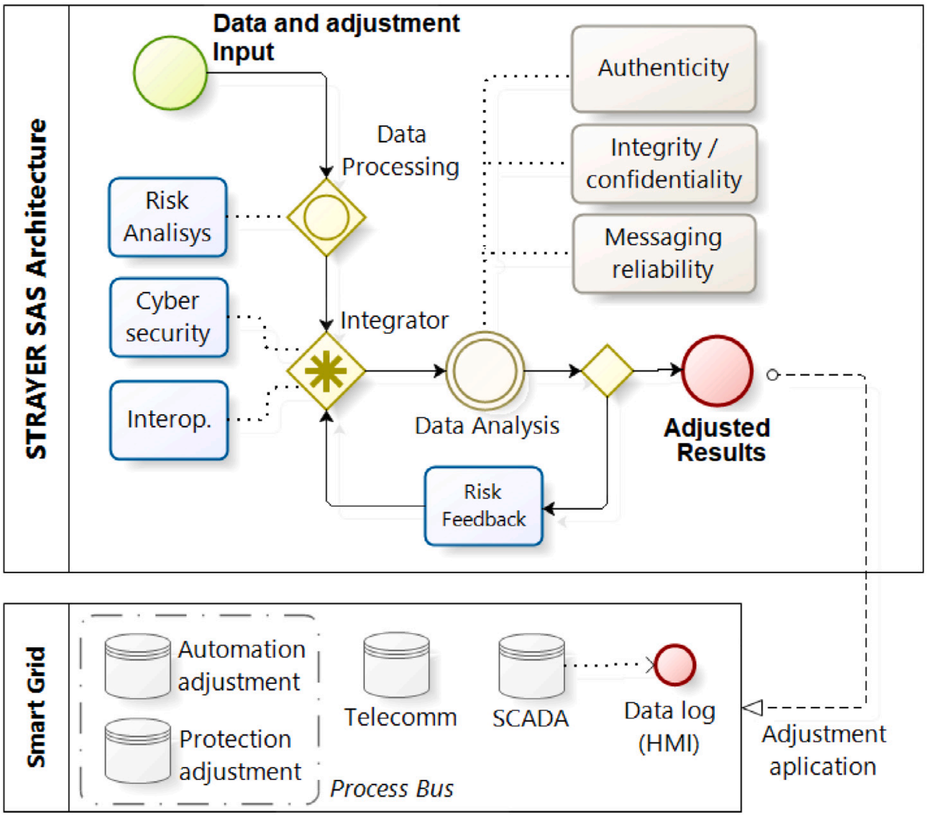


Fig. 2. STRAYER logic flow.

keeping the STRAYER administrator (root) always healthy. The Data Analysis uses another server running Kali Linux OS with NMAP capabilities.

- **Risk Feedback**. This process performs, practically, the same role as the Data Processor that uses the risk analyzer. However, with one difference: instead of letting the first inspected adjustment go through, it denies the passage of data if it does not comply with STRAYER's security rules. It then works with an internal STRAYER firewall, with the same access list (ACL) and policies scheme. If the automation, protection or communication settings still do not comply with the rules, they will be returned to the Integrator. This avoids passing inappropriate adjustments to the Smart Grid. The rules used were assembled with the Linux *iptables* system. In addition to some permission/deny rules for IP addresses, TCP flag bits (*e.g.*, TCP SYN, TCP ACK) and datagrams that enter and leave the OT network, some basic policies and configurations were implemented, such as: (i) Preventing route tracking on the OT network, by discarding all outgoing ICMP traffic with expired TTL, and; (ii) Preventing a DoS Smurf attack on the OT network by discarding all *ping* packets that are going to a broadcast address.
- **Adjusted result and application on Smart Grid**. This is the final automation, protection and communication data and duly adjusted through all the steps of the STRAYER logic flow. Data such as: IED's supervision logic, circuit breakers maximum current trip time, and, checking SCADA point time, will be applied in an adapted way in the Smart Grid, different from the original settings. From here, it is now with the adapted SAS architecture.

STRAYER was prototyped with more than one redundancy of switches, that is, with more than one concentrator (Main and Secondary, as shown in Label A, Fig. 3), to maintain a better-structured architecture in terms of security. The number of switches of each concentrator will be determined by the number of Input/Output (I/O) ports of the IED's. There are IED models on the market with a varied number of ports depending on each manufacturer. However there is unanimity in IED's models with two ports in most of them. Therefore, to maintain the situation of redundancy in IED's and the reasonable cost-benefit ratio for STRAYER, the architecture is two-ported structure. As a result, each IED will be supplied by two concentrators, each on different ports (Label B, Fig. 3).

In this architecture, the concentrators are interconnected in a ring topology, via Gigabit Ethernet fiber optic, and all IED's are be interconnected and managed by automatic reconfiguration protocols to ensure the communication flow between them. In consequence, the IED's and Smart Grid equipment will be able to exchange information with each other, regardless of the type of equipment to which each one is subject. Additionally, through SAMU devices (or simply Merging Units — MU), messages are digitized on the Smart Grid Process bus to comply with IEC 61850 standard. The MU will stay between the IED and a possible analog equipment in order to digitize information on electrical quantities from these Smart Grid equipment.

For the STRAYER adapted communication requirement there is the use of SV messages [27,28] in vertical and horizontal communication, as shown in Label C of Fig. 3, and GOOSE messages in strictly horizontal communication, with restricted VLAN's. In comparison with the security determination of the communication protocols of the IEC 62351-6 standard, which aims to immobilize the way of issuing GOOSE and SV messages in specific procedures (*e.g.*, leaving the communication in GOOSE both horizontally and vertically) [29], it was preferred the more open use of communication messages proposed by IEC 61850-90-2. In this way, it is possible for STRAYER to have more dynamism in the exchange of messages and not saturate the communication with many GOOSE messages (which is heavier than SV messages) on the SAS Process bus.

Another important implementation carried out in STRAYER was the use of MMS (Manufacturing Message Specification) communication protocols as vertical communication between user interface IED's, as

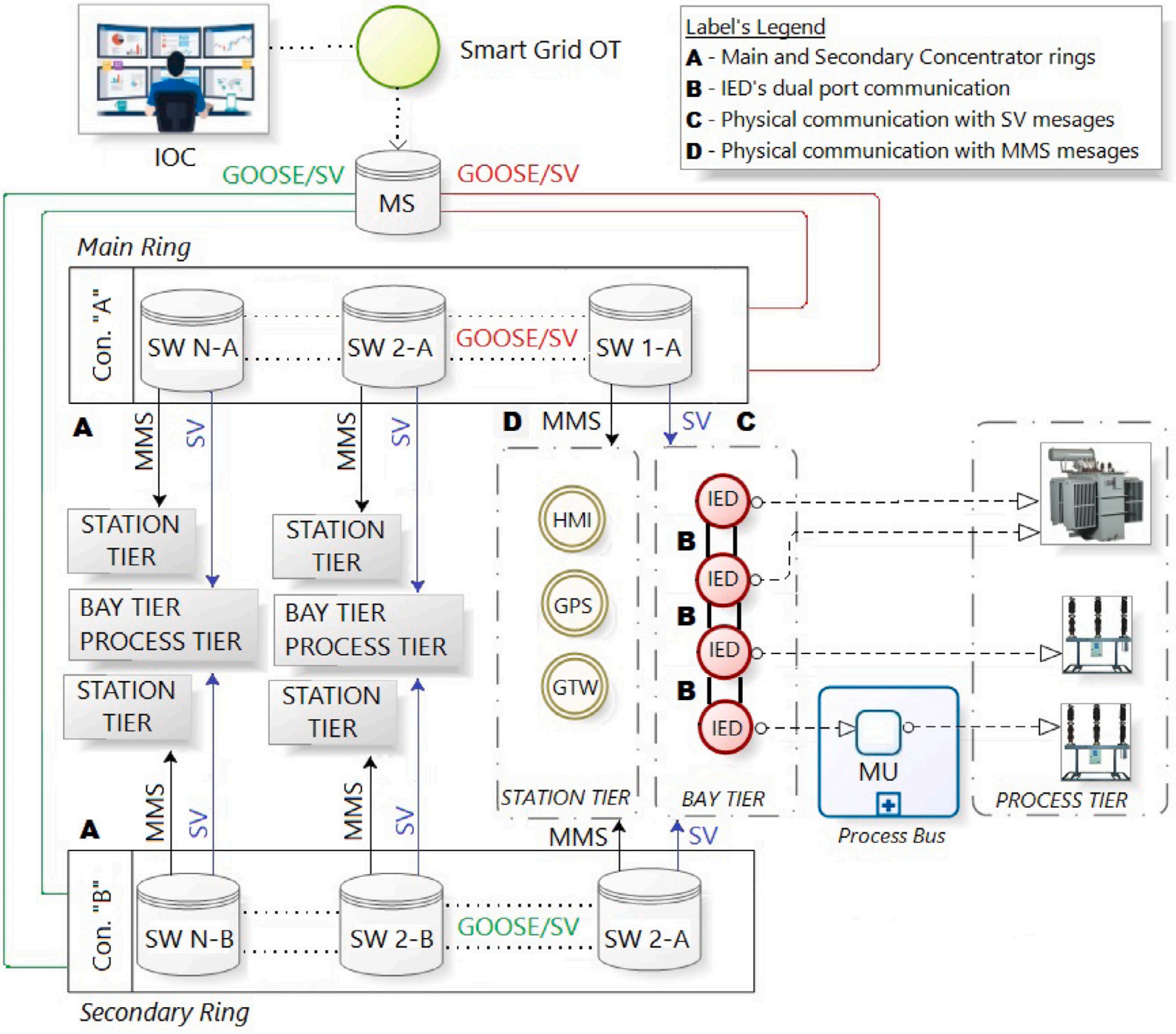


Fig. 3. STRAYER adapted of an IEC 61850 Smart Grid traditional architecture.

presented in Label D of Fig. 3, different from traditional architecture. In STRAYER, the MMS protocols [30,31] meet the interoperability criteria since it works easily in real-time data processing between devices from other manufacturers. The MMS creates a virtual device, common in all interfacing equipment (HMI — Human Machine Interface) or exchange of messages between users, such as SCADA (Supervisory Control and Data Acquisition), but maintaining the level of security for remote access, as requested in IEC 61850-7-410 standard [32]. As for time synchronization protocols, unlike the traditional architecture, STRAYER takes advantage of the Process Bus itself to implement the protocols, which is permitted in some guidelines.

STRAYER's main contribution is its success reduction factor in attacks on IED's and maneuvering equipment, such as Smart Grid circuit breakers, in addition to maintaining, for as long as possible, the integrity of the SAS and the supervisory networks. The secondary contribution, is the communication between equipment from different manufacturers in a dynamic, secure and manageable way. Dynamism is necessary, as it is known that it is impossible to practice the acquisition of various equipment by a single manufacturer. Another contribution of this architecture is the ability to analyze risk situations using as a method, logic test and protection control of Smart Grids. This facilitates the management of administrative parameters such as company KPI's (Key Performance Indicators), costs and better asset management.

These are the minimum requirements and the contributions of STRAYER, emphasizing that each Smart Grid will adapt to its architecture according to its plant topology, load, and strategic visibility. With the application of the architecture data in new Smart Grid projects or retrofits, the result will be invulnerable to external agents harmful to the electrical system of the determined region, inside or outside the electric company administrator. Next, the evaluation of the STRAYER will be presented.

5. Performance evaluation

This section shows the validation of the STRAYER, compared with the traditional architecture used in current Smart Grids. For this, STRAYER was validated in three stages: (i) performance evaluation to attack the SAS through the OT network; (ii) performance evaluation to attack the SAS through the company's IT network; and (iii) performance evaluation to attack the SAS remotely. With such stages, it was possible to identify the major advances that the STRAYER has compared to traditional architecture. Next, the modeled scenario, the metrics used, and prototype built to generate the results will be presented.

5.1. Scenario setup

To evaluate the STRAYER, we built a prototype that is commonly used in smart grids, adapting it to the STRAYER, as presented in Fig. 4. The setup of the traditional architecture contemplated equipment from the same manufacturer, while at the STRAYER, it was decided to use

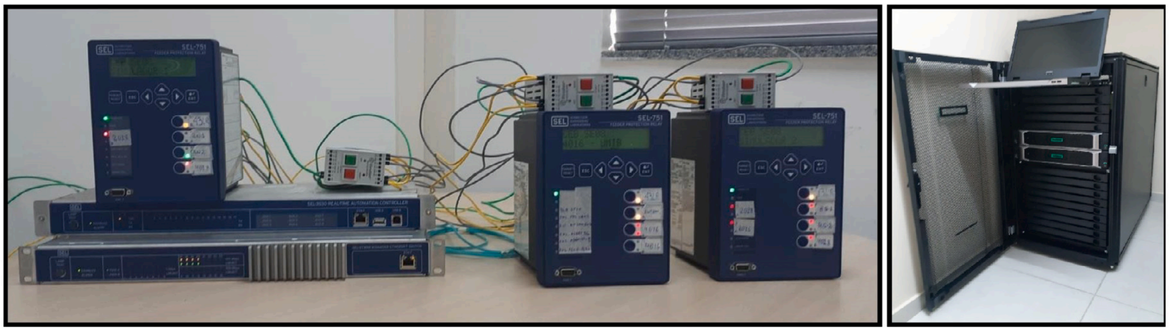


Fig. 4. Prototype developed as a proof of concept to validate the proposed architecture.

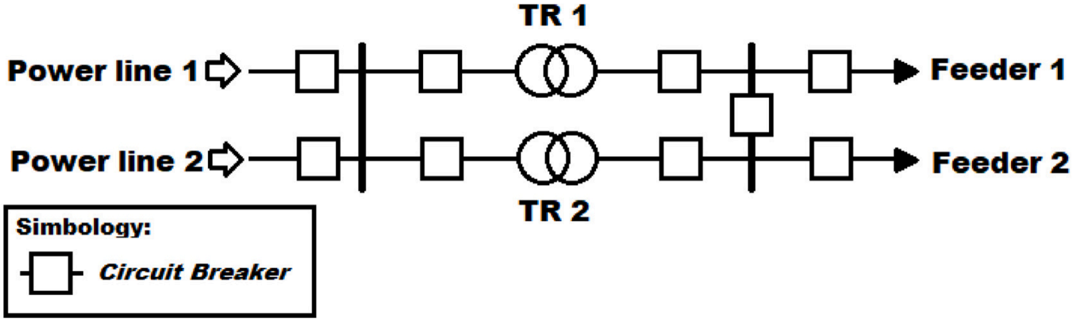


Fig. 5. Smart Grid single-line diagram modeled on the prototype.

Table 1
Amount of SAS devices and Smart Grid equipment per scenario.

Device	Traditional	STRAYER	Equipment	Traditional	STRAYER
IED	3	8	Transformer	2	2
Main Switches	1	2	Circuit Breaker	9	9
Concentrator	1	3	Lines	2	2
Merging Unit	1	7	Feeder	2	2
HMI	1	1	CT	8	8
GPS	1	2	PT	4	4
Gateway	None	2	Seccionalyzer	10	10

different manufacturers, maintaining only interconnection in a distributed infrastructure security system and avoiding an adHoc solution, as this tends to facilitate interoperability breakdown. Even though the IED's are in direct connection, these are just branches of the main nodes (switches). To make a fair comparison between the architectures, both used the same infrastructure composed of two entrance power lines, two power transformers, two feeders, and nine circuit breakers, as shown in Fig. 5. The equipment description used in the scenario to generate the experiments are presented in Table 1.

In addition, to validate the STRAYER, was used the OMICRON™ IEDScout© software [33] to virtualize the IED's.

STRAYER will feed the IED's adjustment data as described in the Logic flow. In practice, STRAYER servers (equipment to the right of Fig. 4) are located between the IOC and the first operational network access of the Smart Grid, in case the Main Switch. Everything that enters the Smart Grid must strictly evaluate the internal processes of the Logical Flow. Therefore, possible attacks will be redirected to the Risk Analysis process. Another important point is that the SAS architecture adapted from the Smart Grid is mapped to the servers. Also, even if STRAYER does its complete analysis, if a particular Smart Grid has a different architecture than the one defined, there will be a conflict, and the adjustments will not be passed on.

Once the scenario is set up, the objective is to attack the electrical commands and the automation logic of the IED's, remotely or locally, accessing the privileges of the GOOSE or SV messages and disabling the remote authenticity access by the IOC. For this, three Penetration Testing techniques (PENTEST) for Industrial Control Systems (ICS) were used: (i) SNIFFING; (ii) BRUTE FORCE, and; (iii) ROOTKIT. The concepts of attacks and open/proprietary software used in the test are described as follows.

- **(i)** SNIFFING. According to the MITRE's ATT&CK for ICS database, Sniffing (code T1040) is an attack that monitors or captures information from a given network, precisely by an asset on the same network, regardless of the flow of packets. This practice usually "mined" essential information for a more elaborate future attack. Poisoning of ARP or DNS protocols can be used to capture credentials for websites, proxies and internal systems redirecting traffic to an attacker [34]. For the test, a software widely used by *NIX network administrators was the "TCPDump". To capture the network, it was necessary to add 18 more addressing bytes to the maximum 1500 bytes of the Ethernet network, remaining with a total of 1518 bytes. Once the network activity log is recorded, it is possible to analyze it with a simple TCPDump "-r" command.
- **(ii)** BRUTE FORCE. Considered in the category of sub-attack technique by MITRE's ATT&CK for ICS, the Brute Force, code T1110, consists of gaining access to networks when passwords are unknown or when hashes are obtained. This can also be done systematically by the attacker using replay or iteration mechanisms of the credential validation services. Brute Force access leverages knowledge gained from other post-compromise behaviors, such as operating system credential dump, account discovery, or password policy discovery, or combinations of these attacks [35]. For PENTEST, the scenarios were stressed with the widely known "John The Ripper" for Linux OS, which uses C language to scan the wordlists.
- **(iii)** ROOTKIT. The Rootkit is a set of actions aiming to clean the traces for a main attack. According to MITRE's ATT&CK for ICS (by code T1014), it serves to hide the presence of programs, files, network connections, services, drivers and other components, malicious or not, of the system [36]. It intercepts and modifies OS interfaces. The ultimate intent of Rootkit is almost total control

Table 2
Stages.

STAGE	DESCRIPTION
OT direct Access	Access to the company Integrated Operations Center (IOC). Once inside, you can access the OT Network in addition to the IT network. The IOC holds remote command permission to the IEDs (remote circuit breaker maneuvers, for example).
IT direct Access	Access to the energy company building or headquarters. It is possible to access the company's Corporate Network (IT). This attack is facilitated if you are an insider attacker.
Remote Access	It is non-physical access to any electrical structure, Smart Grid or company building. In this case, the attack is more difficult, but not impossible. Bypassing the firewall is essential.

of the system, capturing the role of the administrator (root). This can result in commands being disregarded and false information being fed to the master device. In the tests, the rootkit was designed to run after SNIFFING and BRUTE FORCE attempts with an advent already existing in Linux, called SetUID. This function is nothing more than the permission that root gives to other users to access certain files. If the aforementioned attacks are successful, the rootkit makes the host work for the system to enable other attacks, such as trojan deployments, other malwares, and backdoor attacks. The latter consists of opening alternative invasion routes once inside the system. In our case, the intention was just to observe if the backdoor installation was successful.

After defining the attack types, they were applied in three stages: (i) OT network access, (ii) IT network access, and (iii) Remote access. These stages are the ways for intrusions into Smart Grids. The OT network access stage is the most direct form of invasion, as it is the network where the SCADA system is located. The IT network works as a second level to access the OT network. Finally, remote access is more difficult but deters the greatest amount of historical intrusions. The arrangement of the steps and their descriptions can be seen in Table 2.

As the objective is to validate the cyberattack problems in STRAYER, the following metrics were selected:

- **Rate of Affected IED's** - percentage of IED's successfully accessed.
- **Rate of Open circuit breakers** – percentage of successfully opened circuit breakers.
- **IOC access elapsed time** – time spent to commit the SCADA system.
- **Real time to access an IED** – time spent to access each IED.

The results achieved with their discussions are presented below.

5.2. Obtained results

All results obtained in this section were outlined above. In sequence, data from the OT, IT and Remote Access network access stages will be presented. Results from both scenarios were compared and quantified in this subsection figures. It was decided to use an exponential time separation following the Fibonacci sequence.

Some of the tests below showed such promising results that they would even lead to the interruption or inhibition of an attack, since one could, for example, activate said countermeasures by the network manager. However, the intent of the tests is to make a performance comparison, specifically, of the attack delay times. This will make the evidence clearer between the results of the two scenarios.

5.2.1. OT access stage

Fig. 6(a) demonstrates the result obtained in the tests related to the Affected IED's Rate metric through a direct OT network. It is noticeable that the number of infected IED's was lower in STRAYER than in the traditional architecture in this stage. 100% of the traditional architecture devices were affected in less than 55 s of the elapsed time. However, only 37.5% of the STRAYER's IED's were compromised. This was due to the performed risk management against promiscuous access. STRAYER noticed several requests in a short time and stopped the acceptance of commands. With this automatic advent, it was possible to set this function for all IED's without spending additional resources.

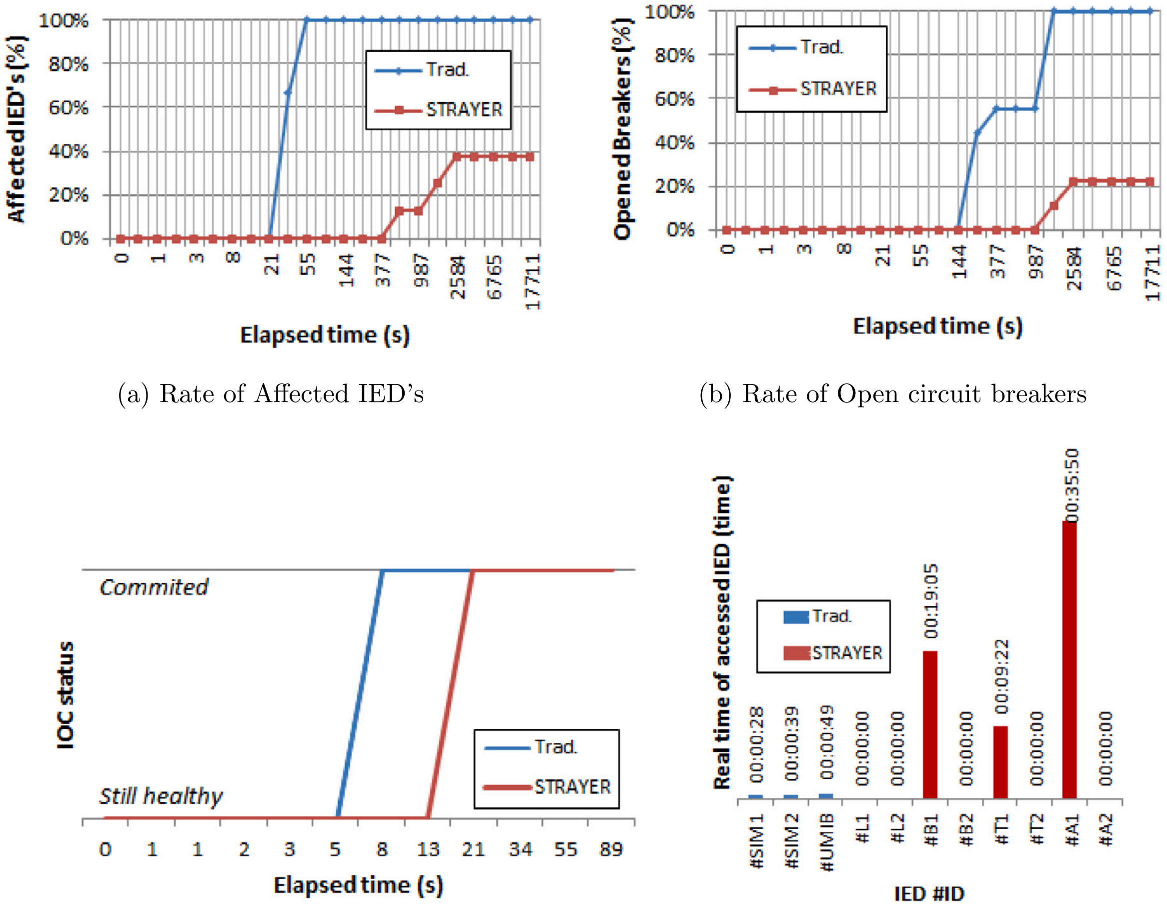
Fig. 6(b) shows a consequence in case of success for the first metric, which is the opening of the affected IED circuit breaker, accessed by the OT network. The result showed that 100% of circuit breakers on the traditional architecture were operated precisely because these devices are all connected to all possible IED's. The first circuit breaker acted in less than 233 s. However, because STRAYER restricts access to all Smart Grid circuit breakers, only 22,2% of them were operated. Precisely two circuit breakers from the same transformer and the interlink bus circuit breaker were the affected equipment. So, STRAYER upon noticing the improper access in one of the two concentrators and temporarily blocked access to the circuit breaker protection commands, delaying access to them.

Fig. 6(c) shows the time elapsed to access the IOC SCADA system from the electric company OT network. Naturally, this system usually does not have adequate access control since several people can do it (due to the insider invaders). As a result, accessing the IOC over the OT network is practically "instantaneous". However, STRAYER managed to delay this access by 13 s compared to the traditional architecture. Therefore, it is appropriate to think that access to SCADA is still a challenge. However, it was evident that STRAYER could mitigate sudden and rapid access to the system. This was possible because STRAYER has more network devices from different manufacturers and redundancies to access the OT network.

Fig. 6(d) showed the time taken to access each IED using the OT access. As expected, the traditional architecture lost its three IED's in very low time, being *00min28sec* for the first one, *00min39sec* for the second and *00min49sec* for the last. STRAYER lost only 3/8 of them in *35min50sec*. The other five STRAYER's IED had their commands blocked by the logic flow. There is no doubt that the amount of security redundancies of STRAYER helps the IED invasion delay. It should also be noted that the three IED's of the traditional architecture caused a total blackout in the Smart Grid, while in the STRAYER, only one transformer bay and low voltage bus fell. However, due to the redundancy of the other transformer, the Smart Grid continued to work. With time so high, it would be possible for a network administrator to block the attack.

5.2.2. IT access stage

Fig. 7(a) reveals the result related to the Rate of Affected IED's, now using the IT electric company network. Even so, the STRAYER's advantage over traditional architecture can be seen again. In this time, the loss of 100% of the IED's traditional architecture remained, with the difference that there was a small delay for that, compared with OT access. In STRAYER, it managed to minimize the loss of IED's about access by OT. Only 12,5% of the IED's were affected in the 2584 s elapsed time. In addition to the countermeasures adopted at the time of invasion by OT, in IT network access, STRAYER flow logic required the



(a) Rate of Affected IED's

(b) Rate of Open circuit breakers

(c) IOC access elapsed time

(d) Real time to access an IED

Fig. 6. Performance impact of STRAYER when compared with IEC 61850 traditional architecture by OT network stage.

need to use two-step authentication. This was possible with a secondary authentication through the IT network firewall.

Fig. 7(b) represent the opening of the affiliated circuit breakers using the IT network. In this stage, the traditional architecture only delayed, in 610 s, the time taken to lose all your 100% circuit breakers about the OT stage. STRAYER maintained the integrity of 71.5% of circuit breakers, losing only two of them simultaneously. However, there was a special situation: The second circuit breaker was only opened by the differential protection system of one of the Smart Grid transformers, not by invasion. In this case, when the protection perceives that one of its circuit breakers has opened improperly, or when there is a current difference between the two sides of the transformer, the two circuit breakers of this equipment open. So actually, STRAYER only lost one circuit breaker due to a cyberattack and another one due to improper protection, just in 2584 s of the elapsed time. Thus, STRAYER proved to prevent a possible attack in a longer time than in traditional architecture, even accessing the IT network stage.

Fig. 7(c) shows the time taken to break the IOC in both scenarios over the IT network. STRAYER managed to delay SCADA access time by 466 s compared to traditional architecture. IT network security equipment helped in both cases. However, in STRAYER, the two-step authentication required by the logic flow managed to keep the supervisory system healthy for 610 s.

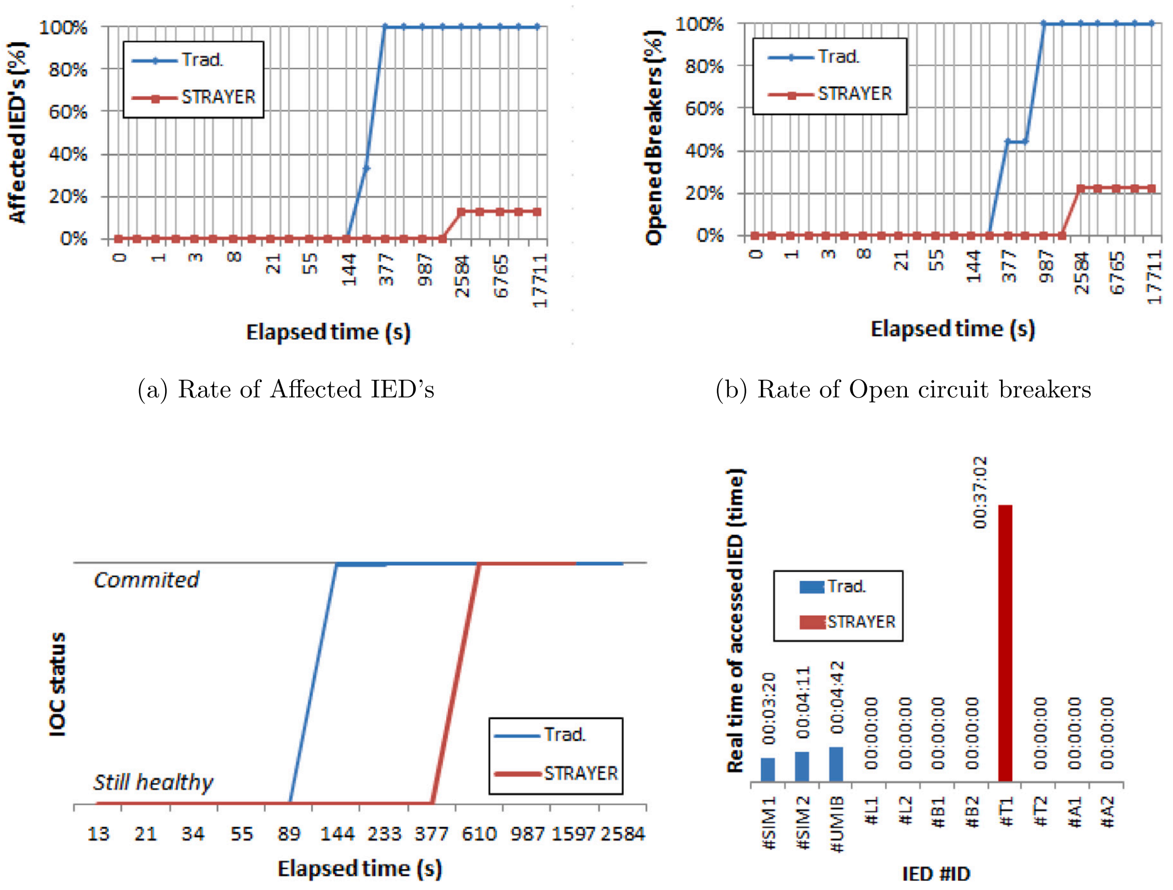
Fig. 7(d) shows the time taken to invade each IED through the IT network. It was quite evident that the STRAYER evolved its performance at this stage compared to the traditional architecture. In addition to keeping a smaller amount of invaded IED's, it significantly delayed the invasion time compared to access by OT. Traditional architecture lost all its IED's at *03min20sec*, *05min11sec* and *04min42sec*, whereas the elapsed time of the only one IED lost by the STRAYER was *37min02sec*, and in this case, it is possible to eliminate the invasion focus with the adoption of countermeasures due to the long time. Through the IT network, STRAYER managed to delay by *32min20sec* the longest break-in time compared to the traditional architecture scenario. Once again, blocking access to STRAYER's IED's was a key part of this result.

5.2.3. Remote access stage

Fig. 8(a) shows the performance of the two scenarios when analyzed according to the Rate of IED's affected metric, now by remote access. The traditional architecture maintained its 100% loss of IED's in the elapsed time of 2584 s, while STRAYER maintained the integrity of 87.5% of its eight IED's. Once again, STRAYER outperformed traditional architecture. The feedback part of the STRAYER logic flow sensed improper access to the SAS Main Switch, preventing further access from being attempted.

Fig. 8(b) presents the number of circuit breakers affected via remote access over a given time. While 100% of circuit breakers were compromised in traditional architecture, only 11.1% of them were opened in STRAYER. It is noticed that, even with the invasion of two IED's, referring to the previous metric, STRAYER prevented the opening of a second circuit breaker, keeping the Smart Grid in full operation. However, there was a total blackout by traditional architecture.

Fig. 8(c) shows the access time to the IOC and its SCADA system remotely. It can be seen that the STRAYER scenario delayed the IOC



(a) Rate of Affected IED's

(b) Rate of Open circuit breakers

(c) IOC access elapsed time

(d) Real time to access an IED

Fig. 7. Performance impact of STRAYER when compared with IEC 61850 traditional architecture by IT network stage.

invasion time by 987 s compared to the traditional IEC 61850 scenario. It is also possible to analyze from the same figure that the access time was longer than the stages of access to IT and OT networks.

Fig. 8(d) brings the list with all the IED's of each scenario, with their respective invasion time, by remote access. The traditional architecture failed to mitigate the attack on its IED's and lost access to all devices within a maximum time of *31min52sec* for remote access. The first metric showed that STRAYER lost only a single IED, and even so, it only happened at the time of *1h43min15sec*, according to Fig. 8(d) of the current metric, which would make it possible to block the attack by a Security Operations Center (SOC). The performance of STRAYER about invasion delay was evidenced in this metric because, in this case, it delayed access by more than an hour. This time is already enough for the company cybersecurity team to have already taken real-time preventive measures to eliminate the invasion.

5.3. Discussion

In this subsection, the results of the previous section will be discussed, making a general comparison between the three access steps, observing the data obtained by the metrics. Initially, looking at the overall results, it is clear that the Remote access stage had better performance than the others. This situation is plausible since the remote access path is longer than for OT and IT networks with more direct access. This is very promising, as the history of intrusions into Smart Grids tends to be by remote access channel [5–7], using protocols such as Telnet, FTP, and other TCP services. In addition, it was noted that there was a faster access block to the IED's for the attempt to access the OT network than in the other stages. As the invasion is faster in this network, consequently, the blocking is also faster. Finally, comparisons between the three access stages were presented.

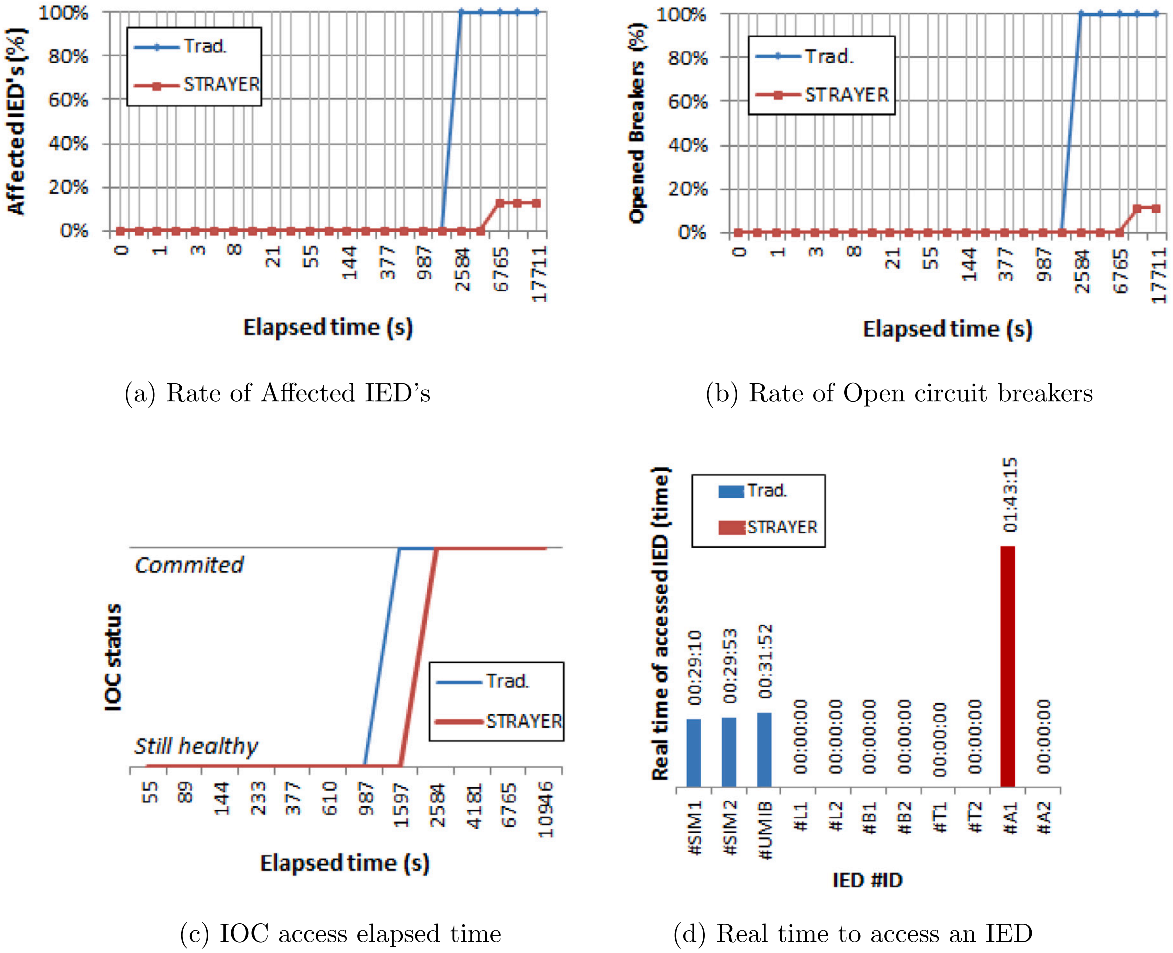
6. Conclusion

Despite the recent advances of Smart Grids and their cybersecurity recommendations, there are still attacks on these structures' automation and protection systems. As a result, this paper presented the systemic and real problem of security vulnerabilities of traditional automation architecture patterns in Smart Grids and proposed the STRAYER architecture to reduce this threat. STRAYER integrates cybersecurity for monitoring and shielding access, interoperability for maintaining communication between equipment/devices, and risk management for maintaining reliability and preventing real-time cyberattacks on Smart Grids. With this, STRAYER analyzed possible cyberattacks using integration factors logic within the network devices of a Smart Grid.

As a proof of concept, a prototype commonly used in smart grids was built to validate the STRAYER designed to operate in a SAS. The results showed that STRAYER has an excellent performance in access control due to the automation and protection logic of an electric power supply system. In addition to the reductions in the amount of IEDs affected by invasions, it was also possible to notice that STRAYER avoided the collapse of a Smart Grid, having only minimal and reversible losses, unlike the traditional architecture.

We highlight the following contributions:

- a new SAS Smart Grid architecture based on logic adaptations to avoid cyberattacks.



(a) Rate of Affected IED's

(b) Rate of Open circuit breakers

(c) IOC access elapsed time

(d) Real time to access an IED

Fig. 8. Performance impact of STRAYER when compared with IEC 61850 traditional architecture by Remote access.

- the security efficiency improvement compared to the previous architectures and related works.
- an experience report of the employment in a real context.

As future work, we intend to employ and evaluate a federated learning architecture on the STRAYER to mitigate cyberattack problems in Smart Grids. Additionally, the reduction of the time of invasion to the IOC will be worked on. With federated learning, it is possible to protect data confidentiality, allowing Smart Grid devices to collaboratively build an efficient defense model against attacks while prioritizing data monitoring. We support the hypothesis that such an architecture can reduce the attack time in a Smart Grid.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Gunduz M, Das R. Cyber-security on smart grid: Threats and potential solutions. Comput Netw 2020;169:107094. http://dx.doi.org/10.1016/j.comnet.2019.107094.

[2] Greer C, et al. NIST SP 1108r3 - NIST framework and roadmap for smart grid interoperability standards, release 3.0. National Institute of Standards and Technology; 2014, p. 1–246. http://dx.doi.org/10.6028/NIST.SP.1108r3, 1108r3.

[3] Cintuglu M, Mohammed O, Akkaya K, Uluagac A. A survey on smart grid cyber-physical system testbeds. IEEE Commun Surv Tutor 2016;19 n1:446–64. http://dx.doi.org/10.1109/COMST.2016.2627399.

[4] Mubarak S, Habaebi H, Islam R, Balla A, Tahir M, Elsheikh A, et al. Industrial datasets with ICS testbed and attack detection using machine learning techniques. Intell Autom Soft Comput 2021;1–16. http://dx.doi.org/10.32604/iasc.2022.020801.

[5] BBC. Report: Hackers behind Ukraine power cuts, says US report. 2016, BBC News. BBC Technology. URL: https://www.bbc.com/news/technology--35667989. [Accessed 26 February 2016].

[6] Zhegulev I. Report: Ukraine asks FBI to help probe suspected Russian hack of burisma. 2020, Reuters. U.S. Legal News. URL: https://www.reuters.com/article/idUSKBN1ZF1KL. [Accessed 16 January 2020].

[7] Costa L. Report: Energisa electric seeks to restore systems after being the target of cyberattack. 2020, Reuters Brazil. Yahoo Finanças. URL: https://br.financas.yahoo.com/noticias. [Accessed 5 May 2020].

[8] Lázaro J, Astarloa A, Rodríguez M, Bidarte U, Jiménez J. A survey on vulnerabilities and countermeasures in the communications of the smart grid. MDPI Electron 2021;10:1881. http://dx.doi.org/10.3390/electronics10161881.

[9] Faquir D, Chouliaras N, Sofia V, Olga K, Maglaras L. Cybersecurity in smart grids, challenges and solutions. AIMS Electron Electr Eng 2021;5:24–37. http://dx.doi.org/10.3934/electreng.2021002.

[10] Yang W, Heng-Xuan L, Shi-Ping E, Kan-Jun Z. Research on classification of substation background information for monitoring. In: International conference on building energy conservation, thermal safety and environmental pollution control. Vol. 136. 2019, p. 01023. http://dx.doi.org/10.1051/e3sconf/201913601023.

[11] Vardhan H, Ramlachan R, Szela W, Gdowik E. Deploying digital substations: Experience with a digital substation pilot in north america. In: 71st Annual conference for protective relay engineers (CPRE) IEEE. 2018, p. 1–9. http://dx.doi.org/10.1109/CPRE.2018.8349795.

[12] Stouffer K, Zimmerman T, Tang C, Lubell J, Cichonski J, McCarthy J. NIST report 8183 - cybersecurity framework manufacturing profile. Vol. 8183. National Institute of Standards and Technology; 2017, p. 1–57. http://dx.doi.org/10.6028/NIST.IR.8183.

[13] Vernadat FB. Enterprise modelling and integration: principles and applications. In: International conference on enterprise integration and modeling technology. Vol. 1. 2002, p. 25–33. http://dx.doi.org/10.1007/978-0-387-35621-1_4.

[14] Chede C. Open standards, interoperability and public interest. Politics Nupef J 2008;1.

[15] ISO. ISO 31000 - risk management – guidelines - second edition. Vol. 31000. International Organization for Standardization; 2018, p. 1–23.

[16] ISO. ISO 31010 - risk management — risk assessment techniques. Vol. 31010. International Organization for Standardization; 2021, p. 1–150.

[17] IEC. IEC 61850-9-2 - communication networks and systems for power utility automation - part 9-2: specific communication service mapping (SCSM) - sampled values over ISO/IEC 8802-3. International Electrotechnical Commission; 2011, p. 1–65, 61850-9-2.

[18] Fontes M. Compliant didactic platform design for commissioning a IEC 61850 digital power substation control and protection system. Masters Dissertation from Rio Grande Do Norte Federal University; 2015, p. 1–150, 129f.

[19] Heinisch A, Leite L, Spyer B, Rabello M. Segurança cibernética para processos operativos em sistemas de energia elétrica. Published in the Technology and Innovation Management Center - CGTI; 2012, Library of Articles/Reports.

[20] Lellys D, Paulino M, Alves dC, Schimitt M. Process bus (merging unit): concept, architecture and impact on substation automation. Technology and Innovation Management Center - CGTI; 2016, p. 1–7, Library of Articles/Reports.

[21] Kimura S, Rotta A, Abboud R, Moraes R, Zanirato E, Bahia J. Applying IEC 61850 to real life: Modernization project for 30 electrical substations. In: 1st Annual protection, automation and control world conference. 2010, p. 1–18.

[22] Li-Qing G, Jian-Feng W, Jing-Yu T, Ming Y. Research and application of one-key sequence control technology for substations. In: International conference on building energy conservation, thermal safety and environmental pollution control. Vol. 136. 2019, p. 01022. http://dx.doi.org/10.1051/e3sconf/201913601022.

[23] Vicente DT. Application of IEC 61850 standards in electrical power transmission/distribution shared substations. Thesis from Sao Paulo University; 2011, p. 1–117. http://dx.doi.org/10.11606/D.3.2011.tde-09032012-151057.

[24] Pandey R, Misra M. Cyber security threats-smart grid infrastructure. In: 2016 National power systems conference. 2016, p. 1–6. http://dx.doi.org/10.1109/NPSC.2016.7858950.

[25] IEC. IEC 61850 - communication networks and systems in substations. Vol. 61850. 1st ed.. International Electrotechnical Commission; 2007.

[26] IEC. IEC 61850-8-1 - communication networks and systems in substations - part 8-1: specific communication service mapping (SCSM) - mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. International Electrotechnical Commission; 2004, p. 1–140, 61850-8-1.

[27] IEC. IEC 61850-90-1 - communication networks and systems for power utility automation - part 90-1: Use of IEC 61850 for the communication between substations. International Electrotechnical Commission; 2020, p. 1–79, 61850-90-1.

[28] IEC. IEC 61850-90-2 - communication networks and systems for power utility automation - part 90-2: using IEC 61850 for communication between substations and control centres. International Electrotechnical Commission; 2020, p. 1–188, 61850-90-2.

[29] IEC. IEC 62351-6 - power systems management and associated information exchange - data and communications security - part 6: security for IEC 61850. International Electrotechnical Commission; 2020, p. 1–67, 62351–6.

[30] IEC. IEC 9506 - industrial automation systems — manufacturing message specification. Vol. 9506. International Electrotechnical Commission; 2003, p. 1–316.

[31] IEC. IEC 62351-4 - power systems management and associated information exchange - data and communications security - part 4: profiles including MMS and derivatives. International Electrotechnical Commission; 2018, p. 1–494, 62351–4.

[32] IEC. IEC 61850-7-410 - basic communication structure - hydroelectric power plants - communication for monitoring and control. International Electrotechnical Commission; 2015, p. 1–284, 61850-7-410.

[33] OMICRON. Test solutions for protection and measurement systems. 2021, p. 35, Product Catalog.

[34] MITRE. Network sniffing. 2022, ATT&CK for ICS. URL: https://attack.mitre.org/techniques/T1040/. (2022 February).

[35] MITRE. Brute force I/O. 2022, ATT&CK for ICS. URL: https://attack.mitre.org/techniques/T1110/. (2022 February).

[36] MITRE. Rootkit. 2022, ATT&CK for ICS. URL: https://attack.mitre.org/techniques/T1014/. (2022 February).

Alexandro de O. Paula (https://orcid.org/0000-0002-9504-7308) is a cybersecurity MsC. at the University of Brasília (UnB), scheduled for conclusion in 2022. Received the MBA degree in Project Management from the University North of Paraná (UNOPAR). He has an Electrical Engineering Bachelor's degree from the Rio Grande do Norte Federal University (UFRN) since 2013. Currently, he is the Subtransmission Maintenance Coordinator at Iberdrola Neoenergia Brasilia. Responsible for the entire process of planning and executing maintenance on smart grids in the Federal District, Brazil, using the concepts of network security and risk management to keep the system in operation. Proficiency in Energy Distribution, Protection, Automation, Telecommunications, Renewable Energies, and Maintenance engineering.

Rodolfo I. Meneguete is an Assistant Professor of the Institute of Mathematics and Computer Science (ICMC) at the University of São Paulo (USP). He received his Bachelor's degree in Computer Science from the University of São Paulo, Brazil, in 2006. He received his master's degree in 2009. He received his doctorate from the University of Campinas (Unicamp), Brazil, in 2013. He did his post-doctorate in the PARADISE Research Laboratory, University of Ottawa, Canada, in 2017. His research interest are in the areas of vehicular networks, resources management, flow of mobility and vehicular clouds.

Felipe T. Giutini received the Ph.D. degree in computer science and computational mathematics from the University of São Paulo (USP), Brazil, and the master's degree from the Federal University of São Carlos (UFSCar), in 2016. He is currently a Full Researcher with Sidia Research and Development Institute. He is interested in applied research involving mobile devices, smart environments, networks, data science, and affective computing.

Maycon L.M. Peixoto is a postdoctoral researcher at University of Campinas (UNICAMP), Brazil. He is also a professor at the Department of Computer Science of the Federal University of Bahia (UFBA). He holds a Ph.D. in Computer Science from the University of Sao Paulo (USP), Brazil, 2012 and his Master degree in Computer Science from the University of Sao Paulo, 2008. His main research interests include urban computing, smart grids, vehicular ad hoc networks, performance evaluation, cloud, edge, and fog Computing.

Vinícius P. Gonçalves (https://orcid.org/0000-0002-3771-2605) has a Ph.D. in Computer Science and Computational Mathematics (2016) from the University of São Paulo (USP). He was also a research fellow at the University of Arizona (USA) before joining the University of Brasília (UnB). Dr. Gonçalves was a Postdoctoral Researcher at the USP Medical School, with a CAPES Fellowship. Currently, he is an Assistant Professor in the Electrical Engineering Department (ENE) at UnB, Brasília, Brazil, where he is a member of the Graduate Programs in Electrical Engineering (PPGEE and PPEE). Dr. Gonçalves is a researcher and member of the AQUARELA Group; his main research interests include Human–Computer Interaction, Internet of Things, Cybersecurity, Mobile Health, Image Processing and Machine Learning.

Geraldo P. Rocha Filho (https://orcid.org/0000-0001-6795-2768) is an Assistant Professor at the Computer Science Department (CiC) at University of Brasılia (UnB). He received his Ph.D. in Computer Science from the University of São Paulo (USP) in 2018. He received his M.Sc. from the USP in 2014. He was also a post-doctoral research fellow at the Institute of Computing at UNICAMP before joining the UnB. His research interests are wireless sensor networks, vehicular networks, smart grids, smart home and machine learning.