Evaluation of IPS Systems in the Prevention of Cyber Attacks on Digital Substations: Validation and Analysis in a Real-Time Simulation Environment

J. OSPINA*
Kinnesis Solutions
Colombia
jeospina@kinnesis.com

L. ISAZA-GIRALDO
Kinnesis Solutions
Colombia
lisaza@kinnesis.com

D.A. PÉREZ
Kinnesis Solutions
Colombia
dperez@kinnesis.com

B.A. POTOSÍ
Kinnesis Solutions
Colombia
bapotosi@kinnesis.com

B.A. ARBOLEDA
XM
Colombia
barboleda@xm.com.co

Abstract *– Due to the growing integration between IT (information technology) and OT (operational technology), vulnerability to cyber threats has increased in critical infrastructure, particularly in electrical substations. This situation requires an extra step in terms of security measures. The article that will be presented, addresses the benefits of intrusion prevention systems (IPS) in OT networks, analyzing their performance in a controlled test environment. The technical challenges and limitations that may arise during implementation will be detailed and the discussion on the conditions and strategies that would provide a comprehensive overview to help strengthen substation security will be presented afterwards.*

Palabras clave: **Operation – Information – Substations – Infrastructure – Cibersecurity – Systems – Prevention – Detection – Intrusions - IPS**

1 INTRODUCTION

Critical infrastructure is defined as infrastructure that is so vital that its destruction or disablement would have a debilitating effect on a country's defense or economic security. This infrastructure includes a country's electrical system, and within this system are the assets that perform the fundamental operational functions [1]. In the particular instance of electrical energy, the infrastructure consists of both an IT (information technology) component and an OT (operational technology) component. These components are responsible, respectively, for managing all data and information in digital communications networks and for physically managing the various operational processes [2].

However, despite the fact that both components were initially siloed, there convergence between these two worlds is increasing each day, revealing a technical vulnerability in electrical grid operating equipment, as these are elements with long life cycles and low rate of actualization and, as time passes, the number of cyber threats to which these devices could be exposed increases [3]. The severity of these threats lies in the specificity of the attacks and threats generated from different areas, as they can be potentially catastrophic for equipment in the sector [4] and, therefore, for the entire electrical system of the country.

It is therefore necessary to have devices such as intrusion detection systems (IDS), which analyze substation traffic in a non-invasive manner, or intrusion prevention systems (IPS), which can block malicious traffic by directly influencing substation communications [5], since in critical infrastructure security, it is not usually possible to achieve security objectives through the application of a single countermeasure or technique. Therefore, cybersecurity standards for the industrial sector, such as ISA/IEC 62443 1-1, propose the use of a

* jeospina@kinnesis.com, Medellín, Cra 25# 1A Sur 155 Oficina 1453

in-depth-defense strategy, based on the principle of using multiple security countermeasures in a staggered or layered manner [6].

Accordingly, the response of an IDS, which focuses primarily on identifying attacks, cannot be considered a robust security policy in itself, and it has been shown that the security of critical infrastructure could benefit from the support of an IPS [7].

This article focuses on identifying potential technical issues and limitations in the integration of these cybersecurity solutions, particularly IPSs, identifying potential vulnerabilities, and providing recommendations and strategies that can facilitate the use of this equipment for optimal implementation in substations, ensuring the security of electrical substation networks and improving resilience to cyberattacks. This proactive approach to cybersecurity is essential in an increasingly digitalized world with constantly evolving cyber threats, thus ensuring the continuity and reliability of the electricity supply.

The materials and methods section details the devices and technologies used, as well as the experimental and testing environment. The results section shows the behavior of the IPS when subjected to the tests described in the previous section. The discussion section addresses the cost-effectiveness of the system, and finally, the conclusions section summarizes the key ideas, lessons learned, and next steps in this line of research.

2 MATERIALS AND METHODS

2.1 Description of the devices and technologies used

The following equipment was used to proceed with the tests, aiming to identify possible technical issues and limitations in integrating an IPS into a simulated substation environment in the laboratory:

- IPS (Intrusion Prevention System): Network security tool with the same threat detection functions as an IDS, but with prevention capabilities to directly block malicious network traffic.
- IEDs (Intelligent Electronic Devices): Intelligent electronic devices that can be programmed to collect data, process this data, and take appropriate action, commonly used in industrial automation and electrical sector protections.
- Switches: Devices used in networks with high port availability to interconnect various devices, allowing them to communicate with each other and share information within a LAN.
- DoS (Denial of Service): An attack aimed at disrupting the service of a system or network by sending a large amount of traffic from a single device, which consumes the victim's resources to the point that its response capacity is reduced to the point that it begins to reject legitimate requests.
- Ping: A command line tool that measures the latency between the connection of two network devices.

2.2 Experimental environment

A network architecture for an electrical substation was designed and implemented, with physical equipment interconnected and installed in the same rack. Said equipment was integrated into a controlled testing environment using protocols in accordance with the IEC61850 standard. With all the equipment in place, an IPS cybersecurity equipment was strategically installed within the network to facilitate the detection and containment of malicious attacks. Having the experimental environment ready, the IPS equipment was configured according to the test requirements, which consisted of protecting the vulnerabilities of the IED equipment from a cyberattack.

The IPS has two protection modes, Offline mode and Online mode. For these tests, it is strictly necessary to use it in Online mode so that all network traffic reaching the victim device, in this case the IED, passes through the IPS (see Fig. 1) and, in this way, according to the profile, policies, and rules enabled in the IPS, it can contain the cyberattack.

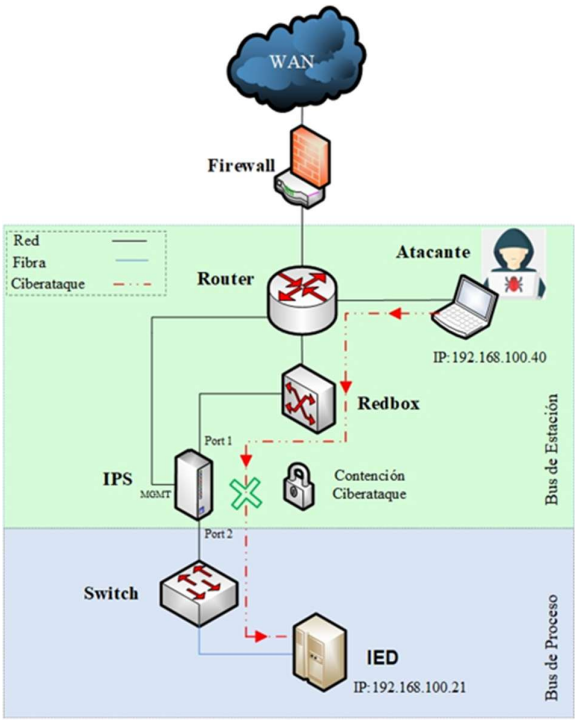

Fig 1. Schematic diagram of the simulated substation network.

In order for the IPS to contain the attack, it is important to properly configure policies and rules that do not affect the network traffic necessary for the normal operation of the IED equipment. To do this, profiles such as IEC61850 are defined, which uses Generic Object Oriented Substation Events (GOOSE) protocols, Manufacturing Message Specification (MMS), and Sampled Values (SV), which are specific to the electrical sector. Rules are then configured to help identify what type of network traffic is secure. To do this, the IPS has a self-learning mode that is programmed for a specific period of time and, during this mode, is able to create its own rules based on the traffic it analyzes on the network. In this process, it is the user's responsibility to validate which rules are not appropriate and eliminate them so as not to cause unnecessary blocking in the operation of the IED and, if necessary, to add custom rules. Once the profile and rules have been created, security policies are configured specifically to contain DoS-type attacks.

2.3 Simulation scenarios: DoS cyber-attack and system response

If a malicious person identifies vulnerabilities in the IED equipment installed in the substation network and manages to gain access to it to execute a DoS attack, this attack aims to send a large number of requests or data that overloads the equipment, leaving it inaccessible to those who legitimately need it. To validate the effectiveness of implementing an IPS in an OT network, two scenarios are considered: the first is when the network does not have a cybersecurity protection scheme in place, and the second is when network protection is implemented with IPS equipment.

3 RESULTS

3.1 Evaluation of IPS performance against simulated attacks

To understand the effectiveness of an IPS against an attack, a sustained ping is sent to the IED's IP address and latency and packet loss are monitored. At the same time, the availability and response time of the web interface, accessible through port 4443 of the IED, is inspected. The objective of this test is to determine whether the attack manages to stop the service, observing packet loss or unavailability of the web service.

3.1.1 Scenario 1: no protection scheme.

For the first scenario, the DoS attack was executed without implementing IPS equipment or configured passively in network monitoring mode. As a result, packet loss was observed, evidencing communication problems with the IED on the network, causing serious damage to the substation (see Fig. 2).

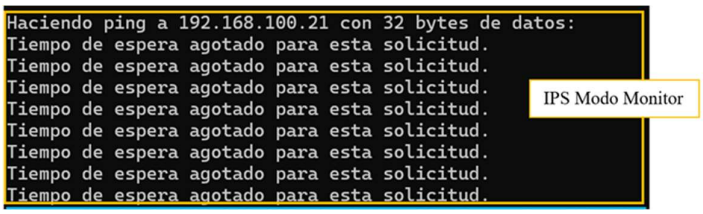

Fig 2. Loss of communication with the IED, IPS in monitor mode.

3.1.2 Scenario 2: protection scheme with IPS.

For the second scenario, the DoS attack is executed when an IPS is implemented and configured in prevention mode with the rules and profiles previously configured to protect the vulnerabilities of the victim computer or IED. In this case, it can be seen that during the attack, the IED never lost network communication and operated normally (see Fig. 3), demonstrating that the IPS was able to contain the attack and identify the type of attack, where it originated, and which device was the victim (see Fig. 4).

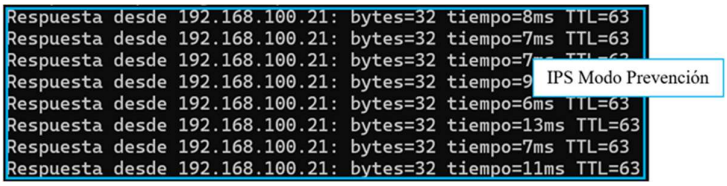

Fig 3. Communication with IED without loss of packets.

Time	Function Type	Protocol Layer	Security Category	Security Severity	Security Rule Name	Interface	Attacker	Victim
2025-01-22T17:15:34-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:29-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:24-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:19-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:14-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:09-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:04-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21

Fig 4. IPS event log during the attack.

4 DISCUSSION

A key aspect identified in this research is the need for IPS personnel to have specialized knowledge of both the interactions and operation of the protocols used by substation devices (MMS, GOOSE, IEC 60870-5-101, IEC 60870-5-104, DNP3, Modbus, etc.), as well as the operation and parameterization of the IPS, with the aim of enabling proper fine-tuning of detection and containment actions, minimizing false positives, such as unnecessary traffic blockages in IEDs in the substation. Although this may be difficult to find in a single profile

within organizations, joint and complementary work between operations personnel and the cybersecurity team becomes necessary.

The above describes the main challenge when implementing an IPS in a substation environment and also in an industrial environment: blocking OT traffic during the production stage. Evaluating the operation of an IPS in a laboratory environment is essential in order to identify in advance the different protocols and communications involved in the process, as well as the various functions and OT protocol support offered by the IPS solution, whether it is designed for substations or industrial environments. This can be seen in previous studies [8] which validate the existence of multiple IPS solutions for industry, as well as helping to visualize, as a strategy for its parameterization, a preliminary stage of traffic monitoring in passive mode or detection as IDS before operating it in active mode as IPS.

The results of this research provide an initial approximation of the scenario for implementing an active IPS-type technological solution, which supports the analyses that companies in the electricity sector in Latin America can opt for in response to the growing digitization of electrical substations and the sophistication of the cyber threats to which they may be exposed. However, the implementation of a cybersecurity event monitoring or prevention solution should be the result of the application of standards or regulations, policies, and a risk analysis to determine its technical and economic feasibility.

The cost-benefit analysis of a cybersecurity solution is an important and complex factor to consider when implementing it, as it requires assessments of risks, vulnerabilities, compliance with standards, organizational culture, accompanied by metrics for measurement [9], the quantification of the direct costs of its acquisition, implementation, and maintenance, as well as the assessment of the costs that could arise in the event of an incident such as a substation blackout, in addition to the loss of reputation if the incident cannot be prevented or contained.

In the case of implementing an IPS-type solution, a starting point for performing this analysis is to know its market cost, which depends on the components sized for its operation (hardware, software, management platform, etc.), to which the cost of implementation services must be added. The total quantification of the cost-benefit ratio will require the application and detailed analysis of the above factors, taking into account the operational situation of each case.

Recent reports by leaders in cybersecurity solutions have revealed that critical infrastructure sectors such as energy and oil/gas have suffered ransomware attacks, mainly due to the exploitation of vulnerabilities (49%), suggesting that patch implementation should be prioritized based on a risk analysis. Such attacks have demanded ransom payments between USD$1M and USD$5M in 71% of cases, as well as recovery costs averaging USD$3.12M in 2024 [10]. The IPS solution with virtual patching capabilities for legacy equipment offers an alternative solution to prevent and contain the exploitation of vulnerabilities in cases where patching is no longer possible.

5 CONCLUSIONS

The implementation of an IPS in substations improves the security and availability of OT networks, if it is configured correctly, achieving real-time detection and mitigation of cyberattacks. Proper configuration ensures the correct functioning of the system without affecting communication within the substation.

Not paying attention to IPS customization parameters such as profiles, protocols, or specific addressing requirements can lead to major problems when implementing an IPS in a substation. Therefore, it is ideal for those in charge of managing this type of solution to be multidisciplinary professionals with knowledge of both OT and IT, or, failing that, for there to be practical convergence between these two areas.

There are still numerous opportunities for research in this field, particularly about the optimization and application of protection alternatives for OT networks.

The effectiveness of implementing cybersecurity equipment in an OT network depends on several factors, such as the technical capabilities of the IPS equipment and the knowledge of the operators and administrators of the OT network to be protected. This combination guarantees effective protection against attacks by malicious individuals.

6 REFERENCES

[1] J. Moteff, C. Copeland, y J. Fischer, «Critical Infrastructures: What Makes an Infrastructure Critical?».

[2] P. K. Garimella, «IT-OT Integration Challenges in Utilities», en 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu: IEEE, oct. 2018, pp. 199-204. doi: 10.1109/CCCS.2018.8586807.

[3] R. Flosbach, J. J. Chromik, y A. Remke, «Architecture and Prototype Implementation for Process-Aware Intrusion Detection in Electrical Grids», en 2019 38th Symposium on Reliable Distributed Systems (SRDS), Lyon, France: IEEE, oct. 2019, pp. 42-4209. doi: 10.1109/SRDS47363.2019.00015.

[4] C. Konstantinou y M. Maniatakos, «Impact of firmware modification attacks on power systems field devices», en 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA: IEEE, nov. 2015, pp. 283-288. doi: 10.1109/SmartGridComm.2015.7436314.

[5] S. Major y E. Fekovic, «Securing intelligent substations: Real-time situational awareness», en 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, Croatia: IEEE, may 2014, pp. 711-715. doi: 10.1109/ENERGYCON.2014.6850504.

[6] K. A. Scarfone y P. M. Mell, «Guide to Intrusion Detection and Prevention Systems (IDPS)», National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-94, 2007. doi: 10.6028/NIST.SP.800-94.

[7] A. L. Giri y S. Annamalai, «Intrusion Detection System for Local Networks – A Review Study», en 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India: IEEE, abr. 2022, pp. 1388-1393. doi: 10.1109/ICACITE53722.2022.9823433.

[8] Adrián Soucase Iranzo. «Implementacion de un Sistema de Prevencion de Intrusiones IPS en un modelo de red industrial.» (2021). *Escuela Técnica Superior de Ingeniería de Telecomunicación*, *Universitat Politècnica de València*. https://riunet.upv.es/handle/10251/178959

[9] P. Rathod y T. Hamalainen, «A Novel Model for Cybersecurity Economics and Analysis», en 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland: IEEE, ago. 2017, pp. 274-279. doi: 10.1109/CIT.2017.65.

[10] Sophos Whitepaper. «*The State of Ransomware in Critical Infrastructure*» *2024*. https://assets.sophos.com/X24WTUEQ/at/75tnw38cqsnrrv56wpwc78k/sophos-state-of-ransomware-critical-infrastructure-2024.pdf