Protection Management Systems to Optimize Operative and Maintenance Processes in Electricity Sector Companies

Herramientas de Gestión de Protecciones para Optimizar Procesos Operativos y de Mantenimiento en Empresas del Sector Eléctrico

DOI: http://dx.doi.org/10.17981/ingecuc.20.2.2024.03

Artículo de Investigación Científica.
Fecha de Recepción: 23/02/2023, Fecha de Aceptación:10/05/2023

Oscar A. Tobar-Rosero
Universidad Nacional de Colombia.
Medellín, Colombia
oatobarr@unal.edu.co

Rodolfo García-Sierra
Enel Colombia
Bogotá, Colombia
rodolfo.garcia@enel.com

Jar Hernán-Vargas
Universidad Nacional de Colombia.
Medellín, Colombia
jhvarga0@unal.edu.co

Germán Darío Zapata-Madrigal
Universidad Nacional de Colombia.
Medellín, Colombia
gdzapata@unal.edu.co

John E. Candelo-Becerra
Universidad Nacional de Colombia.
Medellín, Colombia
jecandelob@unal.edu.co

To cite this paper:
O. Tobar-Rosero; J. Hernán-Vargas; R. García-Sierra; G. Zapata-Madrigal & J. Candelo-Becerra "Protection Management Systems to Optimize Operative and Maintenance Processes in Electricity Sector Companies," INGE CUC, vol. 20, no. 2, 2024. DOI: http://dx.doi.org/10.17981/ingecuc.20.2.2024.03

Abstract
Introduction: Electrical protections have gone from being a security element to becoming a system that has a lot of information and that can be used for functions such as signal recording, control, automation, communications, and others. However, many companies have installed advanced devices that are not being used to their fullest potential, and it may be interesting to exploit these possibilities in the electricity sector.
Objective: This article aims to evaluate the performance of functionality, handling, and cybersecurity in five different protection management systems (PMS).
Methodology: An experimental work is conducted with quantitative analysis evaluating three main categories: cybersecurity, handling, and functionality. In addition, thirteen aspects and five PMSs are compared. The data transmitted in the communication architecture from the electrical protection equipment is captured by a network monitoring software for its respective comparison with the original data validated with the hash technique that verifies its integrity. A comparison between the information that comes out of each intelligent electronic device (IED) with the one that reaches the PMS is performed, evaluating its behavior and data delivery times. Finally, the thirteen aspects are compared, describing their advantages and disadvantages, and achieving a quantitative performance assessment.
Results: The results show a quantitative weighting assigned for cybersecurity at 40%, handling at 30%, and functionality at 30%. PMS 1 obtains an overall performance of 73.1%, PMS 2 of 59.6%, PMS 3 of 59.6%, PMS 4 of 48.8%, and PMS 5 of 24.6%. PMS 4 obtained in cybersecurity a maximum of 90.4%, PMS 3 in handling 74.4%, and PMS 1 in functionality 77.6%. Finally, a risk analysis of the PMSs is conducted based on a qualitative assessment of compatibility, scalability, interoperability, data management, information cybersecurity, and backups. PMS 2 presents a predominantly high risk, PMS 4 reaches a low risk, and the other PMSs obtain a medium risk.
Conclusions: It is concluded that the performance of the IEDs in the evaluated PMSs can occur with different performances and behaviors. Therefore, conducting this type of analysis before business implementations is important. Cybersecurity is a matter of business continuity, so the results obtained in this matter from each PMS should be strongly considered, as is the case of the vulnerability of the TLSv1.0 protocol and the OpenVPN protocol, combined with the vulnerabilities generated using operating systems that require a constant update of the system.

Keywords: Electrical protections, process optimization, Intelligent electronic devices, protection management systems, cybersecurity.

Resumen
Introducción: Las protecciones eléctricas han pasado de ser un elemento de seguridad a convertirse en un sistema que cuenta con mucha información y que puede ser utilizado para funciones como registro de señales, control, automatización, comunicaciones, entre otras. Sin embargo, muchas empresas han instalado dispositivos avanzados que no están siendo aprovechados al máximo y puede ser de interés explotar estas posibilidades en el sector eléctrico.
Objetivo: Este artículo tiene como objetivo evaluar el desempeño de la funcionalidad, manejo y ciberseguridad en cinco diferentes herramientas de gestión de protecciones (HGPs).
Metodología: Se realiza un trabajo experimental con análisis cuantitativo evaluando tres categorías principales como son la ciberseguridad, el manejo y la funcionalidad. Además, se comparan trece aspectos y cinco HGPs. Los datos transmitidos en la arquitectura de comunicación desde los equipos de protección eléctrica son capturados por un software de monitoreo de la red para su respectiva comparación con los datos originales validados con la técnica hash que verifica su integridad. Se realiza una comparación entre la información que sale de cada dispositivo electrónico inteligente (IED) con la que llega a las HGPs, evaluando su comportamiento y tiempos de entrega de datos. Finalmente, se comparan los trece aspectos, describiendo sus ventajas y desventajas y logrando una valoración cuantitativa de su desempeño.
Resultados: Los resultados muestran una ponderación cuantitativa asignada a ciberseguridad 40%, manejo 30% y funcionalidad 30%. La HGP 1 obtiene un rendimiento global del 73,1%; la HGP 2 del 59,6 %, la HGP 3 del 59,6 %, la HGP 4 del 48,8 % y la HGP 5 del 24,6 %. La HGP 4 obtuvo en ciberseguridad un máximo de 90,4%, la HGP 3 en manejo 74,4% y la HGP 1 en funcionalidad 77,6%. Finalmente, se realiza un análisis de riesgo de los HGPs basado en una evaluación cualitativa en aspectos como compatibilidad, escalabilidad, interoperabilidad, gestión de datos, ciberseguridad de la información y respaldos. La HGP 2 presenta un riesgo predominantemente alto, la HGP 4 alcanza un riesgo bajo y las demás HGPs obtienen un riesgo medio.
Conclusiones: Se concluye que la actuación de los IED en las HGPs evaluadas puede darse con diferentes actuaciones y comportamientos. Por lo tanto, es importante realizar este tipo de análisis antes de las implementaciones empresariales. La ciberseguridad es un tema de continuidad del negocio, por lo que los resultados que se obtengan en esta materia de cada HGP, como es el caso de la vulnerabilidad del protocolo TLSv1.0 y del protocolo OpenVPN, combinado con las vulnerabilidades generadas utilizando sistemas operativos que requieren una constante actualización del sistema.

Palabras clave: Protecciones eléctricas, optimización de procesos, dispositivos electrónicos inteligentes, herramientas de gestión de protecciones, ciberseguridad.

I. INTRODUCTION

In the context of digital transformation that starts from a renewal and technological adoption for the electricity sector, it is essential to identify strengths and weaknesses in the process. This identification supports management changes in electricity sector companies and engineering groups [1]. In this sense, a key element in adopting technology is establishing its characteristics and attributes, optimizing the use of infrastructure resources, and optimizing the operation and maintenance processes at the companies. At last, these changes impact costs, but complement quality and security indicators in service supply, without neglecting the stability and reliability of the operating system [2], [3].

A transformation of the essential equipment that helps to maintain the power system safe, such as electrical protection, has occurred in recent years [4]. These elements have gone from being only protection systems to becoming intelligent electronic devices (IEDs) [5][6]. These new devices integrate information and communication technologies (ICTs) for management processes, parameterization and integration with other systems, communication protocols and standards or application profiles, advanced algorithms with multiple simultaneous protection functions in a single device, systems registration and control of events at the substation level, and other operational characteristics [7][8].

However, there are also relevant factors such as interoperability and protection performance [4]. Therefore, to get the most out of the attributes in IEDs, it is necessary to identify complements and applications that derive improvements for the integration and operation of the system [8]. This is where a protection management system (PMS) comes into play, seeking to take advantage of IED improvements to provide greater added value to system end users [6]. For example, a PMS can develop activities like managing settings and records in the IEDs based on communication protocols. It could also continuously monitor the operation of the devices, manage accessibility, record changes in the equipment, and establish computer security protocols, and other applications [9].

Similarly, applications could focus on wide-area protection schemes and adaptive protection algorithms currently being studied worldwide [10]. One advantage is that it helps significantly reduce unexpected element outages, small contingencies, and unscheduled events presented in the network [11][12][13]. The difference factor in this process lies in the ability to access the different devices, regardless of the manufacturer or equipment reference. This allows engineering staff to improve the analysis and evaluation of the behavior of the system [7]. In addition, it also allows the possibility of developing a behavior profile to predict unusual actions or unexpected events, which can ultimately be considered in the development of adaptive algorithms for the system [14][15] [16].

In the electrical sector, and particularly for the companies operating the system and public service providers, it is of great importance to have adequate supervision and control of their assets, having as a main reference the protection, control, and measurement equipment in the system [16][17]. Therefore, there is a range of PMSs on the market, with characteristics and attributes that could benefit companies as end users [7][18]. However, given the variety of tools, the continuous commercial offer of the suppliers, and the operational characteristics of each company, it is important that the evaluation and selection process of this type of system is performed objectively and with the appropriate technical support.

Figure 1 shows the diagram of the general communication architecture used to analyze the different PMSs in the electricity market. The basic architecture is proposed to quantify the performance of the PMSs, taking as reference three main categories considered in this study: cybersecurity, handling, and functionality. The results and the analysis process help identify the potential benefits companies can obtain from implementing this technological solution.

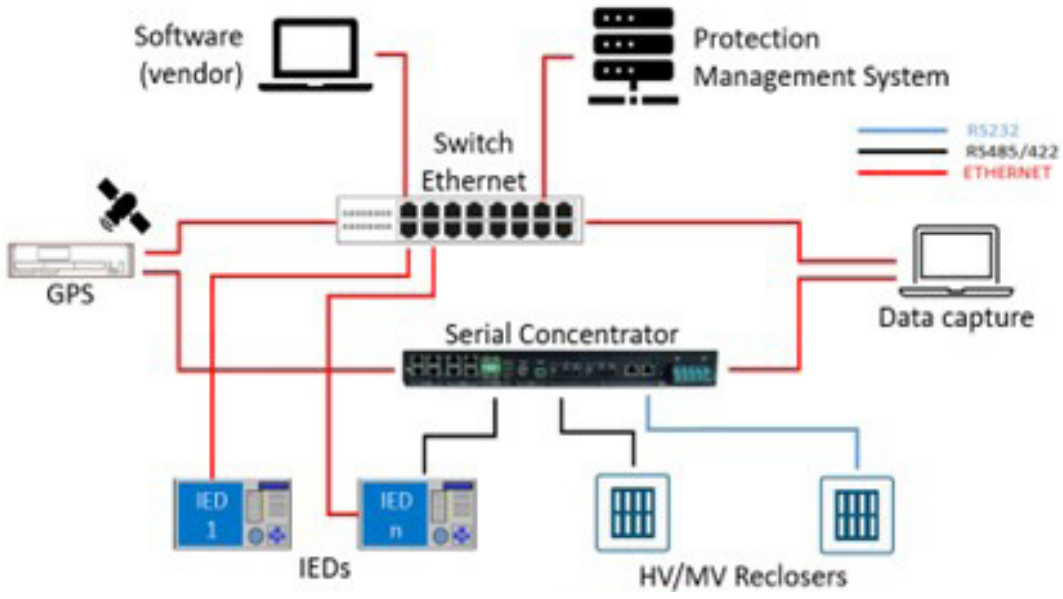

Fig. 1 General communication architecture.
Source: the authors.

II. LITERATURE REVIEW

Over the years, the need for reliable communication systems has become a mandatory premise when designing protection and control systems [17]. Here, communication is an important element for wide-area protection, control, power management, and monitoring [11].

The concept of centralized protection and control emerges as an alternative linked to the optimization of resources and improvement of reliability in the electrical system. It goes back almost to the beginning of the adoption of computers for companies, evidencing a first proposal published in 1969, and the first installation as a field test in 1971 [15][19]. The first experimental systems focused on computer broadcasting, which was limited by the technology available at the time. Projects in the late 1980s and early 1990s began to specifically experiment with centralized protection and control [11][20].

Modern communication technologies, including the Internet, are used for remote monitoring, configuration, and load and fault data recovery. Multifunctional and communicative intelligent units have replaced traditional mechanical and static instruments [21]. The next step in the automation of these systems towards fully integrated substations requires the possibility of exchanging information from all power devices towards a management system, initially finding some limitations for the integration of technologies [14][22].

However, scalability and flexibility issues are not exclusive to hardware [23]. The software must be able to support the same features. The software has its form of modularity based on functionality including [15][22]: protection elements, programmable logic, metering, data capture and event storage, processing digital signals, human-machine interface (HMI), and communications. Utility companies have identified the advantages of these new products, and today an increasing number of these systems are installed in substations [24]. However, to make full use of this new technology, a means is needed locally to collect and organize the data produced by these new products in the substations [15][20].

In the past, most were manual instruments or electric meters used to adjust and calibrate electrical protection devices. However, these conventional tools had some limitations, such as the lack of monitoring capability and the need for manual testing in the field [15][19]. Later, protection relays began to incorporate microprocessors, which allowed a greater degree of intelligence and functionality. Configuration and monitoring tools for these relays started to use more sophisticated graphical user interfaces and programming languages [8].

In the 1990s, PMSs began to be integrated into substation automation systems [5][25]. In addition to coordinating protections, these systems could monitor the status of the equipment and generate alarms in case of faults. Nowadays, with the technologies of network communication, it has become possible to integrate protection relays into a control and monitoring network [26]. Consequently, PMS began to incorporate network communication capabilities to allow remote monitoring and real-time management of electrical protections [11][14].

These systems provide a centralized platform for configuring, monitoring, and analyzing electrical protections [27][17]. In addition, they allow the integration of multiple electrical protection devices and provide a single and complete view of the electrical protection status [6]. Some PMSs offer event analysis capabilities and diagnostic tools to help identify electrical protection issues [16].

PMS are tools for managing protection functions in complex electrical systems, such as high-voltage transmission and distribution networks. These systems aim to guarantee the stability, safety, and reliability of electrical systems [14][15]. The PMSs are made up of hardware and software that allow the supervision and management of the protection of equipment and power lines, as well as the recording and analysis of protection events. Some of the most common features of PMS are:

- Monitoring of protections: they can monitor equipment and line protections in real time. If a fault or unexpected event is detected, the system activates the corresponding protection to prevent damage to the equipment and electrical system.
- Event logging and analysis: record all protection events, including faults, alarms, and protection operations. The logs can be further analyzed to identify faults patterns and improve protection system performance.
- Integration with other systems: they can integrate with other systems of the electrical network, such as SCADA and EMS systems, which allows better coordination between the systems and a faster response in case of faults or unexpected events.
- Fault diagnosis: they allow the diagnosis of faults in the protection system and electrical equipment. This optimizes processes for early detection of faults and a rapid solution of issues.
- Configuration and maintenance: they allow the configuration and maintenance of the protection relays, speeding up the configuration processes of the protection parameters. Thus, this is a quick solution to protection relay failures.

The evolution of PMS has been remarkable in recent years. Significant advances have been made in terms of functionality, usability, and integration capacity [28]. However, one of the main difficulties presented by PMSs lies in interoperability with different brands [26], [29]. Currently, there are many vendors, which require specific software and make the information downloading process slow [26].

Consequently, personnel have been affected by repetitive tasks susceptible to human failure. These activities consume critical time that can be used to restore the electrical system after faults [17]. The rapid and effective recovery of different types of information stored in this equipment is vital, such as oscillographs, event signals, information on the operation of the protections, and others [30][31]. Therefore, the use of software that supports multi-manufacturer drivers is required. In addition to communicating with equipment of different brands, this software must allow other functionalities for the operation [32]. One of the main functionalities is the download of the different registry and configuration files. In addition, supervision and monitoring functionalities are required.

For the present study, some necessary basic functionalities that must be present in PMSs were defined, and then fundamental operation characteristics, integration, and performance were evaluated.

III. METHODOLOGY

For the development of this study, multiple attributes found in a PMS are considered. These attributes can positively impact the operating processes conducted by electricity companies. Based on the wide range of technological solutions for protection management available in the market, an analysis is performed with the participation of some providers in the sector. The following thirteen aspects are key factors in comparing and evaluating the five PMSs.

1. Multivendor driver compatibility.
2. Download records, event history, fault records (disturbances), or settings and logics.
3. Multiuser platform.
4. Automatic monitoring of the network using a georeferenced map.
5. Administration, availability, and accessibility of backups.
6. Configuration of downloads (Manual, automatic, scheduled).

7. Downloads of fault events.
8. Real-time measurements.
9. Cybersecurity (Password management, communication encryption, profile management).
10. Availability of equipment.
11. Module for equipment configuration and administration.
12. Parameterization of the system. Supports different configurations of substations and equipment (available ports, download type, download parameterization by protocol, download parameterization by software control).
13. User Availability.

Some architectures that integrate different protection devices and PMSs are proposed for this process. The network monitoring software captures the data transmitted in the communication architecture from the protection equipment or IED. The data measured in the test is then compared with the original data validated with the hash technique that checks its integrity.

The protection equipment and reclosers that are part of the architecture are listed in Table 1. In addition, the table presents the software and the communication protocol that operates the equipment. The tools under study have a particular communication architecture that considers properties and characteristics. Therefore, a computer with traffic capture software is connected as a mirror port in the main communication node to study network traffic in each test.

TABLE 1
EQUIPMENT USED FOR THE COMMUNICATION ARCHITECTURE.

Brand	Model	Protocol	Software
ABB	REC670	IEC 61850	PCM 600
AREVA	MICOM P139	COURIER	Easergy Studio V7
AREVA	MICOM P143	COURIER	Easergy Studio V7
INGETEAM	ARTECHE PD250	PROCOME	INGESYS SIPCON CONSOLE
SCHNEIDER	NU-LEC	DNP3	WSOS
SEL	2032	SEL FAST	QUICK AcSELerator
SEL	311C	SEL FAST	QUICK AcSELerator
SEL	387-E	SEL FAST	QUICK AcSELerator
SEL	421	SEL FAST	QUICK AcSELerator
SIEMENS	SIPROTEC 4 - 7SJ63	IEC 103	DIGSI 4
SIEMENS	SIPROTEC 5 - 7SJ85	IEC 61850	DIGSI 5
ZIV	8ZLV-F3F	IEC 61850	ZIVERCOMPLUS
NOJA	RC01	DNP3	TELUS
Ruggedcom	RS416NC	TELNET	PUTTY

For the presentation of results, equipment is selected randomly for the test and named “Reference #”. This is performed to avoid misinterpretations of the results and only focus on complying with the main objective of this process.

Data that reaches IED is compared with that in the PMS, evaluating behavior and the data delivery times. Finally, the aspects previously defined between PMSs are compared, detailing their advantages and disadvantages, achieving a quantitative assessment of their performance. It is important to highlight that the provider of each PMS implements its communication architecture, taking responsibility for the connectivity of the IEDs available for the tests supplied by the utility-type company of the Colombian electricity sector.

PMSs work in different ways, as they consider distinct management times, operations, and responses. The main differences can be found in communications and the operation of the protection systems. Therefore, the tests considered the independence, impartiality, and confidentiality criteria defined in the Automation and Industrial Communications Laboratory (Universidad Nacional de Colombia, Sede Medellín). The National Accreditation Body of Colombia (ONAC) accredited the laboratory under the ISO/IEC 17025:2017 standard for communication tests focused on digital electrical substations and critical infrastructure. Table 2 shows the main metrics and assigned ratings for the categories defined, such as

cybersecurity, handling, and functionality. As sometimes cybersecurity does not apply to all tests, a different assessment is given, as shown in the same table.

TABLE 2
MAIN WEIGHTING METRICS

	Metrics		
Scenario	Cybersecurity	Handling	Functionality
No cybersecurity	N/A	40%	60%
With cybersecurity	40%	30%	30%

Cybersecurity considers three factors that are defined as follows: availability, integrity, and confidentiality. Table 3 shows the metrics used to evaluate these three factors.

TABLE 3
CYBERSECURITY METRICS

Cybersecurity		
Availability	Integrity	Confidentiality
33.3%	33.3%	33.3%

Table 4 presents the metrics for handling the PMS. The evaluation is centered on reviewing the ease of use and the learning curve necessary to operate it. As these are subjective attributes, the average of the evaluation performed by the laboratory analysts that conducted the tests is considered.

TABLE 4
HANDLING METRICS

Handling	
Ease of use	Learning Curve
50%	50%

Finally, Table 5 presents the functionality metrics to evaluate the performance and the added value of the PMS. This evaluation can facilitate the analysis of the information on the electrical systems.

TABLE 5
FUNCTIONALITY METRICS

Functionality	
Performance	Added Value
50%	50%

Finally, a qualitative risk analysis considers the probability of a risk, impact, and consequence when it becomes a real event. Table 6 shows the high, medium, or low rating assigned after evaluating each PMS and the final assessment specified as the predominant risk.

TABLE 6
RISK ANALYSIS

Risk	Consequence	Rating
1	1	High - Medium - Low
n	n	High - Medium - Low
Predominant risk		High - Medium - Low

A. Case study

The twelve tests to be conducted are based on the architecture provided by each of the PMSs. Therefore, different architectures are used to perform evaluations of PMSs.

Figure 2 shows the architecture of PMS 1, which uses an automatic backup system (network attached storage – NAS), a Linux-based server, and a Windows-based client.

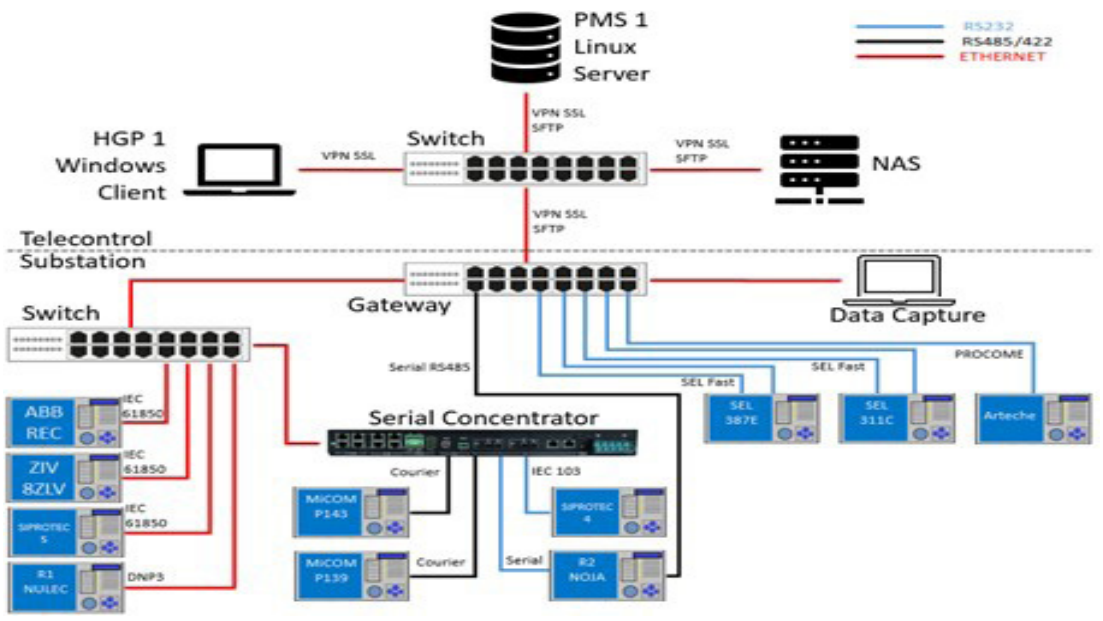

Fig. 2 Architecture of the PMS 1

Figure 3 shows the architecture of PMS 2, which unlike PMS 1 does not have the Arteche IED connected, and the NOJA Recloser does not have a double connection due to the characteristics of the system. Additionally, it lacks an exclusive NAS server, so the server is used for this functionality.

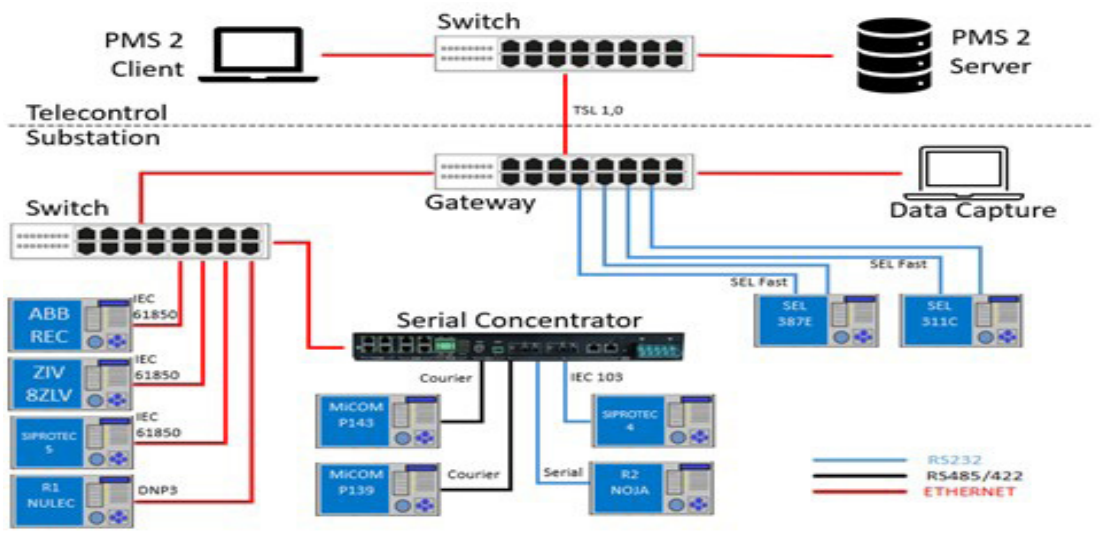

Fig. 3 Architecture of the PMS 2

Figure 4 shows the architecture of PMS 3, exposing the higher complexity of using a server farm and a client-facing firewall. In addition, it changes the Gateway for a computer called the substation server, which also increases the complexity mentioned above.

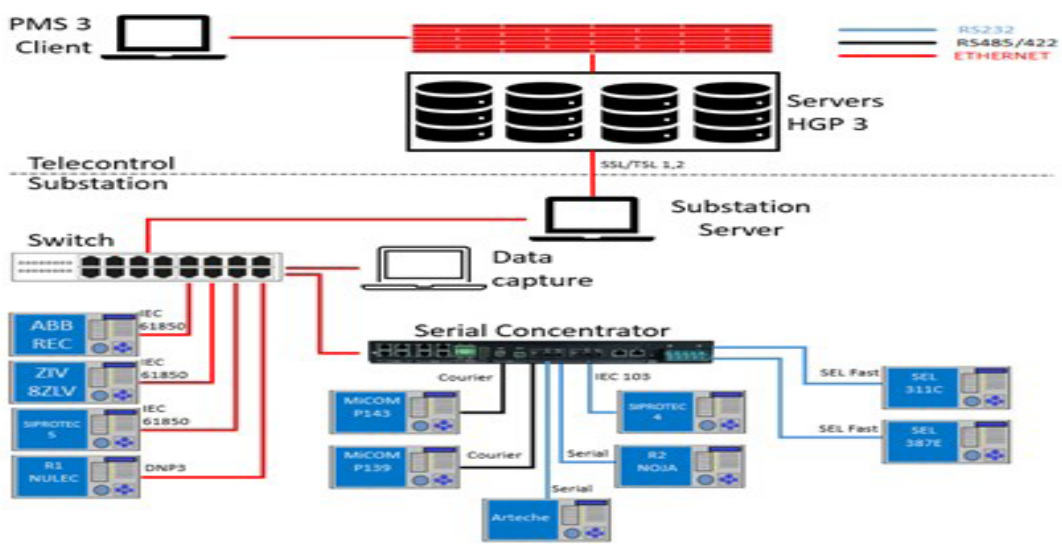

Fig. 4 Architecture of the PMS 3

Figure 5 shows the architecture of PMS 4, which uses IEDs and a firewall that communicates with the Server.

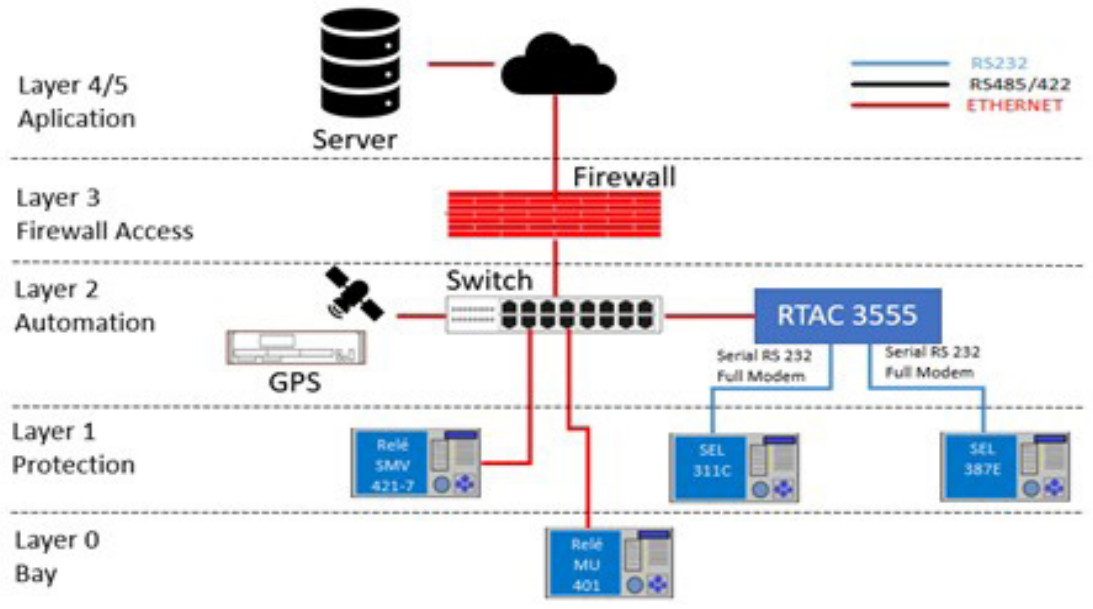

Fig. 5 Architecture of the PMS 4

Finally, Figure 6 shows the architecture of PMS 5, which eliminates most IEDs leaving only four of the inventoried. Additionally, this architecture considers that the IEDs communicate directly with the PMS 5 through the serial port.

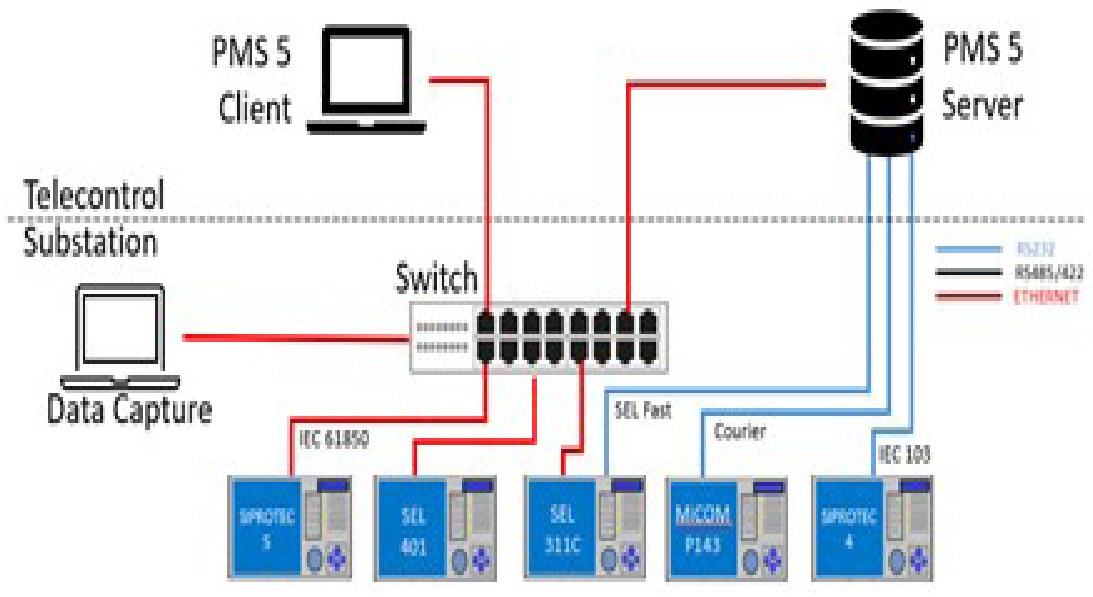

Fig. 6 Architecture of the PMS 6

IV. RESULTS

This section presents the results of evaluating five PMSs on thirteen aspects defined in section 3 (methodology). Each protection reference is evaluated according to the architectures defined in section 3. In addition, the average of the evaluation is displayed to identify the behavior of the different protections. Finally, a summary of the results is presented, showing the performance of each PMS according to the various aspects.

A. Multivendor driver compatibility

This test seeks that the eleven devices listed in Table 1 can be read by each PMS with its architecture and the manufacturer's communication protocol. In addition, it is required to read basic information such as the sequence of events (SoE). Table 7 shows the results of multivendor driver compatibility of each computer with PMS. In addition, the average of all protections is calculated for each PMS.

TABLE 7
MULTIVENDOR DRIVER COMPATIBILITY

Reference	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
1	100%	0%	0%	100%	100%
2	33.3%	100%	100%	100%	0%
3	66.6%	66.6%	66.6%	0%	100%
4	66.6%	66.6%	0%	0%	100%
5	100%	0%	0%	0%	0%
6	83.3%	100%	0%	0%	100%
7	100%	33.3%	0%	0%	0%
8	100%	0%	0%	0%	0%
9	100%	0%	33.3%	0%	0%
10	0%	50%	0%	0%	0%
11	0%	50%	0%	0%	0%
Average	68.2%	42.4%	18.2%	18.2%	36.4%

B. File download

File download is evaluated according to the equipment installed at each voltage level. The first set of the equipment is related to HV-MV (high voltage - medium voltage), and the second set of equipment is related to MV-MV (medium voltage - medium voltage). At the HV-MV level, there are IEDs, and at the MV-MV level, there are reclosers. Table 8 shows the performance in downloading IED files from each PMS, composed internally of the download of the event history, the event logs, and the settings and logics. Additionally, the average performance of each PMS is presented by combining the nine IED equipment.

TABLE 8
FILE DOWNLOAD OF THE HV-MV LEVEL

Reference	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
1	0%	0%	0%	0%	0%
2	100%	100%	100%	100%	66.6%
3	33.3%	66.6%	66.6%	100%	0%
4	66.6%	66.6%	0%	0%	66.6%
5	66.6%	0%	0%	0%	100%
6	100%	100%	0%	0%	0%
7	83.3%	33.3%	0%	0%	33.3%
8	0%	0%	0%	0%	0%
9	100%	0%	33.3%	0%	0%
Average	68.2%	40.7%	22.2%	22.2%	29.6%

Regarding the performance of each PMS with each of the two reclosers, Table 9 presents the average of each tool, considering that only two of these could manage them totally or partially.

TABLE 9
FILE DOWNLOAD OF THE MV-MV LEVEL

Reference	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
10	100%	50%	0%	0%	0%
11	100%	50%	0%	0%	0%
Average	100%	50%	0%	0%	0%

C. Multiuser platform

Table 10 shows the performance obtained from the different PMSs with respect to the multiuser platform. In general, they all have a high value, creating several different types of users and roles that determine what they can see and edit and what computers or systems they can access. The main changes are related to the type of licensing to add users and the number of these that can access simultaneously, for example, PMS 3.

TABLE 10
MULTIUSER PLATFORM

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	100%	100%	100%	100%	100%
Handling	82.5%	100%	100%	90%	100%
Functionality	90%	100%	100%	100%	100%
Weighting	90.8%	100%	100%	97%	100%

D. Georeferenced map

Table 11 shows the behavior of the PMS with respect to the use of a georeferenced map. The test considered the location of the electrical substation and the IED equipment or reclosers. In addition, the test considered the communication status of the equipment identified by colors. Only PMS 1 and PMS 3 have the option of a georeferenced map. PMS 1 uses Google Maps for the location of the device, while PMS 3 uses Bing Maps with a color variation in the communication status indicator. However, they do not display detailed information about the equipment inside the substation.

TABLE 11
GEOREFERENCED MAP

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	100%	0%	100%	0%	0%
Handling	80%	0%	100%	0%	0%
Functionality	80%	0%	60%	0%	0%
Weighting	88%	0%	88%	0%	0%

E. Backup Management, Availability, and Accessibility

Table 12 shows the performance of cybersecurity in each of the PMS. PMSs 1 and 5 obtained values below 100%, as not all the tests were performed due to the lack of configuration of the PMS, preventing evidence of the handling and functionality of this item. PMSs 2, 3, and 5 use a backup in a database encrypted in Microsoft SQL, while PMS 4 has its backup storage system with optimal results.

TABLE 12
BACKUP MANAGEMENT

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	68.3%	100%	100%	100%	100%
Handling	0%	100%	100%	100%	100%
Functionality	0%	100%	100%	100%	18.2%
Weighting	27.3%	100%	100%	100%	75.46%

F. Download settings

Table 13 shows the performance of manual and automatic downloads of the different PMSs. In this case, only handling and functionality are considered in the evaluation. The results show that PMS 4 has optimal performance with compatible equipment. PMS 1 obtains a better performance, mainly due to the automatic reading configuration repeated twice, ensuring that the process is carried out satisfactorily.

TABLE 13
DOWNLOAD SETTINGS

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	NA	NA	NA	NA	NA
Handling	60%	85%	100%	100%	100%
Functionality	100%	70%	20%	100%	18.2%
Weighting	84%	76%	52%	100%	50.9%

G. Download on fault events

Table 14 shows the performance of each PMS in terms of automatic downloads when a fault occurs. The result shows slight compatibility in PMS 1 and total compatibility in PMS 4. The other PMSs showed no activity in this regard.

TABLE 14
DOWNLOAD ON FAULT EVENTS

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	NA	NA	NA	NA	NA
Handling	0%	0%	0%	100%	0%
Functionality	20%	0%	0%	100%	0%
Weighting	12%	0%	0%	100%	0%

H. Real-time measurements

Table 15 shows the performance of the PMSs with respect to the real-time acquisition of measurement records. It should be noted that the cybersecurity metric is not qualified for this item. Once again, the PMS 4 stands as the only one adequate in handling and functionality, but the limitation regarding compatibility with the equipment must be considered. In addition, both PMSs record accuracy in milliseconds when printing the time in measurements; thus, adequate accuracy is guaranteed when compared with the synchronized time of the system.

TABLE 15
REAL-TIME MEASUREMENTS

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	NA	NA	NA	NA	NA
Handling	50%	0%	0%	100%	0%
Functionality	100%	0%	0%	100%	0%
Weighting	80%	0%	0%	100%	0%

I. Cybersecurity

Table 16 shows the performance of the PMSs with respect to cybersecurity. It is important to note that PMS 4 did not obtain any rating due to the dependence on firewall equipment, not considered in the initial architecture. The greatest value obtained for cybersecurity is provided by PMS 3, as its infrastructure consists of segmented networks with servers separated by roles, where users access through credentials administered by Active Directory. In addition, communications are always encrypted with TLS v1.2

TABLE 16
CYBERSECURITY

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	68.3%	50.0%	90.0%	0%	36.4%
Handling	80.0%	100%	100%	0%	80.0%
Functionality	100%	100%	100%	0%	36.4%
Weighting	80.7%	80%	96%	0%	49.5%

PMS 5 registers the lowest performance due to a lack of functionalities compared to other tools, such as password encryption or auditing for user control traceability.

Equipment availability

Table 17 shows that PMS 1 obtains the highest performance in the equipment availability test when the concentrator equipment is disconnected and reconnected. The reconnection time is measured in the test, considering that a manual process to finish starting some computers is required. In PMS 3, manual intervention is required to restore communication. Then, the command console (CLI) is accessed to restart transmission. Therefore, the performance only obtained 28.2%.

TABLE 17

EQUIPMENT AVAILABILITY

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	100%	66%	33%	66%	100%
Handling	80%	100%	50%	100%	100%
Functionality	100%	60%	0%	80%	18.2%
Weighting	94%	74.4%	28.2%	80.4%	75.5%

K. Configuration and administration module

Table 18 shows the performance of the configuration and administration module for each PMS. Here, the required parameterization is reviewed, in addition to their associations with electrical substations, communications status, firmware version, accessibility, and reading records.

TABLE 18

CONFIGURATION AND ADMINISTRATION MODULE

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	100%	80%	100%	100%	100%
Handling	90%	100%	50%	100%	100%
Functionality	80%	90%	50%	80%	33.3%
Weighting	91%	89%	70%	94%	80%

PMSs 1 and 4 showed the best performances, driven primarily by cybersecurity, albeit with differences in handling and functionality. However, PMS 3 reduced the values in the handling and functionality metrics.

I. System parametrization

Table 19 shows the results of the performance of the system parameterization. The test determines which PMS has more communication parameters or what types of downloads and their parameterization allow to be configured.

TABLE 19

SYSTEM PARAMETRIZATION

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	60%	80%	100%	60%	100%
Handling	60%	80%	60%	100%	50%
Functionality	100%	60%	20%	100%	18.2%
Weighting	72%	74%	64%	84%	60.5%

M. User availability

Table 20 shows the results of the performance of the PMS with respect to the user availability test. There is a positive test case where several users enter and work simultaneously in each tool. In addition, there is also the negative test case where a user tries to access two different clients.

TABLE 20

AVAILABILITY OF USERS

Metric	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
Cybersecurity	100%	100%	100%	100%	100%
Handling	80%	90%	100%	75%	50%
Functionality	100%	100%	100%	100%	33.3%
Weighting	94%	97%	100%	92.5%	65%

N. Summary of the results

Table 21 consolidates the performance of each PMS with respect to the thirteen tests. It should be noted that test 2 is divided into five elements ranging from 2.1 to 2.R2 (Recloser 2).

Finally, an average of the performance of each tool is made, and the respective analyzes and conclusions are generated.

TABLE 21
WEIGHTING OF PMSS IN THE THIRTEEN TESTS

#	Description	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
1	Compatibility	68.2%	42.4%	18.2%	18.2%	36.4%
2.1A	File Download (AT-MT)	68.2%	40.7%	22.2%	22.2%	29.6%
2.2B	File Download (AT-MT)	100.0%	50.0%	0.0%	0.0%	0.0%
3	Multi-user platform	90.8%	100%	100%	97.0%	100%
4	Georeferenced Map	88.0%	0.0%	88.0%	0.0%	0.0%
5	Backups management	27.3%	100%	100%	100%	75.5%
6	Download settings	84.0%	76.0%	52.0%	100%	50.9%
7	Downloads of fault events	12.0%	0.0%	0.0%	100%	0.0%
8	Real-time measurements	80.0%	0.0%	0.0%	100%	0%
9	Cybersecurity	80.7%	80.0%	96.0%	0.0%	49.5%
10	Equipment Availability	94.0%	74.4%	28.2%	80.4%	75.5%
11	Configuration Module	91.0%	89.0%	70.0%	94%	80.0%
12	System Parameterization	72.0%	74.0%	64.0%	84.0%	60.5%
13	User Availability	94.0%	97.0%	100%	92.5%	65%
Average		75%	58.8%	42.8%	63.5%	44.5%

V. ANALYSIS

Each PMS works differently from its conception of kernel programming and is clearly seen in how it is understood with electrical protection equipment. For example, PMS 1 obtains a compatibility of 68.2% with an advantage of 25.8% over the second, and very distant from the last ones that barely reached 18.2%.

Similarly, each PMS has its own way of managing downloads of event history, fault logs, and settings and logics. For example, they must manage an amount of information and the possibility of generating graphs of the fault logs. PMS 1 can manage these processes in both HV-MV and MV-MV, and processing fault currents from reclosers.

Regarding the ability for multiple users to work simultaneously, PMSs use different types of databases. The predominant database is SQL, which implies a licensing issue for each user who wants to connect to the system, incurring higher costs that must be considered in the financial analysis.

As for the georeferenced map, it is notable that the maturity of most PMSs does not contemplate this option. The PMSs with this option must still improve functionality, where detailed information on substations and protective equipment should be accessible.

In the administration of backups, the extensive use of Microsoft SQL software and its encryption methods is noted. It should be noted that PMS 1 is the only one that uses a dedicated NAS (Network Attached Storage) server connected by VPN. However, the other tools allow you to redirect the location of the database backups.

In the download configuration test, PMS 1 obtained the best performance due to its high parameterization capacity in both manual and automatic, favoring the repetition of requests to ensure data acquisition. It should be noted that PMSs 4 and 5 require additional licensing for automatic readings, limiting the execution of the tests and preventing evidence of better behavior.

Now, at the time of fault occurrence, the PMS automatically downloads the event, which implies that the PMS is always in active mode; for example, PMS 4. It should be noted that the IEC61850 and SEL Fast protocols can generate automatic download, while the Courier, IEC 103, and PROCOME protocols download programmatically (Polling). The minimum time changes according to the protocol and can be in milliseconds.

In the real-time measurements test, PMS 1 is compatible with most multi-brand equipment, while PMS 4 is only with one. Thus, both tools obtain data with high precision in synchronization but differ in how to parameterize the data collection. PMS 1 has more parameters to configure than PMS 4, as the last one requires practically no configurations.

In the cybersecurity test, the TLS encryption protocol is detailed. Although PMS 2 uses version 1, which presents a high vulnerability according to CVE (Common Vulnerabilities and Exposures), the score was 10/10. Therefore, the rating of the cybersecurity metric is 50%. It should be noted that the use of TLSv1.2 and TLSv1.3 is suggested for client-server information exchanges. On the other hand, PMS 1 reduces its cybersecurity score because it does not have encryption in the client-server channel, that is, downstream of the communication architecture.

The equipment availability test shows that there is generally a good performance from the different PMSs, which is significantly higher for PMS 1. PMS does not block when one and more pieces of equipment disconnect. When nine pieces of equipment were disconnected, the automatic reset time was 2 minutes, except for one that required manual help.

As for the equipment configuration and management module, it is observed that there is generally a good performance from all the PMSs. PMS 4 has the best performance mainly for its easy and intuitive graphic environment that facilitates the tool operator's work, although PMS 1 is close, especially for its high configuration level.

Reviewing the capacity of parameterization of the system, PMS 4 offers the best performance since a greater amount of detail can be reached in the parameterization of the communication through Serial, Network, and Modem. Contrary to PMS 5, which has factory limitations such as a remote configuration restriction that prevents extracting information and records from IEDs.

Regarding the user availability test, it is observed that the performance is greater than 90%, highlighting the PMS 3 that achieved a correct behavior in the three metrics, allowing multiple simultaneous connections of different users and preventing multiple connections of the same user. Again, PMS 5 presents a lower value than the others, mainly due to the lack of licenses to add more users.

In summary, the weighting per test is reviewed, showing the PMSs that obtain the highest performance for each test and the consolidated performance. The results show a clear advantage of PMS 1 over the second with a difference of 13.5% and 30% with the fifth. Notably, PMS 1 wins in the tests that require compatibility with the largest number of equipment while the other PMSs share the other functionalities.

Table 22 shows a comparison of the metrics used to evaluate each PMS. Finally, the average of the metrics is calculated.

TABLE 22
FINAL WEIGHTING

Tool	Average Metrics			Total
	Cybersecurity	Handling	Functionality	
PMS 1	86.9%	62.2%	77.6%	73.1%
PMS 2	72.0%	68.5%	55.5%	59.6%
PMS 3	90.4%	56.5%	37.4%	48.8%
PMS 4	65.8%	74.4%	51.1%	59.6%
PMS 5	79.6%	47.4%	23.6%	40.1%
Average	78.9%	61.8%	49.0%	56.2%

Based on the above results, PMS 1 obtains an overall performance of 73.1%, PMS 2 of 59.6%, PMS 3 of 48.8%, PMS 4 of 59.6%, and PMS 5 of 43.1%. Cybersecurity obtains a maximum of 90.4% in PMS 3, management 74.4% in PMS 4, and functionality 77.6% in PMS 1. Hence, all PMSs present a lower performance in functionality, requiring improving technology in this aspect.

Finally, Table 23 shows a risk analysis of the PMSs related to compatibility, scalability, interoperability, data management, information cybersecurity, and backups. The table presents a qualitative assessment rated by three concepts: low, high, and medium.

TABLE 23

RISK MATRIX

Risk	Consequences	PMS 1	PMS 2	PMS 3	PMS 4	PMS 5
The system supports new equipment/ protocols/software.	The system does not adapt to new acquisitions, improvements, and changes that occur in the infrastructure.	Medium	Medium	Medium	Medium	Medium
The system partially supports the equipment in the current infrastructure.	The system does not or partially manage certain equipment, leaving a gap in infrastructure manageability that may result in the acquisition of another platform that complements it.	High	High	High	High	Medium
The system requires human intervention to complete information downloads.	By requiring human intervention, the system loses efficiency, speed, and reliability in data acquisition.	Low	High	Medium	Low	Low
The system blocks communications with some equipment, preventing its manual handling.	By blocking communications, partial or total management of some equipment is missed, and thus, the tasks that depend on them are hindered.	Low	High	Low	Low	Low
The system requires modifying the current infrastructure.	Additional costs are required when purchasing, changing, or improving some equipment in the current infrastructure.	Medium	High	Medium	Medium	Medium
The system uses the communication infrastructure efficiently, occupying the channels only when necessary.	The system uses the channels constantly, making manual communications difficult.	Medium	Medium	Medium	Low	Medium
The system compresses the information obtained from the equipment.	The system grows disproportionately, making inefficient use of the infrastructure and decreasing performance.	High	High	High	High	Low
The system protects communications and parameters to keep them safe.	The information is exposed and vulnerable to being hacked.	Medium	Low	Medium	Medium	High
The system protects backups to keep them safe.	The possibility of performing an emergency backup is missed and may affect the correct operability.	Low	Low	Low	Low	Low
Predominant risk of PMS		Medium	High	Medium	Low	Medium

The PMS 2 presents a high-risk level because of the shortcomings in the compatibility of equipment, high human intervention for some processes, such as the blocking of communications with some equipment, and the inefficient use of the communication infrastructure. PMS 4 reaches a low-risk level, and the others a medium-risk level.

VI. CONCLUSIONS

It is concluded that the performance of the evaluated PMSs can occur with different performances and behaviors. Hence, it is important to conduct this type of analysis prior to operational implementation. It is important to note that four of the bidders require the use of Windows Server in their architecture, and only PMS 4 used an industrial computer, which may influence the response times of the tool to the different processes when operating in a company of the electricity sector. It was evidenced that PMS 3 is a very robust solution with a very specific functionality that goes into detail in the configuration of the equipment and its own software. This could become an advantage in the possibilities of connecting equipment of various brands, but in the specific case of the tests, it played a role against it, as being so parameterizable, it makes its configuration very complex and requires more implementation time. PMS 1 was the only one to use a Linux server, with which it performs user authentication tasks. The other tools are based on the Windows Active Directory (DA), being PMS 3 the one that uses them natively through SharePoint, determining greater control over the groups and users of the system.

The network and/or serial concentrator used in the PMS 1 is the only equipment that works as the first line of storage of events and faults in the protection relays; as a second option, it has the Linux server. The other tools require the use of a server, which can be the same one where they have the software, or another, such as a NAS, which is reflected in the performance of each PMS. In today's world, cybersecurity is a matter of business continuity, so the results obtained in this matter from each PMS should be strongly considered, as is the case of the vulnerability of the TLSv1.0 protocol and the protocol OpenVPN. This, combined with the vulnerabilities generated using Windows, requires a constant update of the system. An example of this is that all software is adapted to the NERC-CIP standard at different levels; however, PMS 3 proved to have the highest compliance with it by having it fully immersed in its code. It was observed that PMS 3 proposes a very robust solution composed of four servers and a network and/or serial hub, which most likely requires more time to implement. The other bidders offer the implementation of a server and a network and/or serial concentrator equipment with a simpler implementation that requires less start-up time. PMS 1 is the one that best meets the requirements established for protection management tests based on the importance of equipment compatibility, as this functionality takes the value of all the benefits of the system. Finally, if you want to have more subjective results, according to the needs of each company, it is necessary to complement what is exposed in this testing process with complementary studies that consider technical and operational aspects, to make strategic decisions and obtain a comprehensive solution tailored to business requirements.

CRediT AUTHORSHIP CONTRIBUTION STATEMENT

O. Tobar-Rosero: Conceptualization, Methodology, Investigation, Writing – Original Draft, Writing – Review and Editing.

J. Hernán-Vargas: Conceptualization, Methodology, Investigation.

R. García-Sierra: Conceptualization, Funding Acquisition, Supervision.

G. Zapata-Madrigal: Conceptualization, Resources, Funding Acquisition, Supervision.

J. Candelo-Becerra: Investigation, Visualization, Writing – Review and Editing, Formal Analysis

FUNDING

This research paper is derived from the project titled "Evaluation of Protection Management Systems for a Pilot of CODENSA". Project financed by Enel Colombia from 2019 to 2020.

ACKNOWLEDGEMENT

The authors thank Enel Colombia for the support and trust in the Industrial Automation and Communications Laboratory of the Universidad Nacional de Colombia - Sede Medellín,

and for providing resources for the project. Similarly, the authors thank the Universidad Nacional de Colombia, Sede Medellín, for allowing the use of the laboratory infrastructure and scientific personnel for the research. Special thanks to companies that provided all the technologies and devices for the test, technical support, and tools to develop the study.

REFERENCES

[1] R. J. Van Wykdirector, "Technology: The forgotten science," IEEE Engineering Management Review, vol. 44, no. 3, pp. 28–31, Sep. 2016, doi: 10.1109/EMR.2016.2595179.

[2] M. Yuldasheva and E. Karimova, "Factors of Information Technologies in Intercultural Integration Process," International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2019, Nov. 2019, doi: 10.1109/ICISCT47635.2019.9011951.

[3] Comisión Económica para América Latina y el Caribe - CEPAL Naciones Unidas, "Tecnologías Digitales para un Nuevo Futuro," Santiago, 2021. Accessed: Apr. 10, 2023. [Online]. Available: https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf

[4] O. A. Tobar-Rosero, J. E. Candelo-Becerra, and G. Zapata, "Performance Analysis of Overcurrent Protection in a Digital Substation with Process Bus," Sustainability 2022, Vol. 14, Page 7958, vol. 14, no. 13, p. 7958, Jun. 2022, doi: 10.3390/SU14137958.

[5] J. C. Fong and M. M. Cameron, "Integration of substation protection, control and data acquisition systems," IEEE Conference Record of Annual Pulp and Paper Industry Technical Conference, pp. 171–175, 1996, doi: 10.1109/PAPCON.1996.535995.

[6] R. Wójtowicz, R. Kowalik, and D. D. Rasolomampionona, "Next generation of power system protection automation-Virtualization of protection systems," IEEE Transactions on Power Delivery, vol. 33, no. 4, pp. 2002–2010, Aug. 2018, doi: 10.1109/TPWRD.2017.2786339.

[7] "Looking into the Future Protection, Automation, and Control Systems." https://resourcecenter.ieee-pes.org/publications/technical-reports/PESTR0055.html (accessed Feb. 21, 2023).

[8] A. Kubis et al., "Validation of ICT-based protection and control applications in electric power systems," 2015 IEEE Eindhoven PowerTech, PowerTech 2015, Aug. 2015, doi: 10.1109/PTC.2015.7232644.

[9] "(PDF) Artificial Intelligent Application to Power System Protection." https://www.researchgate.net/publication/2461541_Artificial_Intelligent_Application_to_Power_System_Protection (accessed Feb. 21, 2023).

[10] R. Moxley and F. Becker, "Adaptive protection - What does it mean and what can it do?," 71st Annual Conference for Protective Relay Engineers, CPRE 2018, vol. 2018-January, pp. 1–4, Apr. 2018, doi: 10.1109/CPRE.2018.8349769.

[11] R. Das et al., "Advancements in Centralized Protection and Control Within a Substation," IEEE Transactions on Power Delivery, vol. 31, no. 4, pp. 1945–1952, Aug. 2016, doi: 10.1109/TPWRD.2016.2528958.

[12] "Advancements in Centralized Protection and Control Within a Substation | IEEE Journals & Magazine | IEEE Xplore." https://ieeexplore.ieee.org/document/7414482 (accessed Feb. 22, 2023).

[13] J. A. Montoya-Arias, O. A. Tobar-Rosero, G. D. Zapata-Madrigal, and R. García-Sierra, "Algoritmo adaptativo para protecciones de sobrecorriente en el caso de estudio IEEE9," TecnoLógicas, vol. 22, no. 45, pp. 45–58, May 2019, doi: 10.22430/22565337.1335.

[14] I. De Mesmaeker, "Trends in protection and substation automation systems and feedbacks from CIGRE activities," IET Conference Publications, no. 536 CP, pp. 1–8, 2008, doi: 10.1049/CP:20080001.

[15] Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi, and F. Q. Zhou, "Developments of power system protection and control," Protection and Control of Modern Power Systems 2016 1:1, vol. 1, no. 1, pp. 1–8, Jun. 2016, doi: 10.1186/S41601-016-0012-2.

[16] J. Gejo-García, S. Gallego-García, and M. García-García, "Project Design and Management of Optimized Self-Protection Plans: A Case Study for Spanish Public Buildings," Applied Sciences 2022, Vol. 12, Page 4401, vol. 12, no. 9, p. 4401, Apr. 2022, doi: 10.3390/APP12094401.

[17] I. P. De Siqueira, "Estimating the impact of wide-area protection systems on power system performance and reliability," IET Conference Publications, vol. 2016, no. CP671, 2016, doi: 10.1049/CP.2016.0073.

[18] Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi, and F. Q. Zhou, "Developments of power system protection and control," Protection and Control of Modern Power Systems, vol. 1, no. 1, Dec. 2016, doi: 10.1186/S41601-016-0012-2.

[19] Y. G. Paithankar and S. R. Bhide, "FUNDAMENTALS OF POWER SYSTEM PROTECTION".

[20] M. Adamiak et al., "2015-December WG K15 Report-Centralized Substation Protection and Control i Centralized Substation Protection and Control IEEE PES Power System Relaying Committee Members," 2015.

[21] "Management experiences from digital relay information and its treatment in the Protection Analysis Center | IET Conference Publication | IEEE Xplore." https://ieeexplore.ieee.org/document/224567 (accessed Apr. 28, 2023).

[22] A. Thompson, J. De, L. Reelopez, V. A. Centeno, and R. P. Broadwater, "The Future of Substations: Centralized Protection and Control," 2016.

[23] M. Śliwiński and E. Piesik, "Designing Control and Protection Systems with Regard to Integrated Functional Safety and Cybersecurity Aspects," Energies 2021, Vol. 14, Page 2227, vol. 14, no. 8, p. 2227, Apr. 2021, doi: 10.3390/EN14082227.

[24] J. D. McDonald, Electric Power Substations Engineering, McDonald, John D., vol. Third Edition. 2011.

[25] "Power System Protection – Past, Present Future | GLOMACS Training & Consultancy." https://glomacs.com/articles/power-system-protection-past-present-future (accessed Feb. 22, 2023).

[26] R. N. Meira, R. L. A. Pereira, J. P. Nascimento, N. S. D. Brito, H. Silva, and B. A. Souza, "Analysis of interoperability of relays via teleprotection," SBSE 2018 - 7th Brazilian Electrical Systems Symposium, pp. 1–6, Jun. 2018, doi: 10.1109/SBSE.2018.8395800.

[27] R. Das et al., "Advancements in Centralized Protection and Control Within a Substation," IEEE Transactions on Power Delivery, vol. 31, no. 4, pp. 1945–1952, Aug. 2016, doi: 10.1109/TPWRD.2016.2528958.

[28] W. An et al., "Application of Wide Area Monitoring Protection and Control in an electricity distribution network," IET Conference Publications, vol. 2014, no. 626 CP, 2014, doi: 10.1049/CP.2014.0054.

[29] J. Gurley et al., "Interoperability of System Protection Software," 2022 75th Annual Conference for Protective Relay Engineers, CPRE 2022, 2022, doi: 10.1109/CPRE55809.2022.9776560.

[30] L. Vásquez Ruiz, "Modelo hibrido utilizando agentes de software inteligentes y lógica difusa para el diagnóstico automático de fallas en sistemas de trasmisión de energía," Repositorio institucional UN, 2010.

[31] R. Vaish, U. D. Dwivedi, S. Tewari, and S. M. Tripathi, "Machine learning applications in power system fault diagnosis: Research advancements and perspectives," Eng Appl Artif Intell, vol. 106, p. 104504, Nov. 2021, doi: 10.1016/J.ENGAPPAI.2021.104504.

[32] N. Kabbara et al., "Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges," Energies 2022, Vol. 15, Page 9362, vol. 15, no. 24, p. 9362, Dec. 2022, doi: 10.3390/EN15249362.

Oscar Andrés Tobar R. is an Electrical Engineer and have a master's degree in Electrical Engineering with emphasis in substation automation based on the IEC 61850 standard from UN. Currently, he studies a PhD in Electrical Engineering at National University, and he is member of GT&T at UN. He has experience in formulating and executing projects related to intelligent measurement, digital substations with process bus, wide area protection schemes, testing of protection equipment operating with process bus (IEC 61850-9-2), testing with

real-time simulation tools, and testing with communication redundancy protocols according to IEC-62439. He is currently serving as Lead Analyst of the IEC 61850 Laboratory, where He is responsible for overseeing and reviewing the tests performed in the laboratory. https://orcid.org/0000-0001-9972-5308

Rodolfo Garcia Sierra. Leader of the Innovation Observatory of Enel in Bogotá. Electrical engineer from the National University of Colombia, master's degree in economics, and PhD in engineering. Occasional professor at the National University of Colombia. He has an essential background in implementing and executing technical projects for regulatory issues on electrical operation, operation centres, and information technology. http://orcid.org/0000-0002-3892-6189

Germán Zapata Madrigal. Director of the Research Group on Teleautomatic and Teleinformatic from the National University of Colombia. Electrical engineer from the National University of Colombia, master's degree in Automation and PhD in Applied Sciences. He currently serves as an Associate Professor in the Department of Electric Power and Automation at the School of Mines. Professor Zapata has broad and significant experience implementing research and development projects with major electrical companies in Colombia. https://orcid.org/0000-0002-7739-1578

Jair H. Vargas was born in Florencia, Colombia. He received the B. Sc. degree in Control Engineering from the Universidad Nacional de Colombia, Medellín, Colombia, in 2015 and the M. Eng. D. degree in Industrial Automation from the Department of Electric and Automatic Power, Universidad Nacional de Colombia, in 2022. He worked in the industrial and electrical sectors in areas such as communications, automation, and cybersecurity as a Project Engineer. He currently coordinates research and technological validation projects for the electricity sector at the Industrial Automation and Communications Laboratory of the Universidad Nacional de Colombia, Medellín. His research interests are focused mainly on the interoperability, scalability, and cybersecurity of electrical microgrids and their multiple components. https://orcid.org/0000-0001-6500-6372

John E. Candelo-Becerra received his bachelor's degree in electrical engineering in 2002 and his Ph. D. in Engineering with an emphasis in Electrical Engineering in 2009 from Universidad del Valle, Cali, Colombia. His employment experience includes the Empresa de Energía del Pacífico EPSA, Universidad del Norte, and Universidad Nacional de Colombia - Sede Medellín. He is now an Associate Professor at the Universidad Nacional de Colombia, Sede Medellín, Colombia. He is a Senior Researcher in Minciencias-Colombia and a member of the Applied Technologies Research Group – GITA at the Universidad Nacional de Colombia. His research interests include engineering education; planning, operation, and control of power systems; artificial intelligence; smart grids; and microgrids. https://orcid.org/0000-0002-9784-9494