

Article

Digital Substations: Optimization Opportunities from Communication Architectures and Emerging Technologies

Oscar Andrés Tobar-Rosero ^{1,*}, Octavio David Díaz-Mendoza ^{2,†}, Paola Andréa Díaz-Vargas ³, John E. Candelo-Becerra ^{2,*}, Héctor Andrés Florez-Célis ^{1,†} and Luis Fernando Quintero-Henao ⁴

¹ Departamento de Ciencias de la Computación y Decisión, Universidad Nacional de Colombia Sede Medellín, Medellín 050034, Colombia; haflorez@unal.edu.co

² Departamento de Energía Eléctrica y Automática, Universidad Nacional de Colombia Sede Medellín, Medellín 050034, Colombia; oddiazm@unal.edu.co

³ Detailed Design Enel Grids, Enel Colombia, Bogotá 7115115, Colombia; paola.diaz@enel.com

⁴ Research and R&D Consultant, Enterprise Innovation, Medellín 050034, Colombia; luis.quintero@einnovation.co

* Correspondence: oatobarr@unal.edu.co (O.A.T.-R.); jecandelob@unal.edu.co (J.E.C.-B.); Tel.: +57-317-7506055 (O.A.T.-R.); +57-324-6653450 (J.E.C.-B.)

† Current address: Industrial Automation and Communications Laboratory, Universidad Nacional de Colombia Sede, Medellín 050034, Colombia.

Abstract: Digital electrical substations (DESSs) represent a significant development for the electrical industry. New communication technologies and architectures have emerged alongside the development of DESSs. This paper presents an analysis of typical communication architectures used in DESSs. In addition, some optimization alternatives are identified, assessing the possible impacts on companies. Experimental tests were conducted in a laboratory to support the analysis performed in this research. Finally, some emerging topics and technologies supporting infrastructure optimization and technological adaptability are included. This study has revealed various impacts that companies must consider to effectively incorporate these architectures into the design and implementation processes of DESSs. Finally, effective cybersecurity and access control policies should be implemented across all components of a DES to ensure successful implementations.

Keywords: digital substations; IEC 61850; communication architectures; communication redundancy protocols; process bus; station bus; intelligent electronic device—IED



Academic Editor: Valeri Mladenov

Received: 1 March 2025

Revised: 27 April 2025

Accepted: 30 April 2025

Published: 8 May 2025

Citation: Tobar-Rosero, O.A.; Díaz-Mendoza, O.D.; Díaz-Vargas, P.A.; Candelo-Becerra, J.E.; Florez-Célis, H.A.; Quintero-Henao, L.F. Digital Substations: Optimization Opportunities from Communication Architectures and Emerging Technologies. *Sci* **2025**, *7*, 63. <https://doi.org/10.3390/sci7020063>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Digital electrical substations (DESSs), also called digital substations or smart substations, represent a transformative advancement in the electrical sector, integrating digital communication technologies into traditional substation infrastructure to improve operational efficiency, reliability, and adaptability. Often embedded within Substation Automation Systems (SASs), DESSs leverage standards such as IEC 61850 in addition to the digitalization of signals and functions to replace conventional analog wiring with high-speed data communication networks. This shift benefits network owners, operators, and maintenance teams by enabling real-time monitoring, advanced automation, and optimized resource use [1]. However, this type of system also brings significant technical challenges in cybersecurity and interoperability, from the design stage to its implementation and final configuration. The transition to a digital environment has multiple implications, such as system conceptualization, knowledge acquisition, performance analysis, and optimization [2]. This can

only be achieved when the engineering teams have sufficient knowledge to contribute to the planning, design, and implementation of DESs.

DESs introduce critical implications, including increased vulnerability to cyberattacks on communication channels. Studies such as Aljohani and Almutairi (2024) highlight how distributed denial-of-service (DDoS) attacks can disrupt traffic in digital energy systems [3], while Ashraf et al. (2021) note delays in IEC 61850-based protection responses under such threats [4]. However, Efiog et al. (2025) further emphasize the need for robust defenses, simulating cyber risks in virtual DES environments [5].

Therefore, when implementing DESs, companies must consider factors such as the security and reliability of the power system [6]. Hence, robust substations are designed with redundancy in multiple pieces of equipment, such as merging units (MUs), intelligent electronic devices (IEDs), and communication switches [7]. In addition, it is generally complemented with redundant communication protocols, such as Rapid Spanning Tree Protocol (RSTP), Parallel Redundancy Protocol (PRP), and High-availability Seamless Redundancy (HSR). These alternatives are selected based on the operational conditions and the criticality level of each electrical substation.

When implementing DESs, the IEC 61850 standard recommends specific technologies and communication protocols depending on the application [8]. At the same time, different operation levels defined as (i) Level 0—process, (ii) Level 1—bay, and (iii) Level 2—station are defined within the electrical substation. The concepts of process bus and station bus are established as communication buses that allow integration between Level 0 and Level 1, or between Level 1 and Level 2 [9].

For example, the process typically uses sampled values (SVs) and generic object-oriented substation event (GOOSE) messages [10]. They link the information obtained in the substation bay and the response of the protection, control, and measurement equipment, accompanied by synchronization protocols such as the Precision Time Protocol (PTP) [11]. In addition, Manufacturing Message Specification (MMS), GOOSE, PTP, and Network Time Protocol (NTP) messaging are observed mainly at the station level [12]. MMS and GOOSE are used to supervise and monitor the status of elements or variables in the system. PTP and NTP are used to synchronize the DES infrastructure [13,14]. The use of these protocols depends on the implementation characteristics and performance requirements of the company, according to the relevance of the information transmitted [15,16]. Therefore, in the component of the station bus and the process bus, technologies, architectures, and communication schemes are implemented to achieve the desired system reliability [17].

However, as the architecture becomes more robust, there is also a direct impact on investment costs and the use of engineering resources [18]. Therefore, performing an analysis of different technologies and architectures applicable to DESs becomes relevant to study risks and implications, and, in addition, to develop optimization solutions [19,20]. For this reason, the optimization of the digital substation infrastructure becomes a determining factor when planning or developing any project of this type [21].

Emerging technologies available in the market might be used in these systems. A clear example is traffic optimization complemented by the analysis and selection of network interfaces suitable for the level of traffic expected in a substation [22]. This selection can be achieved based on saturation tests in the communication infrastructure [23]. The evaluation of interoperability and performance can be accomplished based on new technologies for the protection, control, measurement, and registration of signals in substations [24,25].

Nevertheless, one of the main limitations of studies and research related to the optimization of DESs is the use of standard communication architectures and conventional technologies for these systems [13,26]. Furthermore, research on this subject focuses on the requirements of local operators or utilities established by the IEC 61850 standard and

the base infrastructure of the DESs, leaving aside the design of architectures, components, or particular technologies of the communication system [27–29]. Finally, a key limitation in this analysis is the limited availability of published material, as most of the results from DES design and implementation remain restricted to private documentation [30].

Therefore, the typical architectures implemented in DESs and emerging implementation solutions are examined in this paper. In addition, information and suggestions from the IEC 61850 standard are considered. Furthermore, architectures based on optimizing DES resources and using emerging technologies are proposed, with a positive economic impact on companies and without threatening the operation of the power system. Possible improvements and impacts of implementing emerging technological solutions are identified. The results show that the integration of emerging technologies can impact the efficiency of engineering processes, leading to the development of new architectures that enable better traffic management while reducing costs. These are promising results for improving the optimization processes of companies.

The contributions obtained from the research are the following:

- The work provides a comprehensive and objective analysis of emerging technological trends and communication architectures in DESs, identifying optimization opportunities from both technical and operational perspectives. This study benefits from a collaborative approach between academia, research institutions, and industry experts, ensuring a balanced and practice-oriented vision.
- Qualitative and quantitative analyses of communication architectures in DESs are performed, demonstrating a potential reduction of up to 50% in communication equipment through a proposed universal bus architecture, validated by laboratory tests.
- An empirical evaluation of centralized protection and control (CPC) systems reveals response times up to 60% faster (e.g., <1 ms for GOOSE messaging) than some distributed IEDs in multivendor setups, improving scalability and efficiency.
- Traffic optimization strategies using Software-Defined Networking (SDN) are identified, reducing bandwidth saturation risks under high traffic conditions, and introducing cybersecurity improvements that would support the development of universal buses.

2. Background

This section presents the background of technological alternatives for DESs. Hence, the section is structured as shown in Figure 1, where details about conventional technologies, communication architectures, and emerging technologies are exposed.



Figure 1. Structure of the background.

2.1. Conventional Technologies in DES

The integration of new technologies has led to significant changes in technological substations. A DES is an integral evolution of the entire substation, where all systems are digitized and converge towards an architecture based on data, digital communications, and virtualization, which demands robust and reliable communication to operate the

system; in this case, selecting, analyzing, and identifying aspects such as communication interfaces, communication channels, and especially communication equipment that will be part of the infrastructure [31]. However, to make informed decisions about the selection of these components, it is crucial to have a deep understanding of the infrastructure that will be part of the DES. The communication protocols associated with the different devices that can be part of a DES provide valuable insight into the capabilities required for the communication system [32,33]. This emphasis on understanding the infrastructure will make the audience feel informed and prepared to select components.

For DESs, the best communication channels are those that use optical fiber. It has the option of using single mode or multimode, depending on the characteristics of the system and the information flow with which it operates [34]. In turn, using this channel type requires appropriate communication interfaces that can be ST (Straight Tip) or LC (Lucent Connector or Little Connector) type; the latter being the preferred and most used in DESs.

Switch (SW) communication devices must be considered from a conventional point of view. They must have a good processing capacity, a sufficient number of communication interfaces, and compatibility with the different protocols implemented in DESs. At this point, the validation of this type of technology is highlighted according to the suggestions in the IEC 61850 standard, particularly considering Sections 3 and 90-4, where fundamental aspects are identified for this type of device [8,34,35]. The number of communication switches will depend on the size of the DES, depending on the number of devices, and the communication protocols selected for this type of system. These are fundamental factors for design processes, with an emphasis on optimizing resources in DESs. These technologies and protocols are the foundation of DES functionality, and their deployment is based on specific communication architectures, as explained below.

2.2. Communication Architectures

Although each DES infrastructure is defined based on its components, they have common characteristics. Hence, a reference can be established for communication architectures, equipment, and integration of elements [36]. In addition, the IEC 61850 standard exposes several types of DES architectures, highlighting some of their benefits and limitations.

In a DES, there is typical equipment, such as Gateways (GWs) and Human–Machine Interface (HMI) (Level 2); protection, control, and measurement IEDs (Level 1); and MUs or signal processing equipment (Level 0). Typically, these devices are integrated at two communication levels: the station bus (Level 2 and Level 1) and the process bus (Level 1 and Level 0) [15,37,38]. Figure 2 shows a base architecture for a DES, which links the aforementioned equipment to the corresponding communication levels.

The amount of equipment used depends exclusively on each substation, according to its operational and technical conditions. This architecture implements a single-star topology by integrating devices into the station bus. In the process bus, a single star complemented by a ring, comprised of communication equipment (switches—SWs), is observed. This type of connection can be used to implement an RSTP redundancy, considered in the IEC 61850 standard, but it is recommended only for the station bus level due to performance requirements and response times.

Companies or engineering teams carefully design and implement the final architecture that integrates various components. The decision is based on the operational characteristics and availability criteria of the system, ensuring compliance with the necessary security and stability requirements [36]. To ensure the availability of information flow and to adhere to the IEC 61850 standard for messaging, there is an opportunity to develop communication architectures that enhance the availability, stability, and flexibility of DESs. This can help to guarantee the continuity of communication between the system devices [39].

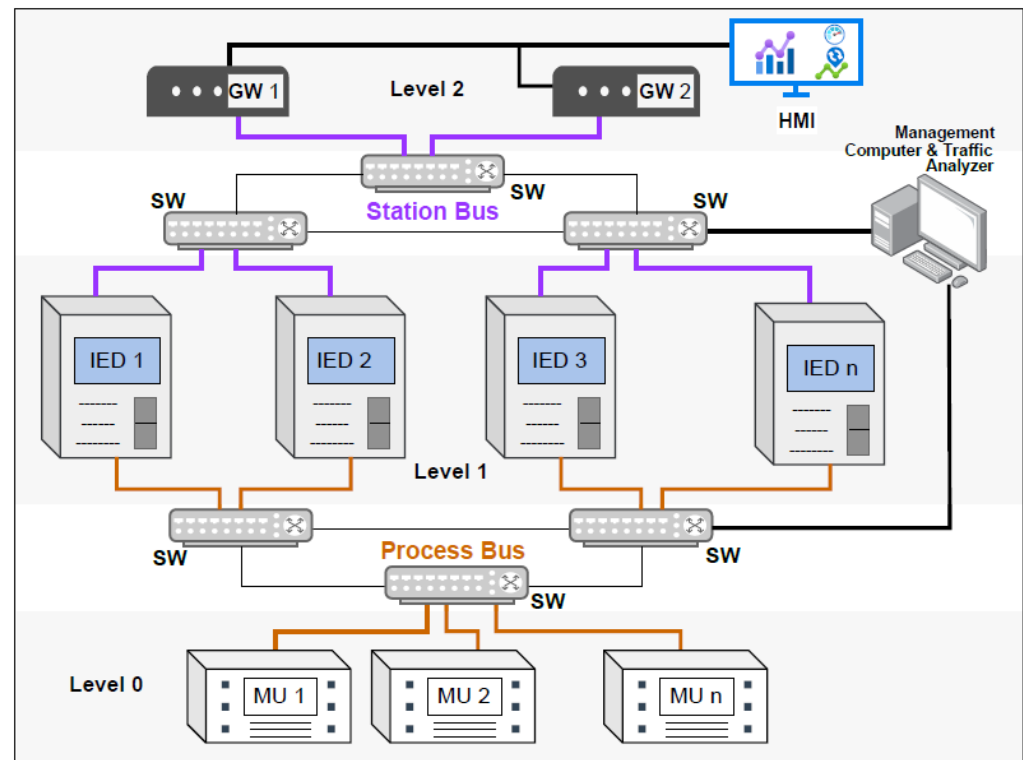


Figure 2. Example of a base communication architecture for a DES.

Local companies have chosen to start and extend the implementation of station bus components in DESs. They have integrated IED devices for protection, control, measurement, and registration with the infrastructure to perform monitoring (HMI and GW) in the electrical substation. At this level, different redundancy schemes have been evaluated, both at the hardware level (switches, IEDs, etc.) and at the protocol level (RSTP/PRP/HSR) [38,40]. Therefore, this study considers these implementations to show the typical communication architectures in local companies, without neglecting that there may be combinations of these to improve power system reliability.

Figure 3 shows the base devices for the level of the station bus in a DES. In this case, the PRP redundancy scheme is implemented. Here, a double-star architecture is identified in which at least two switch-type communication equipment are required as central nodes (LAN A and LAN B). All published information must have two simultaneous output channels in this architecture, and the devices that integrate it must be compatible with the protocol. The information that is transmitted is practically the same, with the only difference being the LAN tagging to which it belongs. In some cases, this architecture is complemented by redundancy in communication equipment (similar to what is described in Figure 2).

Similarly, Figure 4 shows the same station bus devices but employing HSR redundancy. This illustrates a ring-type architecture between the IEDs, without considering intermediate switch-type communication equipment. In HSR redundancy, each device publishes identical messages simultaneously via two communication interfaces, adding the Line A and Line B tags to these messages so that they are verified, approved, or discarded, regardless of the sequence in which they arrive at the receiving device.

Redbox devices can be included in an HSR network due to the lack of communication equipment (SW). This device enables non-compliant equipment to connect to HSR or PRP redundant networks in digital substations (e.g. management computer or traffic analyzer), ensuring high availability and continuity of critical communications. Redbox lacks enough communication interfaces or compatibility with the implemented redundancy protocol, but allows the flow of information within the ring to be analyzed.

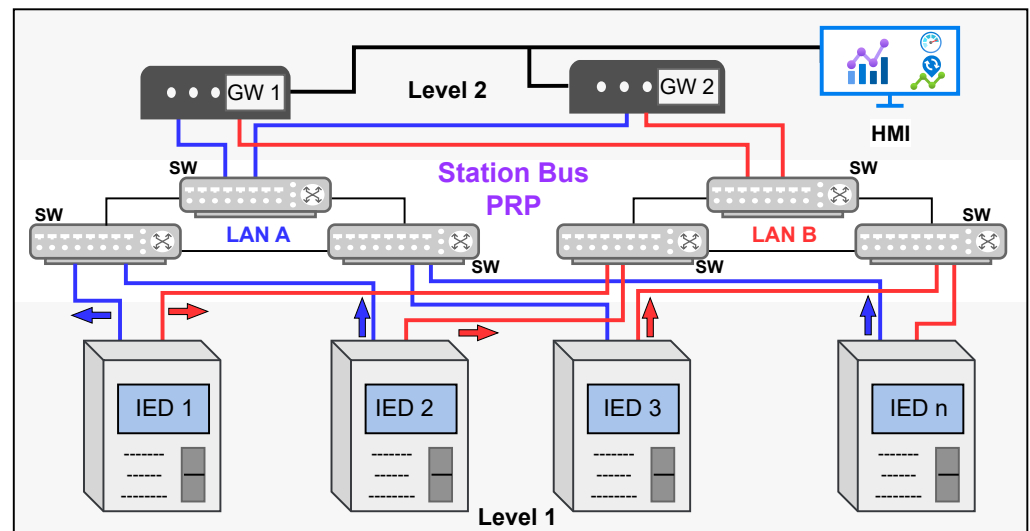


Figure 3. Communication architecture for DES with PRP redundancy on station bus.

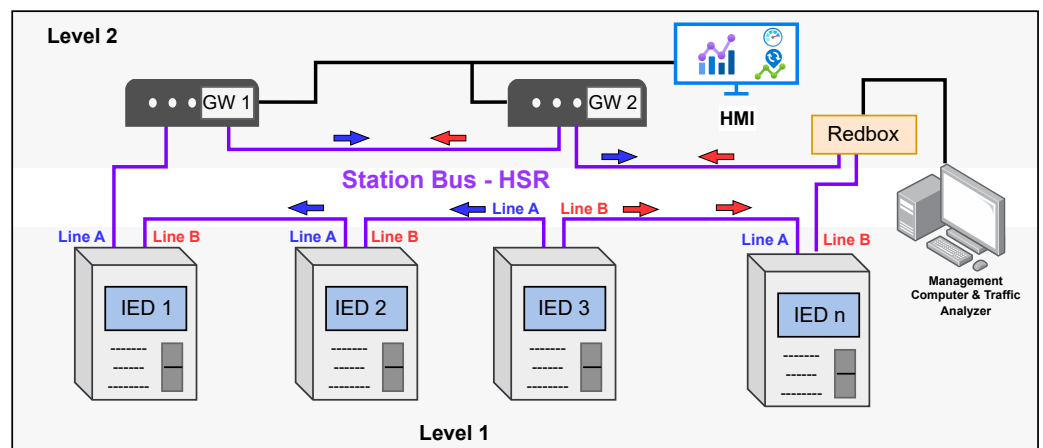


Figure 4. Communication architecture for DES with HSR redundancy on station bus.

In both cases (Figures 3 and 4), when an event ends with the loss of one of the communication channels, the network is not affected. It has a parallel channel for simultaneous information transfer and identical characteristics. Therefore, the subscriber device or end user of the information is guaranteed to always have access to it. Implementing these protocols is related to the compatibility that devices that are part of the infrastructure may have with them and the technical and economic characteristics of the substation and/or those provided by the company for its systems [41].

Companies must also consider the advantages and drawbacks of typical communication architectures, such as star, double-star, and ring configurations, when choosing components, designing, and implementing these systems [32,42].

It should be noted that at this point, there is an important gap in the literature, leaving aside the design of communication architectures and generally focusing on traffic control or using devices that improve system performance. Therefore, it is an important opportunity to expose the different alternatives that can be developed by combining designs with emerging technological solutions. In this way, companies implement innovation processes that impact the efficiency of operations and implement systems that positively impact investment, operation, and maintenance costs. At the same time, processes such as technological appropriation and the generation of new knowledge are encouraged.

The hardware-intensive nature of these communication architectures drives the adoption of emerging technologies to improve efficiency and flexibility. Thus, emerging tech-

nologies, coupled with engineering processes and tools, allow conventional architectures to be adapted to a more reliable and secure environment based on their performance needs.

2.3. Emerging Technologies for DES

Technological development is a continuous process, and alternative devices are emerging that can be used at different levels for the operation of DESs [43]. Software-Defined Networking (SDN) can be used as the first alternative in a communication system. This type of system is an emerging paradigm that has been used in IT systems, with excellent results in terms of information flow control, process automation, and optimization of resources and response times in such systems [44].

These systems can be considered as a novel and timely alternative to optimize infrastructure in a DES [45]. SDN decouples the control logic of the network (control plane) from the underlying devices that handle traffic (data plane), which requires network devices, such as switches, to become data exchangers or devices that host the control logic implemented by a logically centralized controller, known as a network operating system [46]. SDN transforms network switches into efficient data forwarders or hosts for centralized control logic.

Recent studies that have evaluated the benefits of using SDN in DESs have shown improved cyber resilience by implementing advanced security controls and network segmentation. It reduces the attack surface and enables rapid response to cyber threats [47,48]. It also facilitates resilience to failure, with fast failover capabilities that ensure operational continuity [49]. At the security level, SDN helps meet standards such as IEC 62443, automating critical functions to ensure compliance [50,51]. In addition, SDN enables flexible traffic management, optimizes performance, and minimizes downtime through dynamic reconfiguration. Bandwidth optimization is another key benefit, prioritizing critical data such as GOOSE messages [48]. SDN also promotes scalability and adaptability, enabling the integration of new devices and services without significant changes to physical infrastructure [52]. In general, SDN improves the efficiency, security, and resilience of DESs, supporting the modernization of critical infrastructure.

SDN is a potential alternative to better manage traffic in digital substations, as it might provide greater automation, management, and supervision of the communication system with a reduction in infrastructure. It might also improve cost, quality of service, resilience, and cybersecurity [44,53]. Some opportunities to improve DESs with SDN are summarized below.

- Flexibility in management: It allows centralized and dynamic network reconfiguration according to traffic needs.
- Enhanced security: It facilitates network segmentation and automatic real-time responses to possible cyberattacks.
- Resource optimization: It reduces hardware complexity and minimizes operating costs by eliminating complex local configurations.
- High availability and resilience: It detects failures and automatically redirects traffic, ensuring operational continuity.
- Real-time monitoring: it allows continuous network monitoring, identifying potential failures and bottlenecks.
- Interoperability: It promotes compatibility between devices from different manufacturers, simplifying integration.
- Integration of new technologies: It facilitates the adoption of new technologies without disrupting the existing infrastructure.

However, few documents expose experiences related to real applications in DESs. Thus, in the electricity sector, there is not enough confidence in its implementation. In this

way, the use and application of this paradigm in digital substation communication systems can be explored to consolidate accurate results and determine if the benefits are applicable in a real environment.

Another technology that has generated significant interest in recent years is a centralized protection and control (CPC) system [54]. This type of technological solution represents a significant change and perhaps the greatest opportunity for DESs to reduce infrastructure, physical space, and engineering processes [55]. A CPC, by consolidating a set of protection and control equipment within a single device (see Figure 5), offers the potential to streamline operations and improve control in DESs [56]. This promising technology instills a sense of optimism about the future of DESs [57].

From an analysis of the characteristics of this technological solution, the reduction in operating and maintenance costs can be seen by eliminating the need for multiple distributed protection relays and consolidating the functions in a single device [58]. This also contributes to optimizing the space in the control room by reducing the number of control panels and relays required [59]. In addition, it improves the flexibility and scalability of the system, allowing new protection and control functions to be implemented through software without hardware changes [60,61]. The CPC also facilitates greater interoperability between devices from different manufacturers, as it is based on standards such as IEC 61850, improving integration and communication within the substation [58,62]. Finally, it offers resilience and operational efficiency, centralization of critical operations, and optimization of response to system failures [60].

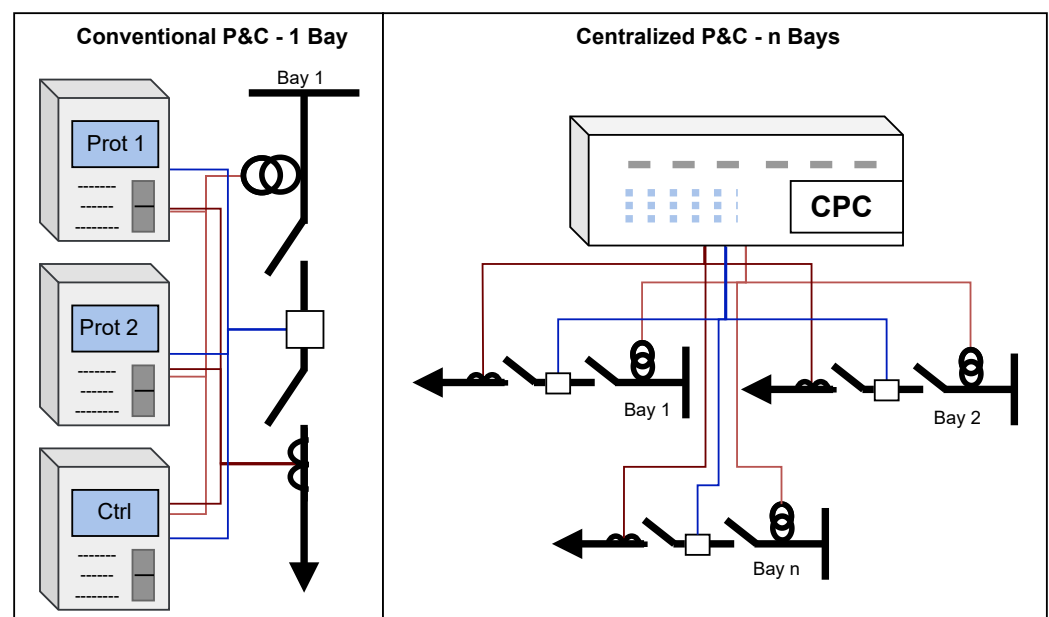


Figure 5. Conventional P&C vs. centralized P&C.

This type of solution allows the development of logic systems, interlocks, and engineering processes to have greater control over the operation of DESs and electrical systems, focusing on the confidence of the same device [63,64]. Some potential benefits derived from CPCs in digital substations are described below.

- **Equipment reduction:** It decreases the number of physical devices in the substation.
- **Space optimization:** It allows the reduction of physical space and simpler installations.
- **Simplified maintenance:** It facilitates lower maintenance costs and more efficient management.
- **Increased flexibility:** It facilitates adaptation to operational or technological changes through software, without the need to modify the hardware.

- Improved resilience: It enables faster response to failures and more efficient system recovery.
- Interoperability: It provides an improved integration of devices and technologies from multiple manufacturers by standardizing communications and functions.
- Scalability: It enables faster growth without large investments in physical infrastructure.

However, while this represents an excellent opportunity, it also implies more significant risks to the operation of the system. Failure or violation of one of these devices can cause more problems for electrical systems [62]. In addition, it is also important to consider that the use of these devices must be supported by the local regulatory framework, which in some countries is a weak point because the use of certain equipment (separately) can be required by law that can allow the use of CPC in DESs [60].

It would be important to examine the future implementation of distributed or centralized protections according to local standards and technical specifications. At the same time, proposing parallel implementation strategies for CPC with distributed protections might be an essential initiative to update and support regulations that establish precise rules for using CPC without exposing the electrical system.

Furthermore, machine learning (ML) has emerged as a powerful tool for DES optimization and security [65,66]. Techniques such as supervised learning (e.g., regression for traffic prediction) and unsupervised learning (e.g., clustering for anomaly detection) enable predictive maintenance and real-time fault analysis [67]. Early access studies suggest that ML can complement SDN by forecasting bandwidth saturation or enhance CPC by optimizing protection logic, and use digital twins for process validation [68]. These methods expand the scope of DESs beyond traditional protocols and applications.

The analysis of architectures and system optimization proposed in this article considers the emerging technologies mentioned and discusses their use and main benefits, as well as some impacts and considerations to be taken into account in the digitization of electrical substations.

3. Methodology

This section addresses the methodological proposal implemented in this research. The aim is to establish base criteria to characterize the communication systems of DESs. From this, the implementation of DES schemes is proposed to optimize the use of resources from communication architectures and new technologies, or to integrate both aspects.

Table 1 shows three types of architecture implemented in DESs. This is in line with the explanation in the previous section. In turn, each architecture is related to the minimum amount of equipment required for the correct implementation and operation in an electrical substation bay. It should be emphasized that each company or engineering group may have additional communication equipment (switches or Redbox) to strengthen its architecture and provide greater reliability and security to its systems.

Table 1. Initial characterization of the base infrastructure for a DES bay.

DES Infrastructure requirements per bay	Architecture Type (Conventional Digital Systems)		
	Basic star—simple (non-redundant)	Double star—PRP redundancy	Ring—HSR redundancy
Gateways		at least 2 *	
IEDs		at least 2 or 3 *	
Merging Units		at least 2 *	
GPS		at least 1	
Switches	at least 2	at least 4	none
Communication channels	at least 8	at least 16	at least 8

* Depends on local or corporate regulations (e.g., CREG standards in Colombia).

Additionally, Tables 2 and 3 present the reference costs and energy consumption, taken as approximate average values. The final costs may vary depending on the technology provider, the location of the project, and local economic factors. The power consumed may vary depending on the brand and model of the devices, the scheduled tasks, and the information traffic that they must process. The values presented here are obtained from the multiple technological offers analyzed for each type of device or infrastructure necessary for a digital substation. In addition, a survey of information from technology suppliers and information from utilities and engineering teams that participated in this project is considered. To better understand the process, this table uses the same reference infrastructure to establish the types of architecture in a digital substation used in Table 1.

Table 2. Initial characterization of infrastructure costs for a DES bay.

DES Infrastructure requirements per bay	Architecture Type (Conventional Digital Systems)		
	Basic star—simple (non-redundant)	Double star—PRP redundancy	Ring—HSR redundancy
Gateways		US\$21,000	
IEDs		US\$19,000–US\$28,000	
MUs		US\$12,000	
GPS		US\$8000	
Switches	US\$8000	US\$16,000	none
Communication channels	US\$2000	US\$4000	US\$2500

Table 3. Initial characterization of infrastructure power consumption for a DES bay.

DES Infrastructure requirements per bay	Architecture Type (Conventional Digital Systems)		
	Basic star—simple (non-redundant)	Double star—PRP redundancy	Ring—HSR redundancy
Gateways		150 W	
IEDs		160–240 W	
MUs		90 W	
GPS		40 W	
Switches	140 W	280 W	none
Communication channels	none	none	none

The procedures delineated within this document, along with the data presented in the various tables and results, relate to the implementation of a bay in a digital substation. Therefore, these data could be multiplied depending on the number of substation bays to calculate the cost and consumption of a larger system under the same scheme.

Under this premise, the alternatives that might be developed are analyzed in a DES with one or more bays. This is performed with resource optimization as a priority without generating risks in system operation. Therefore, in this research, the occupation of the communication network is considered based on the different communication protocols exchanged between the devices that are part of the DES. For this, the occupancy sizes considered by the standard or obtained from practical experience in laboratory tests are considered as a reference. The values presented in Table 4 are used as a reference. However, they do not necessarily coincide with any system because the number of variables and the mapping of signals in the data sets created for the publication of messages on each device may cause these reference values to vary.

Table 4. Communication protocol characterization for DES.

Communication Protocol		Size [Bytes/s] *
MMS		12.5 k
GOOSE	Heavy (burst/Trips) (e.g., “during fault events”)	125 k
GOOSE	Lite (steady state)	125
Sampled Values		4.8–6.2 M

* Values per message type from IED or MU in DES.

The proposed implementation alternatives for DESs consider the type of architecture (with a redundancy scheme, as suggested in IEC 61850-90-4), the number of devices, and the number of messages published by each device. The proposed solutions are based on the IEC 61850 standard, which suggests having a maximum occupancy of 60% of the bandwidth for the interfaces and communication channels used in the DES architecture as a limit.

Furthermore, it should be noted that the development of these architectures was carried out based on a joint work between the private sector (Enel Colombia), academia, and research, supported in turn by test results in the laboratory. The test was conducted in the Laboratory of Automation and Industrial Communications—LACI—of the National University of Colombia, Medellín. Different communication architectures for digital substations were implemented, integrating devices from multiple manufacturers and with various operating capabilities. As a product of this research process, several aspects were analyzed and some relevant results were found, as defined next.

- Integration and interoperability (according to IEC 61850) between protection, control, and supervision devices, focusing on multivendor systems.
- Performance evaluation of protection and control equipment (IEC 61850-10).
- Evaluation of protocol conversion to supervisory systems.
- Evaluation of interoperability and performance in communication systems.
- Evaluation of the performance of the CPC system.
- Traffic analysis, packet loss, or anomalies in information transfer.
- Application of traffic management (Quality of Service—QoS) through segmentation using VLAN and MAC-Multicast filtering.

Finally, the test considers performing various analyses for events such as redundancy protocols (PRP and HSR), network traffic saturation, failure events in the electrical system, loss of synchronization, and cyberattacks. Some products of the research and

testing progress made can be found in the following data sets [69,70], in addition to the complementary publications that will be reviewed in the presentation of the results.

Although numerical simulations were not performed due to resource constraints, the experimental setup in the LACI laboratory replicated real-world DES conditions using multivendor devices. These tests, detailed in Section 4, provide empirical insight into architecture performance, serving as a practical alternative to simulation-based analysis.

4. Results and Analysis

This section addresses the different alternatives considered as opportunities for resource optimization in DESs. For this, the evolution processes of the companies for the assimilation of DESs have been considered. Consequently, the revision begins with the transition from the digitization of the station bus to the digitization of the process bus to achieve a full DES, where it is possible to include emerging technologies for protection, control, and automation. In addition, this section includes the results of the tests carried out in the laboratory, along with the technologies that support the approach of the proposed architectures.

4.1. Lab Test—Preliminary Results

Effective interoperability with GOOSE, SV, MMS, and PTP messaging was validated using equipment from different manufacturers, including ABB, GE, SEL, and SIEMENS. In some cases, background configurations in the IEDs were required to achieve interoperability. Some of these experiences and considerations to ensure interoperability between multi-manufacturer technologies are evidenced in [9,15]. These results highlight the importance of knowing the substation configuration language (SCL) files in detail, identifying structures, data types, data objects, logical nodes, data sets, and the association of signals for the publication schemes required in each protocol.

Once integration and interoperability were guaranteed, GOOSE trip messaging in multivendor architectures measured equipment performance. The estimated transfer times in GOOSE messaging for IEDs met the requirements outlined in the IEC 61850 standard. Some of the results associated with this process can be seen in [71,72]. In addition, Figure 6 shows the results obtained in the multiple performance tests carried out with the IEDs of the manufacturers that participated in this research process. The blue box shows where the middle 50% of the data measured falls, giving a sense of the typical range. The red line inside marks the median, or the results' midpoint. The thin black lines, or whiskers, extend to the most typical values, while any dots beyond them are outliers — unusual values that fall outside the expected range.

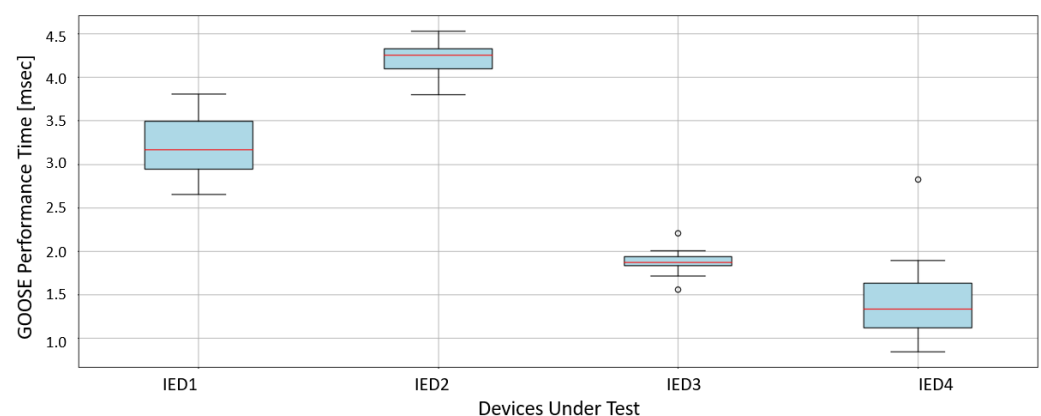


Figure 6. GOOSE performance for IEDs under test.

This graph shows that all the devices under test have transfer times of less than 5 ms. This indicates the good performance of the devices that execute protection and control operations with GOOSE messaging in different scenarios, varying traffic levels, and operating systems. These results show that even though the test scenarios considered integration and interoperability, there are no difficulties in meeting the requirements established in the standard.

The conversion of MMS protocols from the substation to IEC 60870-5-104 (typically named 104) in control centers was evaluated, with gateway equipment as devices under test. The results showed a signal mapping related to the scenarios under test, according to IEC 61850-80-1. However, in some cases, there are limitations with particular attributes that could be required from the control center. These limitations are generally associated with specific requirements established by each company or constraints it may have from the SCADA system or control center with which the signals are exchanged.

This research evaluates the integration capability of communication devices from different vendors. In addition, it assesses the feasibility of building multibrand architectures, implementing redundancy protocols, measuring reset times, and ensuring compatibility with various communication protocols. Furthermore, performance tests were conducted with communication equipment from vendors such as Bitstream, CISCO, GE, Hirschmann, and SIEMENS. This study also examines redundancy schemes in communications, such as RSTP, and redundancy protocols such as PRP. However, some manufacturers use proprietary protocols or variations of existing standards, leading to better interoperability between devices of the same brand compared to those of different vendors.

A CPC system was evaluated, which performed better than the IEDs evaluated in equivalent scenarios [73]. Performance was measured with GOOSE trip messaging in multivendor architectures. The scenarios under test were the same as those considered in the IED performance evaluation. Thus, the test is performed to establish whether the performance of the CPC is adequate or presents limitations compared to that of the IEDs.

Figure 7 shows the average performance times of the CPC and the IEDs. These results show that the CPC has a response time lower (less than 1 ms) than distributed IEDs. In addition, this reveals CPC response times up to 60% faster than some distributed IEDs in multivendor configurations, enhancing scalability and efficiency.

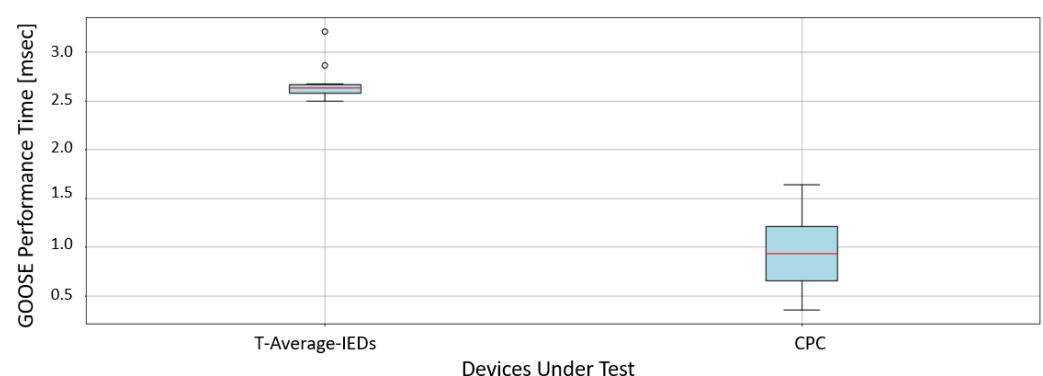


Figure 7. CPC vs. IEDs: GOOSE performance.

Based on the above results, it is evident that the CPC is an attractive solution for digital substations. It does not present interoperability risks and brings benefits in terms of cost reduction and optimization of engineering processes.

Traffic analysis showed that packet loss can occur in systems saturated with information. Similarly, when proper data flow analysis is not performed, response times can be

higher than the desired performance for each message type. This is a common denominator for all systems, indicating that traffic management is essential in digital substations [9].

Figure 8 shows a sample of GOOSE traffic, with the flow of these messages with the digital substation in steady state at the top of the graph. Here, messages vary as a function of time due to the number of messages present in the network for the scenarios analyzed and the periodicity of the retransmission of each message. This sample shows that the maximum size reached is always less than 200 bytes, representing a bandwidth occupation close to 1.5 Kbps.



Figure 8. Traffic analysis with GOOSE message.

Similarly, this graph includes an analysis of the GOOSE messaging traffic in the occurrence of failure events at the digital substation. It shows the dynamics of this protocol and the increased occupation generated from the bursts of messages in each event. Therefore, the graph shows how a size close to 1500 bytes is reached for these scenarios, representing an occupation of approximately 11.7 Kbps in the bandwidth of the digital substation.

These results help identify that although the GOOSE messaging flow is highly relevant for the operation of the digital substation, it does not represent a high risk of reaching traffic saturation in the digital substation communication system. Moreover, a stream of sampled values is considered to range between 4.8 and 6.2 Mbps, which is considerably higher than the maximum flow achieved in the analysis of the GOOSE message. Figure 9 shows a sample with four MUs publishing sampled values to a system, evidencing different levels of bandwidth occupancy. These variations are due to the length of encapsulation of each sampled value, with the understanding that there are attributes that are free to choose for companies, so some may or may not be published depending on the needs of each client.

To evaluate the response of the communication system according to different saturation levels, a traffic volume close to 40% (IEC 61850-90-4) of the theoretical bandwidth of a fast system (100 Mbits) was selected. MUs were added as SV publishers in a digital substation. Figure 10 shows the packet loss behavior in the system. In turn, these same scenarios were tested with a Giga communication system, which, in the graph, shows the normal information flow in the different scenarios considered for the saturation test. This process shows the importance of executing a rigorous planning and design process of the digital substation, both new and in an upgrade or expansion, because the amount of equipment or data flows that are part of it may represent a limitation for its proper operation.

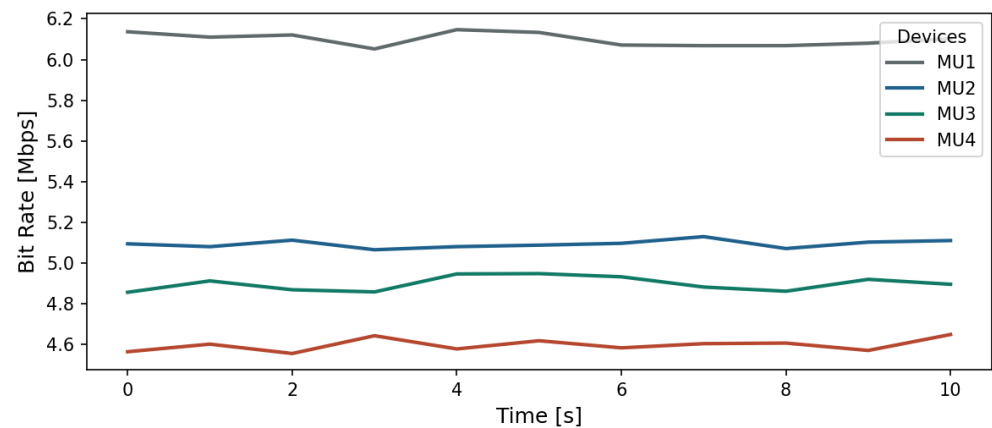


Figure 9. Analysis of bandwidth occupied by different MUs.

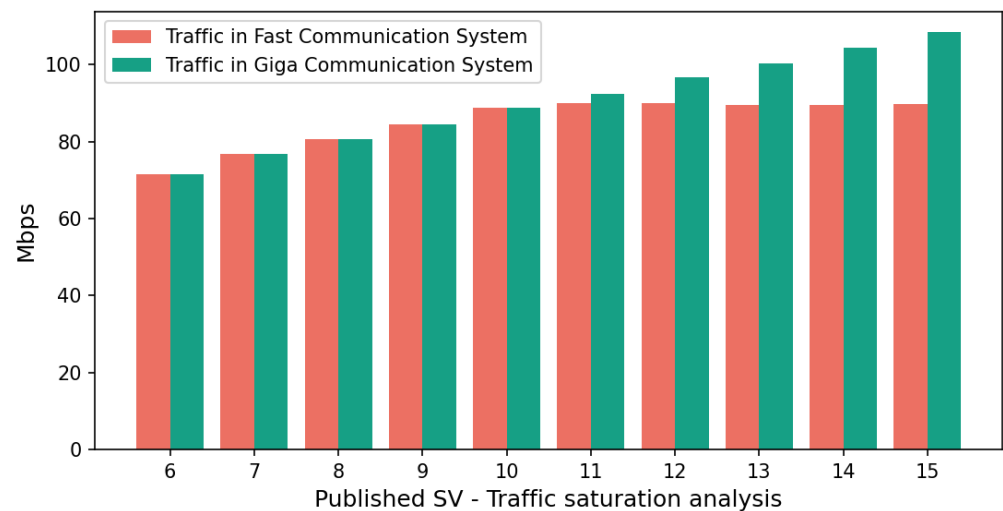


Figure 10. Sampled values' saturation test results using multiple MUs.

Figure 11 shows the behavior of a flow of sampled values where packet loss occurs. This image represents the capture of two signals to show how the information would be perceived in the IEDs subscribed to the SV of the MU with packet loss. Naturally, this will be reflected in an operation failure, which in turn may trigger unwanted events with an impact on the digital substation. This could represent a high risk to the operation of the electric system to which it belongs.

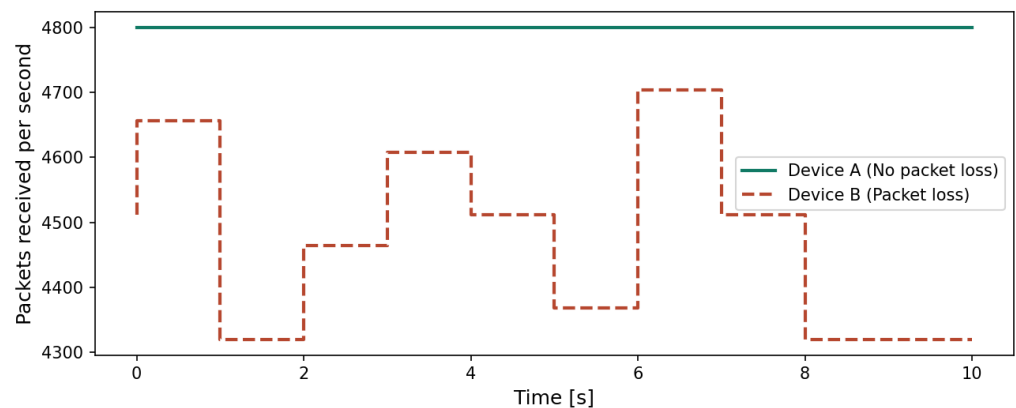


Figure 11. Packet loss in traffic saturation tests with sampled values.

In turn, in the research process, it was shown that using QoS in digital substations significantly improves system performance, reduces response times, and provides cyber-

security improvements (e.g., through network segmentation and real-time threat detection) [74]. This aspect, evaluated in conventional communication systems, can be an even more significant advantage using SDN, considering the characteristics highlighted above for this communication paradigm.

4.2. Initial Optimization Alternatives

When selecting an electrical substation architecture, companies and engineering teams must consider the economic factor without neglecting security and integrity. Different aspects are evaluated to optimize resource usage. Optimizing means reducing the amount of equipment needed or maximizing the use of current devices without compromising the operation of the system. A high-level complementary configuration also impacts the complexity and costs of implementing DESs.

Ensuring seamless adoption of DES architectures is critical for operational continuity. Then, it is assumed that companies with a station bus will evaluate their process bus. Hence, the first recommendation for implementation is to have a low impact on the typical station bus architecture. Thus, Figure 12 illustrates the DES architecture with the station bus and the process bus. At the supervision level (station), a redundancy scheme with PRP is implemented, while, in the process bus, it enters the system with an HSR redundancy scheme.

Although simulation results are not performed, laboratory tests emulate operational scenarios such as traffic saturation and packet loss to assess architecture efficacy.

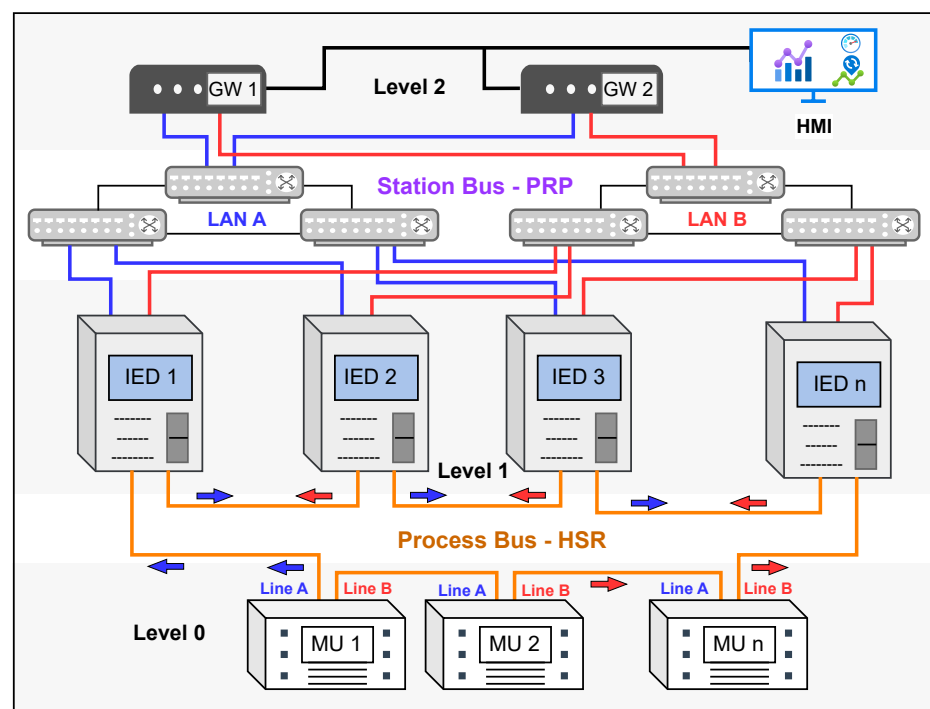


Figure 12. Inclusion of process bus via HSR redundancy in a DES with PRP implementation on station bus.

An architecture of this type allows companies and engineering teams to perform an initial evaluation of the performance of IEDs, MUs, and communication infrastructure. This assessment is based on the volume of data and performance times required for the response of electrical protections operating with SV and the exchange of GOOSE messages on trips [71]. The above acts without directly intervening in a new or existing redundant architecture (PRP) for the station bus. Therefore, complementary configurations are not

necessary for IEDs, as there is no communication equipment present in the ring process bus. The communications engineering work in this implementation is also reduced.

In this case, it is important to mention that the viability of this execution is related to the compatibility of the devices with the HSR redundancy protocol and a preliminary evaluation of the maximum volume of traffic that would take place on the process bus.

4.3. Proposed Architectures

As a result of the study carried out around communication architectures for DESs, some technical characteristics are determined that can be optimized. Intervening in the processes of communication engineering and performing adequate management of information can maximize the use of resources, with low risk in power system security, and guarantee reliability and stability in the operation. The proposed case studies consider the imminent integration of devices at Level 0 or those typically part of the process bus.

Figure 13 presents an alternative unification for a process bus and a station bus, identified as a universal bus. Level 0, Level 1, and Level 2 are connected to the interior of a DES, forming a system where the information and communication equipment (switches) are centralized. Therefore, the corresponding management must be carried out to segment the total traffic seen in the electrical substation, directing communication exclusively between the devices that require it.

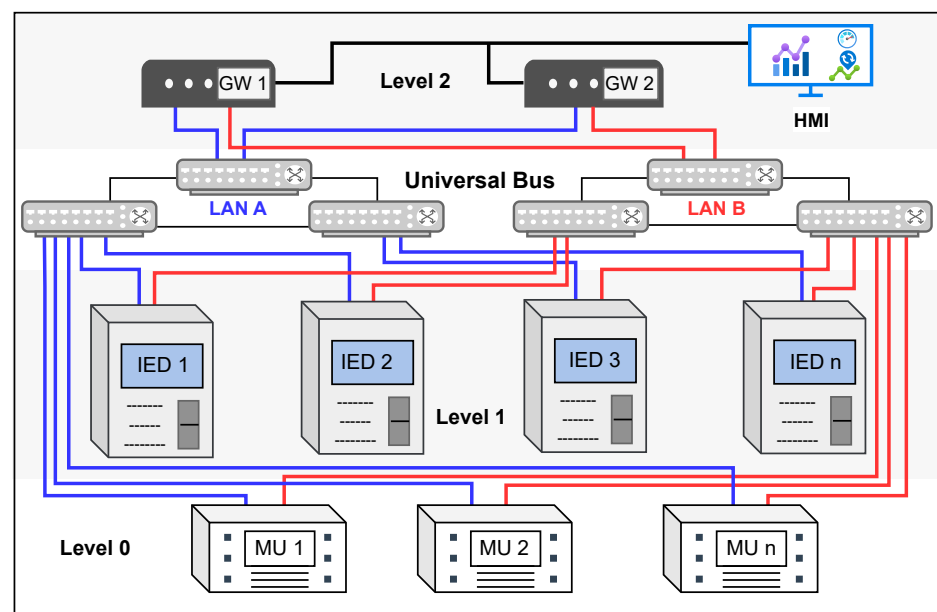


Figure 13. Architecture for DES with universal bus and PRP redundancy.

The proposed architecture would have at the same point the information on IEDs, MUs, synchronization, and supervision information required by Gateways and HMI. Therefore, it is necessary to perform a parameterization that limits the access to information from and to each device, preventing them from being saturated by a volume of traffic that is not useful for their operation.

With this type of implementation, there is evidence of a reduction in the use of communication infrastructure, considering switches, fiber optic channels, and even redundancy in time synchronization. Furthermore, preliminary analysis of communication architectures in DESs demonstrates a potential reduction of up to 50% in communication infrastructure (e.g., switches) through a proposed universal bus architecture and validated via laboratory tests.

At the same time, from the point of view of failure analysis in this architecture, the number of points of failure is reduced, as the number of connections with intermediate

equipment between one level of operation and another is reduced. For cases like this, in information management processes, the use of SDN is also considered, where it is possible to automate operating rules for traffic control, unauthorized access control, automate the organization of the infrastructure, and other benefits derived from this application.

For the architecture proposed in Figure 14, the possibility of implementing new or recently emerging systems, such as protection servers or centralized protection and control (CPC) systems [54,75], is also contemplated. The architecture establishes the creation of a universal bus with a PRP redundancy scheme. Devices in Level 0 (merging units or signal processing equipment) are integrated, delivering to this common node the sampled values obtained from current transformers (CTs) and potential transformers (PTs) in the electrical substation. An advanced computing device or a main protection server makes use of the variables necessary to perform protective functions oriented towards several bays of a substation. In addition, centralized protections considerably reduce the amount of equipment in the DES because a single device can control several bays.

As a complementary system of hardware redundancy, a backup protection server is proposed to operate synchronously with the server arranged as the main one. The protection, control, measurement, and registration of IEDs are not employed, and the economic impact of this type of architecture is relevant in substations with a large number of IEDs.

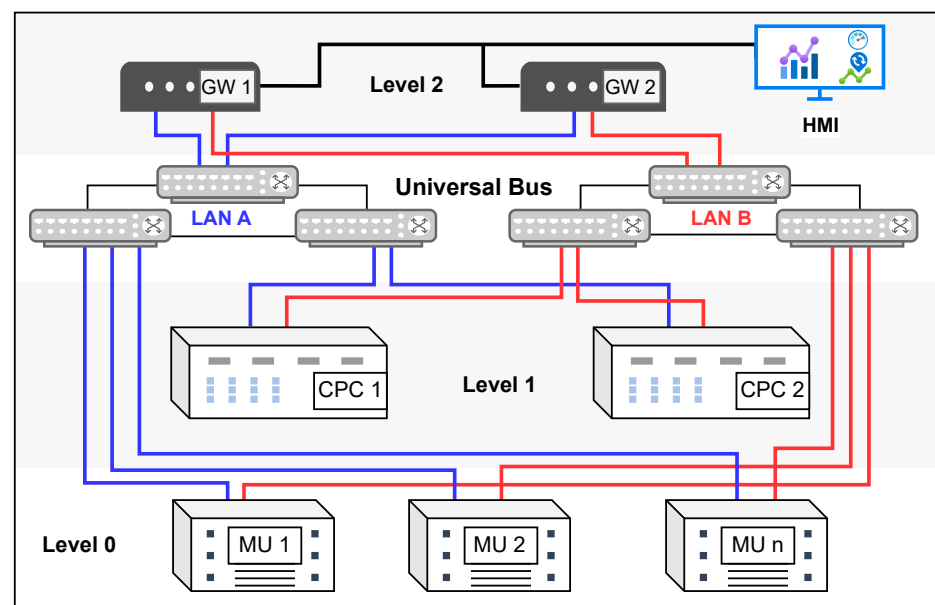


Figure 14. Architecture for DESs with universal bus, PRP redundancy, and centralized protection.

In both alternatives, the greatest use of the initial available infrastructure and the improvement of engineering processes are encouraged to guarantee the reliability, security, and stability of the operation of DESs. In addition, depending on the type of substation and its technical characteristics, the benefits and difficulties in these new processes will be reflected in a higher or a smaller average.

It should be noted that the architectures proposed in this document are based on the capabilities of the technologies considered for integration, such as CPC or communication equipment. This implies that, when selecting architectures and equipment for a system, it is essential to carry out performance, integration, and interoperability tests, as suggested by the IEC 61850 standard.

Devices used at each level of DES operation may have particular operating characteristics. These devices can present significant challenges for corporations or engineering teams in terms of system integration and achieving interoperability. Consequently, the use of

specific information within each company or region may require a comprehensive analysis to achieve the implementation of a feasible technological solution. In addition, during the decision-making process, it is recommended to perform a thorough examination of the characteristics inherent to each system and technology, as well as to select relevant standards applicable for use.

5. Discussion

This section presents a comparative analysis of the evolution of DESs. For this purpose, aspects of the new technological trends that are currently in the market, such as CPC or VPAC (Virtualization Protection, Automation, and Control), are considered [57,76].

The discussion considers multiple factors, including implementation costs, ease of maintenance, operating costs, security, interoperability, and implementation challenges. This type of system has been extensively studied by utilities and academia working groups and is analyzed according to a rigorous bibliographic study.

Table 5 shows the comparison between a traditional architecture and a centralized protection and control architecture used in substations. This approach is taken from the IEEE PSRC-WG CPCWS K15 group.

Table 5. Comparison of substation with traditional architecture and centralized protection and control architecture.

Approach	Traditional Architecture	Substation Centralized Equipment
Relay Asset Management Device Management	Many relays must be identified, specified, configured, tested, and maintained separately, along with separate records for each device. Each protection IED in a substation usually has numerous configuration options to enable various features.	A limited number of devices need to be identified, specified, configured, tested, and maintained, along with separate records for each device. A small number of devices makes it easy to manage, and also the feature set is reduced and limited compared to traditional methods.
Maintenance	Routine maintenance can be frequent and require experienced and well-trained personnel along with expensive calibrated test equipment. P&C IED maintenance per bay is easily accomplished due to the bay-separated IEDs.	Limited maintenance is required as the entire substation P&C system uses fewer physical devices, although experienced personnel are still required for maintenance. More robust and reliable systems can be designed at a lower cost.
Security	Multitude of protection IEDs Provides more access points for cyber threats.	Very limited number of access points that can also be better managed.
Interoperability	Disparate protocols that are difficult to standardize. Substation Automation System modifications can be complicated.	It primarily leverages IEC 61850 technology and can be more easily adopted than the distributed protection IED model. Substation engineers are required to have networking knowledge.
Substation Master Interface	Depending on the technology, the protection IED may not be able to be monitored by an RTU or data concentrator. Newer technologies have protective IEDs with limited computation and communication interfaces to transfer data in and out of the substation.	The CPC becomes the “Gatekeeper” of dynamic device models. Relays are ubiquitous. This provides a master smart node for interaction between substations and control centers. Tremendous reduction in communication needs.

In this study, a comparative analysis is performed, contrasting the different architectures and including a typical architecture with only a station bus. The analysis considers the variables cited in various scientific articles on the subject, considering the assets currently

recognized by the Colombian regulation CREG (Table 6). The evaluation is carried out using experience in the construction of different types of substations.

Table 6. Comparison between traditional architecture and proposed architectures.

Approach	Current Architecture	Architecture 1 Optimization Alternative	Architecture 2 Universal Bus	Architecture 3 Universal Bus and CPC
Relay Asset Management Device Management	Reduced	Reduced only in communications	Reduced single bus process	Significantly reduced
Maintenance	Low	Low	Low	Very low
Security	High	Medium	Medium	High
Interoperability	Medium	Medium	Medium	High
Substation Master Interface	Unique	It depends on the technology of each IED	It depends on the technology of each IED	Unique
Built area	High	High	Medium	Low
IED quantity	Medium	Medium–high	Medium	Low
Implementation time *	6 to 8 months	6 to 8 months	4 to 7 months	1 to 3 months
Deenergization is required for maintenance	Yes	No (redundant protection)	No (redundant protection)	No
Implementation Cost	Middle	Medium–High	Medium–Low	Very Low

* Implementation time: process from engineering to commissioning in SAT tests.

A key consideration in DES optimization is the trade-off between cost reduction and resource improvement. Table 7 quantifies this balance for the proposed architectures. The universal bus reduces switch costs by approximately USD 8000 per bay (from USD 16,000 in PRP to USD 8000) and power consumption by 240 W, but requires increased switch processing capacity to handle integrated traffic. In contrast, the CPC-based architecture reduces IED costs by USD 19,000–28,000 per bay and reduces implementation time to 1–3 months, yet demands higher initial investment in a centralized server (estimated at USD 30,000) and robust cybersecurity measures. These trade-offs suggest that while cost savings are significant, companies must weigh them against increased engineering complexity and potential risks, such as single points of failure.

Table 7. Trade-off analysis between cost reduction and resource improvement.

Architecture	Cost Reduction (US\$/bay)	Resource Improvement	Trade-Off Considerations
Current (PRP)	Baseline (US\$70,000)	High redundancy	High equipment count
Universal Bus	~US\$8000 (switches)	Up to 50% less equipment	Higher traffic load
Universal Bus + CPC	~US\$27,000 (IEDs)	50% faster response	Centralized failure risk

Impacts and Risks Derived from the Proposed Alternatives

The analysis of optimization alternatives has revealed various impacts and considerations that companies must consider to effectively incorporate these architectures into their DES design and implementation processes. Some of the most relevant impacts considered in this study are as follows.

- **Greater simplicity of the system:** In the proposed architectures, by integrating all devices with connection to a universal communication bus, their integration is considerably simplified, and their accessibility is improved, from the same central point that can be any of the communication equipment (LAN A or LAN B) proposed in the architecture.
- **Greater flexibility:** By combining the information with the DES, it becomes feasible to improve protection, control, and measurement systems. This includes incorporating new bays or parallel technologies for performance assessment or integration with the current system.
- **Cost reduction:** Leaving aside the separation of process and station buses in the DES implies a decrease in equipment and communication channels and spaces in boards destined for the infrastructure. In turn, this can have a greater impact, if a centralized protection system is implemented or, as shown in Figure 14, a main protection server with its corresponding backup.
- **Greater volume of traffic:** A common point for integrating all devices into the system implies that the information from this equipment converges at that point. This is why the volume of traffic increases considerably in space if the integration of multiple bays with the process bus in a DES is considered. In this case, it is required that the communication infrastructure used be able to tolerate and process the levels of information that it will face.
- **Greater information management:** A large traffic volume requires greater control, particularly when its totality is not necessarily relevant for all devices that are part of the DES infrastructure. Therefore, it is necessary to perform engineering work that optimally guides the information to be exchanged exclusively between the devices that require it. This reduces the processing load and mitigates the risks of loss or saturation in the network due to high volumes of data.
- **Greater IT security management:** The simplicity of the system and its accessibility to its devices also imply a risk that must be controlled in DESs. Therefore, it is necessary to implement effective cybersecurity and access control policies for the different devices to mitigate the risks of vulnerability or unwanted actions in the operation of DESs.

However, the use of emerging solutions and the development or implementation of communication architectures optimized for DESs also bring aspects that can be considered as possible challenges or risks associated with these processes. The following are some of the most important aspects.

- **Cybersecurity:** By centralizing control and using programmable networks, substations become more vulnerable to cyberattacks, which could compromise critical protection and control systems.
- **Single point of failure:** Consolidating functions on a single device or server (CPC or SDN) means that a failure in the centralized system could affect multiple protections and controls simultaneously.
- **Implementation complexity:** SDN networks and programming protections in CPC require advanced architecture and trained personnel, which can initially increase the complexity of deployment and maintenance.
- **Latency:** In solutions such as SDN and CPC or VPAC, network latency can affect the response time of protection systems, compromising the speed of actions in the event of power grid failures.
- **Interoperability:** Although SDN and CPC improve interoperability, the integration of technologies from multiple manufacturers can generate incompatibilities or communication problems if standards are not met adequately.

- Virtualization reliability: Virtual environments could generate risks related to the stability and performance of the underlying hardware, compromising critical operations if infrastructure failures occur.

To mitigate this, it is essential to implement advanced cybersecurity measures and continuous monitoring to detect threats. In addition, it is advisable to ensure redundancy in hardware and software to avoid a single point of failure. In turn, it is essential to adequately train personnel to handle the technical complexity of these technologies. Network optimization is crucial to ensure fast response times in protection systems. It is also essential to conduct thorough interoperability testing between devices from different manufacturers before implementation and maintain constant monitoring of the overall system. These strategies will ensure the safety, resilience, and operational efficiency of DESs.

6. Conclusions

This paper presented an analysis of the conventional communication architectures used in DESs. The study was carried out locally, where cost reduction and resource improvement are required for construction and operations. The results obtained in this study lead to the following conclusions:

- The study and characterization of communication technologies and architectures currently applied to DESs show that companies incur significant costs associated with excessive redundancies in communication equipment and protocols. Limitations of this research include reliance on laboratory tests, limiting generalizability, and cost estimates based on average vendor data.
- DESs require experts to design, operate, and maintain facilities. Knowledge of the communication component is relevant for selecting technologies, designing, and configuring different elements of DESs. Therefore, specialized courses are required to qualify people for employment in these facilities.
- The appropriate use of technology and knowledge on topics such as SDN or centralized protections can represent an important advance in optimizing the use and performance of these systems.
- Communication architectures for DESs, which integrate conventional architectures with redundancy protocols, efficient traffic management, and technologies for centralized protection in electrical substations, reduce costs in new implementations, and evaluate the performance of the different components of a DES to make implementation viable.
- It is crucial to communicate the knowledge gained from the experience in utilities to regulatory entities. These entities are important in incentivizing investments in such topologies, leading to improved service quality, CO₂ emission indicators, cybersecurity, and overall profitability of companies. These findings support improved service quality and profitability through optimized DES designs.

Author Contributions: Conceptualization, O.A.T.-R., P.A.D.-V. and L.F.Q.-H.; methodology, O.A.T.-R., O.D.D.-M. and J.E.C.-B.; formal analysis, H.A.F.-C., J.E.C.-B. and O.D.D.-M.; investigation, O.A.T.-R., P.A.D.-V. and L.F.Q.-H.; resources, L.F.Q.-H. and H.A.F.-C.; writing—original draft preparation, O.A.T.-R., P.A.D.-V. and J.E.C.-B.; writing—review and editing, O.A.T.-R. and J.E.C.-B.; visualization, O.A.T.-R. and J.E.C.-B.; supervision, O.D.D.-M. and P.A.D.-V.; project administration, L.F.Q.-H. and H.A.F.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Datasets used in this article can be found in the following repositories: GOOSE-Secure: Test data with GOOSE messaging on physical infrastructure operating in a controlled environment, where spoofing attacks have been generated for behavioral analysis. Available online: <https://ieee-dataport.org/documents/goose-secure> (accessed on 28 February 2025). Process Bus Scalability with MU and Emulated SV: Data set generated with physical infrastructure and traffic simulators, to evaluate SV's characteristics and analyze the communication network's responsiveness to different levels of traffic. Available online: <https://ieee-dataport.org/documents/process-bus-scalability-mu-and-emulated-sv> (accessed on 28 February 2025).

Acknowledgments: The authors thank the Industrial Automation and Communications Laboratory—LACI—and the Universidad Nacional de Colombia Sede Medellín for the support provided to perform this research.

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

References

1. Aftab, M.A.; Hussain, S.M.; Ali, I.; Ustun, T.S. IEC 61850 based substation automation system: A survey. *Int. J. Electr. Power Energy Syst.* **2020**, *120*, 106008. [\[CrossRef\]](#)
2. Guo, R. Design and Optimization of Digital Substation Integrated Automation System Based on Improved Genetic Algorithm. In Proceedings of the Proceedings—2023 International Conference on Power, Electrical Engineering, Electronics and Control, PEEEC 2023, Athens, Greece, 25–27 September 2023; pp. 41–46. [\[CrossRef\]](#)
3. Aljohani, T.; Almutairi, A. Modeling Time-Varying Wide-Scale Distributed Denial of Service Attacks on Electric Vehicle Charging Stations. *Ain Shams Eng. J.* **2024**, *15*, 102860. [\[CrossRef\]](#)
4. Ashraf, S.; Shawon, M.H.; Khalid, H.M.; Muyeen, S.M. Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat Towards Smart Substation Pathways. *Sensors* **2021**, *21*, 6415. [\[CrossRef\]](#) [\[PubMed\]](#)
5. Efiog, J.E.; Akinwale, A.; Akinyemi, B.O.; Olajubu, E.; Aderounmu, S. CyberGrid: An IEC61850 Protocol-Based Substation Automation Virtual Cyber Range for Cybersecurity Research in the Smart Grid. *Cyber-Phys. Syst.* **2024**, *11*, 47–66. [\[CrossRef\]](#)
6. Rahat, R.M.; Hasan Imam, M.; Das, N. Comprehensive Analysis of Reliability and Availability of Sub-Station Automation System with IEC 61850. In Proceedings of the 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 10–12 January 2019; pp. 406–411. [\[CrossRef\]](#)
7. Vardhan, H.; Ramlachan, R.; Szela, W.; Gdowik, E. Deploying digital substations: Experience with a digital substation pilot in North America. In Proceedings of the 2018 71st Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 26–29 March 2018; pp. 1–9. [\[CrossRef\]](#)
8. *Std. IEC 61850*; Communication Networks and Systems for Power Utility Automation. International Electrotechnical Commission: Geneva, Switzerland, 2023.
9. Tobar-Rosero, O.A.; Roa-Romero, O.A.; Rueda-Carvajal, G.D.; Leal-Piedrahita, A.; Botero-Vega, J.F.; Gutierrez-Betancur, S.A.; Branch-Bedoya, J.W.; Zapata-Madrigal, G.D. GOOSE Secure: A Comprehensive Dataset for In-Depth Analysis of GOOSE Spoofing Attacks in Digital Substations. *Energies* **2024**, *17*, 6098. [\[CrossRef\]](#)
10. Daboul, M.; Orságová, J. Evaluation IEC 61850 Protocols based Protection Schemes of Digital Substation. In Proceedings of the 2023 23rd International Scientific Conference on Electric Power Engineering, EPE 2023, Brno, Czech Republic, 24–26 May 2023. [\[CrossRef\]](#)
11. Mlynec, P. Communication Testbed for Smart Substations. *Int. Congr. Ultra Mod. Telecommun. Control. Syst. Work.* **2022**, *2022*, 128–132. [\[CrossRef\]](#)
12. Soares, A.A.; Lopes, Y.; Fernandes, N.C.; Muchaluat-Saade, D.C.; Mosse, D. Enabling Digital Twins for Smart Substation Networks. In Proceedings of the 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2023—Proceedings, Glasgow, UK, 31 October–3 November 2023. [\[CrossRef\]](#)
13. Ingalalli, A.; Silpa, K.S.; Gore, R. SCD based IEC 61850 traffic estimation for substation automation networks. In Proceedings of the 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, Cyprus, 12–15 September 2017; pp. 1–8. [\[CrossRef\]](#)
14. Ustun, T.S.; Aftab, M.A.; Ali, I.; Hussain, S.M.S. A Novel Scheme for Performance Evaluation of an IEC 61850-Based Active Distribution System Substation. *IEEE Access* **2019**, *7*, 123893–123902. [\[CrossRef\]](#)
15. Tobar Rosero, O.A.; Santamaria Isaza, R.J.; Dario Zapata Madrigal, G.; Olaya, J.C. Relevant aspects for interoperability in electrical substations under implementation of process bus IEC 61850-9-2 with multi-vendor devices. In Proceedings of the 2019 FISE-IEEE/CIGRE Conference—Living the energy Transition (FISE/CIGRE), Medellin, Colombia, 4–6 December 2019; IEEE: Piscataway, NJ, USA, 2019.

16. Habib, H.; Fawzy, N.; Brahma, S. Hardware in the Loop Testing of a Protection Scheme for Microgrid using RTDS with IEC 61850 Protocol. In Proceedings of the 2020 IEEE Industry Applications Society Annual Meeting, Detroit, MI, USA, 10–16 October 2020; pp. 1–8. [\[CrossRef\]](#)
17. Ingram, D.M.E.; Schaub, P.; Taylor, R.R.; Campbell, D.A. Performance Analysis of IEC 61850 Sampled Value Process Bus Networks. *IEEE Trans. Ind. Inform.* **2013**, *9*, 1445–1454. [\[CrossRef\]](#)
18. Valtari, J.; Verho, P.; Hakala-Ranta, A.; Saarinen, J. Increasing cost-efficiency of substation automation systems by centralised protection functions. In Proceedings of the IET Conference Publications, Dublin, Ireland, 10–11 June 2009; IET: London, UK, 2009.
19. Santos, G.R.; Zancul, E. A framework to assess the impacts of digital electrical substations. *Smart Energy* **2023**, *12*, 100125. [\[CrossRef\]](#)
20. Cabral, E.A.; Tofoli, F.L.; Sampaio, R.F.; Leão, R.P.S. Reliability assessment applied in the design of an industrial substation in the context of Industry 4.0. *Electr. Power Syst. Res.* **2024**, *231*, 110365. [\[CrossRef\]](#)
21. Vasudevan, B.; Groat, J.; Vandiver, B. Testing Challenges of a Complete PAC Digital Substation. In Proceedings of the 2023 76th Annual Conference for Protective Relay Engineers, CFPR 2023, College Station, TX, USA, 27–30 March 2023. [\[CrossRef\]](#)
22. Xu, L.; Li, H.; Dong, F.; Zhou, Y. Evaluación de los Métodos de Control de Flujo de Datos y su Rendimiento en Subestaciones Digitales basadas en IEC61850. In Proceedings of the 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China, 21–24 October 2019; pp. 1408–1412. [\[CrossRef\]](#)
23. Stinskiy, A.; de Oliveira, E. Digital Substation with Process Bus—A Comparative Review of IEC61850-9-2 and IEC 61869-9 Standards. In Proceedings of the 2024 77th Annual Conference for Protective Relay Engineers (CFPR), College Station, TX, USA, 25–28 March 2024; pp. 1–5. [\[CrossRef\]](#)
24. Zhang, Y.; Cai, Z.; Li, X.; He, R. Analytical Modeling of Traffic Flow in the Substation Communication Network. *IEEE Trans. Power Deliv.* **2015**, *30*, 2119–2127. [\[CrossRef\]](#)
25. Oliveira, L.B.; Zapella, M.; Sarda, A.; Zanatta, W. Managed Ethernet switches performance over IEC 61850 networks: Applications with high traffic flow. In Proceedings of the 13th International Conference on Development in Power System Protection 2016 (DPSP), Edinburgh, UK, 7–10 March 2016; pp. 1–6. [\[CrossRef\]](#)
26. Praveen, A.N.; Swarup, K.S.y.S.S. Cálculo de la latencia de comunicación en una subestación compleja basada en IEC 61850. In Proceedings of the 2021 9th Conferencia Internacional IEEE sobre Sistemas de Potencia (ICPS), Kharagpur, India, 16–18 December 2021. [\[CrossRef\]](#)
27. Steinhäuser, F.; Wiecha, A. Behaviour of IEC 61850 protection relays under degraded network traffic conditions. In Proceedings of the 16th International Conference on Developments in Power System Protection (DPSP 2022), Newcastle, UK, 7–10 March 2022; Volume 2022; pp. 268–272. [\[CrossRef\]](#)
28. Comisión-Nacional-de Energía, C. ANEXO TÉCNICO—Exigencias Mínimas de Diseño de Instalaciones de Transmisión, 2020. CNE-Chile. Available online: <https://www.cne.cl/wp-content/uploads/2020/09/EXIGENCIAS-M> (accessed on 22 July 2024).
29. Operador Nacional del Sistema Eléctrico, O. Submódulo 2.11—Requisitos mínimos para os sistemas de proteção, de registro de perturbações e de teleproteção, 2024. Despacho ANEEL n° 1.580/2024. Available online: https://www2.aneel.gov.br/cedoc/adsp20241580_2_1.pdf (accessed on 22 July 2024).
30. Arias-Giraldo, T. Evaluación, Selección y análisis de Arquitecturas de Comunicación para Subestaciones Digitales y su Aplicación en Empresas del Sector Eléctrico. Master's Thesis, Universidad Nacional de Colombia—sede Medellín, Medellín, Colombia, 2020.
31. Samitier, C. *Utility Communication Networks and Services*; Springer International Publishing: Cham, Switzerland, 2017. [\[CrossRef\]](#)
32. Docquier, T.; Song, Y.Q.; Chevrier, V.; Pontnau, L.; Ahmed-Nacer, A. Performance evaluation methodologies for Smart Grid Substation Communication Networks: A survey. *Comput. Commun.* **2023**, *198*, 228–246. [\[CrossRef\]](#)
33. Ayello, M.; Lopes, Y. Interoperability based on IEC 61850 standard: Systematic literature review, certification method proposal, and case study. *Electr. Power Syst. Res.* **2023**, *220*, 109355. [\[CrossRef\]](#)
34. Santos, G.R.; Zancul, E.; Manassero, G.; Spinola, M. From conventional to smart substations: A classification model. *Electr. Power Syst. Res.* **2024**, *226*, 109887. [\[CrossRef\]](#)
35. IEC/TC57; Communication Networks and Systems for Power Utility Automation—Part 90-4: Network Engineering Guidelines. International Electrotechnical Commission: London, UK, 2020. Available online: www.iec.ch (accessed on 28 February 2025)
36. De Klerk, M.L.; Saha, A.K. A Review of the Methods Used to Model Traffic Flow in a Substation Communication Network. *IEEE Access* **2020**, *8*, 204545–204562. [\[CrossRef\]](#)
37. Gómez-Luna, E.; Tobar-Rosero, O.A.; Piñeros-Saldarriaga, J.F.; Hernández-Fúquene, F.; Quintero-Pineda, M.; Castillo-Bautista, W.; Molina-Castro, J.D.; Giraldo-Arenas, C.M. Implementation of the IEC 61850 standard in Colombia—Requirements and challenges in the implementation of digital substations. *ELECTRA* October 2024.
38. Muñoz, P. La Digitalización es el Siguiente Paso en la Evolución de las Subestaciones Eléctricas—CIGRE—Comité Chileno, 2020. Available online: <https://www.cigre.cl/2020/09/03/la-digitalizacion-es-el-siguiente-paso-en-la-evolucion-de-las-subestaciones-electricas/> (accessed on 28 February 2025).

39. IEC 62439-3; Industrial Communication Networks—High Availability Automation Networks—Part 3: Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR). International Electrotechnical Commission: Geneva, Switzerland, 2021.
40. CIGRE-Colombia WG 5.8. Necesidades, Requerimientos y Desafíos en la Implementación de Subestaciones Digitales en Colombia (Implementación del estándar IEC 61850), 2020. Available online: <http://www.cigrecolombia.org/Documents/Documentos-t%C3%A9cnicos/DT-B5.8-Subestaciones%20digitales.pdf> (accessed on 5 July 2023).
41. Das, N.; Islam, S. Analysis of power system communication architectures between substations using IEC 61850. In Proceedings of the 5th Brunei International Conference on Engineering and Technology (BICET 2014), Bandar Seri Begawan, Brunei, 1–3 November 2014; Institution of Engineering and Technology: London, UK, 2014.
42. Bouffard-Vercelli, Y.E.; Andre, B. Future Architectures of Electrical Substations. In Proceedings of the Petroleum and Chemical Industry Conference Europe Conference Proceedings, PCIC EUROPE, Düsseldorf, Germany, 17–19 July 2021. [CrossRef]
43. Gutiérrez, S.A.; Botero, J.F.; Gómez, N.G.; Fletscher, L.A.; Leal, A. Next-Generation Power Substation Communication Networks: IEC 61850 Meets Programmable Networks. *IEEE Power Energy Mag.* **2023**, *21*, 58–67. [CrossRef]
44. Leal, A.; Durán, M.; Botero, J.F. Reliability provision in software defined power substations communication networks. *Comput. Netw.* **2020**, *181*, 107560. [CrossRef]
45. Molina, E.; Jacob, E.; Matias, J.; Moreira, N.; Astarloa, A. Using Software Defined Networking to manage and control IEC 61850-based systems. *Comput. Electr. Eng.* **2015**, *43*, 142–154. [CrossRef]
46. Cankaya, H.C. Software Defined Networking and Virtualization for Smart Grid. In *Transportation and Power Grid in Smart Cities*; John Wiley & Sons.: Hoboken, NJ, USA, 2018; pp. 171–190. [CrossRef]
47. Makrakis, G.M.; Roberson, D.; Kolias, C. WIPP: Towards IEC 62443-3-3 Network Compliance via Software-Defined Networking in Digital Substations. In *2023 Resilience Week, RWS 2023*; IEEE: Piscataway, NJ, USA, 2023. [CrossRef]
48. Girdhar, M.; Hong, J.; Su, W.; Herath, A.; Liu, C.C. SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid. In Proceedings of the 2024 IEEE Power & Energy Society General Meeting (PESGM), Seattle, WA, USA, 21–25 July 2024; pp. 1–5. [CrossRef]
49. Mustafa, H.M.; Basumallik, S.; Fetsick, R.; Srivastava, A. Using SDN to Enhance Cyber Resiliency in IEC 61850-based Substation OT Networks. In Proceedings of the 2023 IEEE International Conference on Energy Technologies for Future Grids, ETFG 2023, Wollongong, Australia, 3–6 December 2023. [CrossRef]
50. Ayodele, B.; Buttigieg, V. SDN as a defence mechanism: A comprehensive survey. *Int. J. Inf. Secur.* **2024**, *23*, 141–185. [CrossRef]
51. Makrakis, G.M.; Roberson, D.; Kolias, C.; Cook, D. Evaluation of SDN security measures in the context of IEC 62443-3-3. *Int. J. Crit. Infrastruct. Prot.* **2024**, *47*, 100716. [CrossRef]
52. Sanchez-Acevedo, S.; D’Arco, S. A SDN Based Method for Blocking Malicious Attacks on Digital Substations Communication. In Proceedings of the Proceedings—2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems, ICPS 2022, Coventry, UK, 24–26 May 2022. [CrossRef]
53. Leal, A.; Botero, J.F. Defining a Reliable Network Topology in Software-Defined Power Substations. *IEEE Access* **2019**, *7*, 14323–14339. [CrossRef]
54. Das, R.; Kanabar, M.; Adamiak, M.; Apostolov, A.; Antonova, G.; Brahma, S.; Zadeh, M.D.; Hunt, R.; Jester, J.; Kezunovic, M.; et al. Advancements in Centralized Protection and Control Within a Substation. *IEEE Trans. Power Deliv.* **2016**, *31*, 1945–1952. [CrossRef]
55. Work-Group, IEEE PES PSRC K15 Centralized Substation Protection & Control | Report of Working Group K15 of the Substation Protection Subcommittee, 2019. IEEE PES. Available online: <https://www.pacw.org/centralized-substation-protection-control> (accessed on 6 September 2024).
56. Halim, S.B.A.; Hatta, M.K.B.M.; Hussein, H.H.B.W.; Shafe’i, F.B.; Azmi, N.A.B.; Othman, F.B. Centralized Protection and Control (CPC): Next Level Of Electrical Protection System Towards Digital Substation (Oil and Gas). In Proceedings of the 2023 IEEE 3rd International Conference in Power Engineering Applications: Shaping Sustainability Through Power Engineering Innovation, ICPEA 2023, Putrajaya, Malaysia, 6–7 March 2023; pp. 285–290. [CrossRef]
57. Wójtowicz, R.; Kowalik, R.; Rasolomampionona, D.D. Next generation of power system protection automation-Virtualization of protection systems. *IEEE Trans. Power Deliv.* **2018**, *33*, 2002–2010. [CrossRef]
58. Carvalho, R.; Antunes, M.; Barraca, J.P.; Gomes, D.; Aguiar, R.L. Design and Evaluation of a Low-Latency CPC Environment for Virtual IEDs. In Proceedings of the 2022 IEEE Conference on Cloud Networking 2022, CloudNet 2022, Paris, France, 7–10 November 2022; pp. 272–276. [CrossRef]
59. Rahman, A.; Yilmaz, O.; Vaze, O.; Mandal, A. Smart Substation Control and Protection Facilitating the Virtualization of Multiple Protection and Control. In Proceedings of the 2023 IEEE International Conference on Energy Technologies for Future Grids, ETFG 2023, Wollongong, Australia, 3–6 December 2023. [CrossRef]

60. Aleixo, A.C.; Jorge, R.D.; Gomes, F.; Antunes, L.; Barraca, J.P.; Carvalho, R.; Antunes, M.; Gomes, D.; Gouveia, C.; Carrapatoso, A.; et al. Challenges and considerations for the design and implementation of a centralized protection and control solution for MV networks. In *IET Conference Proceedings*; The Institution of Engineering and Technology: Stevenage, UK, 2023; pp. 3328–3332. [\[CrossRef\]](#)
61. Ganoo, P.; Joshi, S.; Valtari, J.; Niveri, H. Centralized Protection and Control System: Are We Ready for Deployment in the Chemical, Oil, and Gas Industry? *IEEE Ind. Appl. Mag.* **2022**, *28*, 48–61. [\[CrossRef\]](#)
62. Torres, E.; Eguia, P.; Abarrategi, O.; Larruskain, D.M.; Valverde, V.; Buigues, G. Trends in Centralized Protection and Control in Digital Substations. In *Proceedings of the 21th International Conference on Renewable Energies and Power Quality (ICREPQ'23)*, Madrid, Spain, 24–26 May 2023. [\[CrossRef\]](#)
63. Valtari, J.; Joshi, S. Centralized Protection and Control. ABB—White Paper 2020. Available online: <https://www.pacw.org/centralized-protection-control-uncovering-the-potential> (accessed on 28 February 2025).
64. Flores, E.; Xavier, J.; Niveri, H. Centralized Protection and Control-Enhancing Reliability, Availability, Flexibility and Improving Operating Cost-Efficiency of Distribution Substations. ABB. White Paper 2023. Available online: https://library.e.abb.com/public/6b4a135b4c0f4e7f9b4898bdfca37131/White_paper_SSC600_2NGA001420_ENa.pdf (accessed on 28 February 2025).
65. Nhung-Nguyen, H.; Girdhar, M.; Kim, Y.H.; Hong, J. Machine-Learning-Based Anomaly Detection for GOOSE in Digital Substations. *Energies* **2024**, *17*, 3745. [\[CrossRef\]](#)
66. Eynawi, A.; Mumrez, A.; Elbez, G.; Hagenmeyer, V. Machine Learning-Based Feature Selection for Intrusion Detection Systems in IEC 61850-Based Digital Substations. In *Proceedings of the 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2024*, Oslo, Norway, 17–20 September 2024; pp. 1–7. [\[CrossRef\]](#)
67. Li, J.; Su, H.; Zhang, Y.; Yan, Q.; Liu, L.; Wang, T. Smart Digital Inspection and Maintenance of Substations. In *Proceedings of the 2024 5th International Conference on Power Engineering, ICPE 2024*, Shanghai, China, 13–15 December 2024; pp. 388–393. [\[CrossRef\]](#)
68. Yegorov, P.K.; Lackovitch, A.; Dean, E.; Mustafa, H.M.; Basumallik, S.; Srivastava, A. Analyzing GOOSE Security in IEC61850-based Substation Using ML, SDN and Digital Twin. In *Proceedings of the 2023 North American Power Symposium, NAPS 2023*, Asheville, NC, USA, 15–17 October 2023. [\[CrossRef\]](#)
69. Tobar-Rosero, O.A. GOOSE Secure | Dataset, 2024. Available online: <https://iee-dataport.org/documents/goose-secure> (accessed on 28 February 2025).
70. Posada-Corrales, J.M. Process Bus Scalability with MU and Emulated SV | Dataset, 2025. Available online: <https://iee-dataport.org/documents/process-bus-scalability-mu-and-emulated-sv> (accessed on 28 February 2025).
71. Tobar-Rosero, O.A.; Candelo-Becerra, J.E.; Zapata, G. Performance analysis of overcurrent protection in a digital substation with process bus. *Sustain. Sci. Pract. Policy* **2022**, *14*, 7958. [\[CrossRef\]](#)
72. Fernandez, J.S.C.; Carvajal, G.D.R.; Rosero, O.A.T.; Becerra, J.E.; Madrigal, G.D.Z.; Sierra, R.G. Dynamic Protection Scheme in a Digital Environment of Electrical Systems. In *Proceedings of the Proceedings—2023 IEEE Latin-American Conference on Communications, LATINCOM 2023*, Panama City, Panama, 17–19 November 2023. [\[CrossRef\]](#)
73. Justino, F.M.; Tobar-Rosero, O.A.; Rueda-Carvajal, G.D.; Diaz-Vargas, P. Análisis de interoperabilidad y rendimiento con sistema de control y protección centralizado en subestaciones digitales: Un estudio de caso con el SSC600 de ABB. XVII SEMINÁRIO TÉCNICO DE PROTEÇÃO E CONTROLE, Oct. 2024. Available online: <https://stpc.com.br/programacao/> (accessed on 28 February 2025).
74. Óscar A Tobar Rosero.; Darío, G.; Carvajal, R.; Andrés, H.; Célis, F.; González, E.P.; Felipe, J.; Vega, B.; Bedoya, J.W.B. Importancia de la gestión del tráfico como una primera medida de ciberseguridad en redes inteligentes. In *Proceedings of the Encuentro Internacional de Educación en Ingeniería*, Cartagena, Colombia, 24–27 September 2024; pp. 1–13. [\[CrossRef\]](#)
75. Thompson, A.C. The Future of Substations: Centralized Protection and Control. Ph.D. Thesis, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA 2016.
76. Udren, E.A.; Vandiver, B.; Anderson, J.; Antonova, G.; Apostolov, A.; Beaumont, P.; Beresh, R.; Brunner, C.; Calero, F.; Chelmecki, C.; et al. Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations: Report of Working Group P6 of the Power System Communications and Cybersecurity Committee of the Power and Energy Society of IEEE. In *Proceedings of the 2021 74th Conference for Protective Relay Engineers, CPRE 2021*, College Station, TX, USA, 22–25 March 2021. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.