ISSN: 1692-7257 - Volume 2 – Number 46 - 2025

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Digital Object Identifier: 10.24054/rcta.v2i46.4101

Digital substations: driving sustainability and cybersecurity in the power sector through emerging solutions

Subestaciones digitales: impulsando la sostenibilidad y ciberseguridad para el sector eléctrico a partir de soluciones emergentes

MSc. Oscar Andrés Tobar Rosero [1], **MSc. Luis Fernando Quintero Henao** [2]
PhD. Ernesto Pérez González [1]

[1] ***Universidad Nacional de Colombia****, sede Medellín, Medellín, Antioquia, Colombia.*
[2] ***Enterprise Innovation,*** *Medellín, Antioquia, Colombia.*

Correspondence: *oatobarr@unal.edu.co*

Received: *april 24, 2025.* ***Accepted:*** *july 03, 2025.* ***Published:*** *july 21, 2025.*

How to cite: *O. A. Tobar Rosero, L. F. Quintero Henao, and E. Pérez González, "Digital substations: driving sustainability and cybersecurity in the power sector through emerging solutions", RCTA, vol. 2, no. 46, pp. 132–140, Jul. 2025.*
Recovered from https://ojs.unipamplona.edu.co/index.php/rcta/article/view/4101

Abstract: the digitalization of power substations has become a key component in the modernization of electrical networks, especially within the global transition toward more sustainable and efficient energy systems. This article examines the role of digital substations (DSs) and how their implementation, based on the IEC 61850 standard, enables greater automation, integration, and real-time data analysis. Through the integration of emerging technologies such as Software-Defined Networking (SDN), Blockchain, Machine Learning (ML), and Network Function Virtualization (NFV), DSs not only improve network management and security but also enhance resilience against cyber threats and facilitate the integration of renewable energy sources. This study discusses the main technical and economic challenges associated with adopting these technologies, including cybersecurity, interoperability with legacy systems, and modernization costs, particularly in emerging economies. Additionally, it highlights the opportunities that DSs offer for building smarter and more decentralized electric grids, as exemplified by the Colombian case. The article presents a balanced overview of both the benefits and limitations of implementing digital substations.

Keywords: digital substations, cybersecurity, emerging technologies, communication systems, electric power systems, digital transformation.

Resumen: la digitalización de las subestaciones eléctricas, basada en el estándar IEC 61850, representa un eje fundamental en la modernización de las redes eléctricas hacia sistemas más sostenibles, eficientes y seguros. Este artículo examina el papel de las subestaciones digitales y el impacto de tecnologías emergentes como Software-Defined Networking (SDN), Blockchain, aprendizaje automático (ML) y la virtualización de funciones de red (NFV) en la automatización, análisis en tiempo real y resiliencia frente a amenazas cibernéticas. Se abordan los desafíos asociados a su implementación, incluyendo la interoperabilidad con sistemas legados, los riesgos de ciberseguridad y los costos de modernización, con énfasis en economías emergentes. Asimismo, se identifican oportunidades para avanzar hacia redes más descentralizadas e inteligentes, destacando el caso colombiano como referencia. El análisis ofrece una visión integral sobre las barreras y beneficios de estas tecnologías en la transición hacia infraestructuras eléctricas digitales, interoperables y resilientes.

Palabras clave: subestaciones digitales, ciberseguridad, tecnologías emergentes, sistemas de comunicación, sistemas eléctricos, transformación digital.

1. INTRODUCTION

Digital substations (DSs) have emerged as a cornerstone in the digital transformation of the power sector, driving the modernization of energy networks toward more efficient, secure, and sustainable systems [1]. This process takes place within a global context of energy transition, where the integration of advanced technologies is essential to meet the growing demand for renewable energy and address associated cybersecurity challenges [2].

The digitalization of electrical substations represents one of the most significant changes in the power sector in recent years. Leveraging open standards such as IEC 61850, the implementation of DSs has led to the development of new systems and technological solutions that aim to improve response capabilities, event management, and automate multiple operational processes [3].

At the same time, DSs have encouraged the integration of other types of systems for power generation, monitoring, management, and end-use (see Fig. 1). Due to the features of the IEC 61850 standard, centralized supervision, protection, and control can be carried out for distributed generation systems, microgrids, and legacy systems. Moreover, it enables the management of operational data and cybersecurity for such systems [4].

Additionally, digitalization contributes to asset management optimization and reduction of operational costs through the incorporation of sensors and advanced monitoring systems. This capability opens up a range of opportunities in the power sector, facilitating rapid fault responses, advanced automation, optimized predictive maintenance, and enhanced resilience of critical infrastructure [5], [6]. In countries such as Colombia, DSs are positioned as key tools for modernizing the electric system, aligned with national strategies for cybersecurity and energy sustainability.

In this context, cybersecurity emerges as a central component in the digitalization of critical infrastructures, such as the power sector. The growing interconnection and automation of DSs, together with their reliance on real-time communication systems, make them particularly vulnerable to cyber threats. From denial-of-service attacks to intrusions compromising the integrity of operational data, protecting these infrastructures requires specialized measures, updated regulations, and the integration of advanced technological solutions [7]. Thus, cyber-resilience becomes an essential pillar for ensuring the sustainability of these systems, guaranteeing operational continuity and security in digitized electrical environments.

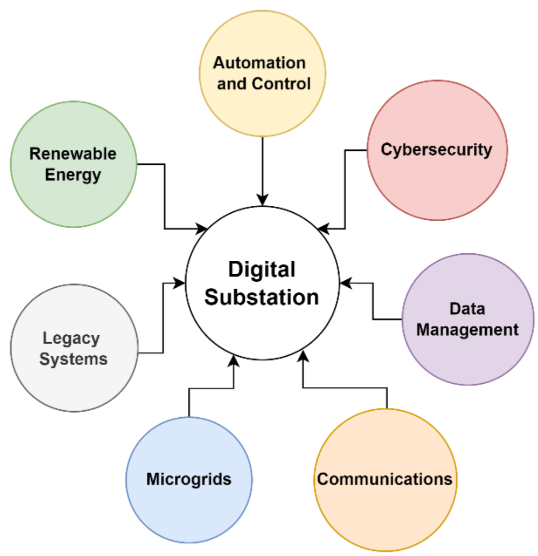

Fig. 1. *Digital substation as a point of integration for multiple systems and technological solutions in the power sector.*
Source: *authors' elaboration.*

This article analyzes the strategic role of DSs in this transformation, exploring emerging solutions that enable their implementation, their impact on the energy transition, and the associated challenges and opportunities. It examines their evolution from conventional models based on analog components to digital architectures supported by the IEC 61850 standard, which optimize communication and real-time control. This transition improves interoperability, automation, and data availability for advanced analytics, transforming substations into intelligent nodes within the power grid. Finally, the paper introduces the analysis of emerging technologies applicable to DSs, aimed at mitigating vulnerabilities and optimizing processes through specialized digital capabilities.

2. CONTEXT AND METHODOLOGICAL APPROACH

Electrical substations serve to transform, control, and distribute electrical energy within the grid, ensuring the balance between generation and consumption. They bring together multiple systems from both the generation and end-use sides, all of which must be monitored, controlled, and protected, along with the associated electrical infrastructure [1]. In this context, the transition from conventional to digital substations has represented a paradigm shift, enabling the use of communication systems to link the various protection, control, automation, and monitoring components within electrical substations.

However, this transformation entails several implications, particularly from the perspective of power systems engineering. The operation and maintenance of digital substations require a sound understanding of communication systems, the protocols used for information exchange between devices, and at least basic knowledge of how to manage the communication infrastructure appropriately (see Fig. 2) [8]. In turn, physical and logical redundancy schemes, along with cybersecurity management, are essential pillars for the secure and reliable development of digital substations [9]. Accordingly, multiple studies and proposals have focused on the performance of these systems, reliability challenges, and vulnerability analysis based on various DS configurations [10].

Numerous investigations have identified critical weaknesses or vulnerabilities in communication systems that are essential to the development of digital substations. A notable example is the limited capacity to manage the communication infrastructure used in current operational technologies, which restricts scalability and the efficiency of real-time data transmission [11]. Likewise, a detailed analysis of standardized communication protocols under the IEC 61850 framework reveals that, although they facilitate information exchange between devices, they also exhibit significant vulnerabilities [12]. The lack of robust authentication mechanisms in these protocols can be exploited through various attacks, compromising data integrity and, consequently, the secure operation of DSs.

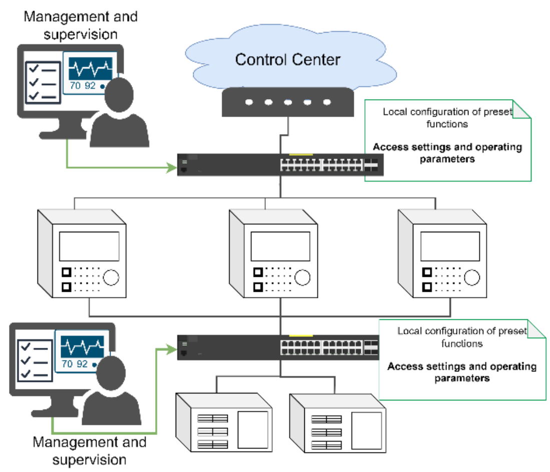

Fig. 2. *Basic architecture of a digital substation, comprising the process, protection, control, and supervision levels.*
Source: *authors' elaboration.*

Although standards such as IEC 62443 and IEC 62351 provide guidelines to ensure secure integration in industrial systems and smart grids, the performance requirements established to guarantee the reliability of DSs often limit the adoption of robust cybersecurity configurations and protocols in these systems [13], [14].

This article employs a mixed-methodological approach, combining both qualitative and quantitative methods, to analyze emerging technologies in communication and cybersecurity systems, examining their impact on the digitalization of electrical substations. The stages of this approach are outlined below:

- Systematic literature review
- Analysis: Use cases and technological evolution
- Characterization of emerging technologies
- Discussion: Opportunities and challenges for the power sector derived from emerging technologies

The research is based on a systematic review of recent scientific, technical, and regulatory literature on digital substations, with a focus on the communication protocols considered in the IEC 61850 standard and their cybersecurity implications. Additionally, this process is complemented by an analysis of selected case studies involving the implementation of digital substations in different regions, with emphasis on Latin American experiences, such as the case of Colombia.

As a result of this analysis, an overview is provided of the evolution from conventional electrical substations to digitized environments, highlighting the importance of communication systems as a structural axis. In turn, some of the main emerging technologies that can be integrated into digital substations are identified and described, emphasizing their key attributes and potential benefits for the power sector.

Finally, a discussion is presented on the main challenges and opportunities arising from the digital transformation in the power sector, and the emerging technological solutions are analyzed.

3. SUSTAINABILITY AND CYBERSECURITY IN THE POWER SECTOR THROUGH SYSTEM DIGITALIZATION

To address sustainability and cybersecurity, it is essential to first establish the level of technological adoption surrounding digital substations (DSs). This allows us to identify a medium to high level of maturity globally, based on multiple documented deployments, particularly in Europe, the United States, and Asia.
For example, operators such as Landsnet in Iceland deployed a significant number of fully digital substations (220–66 kV) in 2023, based on IEC 61850, with low-power instrument transformers and multi-vendor control systems [15]. In the United States and the United Kingdom, the deployment of digital substations is framed within government-led grid modernization programs. Moreover, National Grid (UK) and CFE (Mexico) have adopted IEC 61850-based solutions with GOOSE, MMS, Sampled Values, and PRP redundancy in multiple projects [16], [17].

Focusing on the Latin American region, ISA-CTEEP (Brazil) has stood out for its innovation initiatives, such as the first “Substation 4.0” inaugurated in São Paulo, which is part of a broader digitalization program across several substations operated by the company [18], [19].

Countries such as Mexico, Peru, and Chile have also made significant progress in implementing digital substations, in some cases even proposing preliminary regulatory frameworks to support the adoption of digital technologies in electrical substations [20].

In Colombia, major utility companies have led significant projects, such as the digitalization of the Chinú substation—the first interoperable process bus system in the country—and the Portugal substation (Bogotá), the first fully digital substation project nationwide. Additional projects have been deployed in Tolima, Valle del Cauca, and Antioquia [21], [22]. These examples reflect a clear trend toward the adoption of new technologies and the ongoing transformation within the sector.

Considering the challenges and opportunities presented by the implementation of digital substations in the power sector, it is essential to stay informed about the growing body of global research in this field [9], [23]. These studies have given rise to emerging solutions that, while presenting new challenges, also offer significant possibilities to accelerate digital transformation and advance sustainability goals in energy systems.

One of the most promising strategies is the integration of emerging technologies that can enhance both the operational functionality of DSs and their level of protection against cyber threats. Among these technologies, the following stand out:

- **Software-Defined Networking (SDN):** Enables dynamic and efficient management of communication networks in IEC 61850-based DSs. By decoupling the control and data planes, it provides greater flexibility for traffic management and redundancy scheme implementation, thereby enhancing resilience to cyberattacks and optimizing real-time communication [24], [25].
- **Blockchain:** Offers immutable and decentralized logging mechanisms, which are useful for preserving the integrity of operational and configuration data in DSs, reducing the risk of malicious tampering or accidental errors [26], [27].
- **Machine Learning (ML):** Facilitates real-time data flow analysis through algorithms capable of identifying anomalous patterns, detecting intrusions, and classifying critical events, contributing to cybersecurity decision-making and predictive maintenance [28], [29].
- **Network Function Virtualization (NFV):** Reduces physical infrastructure complexity by implementing network functions on virtualized platforms. This enables a simplified DS infrastructure, increased operational flexibility,

easier integration of heterogeneous solutions, and scalable evolution of the electrical network [30], [31].

The convergence of sustainability and cybersecurity in the power sector requires a comprehensive approach that combines technological innovation with operational rigor. The adoption of solutions such as SDN, Blockchain, ML, and NFV promotes the development of more innovative, more resilient, and more efficient substations, capable of addressing the growing energy and cybersecurity challenges of today's digital environment [28].

The adoption of emerging technologies in digital substations not only addresses technical demands related to modernization and cybersecurity but has also led to a variety of practical experiences and applied studies that validate their functionality in real-world environments. Several use cases have been documented in scientific literature, demonstrating the applicability of solutions such as SDN, ML, NFV, and Blockchain in IEC 61850-based substation operations.

One of the most notable experiences is the work by Girdhar et al. (2024), who proposed a cyber restoration framework for IEC 61850 substations based on SDN [32]. This architecture includes intrusion detection systems (IDS), a centralized SDN controller, and a dynamic port management system. Validated through real-time testing with hardware-in-the-loop (HIL) configurations, the solution demonstrated the ability to maintain operational continuity during cyberattacks, thereby reinforcing system resilience.

Additionally, the same authors developed a hybrid cybersecurity framework combining SDN and IDS to mitigate malicious GOOSE message injection attacks. This solution enables the detection of anomalous events and the automatic blocking of compromised ports, ensuring the integrity of the communications network [33].

Regarding NFV usage, the VirtuWind project (2019) serves as a key reference [34]. This initiative designed an architecture for critical industrial networks—applicable to digital substations—that integrates SDN and NFV to ensure quality of service (QoS), scalability, and function isolation. The architecture supports efficient real-time service management, which is essential for complex power systems.

From the perspective of substation automation, Leal et al. (2021) proposed the S3N architecture (Smart Solution for Substation Networks), which segments the network into three functional layers: infrastructure, virtualization, and services. This approach enables automatic IED configuration, dynamic traffic segmentation, and service adaptation, representing a significant step forward in the evolution of intelligent substations [35].

In the field of Machine Learning, several relevant initiatives have emerged. For instance, Yegorov et al. (2023) and Eynawi et al. (2024) demonstrated the use of anomaly detection and feature selection algorithms in digital substations to detect intrusions, spoofing attacks on GOOSE messages, and operational faults, offering a proactive approach to cybersecurity management [36], [37].

Meanwhile, many Blockchain-based applications remain in early stages or under development. Although there are architectural proposals aimed at managing protection settings through distributed ledgers, large-scale adoption of Blockchain in DSs is still limited due to operational constraints, latency, and interoperability requirements [38].

The use cases documented in recent literature confirm the technical feasibility of integrating solutions such as SDN, ML, and NFV in IEC 61850-based digital substations, contributing to greater automation, operational resilience, and cybersecurity. These experiences form a solid foundation for the future evolution of critical infrastructures, paving the way for smarter, more secure, and more sustainable power grids.

At the local level, the digitalization of substations in Colombia has facilitated the integration of renewable energy sources, aligning with national targets for reducing emissions. However, the implementation of DSs and other emerging technologies presents significant challenges, such as ensuring interoperability with legacy systems and mitigating cybersecurity risks, while also offering opportunities to innovate in sustainable power grid management.

Thus, this chapter provides a preliminary analysis of the outlook facing the power sector amid the digital transformation of multiple systems. As a particular case, it highlights the role of digital substations in redefining the operational paradigms of the electrical system, contributing not only to greater efficiency and security but also to the consolidation of a more sustainable, decentralized, and resilient energy model capable of addressing future contingencies, especially through the integration of emerging technologies.

4. DISCUSSION – CHALLENGES AND OPPORTUNITIES

The implementation of advanced communication systems and the integration of technological solutions, such as those previously described, not only modernize electrical substations but also transform them into dynamic and adaptive systems. These infrastructures are key to meeting the requirements of the energy transition, particularly regarding the growing use of renewable energy sources and the shift toward a decarbonized economy.

The digitalization of substations serves as a strategic pillar in this process, enabling the optimization of microgrid management and facilitating an efficient transition toward decentralized power networks. In this context, the analytical capabilities of digital solutions enhance the prediction of consumption and generation patterns, providing critical information for the formulation of sustainable energy policies.

However, this progress entails a series of technical and strategic challenges that must be addressed rigorously. Notable among these are:

Cybersecurity: The increasing connectivity of digital systems exposes substations to significant risks, such as distributed denial-of-service (DDoS) attacks or the exploitation of vulnerabilities in communication protocols.

Modernization costs: The investments required for specialized hardware and technical training can represent a significant barrier, especially in emerging economies.

Interoperability: The coexistence of legacy systems with modern technologies creates compatibility issues, delaying the effective and large-scale implementation of digital solutions.

On the other hand, the opportunities resulting from the digitalization process are equally significant. Emerging technologies such as SDN and Blockchain enable the development of more secure, resilient, and efficient power systems, capable of responding swiftly to changing operating conditions and sophisticated cyber threats. Table 1 provides a synthesis of the main challenges and opportunities analyzed from different perspectives or categories.

Table 1: *Rule-Based Framework*

Category	Challenges	Opportunities
Security	Vulnerability to cyberattacks (DDoS, spoofing, exploitation of IEC 61850 protocols)	Application of technologies such as SDN and Blockchain to enhance system resilience and security
Economic	High modernization costs (advanced hardware, technical personnel training)	Operational optimization and loss reduction in the medium and long term
Technical	Interoperability issues between legacy systems and modern digital technologies	Implementation of flexible and scalable architectures with NFV and SDN
Operational	Difficulty integrating technologies in environments with limited infrastructure or regulatory support	Improved microgrid management, demand forecasting, and decentralized operation through data analysis and ML
Environmental / Social	Need for policies supporting technology adoption with a sustainable approach	Support for energy transition and achievement of decarbonization goals through digitalization and digital twin simulations

Together, these elements configure a complex yet promising scenario. The development of digital substations not only enhances the technical performance of the electrical system but also strengthens its capacity to adapt to the energy and climate challenges of the 21st century. Digital transformation, supported by cyber-secure infrastructure and emerging technologies, presents a strategic opportunity to transition toward a more sustainable, resilient, and efficient energy model.

5. CONCLUSIONS

The digital transformation of the power sector, particularly in the substation domain, represents a key milestone in the development of more efficient, resilient, and sustainable systems. Digital substations, supported by the IEC 61850 standard, have proven essential for integrating supervision, protection, and control functions into unified platforms that enable more flexible, automated, and secure management of electrical infrastructure.

This article has demonstrated how emerging technologies such as SDN, Blockchain, ML, and NFV can significantly enhance the technical and cybersecurity capabilities of digital substations

(DSs). These tools not only enable greater adaptability to changing operating conditions but also enhance system efficiency, facilitate the integration of renewable energy sources, and bolster resilience against cyber threats.

However, the digitalization of substations involves technical, economic, and regulatory challenges that must be addressed comprehensively. Interoperability with legacy systems, high modernization costs, and the need for skilled personnel represent significant barriers, particularly in emerging economies. Moreover, ensuring cybersecurity in critical infrastructures requires an evolution of traditional protection practices and the implementation of new approaches centered on proactive threat detection and dynamic risk management.

The Colombian case, along with various international experiences reviewed in this article, demonstrates that the transition to digital substations is not only feasible but also strategic for modernizing power systems and meeting global commitments to decarbonization and sustainability. To achieve this, it will be essential to strengthen the regulatory framework, foster investment in technological innovation, and promote collaborative schemes between industry, government, and academia.

Digital substations, enabled by emerging technologies, provide a transformative platform to address the 21st-century challenges of the electrical sector. Their effective implementation will pave the way for smarter, safer, and more adaptive power networks, aligned with the principles of energy sustainability and cyber resilience.

ACKNOWLEDGMENTS

Special thanks to the research team at the Laboratory of Industrial Automation and Communications (LACI) at the Universidad Nacional de Colombia – Medellín campus, whose support, expertise, and recommendations have significantly contributed to this research process.

REFERENCES

[1] G. R. Santos, E. Zancul, G. Manassero, and M. Spinola, “From conventional to smart substations: A classification model,” Electric Power Systems Research, vol. 226, p. 109887, Jan. 2024, doi: 10.1016/J.EPSR.2023.109887.

[2] O. A. Tobar-Rosero, E. Pérez González, G. D. Zapata Madrigal, and J. F. Botero Vega, “Subestaciones digitales y ciberseguridad como factores claves en la transformación digital del sector eléctrico colombiano,” Encuentro Internacional de Educación en Ingeniería, pp. 1–12, Sep. 2023, doi: 10.26507/PAPER.3277.

[3] A. Rahman, O. Yilmaz, O. Vaze, and A. Mandal, “Smart Substation Control and Protection Facilitating the Virtualization of Multiple Protection and Control,” 2023 IEEE International Conference on Energy Technologies for Future Grids, ETFG 2023, p. Wollongong, 2023, doi: 10.1109/ETFG55873.2023.10407293.

[4] C. P. Vineetha and C. A. Babu, “Smart grid challenges, issues and solutions,” Proceedings of 2014 International Conference on Intelligent Green Building and Smart Grid, IGBSG 2014, 2014, doi: 10.1109/IGBSG.2014.6835208.

[5] O. A. Tobar-Rosero, J. H. Vargas-Días, R. G. Sierra, G. D. Z. madrigal, and J. E. Candelo-Becerra, “Herramientas de Gestión de Protecciones para Optimizar Procesos Operativos y de Mantenimiento en Empresas del Sector Eléctrico,” Inge CuC, vol. 20, no. 2, Oct. 2024, doi: 10.17981/INGECUC.20.2.2024.03.

[6] D. Álvarez-Osorio, O. Arenas-Crespo, P. Arregocés-Guerra, J. C. R. Suárez, O. A. Tobar-Rosero, and G. D. Zapata-Madrigal, “Modernización del Sistema de Diagnóstico Automático de Eventos en Líneas de Transmisión y Subtransmisión de Energía Eléctrica,” Revista EIA, vol. 22, no. 43, p. 4335 pp. 1–41, Jan. 2025, doi: 10.24050/reia.v22i43.1768.

[7] O. Roa, J. F. Botero, S. A. Gutierrez-Betancur and O. A. Tobar-Rosero, "GOOSEAttacker: Synthetic Attack Generation Tool for IEC61850," 2023 IEEE Latin-American Conference on Communications (LATINCOM), Panama City, Panama, 2023, pp. 1-6, doi: 10.1109/LATINCOM59467.2023.10361897.

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

[9] Y. E. Bouffard-Vercelli and B. Andre, “Future Architectures of Electrical Substations,” Petroleum and Chemical Industry Conference Europe Conference Proceedings, PCIC EUROPE, vol. 2021-June, 2021, doi: 10.23919/PCICEUROPE50407.2021.9805424.

[10] O. A. Tobar-Rosero, O. D. Díaz-Mendoza, P. A. Díaz-Vargas, J. E. Candelo-Becerra, H. A. Florez-Célis, y L. F. Quintero-Henao, «Digital

Substations: Optimization Opportunities from Communication Architectures and Emerging Technologies», Sci., vol. 7, n.º 2, p. 63, 2025. doi: 10.3390/sci7020063.

[11] M. Adamiak, D. Baigent, G. E. Digital, E. Ralph, and M. Sisco, "IEC 61850 Communication Networks and Systems In Substations: An Overview for Users," The Protection and Control Journal, pp. 61–68, 2009.

[12] O. A. Tobar-Rosero et al., "GOOSE Secure: A Comprehensive Dataset for In-Depth Analysis of GOOSE Spoofing Attacks in Digital Substations," Energies 2024, Vol. 17, Page 6098, vol. 17, no. 23, p. 6098, Dec. 2024, doi: 10.3390/EN17236098.

[13] D. Dolezilek, D. Gammel and W. Fernandes, "Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems," 15th International Conference on Developments in Power System Protection (DPSP 2020), Liverpool, UK, 2020, pp. 1-6, doi: 10.1049/cp.2020.0016.

[14] P. Kaliappan, S. Sudha and D. Shankar, "International Standards for Cybersecurity in Smart Devices for the Power Sector," 2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST), Vijayawada, India, 2024, pp. 1-5, doi: 10.1109/ICCIGST60741.2024.10717531.

[15] PAC World, "Landsnet's Road to a Fully Digital Transmission System," 2023. [En línea]. Disponible en: https://www.pacw.org/

[16] S. R. Patel, "Digital Substation Design and Automation with IEC 61850," *Keentel Engineering Blog*, May 12, 2025. [Online]. Available: https://keentelengineering.com/digital-substation-design-and-automation-with-iec-61850.

[17] Electric Energy Online, "The Digital Substation: A Catalyst for the U.S. Grid Modernization Initiative," 2023.

[18] ISA Energía Brasil, "Nuestra Trayectoria," 2023. [En línea]. Disponible en: https://www.isaenergiabrasil.com.br/

[19] SEL Inc., "CFE México – IEC 61850 Implementation," 2015. [En línea]. Disponible en: https://www.selinc.com/

[20] A. Domínguez et al., "Restoration Strategies in Digital Distribution Substations," Energies, vol. 17, no. 16, p. 4154, 2024. DOI: 10.3390/en17164154

[21] Ectricol S.A.S., "Primera Subestación Digital en Colombia," 2022. [En línea]. Disponible en: https://www.ectricol.com/

[22] La Economía Colombia, "En marcha la primera subestación eléctrica digital del Tolima," 2022. Disponible en: https://economistacolombia.com/

[23] J. Li, H. Su, Y. Zhang, Q. Yan, L. Liu, and T. Wang, "Smart Digital Inspection and Maintenance of Substations," 2024 5th International Conference on Power Engineering, ICPE 2024, pp. 388–393, 2024, doi: 10.1109/ICPE64565.2024.10929212.

[24] U. Ghosh, P. Chatterjee, S. Shetty, U. Ghosh, P. Chatterjee, and S. Shetty, "Securing SDN-Enabled Smart Power Grids: SDN-Enabled Smart Grid Security," https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-6684-3666-0.ch046, vol. 3, pp. 1028–1046, Jan. 1AD, doi: 10.4018/978-1-6684-3666-0.CH046.

[25] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid," 2024 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5, Jul. 2024, doi: 10.1109/PESGM51994.2024.10688802.

[26] I. Hammouti, A. Addaim, and Z. Guennoun, "Proposed Architecture of Cyber Security in Smart Grids, Blockchain as Solution," 2022 IEEE Information Technologies and Smart Industrial Systems, ITSIS 2022, 2022, doi: 10.1109/ITSIS56166.2022.10118374.

[27] Q. Chai et al., "Relay Protection Setting Management System and Method Based on Blockchain Encryption Technology," Proceedings - 2023 International Conference on Power System Technology: Technological Advancements for the Construction of New Power System, PowerCon 2023, 2023, doi: 10.1109/POWERCON58120.2023.10331237.

[28] P. K. Yegorov, A. Lackovitch, E. Dean, H. M. Mustafa, S. Basumallik, and A. Srivastava, "Analyzing GOOSE Security in IEC61850-based Substation Using ML, SDN and Digital Twin," 2023 North American Power Symposium, NAPS 2023, 2023, doi: 10.1109/NAPS58826.2023.10318551.

[29] A. Eynawi, A. Mumrez, G. Elbez, and V. Hagenmeyer, "Machine Learning-Based Feature Selection for Intrusion Detection Systems in IEC 61850-Based Digital Substations," 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2024, pp. 1–7, 2024, doi: 10.1109/SMARTGRIDCOMM60555.2024.10738031.

[30] A. Fahmin, Y. C. Lai, M. S. Hossain, Y. D. Lin, and D. Saha, "Performance modeling of SDN with NFV under or aside the controller," Proceedings - 2017 5th International Conference on Future Internet of Things and

Cloud Workshops, W-FiCloud 2017, vol. 2017-January, pp. 211–216, Nov. 2017, doi: 10.1109/FICLOUDW.2017.76.

[31] K. Kaur, V. Mangat, and K. Kumar, "A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture," Computer Networks, vol. 217, p. 109281, Nov. 2022, doi: 10.1016/J.COMNET.2022.109281.

[32] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid," 2024 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5, Jul. 2024, doi: 10.1109/PESGM51994.2024.10688802.

[33] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "Hybrid Intrusion Detection System using SDN and Machine Learning for IEC 61850," arXiv preprint, 2023. [Online]. Available: https://arxiv.org/abs/2311.12205

[34] E. Sakic, V. Kulkarni, V. Theodorou, A. Matsiuk, S. Kuenzer, N. E. Petroulakis, y K. Fysarakis, "VirtuWind – An SDN- and NFV-Based Architecture for Softwarized Industrial Networks," en *Measurement, Modelling and Evaluation of Computing Systems*, R. German, K.-S. Hielscher y U. Krieger, eds., LNCS, vol. 10740, Cham: Springer, 2018, pp. 251–261, doi: 10.1007/978-3-319-74947-1-17.

[35] A. Leal and J. F. Botero, "Arquitectura para redes de comunicaciones en subestaciones de energía basadas en virtualización y SDN," *Revista Facultad de Ingeniería Universidad de Antioquia*, no. 100, pp. 48–66, Mar. 2021, doi: 10.17533/udea.redin.20210321.

[36] P. K. Yegorov et al., "Analyzing GOOSE Security in IEC61850-based Substation Using ML, SDN and Digital Twin," Proc. NAPS 2023, doi: 10.1109/NAPS58826.2023.10318551

[37] Eynawi et al., "Machine Learning-Based Feature Selection for Intrusion Detection Systems in IEC 61850-Based Digital Substations," IEEE SmartGridComm 2024, pp. 1–7, 2024, doi: 10.1109/SMARTGRIDCOMM60555.2024.10738031.

[38] Q. Chai et al., "Relay Protection Setting Management System and Method Based on Blockchain Encryption Technology," Proc. PowerCon 2023, doi: 10.1109/POWERCON58120.2023.10331237.