

Automatización y ciberseguridad en subestaciones inteligentes: el potencial de SDN en la transformación digital del sector eléctrico

Óscar A. Tobar Rosero¹, Octavio D. Díaz Mendoza¹, Germán D. Rueda Carvajal¹,
Ernesto Pérez González¹, Héctor A. Flórez Celis¹, Luis F. Quintero Henao²

¹Universidad Nacional de Colombia, ²Enterprise Innovation
Medellín, Colombia

Resumen

La digitalización del sector eléctrico ha transformado la arquitectura operativa de las subestaciones, promoviendo el uso de estándares como IEC 61850 para lograr interoperabilidad y eficiencia en la transmisión de datos críticos. No obstante, esta evolución ha expuesto nuevos vectores de ataque que comprometen la integridad y disponibilidad de los sistemas de automatización. En este contexto, las Redes Definidas por Software (SDN) emergen como una alternativa tecnológica para incrementar la resiliencia cibernética y optimizar la gestión del tráfico en entornos de misión crítica.

Este artículo presenta un estudio experimental sobre la integración de SDN en subestaciones digitales mediante una arquitectura híbrida que combina dispositivos SDN y de comunicación tradicionales. Se implementó una metodología dual basada en simulaciones con Mininet y pruebas físicas en un entorno de laboratorio que replica condiciones reales. Se evaluaron métricas técnicas como latencia GOOSE, integridad de SV, tiempo de detección de anomalías y capacidad de reconfiguración dinámica bajo escenarios de ataque.

Los resultados demuestran que SDN permite cumplir con los requisitos temporales del estándar IEC 61850, incluso ante amenazas activas, y facilita la segmentación lógica y el control centralizado de flujos críticos. La arquitectura híbrida se valida como una solución escalable, adaptable y compatible con infraestructuras existentes. Se concluye que SDN representa un habilitador estratégico para la automatización segura de subestaciones inteligentes, y se proponen líneas de investigación futura basadas en inteligencia artificial, y estándares de ciberseguridad.

Palabras clave: subestaciones digitales; IEC 61850; redes definidas por software (SDN); sistemas de comunicación; ciberseguridad; transformación digital

Abstract

The digitalization of the electric sector has reshaped substation architectures by adopting standards like IEC 61850, enabling device interoperability and efficient critical data exchange. However, this transformation also introduces new cyber threats that jeopardize system integrity and availability. In this context, Software-Defined Networking (SDN) emerges as a technological enabler to enhance cyber resilience and optimize data flow management in mission-critical environments.

This article presents an experimental study on integrating SDN into digital substations through a hybrid architecture that combines SDN devices with traditional communication devices. A dual methodology was implemented, including network simulations in Mininet and real-world testing in a physical laboratory environment. Technical metrics such as GOOSE latency, SV integrity, anomaly detection time, and dynamic reconfiguration were evaluated under adversarial conditions.

The results confirm that SDN meets IEC 61850 timing requirements, even under active attacks, while enabling logical segmentation and centralized control of critical traffic. The hybrid architecture is scalable, adaptable, and compatible with legacy infrastructure. The study concludes that SDN is a strategic enabler for the secure automation of smart substations and outlines future research directions involving artificial intelligence, multi-substation scalability, and cybersecurity standardization.

Keywords: *digital substations; IEC 61850; software-defined networking; communication systems; cybersecurity; digital transformation*

1. Introducción

La transformación digital del sector eléctrico ha propiciado una evolución significativa en la infraestructura de las subestaciones, migrando de sistemas analógicos hacia entornos digitales altamente automatizados. Este cambio busca mejorar la eficiencia operativa, la interoperabilidad entre dispositivos y la capacidad de respuesta ante eventos críticos. En este contexto, el estándar IEC 61850 se ha consolidado como un pilar fundamental para la automatización de subestaciones, definiendo protocolos como GOOSE (Generic Object-Oriented Substation Event) y Sampled Values (SV) que permiten una comunicación rápida y estandarizada entre dispositivos electrónicos inteligentes (IEDs) [1].

Sin embargo, la creciente digitalización también ha expuesto nuevas vulnerabilidades en la infraestructura eléctrica. La dependencia de redes de comunicación y la estandarización de protocolos han incrementado el riesgo de ciberataques, como suplantación de mensajes GOOSE y ataques de denegación de servicio, que pueden comprometer la estabilidad y seguridad del sistema eléctrico [2]. Estos desafíos han impulsado la necesidad de integrar soluciones de ciberseguridad más dinámicas y adaptativas.

En este escenario, las Redes Definidas por Software (SDN) emergen como una tecnología prometedora para abordar las limitaciones de las arquitecturas de red tradicionales en

subestaciones digitales. SDN permite una gestión centralizada y programable del tráfico de red, facilitando la implementación de políticas de seguridad en tiempo real y la reconfiguración dinámica de flujos de datos ante eventos anómalos [3]. Estudios recientes como lo expuesto en [4], han demostrado que la integración de SDN en entornos IEC 61850 mejora la resiliencia cibernética, permitiendo detectar y mitigar ataques mediante sistemas de detección de intrusos (IDS) y controladores inteligentes.

Este artículo explora la implementación de una arquitectura híbrida que combina dispositivos SDN con switches tradicionales en subestaciones digitales, evaluando su impacto en la eficiencia de la transmisión de mensajes críticos y en la robustez frente a amenazas cibernéticas. Se presentan resultados obtenidos tanto en simulaciones utilizando Mininet como en pruebas físicas realizadas en el Laboratorio de Automatización y Comunicaciones Industriales (LACI) de la Universidad Nacional de Colombia, sede Medellín. Los hallazgos evidencian que la adopción de SDN no solo asegura y mejora la gestión del tráfico de datos conforme a los requerimientos del estándar IEC 61850, sino que también fortalece significativamente la ciberseguridad en infraestructuras críticas del sector eléctrico.

2. Contexto

Subestaciones Digitales y el Estándar IEC 61850

La evolución hacia subestaciones digitales ha sido impulsada por la necesidad de mejorar la interoperabilidad, eficiencia y capacidad de respuesta en sistemas eléctricos. El estándar IEC 61850 ha sido fundamental en esta transformación, proporcionando un marco para la comunicación entre dispositivos electrónicos inteligentes (IEDs) mediante protocolos como GOOSE y SV. Estos protocolos permiten la transmisión rápida y estandarizada de eventos y valores muestreados, esenciales para la operación y protección del sistema eléctrico [1].

Sin embargo, la adopción de IEC 61850 también ha introducido desafíos significativos. La estandarización y apertura de los protocolos han expuesto vulnerabilidades que pueden ser explotadas por actores maliciosos. Ataques como la suplantación de mensajes GOOSE y la manipulación de SV pueden comprometer la integridad y disponibilidad del sistema eléctrico [2].

Vulnerabilidades y Desafíos de Ciberseguridad

La creciente digitalización de las subestaciones ha incrementado la superficie de ataque, exponiendo sistemas críticos a amenazas cibernéticas. La estandarización de protocolos y la interconexión de dispositivos han facilitado la ejecución de ataques como la suplantación de mensajes GOOSE y la manipulación de SV, que pueden causar operaciones no deseadas y afectar la estabilidad del sistema eléctrico [3].

Además, la implementación de medidas de ciberseguridad en entornos IEC 61850 presenta desafíos técnicos. Por ejemplo, la incorporación de algoritmos criptográficos para proteger la confidencialidad y autenticidad de los mensajes debe considerar las estrictas restricciones de latencia del sistema. Según lo expuesto por [4], se ha demostrado que algoritmos como ChaCha20 y Poly1305 (algoritmos criptográficos modernos diseñados para ofrecer seguridad, eficiencia y

resistencia frente a ataques conocidos), pueden ser adecuados para cumplir con los requisitos de tiempo del estándar IEC 61850, ofreciendo una alternativa viable a los algoritmos tradicionales.

Integración de SDN en Subestaciones Digitales

Las Redes Definidas por Software (SDN) han emergido como una solución prometedora para abordar las limitaciones de las arquitecturas de red tradicionales en subestaciones digitales. SDN permite una gestión centralizada y programable del tráfico de red, facilitando la implementación de políticas de seguridad en tiempo real y la reconfiguración dinámica de flujos de datos ante eventos anómalos [5].

Investigaciones han demostrado que la integración de SDN en entornos IEC 61850 mejora la resiliencia cibernética, permitiendo detectar y mitigar ataques mediante sistemas de detección de intrusos (IDS) y controladores inteligentes. Por ejemplo, se ha propuesto una arquitectura híbrida que combina dispositivos SDN con switches tradicionales, evaluando su impacto en la eficiencia de la transmisión de mensajes críticos y en la robustez frente a amenazas cibernéticas [6].

Arquitecturas Híbridas y Evaluación de Desempeño

La implementación de arquitecturas híbridas que combinan dispositivos SDN con switches tradicionales ha sido objeto de estudio para evaluar su impacto en la eficiencia de la transmisión de mensajes críticos y en la robustez frente a amenazas cibernéticas. Simulaciones utilizando herramientas como Mininet y pruebas físicas en entornos de laboratorio han demostrado que la adopción de SDN no solo optimiza la gestión del tráfico de datos conforme a los requerimientos del estándar IEC 61850, sino que también fortalece significativamente la ciberseguridad en infraestructuras críticas del sector eléctrico [7].

A continuación, se presenta una comparación entre los enfoques tradicionales y los basados en SDN aplicados a subestaciones IEC 61850:

Tabla 1. Comparación entre Red Tradicional y Red con SDN en Subestaciones IEC 61850

| Característica | Red Tradicional | Red con SDN |
|---------------------------------------|--|---|
| <i>Arquitectura de control</i> | Distribuida | Centralizada y programable |
| <i>Flexibilidad de configuración</i> | Estática, basada en CLI | Alta, mediante APIs y controladores |
| <i>Gestión del tráfico GOOSE/SV</i> | Priorización limitada mediante VLAN y QoS | Priorización dinámica por flujo en tiempo real |
| <i>Reconfiguración dinámica</i> | Manual o dependiente de protocolos redundantes | Automática mediante automatismos programados en controlador |
| <i>Visibilidad de red</i> | Limitada al plano físico | Global y en tiempo real |
| <i>Detección de intrusiones</i> | Limitada, requiere sistemas externos | Integrada con controladores SDN/IDS |
| <i>Aislamiento de tráfico crítico</i> | Mediante VLAN manuales | Aislamiento por flujo, microsegmentación |

| | | |
|---|-------------------------------------|---|
| <i>Compatibilidad con IEC 61850</i> | Alta, con switches industriales | Alta, compatible con OpenFlow/IEC 61850 |
| <i>Implementación de políticas de seguridad</i> | Limitada a configuraciones manuales | Programable y adaptable en tiempo real |

3. Metodología

La validación del potencial de SDN en subestaciones inteligentes se llevó a cabo mediante una estrategia dual, que contempla la simulación controlada en un entorno virtual (Mininet) y experimentación en un banco de pruebas físico en LACI de la UNal sede Medellín. Esta metodología permite contrastar el comportamiento teórico del sistema bajo condiciones ideales frente a escenarios reales con hardware industrial y tráfico operativo.

En tal sentido, la metodología planteada para esta investigación se desarrolla en función de la siguiente secuencia de fases o actividades clave en el proceso.



Figura 1. Metodología de desarrollo para la investigación

A continuación, se describe cada una de las etapas consideradas en la metodología de investigación:

3.1 Diseño de la Arquitectura Híbrida

Se diseñó una topología híbrida en la cual coexisten switches tradicionales y dispositivos SDN, todos conectados a un controlador basado en Ryu. Esta configuración permite conservar compatibilidad con infraestructuras existentes y, al mismo tiempo, beneficiarse de las ventajas de control centralizado y segmentación dinámica.

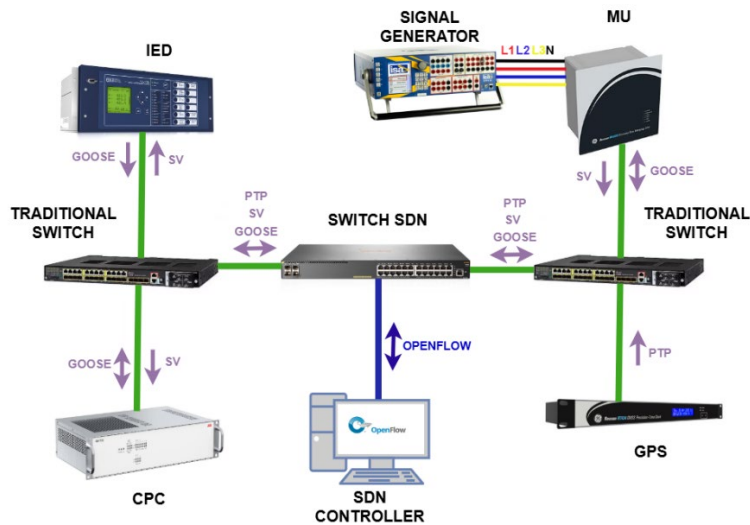


Figura 2. Diseño de arquitectura para integración de SDN en infraestructura convencional de una subestación digital

La arquitectura implementada se basa en una topología jerárquica alineada con el modelo IEC 61850, en la cual se integran dispositivos convencionales con dispositivos SDN. El diseño se caracteriza por:

- Switches tradicionales industriales que mantienen el soporte para funciones legadas.
- Switches SDN (Open vSwitch) conectados a un controlador Ryu en el plano de control.
- Segmentación de red por niveles funcionales (proceso, bahía, estación).
- Tráfico simulado de GOOSE y SV generado por herramientas compatibles con IEC 61850.
- Políticas de reconfiguración dinámica en respuesta a condiciones de fallo o ataque.

3.2 Entorno de Simulación

Se implementó una red virtual en Mininet que emula una subestación digital con múltiples IEDs, MUs y dispositivos de supervisión. El tráfico GOOSE y SV fue generado utilizando librerías que implementan el estándar IEC 61850. El controlador SDN aplicó reglas OpenFlow para dar prioridad a tráfico GOOSE y permitir la reconfiguración dinámica en caso de detección de ataques o eventos no deseados. La topología emula una subestación compuesta por:

- **MUs** que simulan sensores y mediciones primarias.
- **IEDs** que interpretan señales y ejecutan funciones de protección.
- **Servidor SCADA/HMI** que interactúa a nivel estación.

En este entorno se evaluaron los siguientes aspectos:

- Latencia media y máxima de mensajes GOOSE.
- Tasa de entrega de SV válidos.
- Eficiencia al reencaminar flujos en fallos de enlace.

3.3 Implementación Física

Para validar los resultados de la simulación, se replicó la arquitectura híbrida en un entorno físico compuesto por switches SDN (Open vSwitch), equipos Cisco, IEDs de diferentes fabricantes y MUs multifabricante. Se generaron ataques de suplantación y saturación de tráfico, mientras se monitorearon las métricas de latencia, jitter, tasa de entrega de mensajes críticos, y capacidad de reacción del sistema.

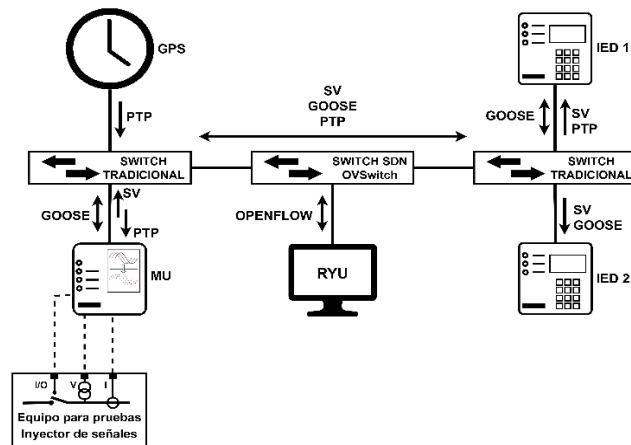


Figura 3. Arquitectura de comunicación física de prueba

La arquitectura de pruebas incluyó:

- Switches SDN (Open vSwitch sobre hardware x86).
- Switches industriales.
- Dispositivos IEDs con soporte para GOOSE/SV.
- GPS publicador de PTP para la sincronización de los equipos
- MUs publicadores de SV y subscriptores de GOOSE.
- Controlador Ryu desplegado sobre una máquina Linux dedicada.

Se implementaron ataques de red controlados, incluyendo:

- Suplantación de mensajes GOOSE mediante herramientas como Scapy.
- Saturación de enlaces (ataques DoS) para observar la reacción de la topología SDN.

3.4 Métricas de Evaluación

Las métricas seleccionadas permiten una comparación objetiva del desempeño del sistema en distintos escenarios:

- **Latencia GOOSE (ms):** tiempo total de transmisión desde emisión hasta recepción. El estándar IEC 61850-5 exige que la latencia de la mensajería GOOSE esté por debajo de los 20 ms cuando son mensajes generales y debajo de los 3 ms cuando son mensajes de disparo.

- **Integridad de SV (%):** proporción de paquetes válidos sin modificación. El estándar IEC 61850-5, sugiere que las pérdidas de paquetes sean menores al 1%.
- **Tasa de pérdida bajo ataque (%):** pérdida relativa de paquetes críticos en situaciones adversas.

Esta metodología busca demostrar de forma cuantificable el valor agregado de SDN en la operación segura, eficiente y resiliente de subestaciones inteligentes frente a las exigencias contemporáneas del sistema eléctrico.

4. Resultados

En esta sección presentamos los hallazgos obtenidos tras la evaluación de la arquitectura híbrida en los dos entornos de prueba: la simulación en Mininet y la implementación física en el laboratorio LACI.

Los resultados se analizan con base en las métricas definidas, considerando tanto el cumplimiento de los requisitos operativos de IEC 61850 como la respuesta frente a ataques cibernéticos.

4.1 Resultados de la Simulación en Mininet

En el entorno virtual se observaron los siguientes comportamientos clave:

- **Latencia GOOSE:** En condiciones normales, la latencia promedio se mantuvo en 2.3 ms y no superó los 3 ms durante ataques DoS leves, cumpliendo con los umbrales establecidos por IEC 61850.
- **Integridad de SV:** La tasa de entrega de SV válidos fue superior al 98% incluso con congestión inducida en los enlaces.

Estos resultados indican que SDN puede mantener la operación confiable del sistema incluso bajo condiciones adversas, con capacidad de adaptación y control granular del tráfico.

4.2 Resultados de la Implementación Física

Los experimentos en laboratorio evidenciaron que el sistema híbrido mantiene sus beneficios también en entornos reales. Entre los principales hallazgos se encuentran:

- **Latencia GOOSE:** La media fue de 2.6 ms y se mantuvo dentro de límites aceptables bajo ataques de suplantación.
- **Operatividad bajo ataque:** Se mantuvo continuidad operativa frente a eventos de saturación, redirigiendo tráfico mediante reglas de fallback configuradas en el controlador.

4.3 Discusión y Análisis Comparativo

La integración de SDN en subestaciones digitales representa una evolución significativa respecto a las arquitecturas tradicionales. Los datos recopilados en ambos escenarios permiten extraer los siguientes análisis comparativos:

- **Confiabilidad operativa: SDN** cumple con los límites de latencia definidos en IEC 61850 para tráfico GOOSE y SV.
- **Capacidad de adaptación:** La arquitectura es resiliente frente a fallas y ataques, gracias a la reconfiguración automática de rutas y la visibilidad global que proporciona el plano de control centralizado.
- **Compatibilidad y escalabilidad:** La implementación híbrida facilita una adopción progresiva sin necesidad de sustituir toda la infraestructura legada.
- **Seguridad incrementada:** El uso de SDN posibilita el despliegue de mecanismos de detección y contención de amenazas en tiempo real, algo difícil de lograr con arquitecturas convencionales.
- **Flexibilidad operativa:** mediante la reprogramación de flujos en tiempo real.
- **Visibilidad y monitoreo:** gracias a la integración de SDN con mecanismos de detección de intrusos. Mediante el controlador es posible supervisar los flujos de datos en la red de la subestación digital.

Desde una perspectiva práctica, estos resultados posicionan a SDN como una tecnología clave para robustecer las redes de automatización industrial en entornos eléctricos. No obstante, se identificaron desafíos adicionales como la necesidad de personal capacitado en programación de controladores SDN, y la integración con sistemas de gestión de eventos complejos (SIEM) en tiempo real.

En conjunto, el análisis evidencia que la arquitectura híbrida SDN/no-SDN es técnicamente viable, operativamente confiable y estratégicamente valiosa para la transición digital del sector eléctrico. Además, se evidenció que la transición hacia SDN no requiere una sustitución total del hardware existente, lo que refuerza su viabilidad como solución escalable y económicamente razonable.

5. Conclusiones, recomendaciones y trabajos futuros

Los resultados de esta investigación confirman que la integración de SDN en subestaciones digitales representa una solución robusta para afrontar los retos actuales del sector eléctrico en términos de automatización, ciberseguridad y eficiencia operativa. La arquitectura híbrida evaluada, compuesta por dispositivos tradicionales y nodos SDN bajo control centralizado, demostró cumplir con los exigentes requisitos de latencia definidos por IEC 61850 incluso en escenarios de ataque, lo cual valida su aplicabilidad en entornos reales. Tanto en la simulación como en el entorno físico, se logró mantener la integridad del tráfico crítico, garantizar la continuidad operativa mediante reconfiguración dinámica de flujos, e implementar mecanismos de detección y contención de amenazas en tiempo real.

A partir de estos hallazgos, se recomienda fomentar la adopción progresiva de arquitecturas híbridas como una estrategia de transición viable, especialmente para operadores que disponen de infraestructuras legadas. Asimismo, se sugiere establecer políticas de red que prioricen y protejan el tráfico GOOSE y SV, integrar sistemas de detección de intrusos con lógica de respuesta automatizada, y desarrollar controladores SDN con capacidad de operar ante fallos del plano de control. Estas recomendaciones pueden mejorar la resiliencia del sistema, incrementar su flexibilidad operativa y reducir el tiempo de respuesta ante ciber-incidentes.

Como líneas de trabajo futuro, se plantea la ampliación del modelo hacia topologías de múltiples subestaciones distribuidas, con el fin de evaluar el impacto del escalamiento en términos de latencia, sincronización y carga del controlador. Adicionalmente, se propone la incorporación de técnicas de inteligencia artificial, como aprendizaje supervisado y reforzado, para anticipar comportamientos maliciosos y optimizar dinámicamente las políticas de red. También se considera prioritario el análisis de la compatibilidad con normativas como IEC 62351 y el estudio de esquemas de alta disponibilidad mediante protocolos redundantes como PRP y HSR. Finalmente, es necesario explorar aspectos económicos y regulatorios asociados a la adopción de SDN, así como el desarrollo de estándares específicos que formalicen su integración en subestaciones inteligentes.

Para finalizar, cabe resaltar que la evidencia técnica y experimental obtenida posiciona a SDN como un pilar fundamental a ser considerada para garantizar la evolución segura y resiliente de las infraestructuras eléctricas del futuro, permitiendo una automatización inteligente y una defensa activa frente a los riesgos emergentes en redes críticas.

6. Referencias

- [1] F. Alonso, B. Samaniego, G. Farias, y S. Dormido-Canto, "Analysis of Cryptographic Algorithms to Improve Cybersecurity in the Industrial Electrical Sector," *Applied Sciences*, vol. 14, no. 7, p. 2964, 2024. <https://doi.org/10.3390/app14072964>
- [2] O. A. Tobar-Rosero et al., "GOOSE Secure: A Comprehensive Dataset for In-Depth Analysis of GOOSE Spoofing Attacks in Digital Substations," *Energies*, vol. 17, no. 23, p. 6098, 2024. <https://doi.org/10.3390/en17236098>
- [3] M. Girdhar, J. Hong, W. Su, A. Herath, y C.-C. Liu, "SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid," *arXiv preprint arXiv:2311.12205*, 2023. <https://doi.org/10.1109/PESGM51994.2024.10688802>
- [4] F. Alonso, B. Samaniego, G. Farias, y S. Dormido-Canto, "Analysis of Cryptographic Algorithms to Improve Cybersecurity in the Industrial Electrical Sector," *Applied Sciences*, vol. 14, no. 7, p. 2964, 2024. <https://doi.org/10.3390/app14072964>
- [5] G. M. Makrakis, D. Roberson, C. Koliass, y D. Cook, "Evaluation of SDN Security Measures in the Context of IEC 62443-3-3," *International Journal of Critical Infrastructure Protection*, vol. 47, p. 100716, 2024. <https://doi.org/10.1016/j.ijcip.2024.100716>
- [6] M. Girdhar, K. Park, W. Su, J. Hong, A. Herath, y C.-C. Liu, "SDN-Based Smart Cyber Switching (SCS) for Cyber Restoration of a Digital Substation," *arXiv preprint arXiv:2411.07433*, 2024.
- [7] M. Girdhar, J. Hong, W. Su, A. Herath, y C.-C. Liu, "SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid," *arXiv preprint arXiv:2311.12205*, 2023. <https://doi.org/10.1109/PESGM51994.2024.10688802>

Sobre los autores

- **Óscar A. Tobar Rosero:** Ingeniero Electricista, Máster en ingeniería – Ingeniería Eléctrica, Estudiante de Doctorado en la Universidad Nacional de Colombia. Investigador en subestaciones digitales, transformación digital para el sector eléctrico y redes inteligentes; coordinador técnico de LACI y docente ocasional de la Universidad Nacional de Colombia sede Medellín. ootobarr@unal.edu.co
- **Octavio D. Díaz Mendoza:** Ingeniero de Control graduado de la Universidad Nacional de Colombia. Investigador en Subestaciones Eléctricas Digitales, transformación digital del sector eléctrico y comunicaciones industriales basadas en tecnologías disruptivas; analista de pruebas y docente para cursos de extensión impartidos por LACI. oddiazm@unal.edu.co
- **Germán D. Rueda Carvajal:** Ingeniero de Control, Estudiante de Maestría en Ingeniería Analítica, Estudiante afiliado al proyecto CACTUS Universidad Nacional de Colombia. gdruedac@unal.edu.co
- **Ernesto Pérez González:** Director de trabajo de investigación en doctorado, Director grupo de investigación PASS, miembro IEEE, Profesor titular Universidad Nacional de Colombia sede Medellín. eperezg@unal.edu.co
- **Héctor A. Flórez Celis:** Ingeniero de Control, Magister en Ingeniería – Ingeniería Eléctrica, Estudiante de Doctorado en la Universidad Nacional de Colombia. Investigador en Industria 4.0, Docente Ocasional de la Universidad Nacional de Colombia Sede Medellín. haflorez@unal.edu.co
- **Luis Fernando Quintero Henao:** Ingeniero Industrial, Magíster en Ingeniería – Ingeniería de Sistemas con énfasis en Inteligencia Artificial. Profesional en la Universidad Nacional de Colombia y Director de Investigación en Enterprise Innovation S.A.S. Investigador en transferencia de tecnología, transformación digital, gobernanza de datos y automatización; gestor de proyectos CTel con impacto territorial en el Grupo de Investigación - GIDIA. lfquint0@unal.edu.co

Los puntos de vista expresados en este artículo no reflejan necesariamente la opinión de la Asociación Colombiana de Facultades de Ingeniería.

Copyright © 2025 Asociación Colombiana de Facultades de Ingeniería (ACOFI)