# Análisis de las características de las redes de comunicación para la implementación de sistemas industriales robustos en el marco de la industria 4.0

Andrés Vargas Velásquez

Asesor

Violeth Lasso Vivas

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Tecnología en Automatización Electrónica Industrial

2026

**Nota de Aceptación**

Por medio de la presente, se hace constar que la monografía titulada " Análisis de las características de las redes de comunicación para la implementación de sistemas industriales robustos en el marco de la industria 4.0" presentada por el estudiante Andrés Vargas Velásquez para obtener el título de tecnólogo en automatización electrónica industrial (resolución 020924), cumple con los requisitos académicos y técnicos exigidos por la institución.

Tras la evaluación del trabajo, se considera que el documento presenta una revisión bibliográfica sólida, un marco teórico coherente y aportes conceptuales relevantes sobre los protocolos de comunicación (MODBUS, PROFINET, OPC UA) y la integración del IIoT en entornos industriales. En consecuencia, el jurado académico acepta la monografía y autoriza su depósito en el repositorio institucional para consulta y referencia.

Violeth Lasso Vivas

Nombre Director de Trabajo de Grado

Mauricio Alberto García

Jurado

2026

## Dedicatoria

Dedico este trabajo a mi familia, por su paciencia, apoyo incondicional y confianza en cada etapa de mi formación. A mis docentes y compañeros de estudio, quienes con sus enseñanzas, conversaciones técnicas y experiencia alimentaron mi curiosidad y fortalecieron mi compromiso con la industria. Finalmente, a todas las personas con las que trabajo en el área de mantenimiento industrial: su experiencia práctica inspira la búsqueda constante de soluciones más seguras y eficientes.

**Agradecimientos**

Deseo expresar mi sincero agradecimiento a las personas y a la institución que hicieron posible esta monografía. A mi tutor(a), por su guía rigurosa, sus observaciones constructivas y por orientarme en la selección del enfoque y las fuentes más relevantes. A los tutores del programa, cuyas clases y consejos determinaron gran parte de mi formación técnica.

A las bibliotecas y repositorios que facilitaron el acceso a normas, artículos y libros especializados; sin ese material, la revisión teórica no habría sido posible. A los expertos y profesionales del sector que dedicaron su tiempo a responder consultas y compartir experiencias prácticas que enriquecieron la discusión del trabajo.

A mis compañeros de estudio por los intercambios de conocimiento y el apoyo mutuo durante el proceso. Y, en lo personal, a mi familia y amigos por su paciencia, comprensión y ánimo constante en los momentos de mayor exigencia académica.

Finalmente, agradezco a todas las personas y entidades, cuyas voces y publicaciones fueron citadas en este documento, por construir el conocimiento que permitió desarrollar esta investigación sobre el análisis de las características de las redes de comunicación para la implementación de sistemas industriales robustos en el marco de la industria 4.0. ¡Muchas gracias!

**Resumen**

El presente trabajo aborda el papel fundamental de las comunicaciones industriales en el marco de la Industria 4.0, analizando protocolos de comunicación utilizados en entornos industriales, esta investigación se centra en los siguientes protocolos: MODBUS, PROFINET y OPC UA. Modbus es un protocolo abierto maestro, esclavo y permite hasta 247 dispositivos esclavos por maestro en una red estándar, muy difundido por su simplicidad y bajo costo, PROFINET es un protocolo Ethernet industrial abierto, de alto rendimiento, en tiempo real, ampliamente adoptado por su alta velocidad y determinismo, OPC UA es un estándar orientado a servicios que facilita la interoperabilidad vertical y horizontal plena entre dispositivos y sistemas industriales, ofreciendo seguridad integrada y un modelo de datos rico. Cada protocolo tiene características particulares, ventajas, limitaciones y ámbitos de aplicación específicos, asimismo, la integración del Internet Industrial de las Cosas (IIoT) permite conectar sensores y equipos a Internet para mejorar la eficiencia, la interoperabilidad y la gestión de datos en tiempo real, transformando la comunicación industrial tradicional. Otro impacto clave del IIoT es la interoperabilidad, los estándares de comunicación IIoT (como OPC UA y MQTT) permiten que dispositivos de distintos fabricantes intercambien información de forma estandarizada, por ejemplo, OPC UA funciona sobre TCP/IP y HTTPS, habilitando comunicación firewall-friendly entre sistemas de control y la nube. Para el desarrollo de este trabajo se revisaron y se compararon investigaciones y estudios de caso documentados, con el fin de analizar aspectos como el rendimiento, la latencia, la interoperabilidad y la ciberseguridad de las redes industriales.

***Palabras clave*:** automatización, redes, protocolos, comunicación, ciberseguridad.

**Abstract**

This paper addresses the fundamental role of industrial communications in the context of Industry 4.0, analyzing communication protocols used in industrial environments. This research focuses on the following protocols: MODBUS, PROFINET, and OPC UA. Modbus is an open master-slave protocol that allows up to 247 slave devices per master in a standard network. It is widely used due to its simplicity and low cost. PROFINET is an open, high-performance, real-time industrial Ethernet protocol, widely adopted for its high speed and determinism. OPC UA is a service-oriented standard that facilitates full vertical and horizontal interoperability between industrial devices and systems, offering integrated security and a rich data model. Each protocol has specific characteristics, advantages, limitations, and areas of application. Likewise, the integration of the Industrial Internet of Things (IIoT) allows sensors and equipment to be connected to the Internet to improve efficiency, interoperability, and real-time data management, transforming traditional industrial communication. Another key impact of IIoT is interoperability. IIoT communication standards (such as OPC UA and MQTT) allow devices from different manufacturers to exchange information in a standardized way. For example, OPC UA works over TCP/IP and HTTPS, enabling firewall-friendly communication between control systems and the cloud. For the development of this work, documented research and case studies were reviewed and compared in order to analyze aspects such as performance, latency, interoperability, and cybersecurity of industrial networks.

***Keywords*****:** automation, networks, protocols, communication, cybersecurity.

## Tabla de Contenido

## Lista de Figuras

## Lista de Tablas

## Lista de Apéndices

## Introducción

La Industria 4.0 representa una de las transformaciones más significativas en el ámbito productivo y tecnológico de las últimas décadas. Este modelo se caracteriza por la integración de sistemas ciberfísicos, el uso de tecnologías digitales avanzadas, la interconexión de dispositivos inteligentes y la automatización flexible de procesos (Kagermann y otros, 2018). En este contexto, las redes de comunicación industrial se consolidan como un eje fundamental, ya que permiten la interacción fluida entre sensores, actuadores, controladores, sistemas de supervisión y plataformas de análisis de datos. Sin una infraestructura de comunicación eficiente, confiable y segura, la implementación de entornos productivos inteligentes resultaría limitada e incluso inviable (García, 2019a).

La transición de protocolos tradicionales hacia soluciones basadas en Ethernet industrial, junto con la incorporación del Internet Industrial de las Cosas (IIoT), ha abierto nuevas oportunidades para optimizar procesos en tiempo real (Fernández, 2020). Sin embargo, este avance también plantea desafíos relacionados con la interoperabilidad, la ciberseguridad, la gestión del tráfico de datos y la escalabilidad de las redes industriales (Pérez & Martínez, 2018a). En este escenario, la comparación de protocolos como MODBUS, PROFINET y OPC UA se vuelve relevante para comprender sus ventajas, limitaciones y aplicaciones en distintos contextos de la industria (Stallings, 2017a).

El presente trabajo se centra en el análisis crítico y comparativo de estos protocolos de comunicación, considerando su desempeño, vulnerabilidades y posibilidades de integración en arquitecturas modernas. Además, se examinan estudios de caso documentados que muestran la aplicación de dichas tecnologías en sectores como la manufactura, la energía y la automatización

de procesos, lo cual permite extraer aprendizajes y buenas prácticas aplicables al contexto colombiano (González y otros, 2021).

En términos metodológicos, esta monografía se fundamenta en una revisión documental de literatura científica, técnica y normativa reciente, complementada con diagramas y esquemas que ilustran las topologías de red y los mecanismos de seguridad más empleados en la actualidad. A partir de este análisis, se realizan recomendaciones y lineamientos que pueden servir de guía para el diseño de redes industriales robustas, seguras y resilientes.

De esta manera, el trabajo no solo aporta una revisión crítica sobre las comunicaciones industriales en el marco de la Industria 4.0, sino que también busca ofrecer insumos que fortalezcan la formación académica y el ejercicio profesional de los tecnólogos en automatización electrónica industrial, aportando al desarrollo tecnológico y competitivo de la industria nacional (VANEGAS, 2024).

## Planteamiento del Problema

La interconexión de dispositivos y sistemas a través de redes de comunicación se ha convertido en un pilar fundamental para la competitividad y eficiencia de las operaciones industriales. La adopción de tecnologías emergentes, como el Internet Industrial de las Cosas (IIoT), ha impulsado la necesidad de integrar protocolos avanzados (MODBUS, PROFINET y OPC UA) en infraestructuras que históricamente han operado con sistemas de comunicación tradicionales.

La transformación digital enmarcada en la Industria 4.0 ha generado un cambio profundo en los procesos industriales, donde la conectividad y la interoperabilidad entre máquinas, sistemas y personas se han convertido en factores determinantes para la competitividad empresarial. La interconexión de dispositivos a través de redes industriales de comunicación constituye la columna vertebral de este ecosistema, ya que permite la recopilación, transmisión y análisis de grandes volúmenes de datos en tiempo real. Sin embargo, esta evolución tecnológica plantea una serie de desafíos que afectan directamente la eficiencia, seguridad y escalabilidad de las plantas industriales.

Uno de los principales problemas es la interoperabilidad entre dispositivos y sistemas heterogéneos. Tradicionalmente, cada fabricante ha desarrollado sus propios protocolos y estándares, lo que dificulta la integración en entornos de producción modernos. A pesar de los esfuerzos de estandarización, todavía existen barreras técnicas que limitan la comunicación fluida entre equipos de diferentes marcas. Esto impacta la capacidad de las industrias para implementar soluciones de automatización flexibles y escalables.

Otro reto crítico es la ciberseguridad. A medida que las redes industriales se abren a la conectividad con tecnologías de información (TI) y al Internet Industrial de las Cosas (IIoT),

aumenta la superficie de ataque y la exposición a amenazas digitales, esto convierte la protección de infraestructuras industriales en un requisito inaplazable.

La optimización del tráfico de datos representa un tercer problema. Las redes industriales modernas deben manejar un alto volumen de información proveniente de sensores, actuadores y sistemas de supervisión. Factores como la latencia y la pérdida de paquetes pueden degradar la calidad de los procesos productivos, afectando la sincronización y la confiabilidad de la operación (Stallings, 2017b). En industrias altamente sensibles como la farmacéutica, la automotriz o la energética, un retraso de milisegundos puede implicar pérdidas económicas o riesgos para la seguridad.

Así, surge la necesidad de garantizar la escalabilidad y adaptabilidad de las redes. La incorporación de nuevas tecnologías, equipos y protocolos no puede interrumpir la operación crítica de las plantas. Esto obliga a diseñar arquitecturas de red flexibles, capaces de evolucionar sin sacrificar la continuidad del negocio (Sauter, 2021).

Los problemas de interoperabilidad, ciberseguridad, optimización del tráfico de datos y escalabilidad representan barreras que las empresas deben superar para implementar redes industriales robustas en el marco de la Industria 4.0. Ante este panorama, se hace necesario desarrollar un análisis crítico y comparativo de los protocolos de comunicación más relevantes como MODBUS, PROFINET y OPC UA, con el fin de identificar sus fortalezas y limitaciones, y de esta manera proponer lineamientos que orienten el diseño de infraestructuras resilientes y seguras.

De aquí se desprende la pregunta de investigación que orienta este trabajo: ¿Qué características y limitaciones presentan los protocolos de comunicación industrial actuales para garantizar redes industriales seguras y eficientes en el marco de la Industria 4.0?

Y define el objetivo general del estudio: analizar el desempeño de los protocolos MODBUS, PROFINET y OPC UA en dichos sistemas. Los objetivos específicos, por su parte, se orientan a identificar buenas prácticas de implementación, detectar vulnerabilidades y evaluar la eficiencia operativa de cada protocolo considerando las exigencias del IIoT e Industria 4.0. La selección de MODBUS, PROFINET y OPC UA como foco del estudio se justifica por su relevancia representativa en la evolución de las redes industriales.

Modbus es un protocolo legado ampliamente adoptado por su confiabilidad básica en sistemas sencillos, Profinet ejemplifica la transición a Ethernet industrial que aporta alta velocidad y estandarización y OPC UA simboliza la interoperabilidad contemporánea mediante un modelo de datos unificado que facilita intercambios seguros de información.

Esta elección asegura que el análisis abarque las dimensiones técnicas esenciales del problema planteado. Además, el estudio se conecta con tendencias emergentes: la Industria 4.0 impulsa la innovación y competitividad global y demanda protocolos flexibles e integrados; no obstante, en Colombia estos avances se ven frenados por la limitada inversión en digitalización. En consecuencia, la presente monografía adopta un enfoque técnico y contextual para extraer conclusiones sobre buenas prácticas, vulnerabilidades y eficiencia de las comunicaciones industriales modernas, cerrando el planteamiento con una perspectiva amplia y coherente con los objetivos formulados.

## Justificación

La importancia de esta monografía radica en la creciente digitalización y modernización de redes de comunicación industrial que se han convertido en un componente esencial para garantizar el funcionamiento eficiente, seguro y flexible de los procesos productivos en la era de la Industria 4.0. La investigación sobre los protocolos industriales y sus características no solo resulta relevante desde una perspectiva técnica, sino que también tiene un impacto directo en la competitividad empresarial, al facilitar la interoperabilidad, reducir costos derivados de fallas y optimizar la toma de decisiones en tiempo real, en este sentido, se justifica la necesidad de identificar y describir los principales protocolos de comunicación industrial (MODBUS, PROFINET y OPC UA), como punto de partida para comprender su importancia en los entornos industriales actuales.

En primer lugar, este trabajo aporta a la optimización de procesos industriales, ya que permite identificar fortalezas y limitaciones de protocolos como MODBUS, PROFINET y OPC UA, así como analizar las condiciones en las que cada uno resulta más eficiente. Con ello, se ofrece a los tecnólogos en automatización electrónica industrial un marco de referencia sólido que favorece la selección adecuada de tecnologías de comunicación para escenarios específicos.

En segundo lugar, la investigación es pertinente desde el punto de vista de la ciberseguridad industrial. La creciente interconexión de dispositivos mediante IIoT amplía la superficie de ataque, exponiendo a las redes industriales a riesgos de interrupciones, manipulación de datos y vulnerabilidades críticas. Por ello, se vuelve imprescindible examinar vulnerabilidades y riesgos presentes en las redes industriales, así como considerar los mecanismos de protección descritos en la literatura científicas. El análisis comparativo de estrategias de seguridad propuestas en estudios previos permite, formular lineamientos prácticos

de protección que pueden ser considerados en la implementación de infraestructuras industriales (Pérez & Martínez, 2018c).

Además, este trabajo contribuye a la innovación y adaptabilidad tecnológica, dado que proporciona una visión integral de cómo los diferentes protocolos se articulan con la transición hacia la convergencia IT/OT. Esto resulta crucial para la industria colombiana, que enfrenta el reto de modernizar infraestructuras heredadas mientras mantiene la continuidad de la operación (UNAD, 2019). En este contexto, se incorpora el estudio de casos documentados a nivel internacional, latinoamericano y nacional con la información existente disponible, con el fin de comprender el impacto real que tiene la implementación de estos protocolos en diversos entornos productivos.

La pertinencia de esta investigación radica en la importancia estratégica que tienen las redes de comunicación en entornos industriales y en cómo se adecua e influye en la productividad y la seguridad. De esta manera, el analizar los protocolos, vulnerabilidades y estrategias de seguridad permite, sentar bases teóricas sólidas para la formación de tecnólogos en automatización electrónica industrial, y al mismo tiempo, contribuir a la modernización de la industria colombiana en un contexto global altamente competitivo, con base en el análisis y los estudios de caso desarrollados, se busca proponer lineamientos que aporten a la competitividad y modernización, lo cual impacta directamente a la sostenibilidad tecnológica de la industria nacional.

Por último, la monografía no pretende generar una solución técnica inmediata, sino que busca organizar, analizar y sintetizar información existente de manera crítica. De esta forma, se convierte en una herramienta académica que fortalece el proceso formativo del estudiante y

ofrece a la comunidad académica y empresarial un documento de consulta para comprender mejor las dinámicas de comunicación en entornos de automatización industrial.

# Objetivos

## Objetivo General

Analizar y evaluar protocolos e infraestructuras de comunicación industrial, identificando fortalezas, limitaciones y estrategias que optimicen la interoperabilidad, seguridad y eficiencia en entornos de automatización industrial, en el marco de la industria 4.0.

## Objetivos Específicos

Identificar y describir los principales protocolos de comunicación industrial (MODBUS, PROFINET, OPC UA) y su evolución.

Analizar las ventajas, limitaciones y niveles de desempeño de dichos protocolos, identificando aspectos claves relacionados con la interoperabilidad y la eficiencia.

Examinar vulnerabilidades y riesgos en redes industriales, así como medidas de ciberseguridad propuestas en la literatura.

Comparar estudios de caso documentados sobre implementación de protocolos y su impacto en la operación.

Proponer lineamientos de buenas prácticas para el diseño de redes industriales robustas y seguras.

## Metodología

El presente estudio adoptó un enfoque documental y cualitativo, centrado en la revisión sistemática de fuentes secundarias relevantes. Según (Reyes-Ruiz, 2020), la investigación documental consistió en "recolectar, recopilar y seleccionar información de lecturas de documentos" con observación crítica en el análisis de datos. El propósito fue construir un panorama teórico de las comunicaciones y redes industriales, analizando críticamente teorías y resultados previos para generar nuevas interpretaciones cualitativas.

Se empleó una amplia variedad de documentos especializados, en revistas indexadas y actas de conferencias especializadas en automatización industrial, libros y monografías técnicas de ingeniería de control y comunicaciones, así como informes académicos (tesis de posgrado, reportes de investigación) de universidades y centros técnicos. Además, se consideraron normas y estándares industriales relevantes, dado su valor técnico para el tema. También se exploraron repositorios digitales y bases de datos académicas y catálogos de bibliotecas institucionales. Estas fuentes combinan documentación impresa y electrónica, siguiendo la recomendación de incluir fuentes diversas para obtener una visión amplia y profunda del objeto de estudio. En particular, se aprovechó la búsqueda en Internet y en repositorios universitarios para acceder a material actual y confiable.

Los documentos se seleccionaron con base en criterios estrictos de pertinencia y calidad. Se priorizaron fuentes actuales de los años 2015-2025 (de la última década aproximadamente) para garantizar vigencia de la información. Asimismo, se evaluó la relevancia técnica: solo se incluyeron textos que abordaran directamente protocolos, topologías o conceptos de comunicaciones y redes industriales. Se favorecieron documentos con autoría reconocida y rigor científico. De acuerdo con la bibliografía metodológica (García M. C., 2025), los criterios de

selección consideraron la relevancia temática, la credibilidad, metodología rigurosa, la autoría o de procedencia reconocida y la actualidad de la publicación. En suma, se escogieron fuentes pertinentes, confiables y recientes, descartando materiales obsoletos, poco fiables o fuera de contexto, para sustentar sólidamente el estudio.

El trabajo siguió un proceso ordenado de revisión documental. Se sintetizo las principales fases de la siguiente manera.

Búsqueda y recopilación. Se definieron palabras clave relevantes y se realizaron búsquedas avanzadas en bases de datos científicas y catálogos digitales. Se obtuvieron copias de los documentos potencialmente relevantes. Conforme al plan de trabajo preestablecido, cada fuente identificada fue localizada y registrada, organizándose en un gestor bibliográfico o fichas de trabajo. Este registro contenía los datos bibliográficos completos para facilitar las citas posteriores.

Lectura crítica y anotación. Cada documento se leyó de forma detallada y crítica. Durante la lectura se extrajeron conceptos clave, definiciones y resultados importantes, anotando citas textuales o resúmenes en fichas de trabajo. Fue fundamental analizar y sintetizar la información de cada fuente, elaborando fichas que permitan citar, resumir y parafrasear el contenido. Este proceso implicó contrastar los datos de diferentes fuentes y detectar coincidencias o discrepancias en los enfoques teóricos.

Síntesis e integración. Las ideas extraídas se integraron en la redacción del presente documento. Durante la redacción se cuidó la coherencia lógica: primero se presentaron los conceptos teóricos generales, y luego los desarrollos específicos de las comunicaciones industriales. Todas las fuentes se citaron conforme a las normas APA 7a Edición, reconociendo debidamente a cada autor e institución. Este paso cumplió con la ética académica: según (Chong,

2007), al trabajar con cualquier tipo de fuentes documentales se debe otorgar crédito a los autores originales.

Alcance y limitaciones. El estudio se circunscribe a un análisis teórico basado en literatura existente. En consecuencia, no se incluyeron datos primarios ni experimentos de campo. Como señalan varios autores, la investigación documental se apoya en datos secundarios, por lo que sus conclusiones dependen de la calidad de la información publicada. Por ende, los resultados aportan una visión panorámica y conceptual de las comunicaciones industriales, pero no permiten validar empíricamente los hallazgos. Entre las limitaciones inherentes se reconoce la posible obsolescencia de algunos documentos, así como sesgos de publicación; igualmente, el enfoque documental impide la obtención de mediciones directas o datos cuantitativos propios. Sin embargo, al ser un estudio cualitativo de carácter bibliográfico, estas limitaciones fueron asumidas desde el diseño, delimitando claramente el alcance teórico del trabajo sin pretender generalizar más allá de la evidencia documental consultada.

# Marco Conceptual

El análisis de las redes de comunicación industrial en el marco de la Industria 4.0 exige una comprensión clara de los conceptos fundamentales que las sustentan. Estos abarcan desde la automatización de procesos y la evolución de las infraestructuras de red, hasta el papel de los protocolos de comunicación, la integración del Internet Industrial de las Cosas (IIoT) y los desafíos de la ciberseguridad. La definición de estas categorías conceptuales no solo permite delimitar el alcance de la investigación, sino también establecer un marco de referencia coherente para interpretar la literatura revisada y orientar el análisis comparativo de los protocolos más utilizados en entornos productivos modernos (García, 2019; Fernández, 2020).

El estudio de las redes de comunicación industrial y su papel en la Industria 4.0 ha sido ampliamente abordado en la literatura científica y técnica durante las últimas dos décadas. Sin embargo, los enfoques han evolucionado desde la simple comparación de protocolos de campo hasta el análisis de su integración con tecnologías emergentes. A continuación, se presenta una revisión crítica de los aportes más relevantes.

## Conceptos Fundamentales de la Industria 4.0

### *Industria 4.0*

El concepto de Industria 4.0 describe la cuarta revolución industrial, caracterizada por la digitalización, la automatización avanzada, la integración de sistemas ciberfísicos y el uso de inteligencia artificial para la toma de decisiones (Kagermann y otros, 2022). En este marco, las redes de comunicación industrial son el pilar que hace posible la conectividad y la sincronización de procesos inteligentes.

El término industria 4.0 se utiliza de manera generalizada en Europa, si bien se acuñó en Alemania. También es habitual referirse a este concepto con términos como “Fábrica

Inteligente” o "Internet industrial". En definitiva, se trata de la aplicación a la industria del modelo "Internet de las cosas" (IoT). Todos estos términos tienen en común el reconocimiento de que los procesos de fabricación se encuentran en un proceso de transformación digital, una "revolución industrial" producida por el avance de las tecnologías de la información y, particularmente, de la informática y el software.

La industria colombiana se enfrenta a la nueva era de la industrialización llamada “Industria 4.0”. Como lo define (Galvis & Palacio, 2018). Este nuevo paradigma implica la utilización de tecnologías tales como IoT (Internet de las Cosas), Análisis de información en la nube (Big Data), ciberseguridad, manufactura adaptable, automatización y robotización de procesos. Tecnologías que mejorarían sustancialmente la productividad del país haciéndola más eficiente en el uso de los recursos, mejorando la seguridad en la producción. En consecuencia, más confiable y rentable.

En la práctica, la Industria 4.0 no es una sola tecnología sino la confluencia de varias: automatización (PLCs, SCADA, robots), redes industriales (Ethernet industrial, fibra, 5G), protocolos (MODBUS, PROFINET, OPC UA), plataformas IIoT (sensores inteligentes, gateways, nube) y medidas de ciberseguridad. En Colombia esta convergencia se está impulsando desde dos frentes: la política pública y los grandes proyectos corporativos. El Estado impulsa capacidades digitales y ecosistemas, mientras que compañías líderes implementan pilotos y despliegues industriales que sirven como casos de uso para el resto del país.

### *Integración del IIoT y Convergencia IT/OT*

El Internet Industrial de las Cosas (IIoT) ha potenciado la interconexión de dispositivos inteligentes, permitiendo recopilar datos en tiempo real para análisis avanzados y mantenimiento predictivo.

La Convergencia IT/OT es el proceso mediante el cual las Tecnologías de la Información (IT), como sistemas informáticos, redes corporativas, servidores, software empresarial, bases de datos y aplicaciones de gestión, se integran y conectan de forma estratégica con las Tecnologías de Operación (OT),como PLC, SCADA, sensores, actuadores, redes industriales, instrumentación y sistemas de control de procesos, dentro de una organización industrial, con la llegada de la Industria 4.0, la digitalización, el IIoT y la demanda de procesos más inteligentes, eficientes y conectados, ambos dominios están obligados a trabajar juntos, compartiendo datos y capacidades.

Las Tecnologías operativas (OT) han experimentado considerables avances gracias a soluciones como el Internet Industrial de las Cosas (IIoT), la automatización, los sistemas de control de procesos (SCADA) y de los PLC, entre otros, logrando un mejoramiento en la eficiencia y la conectividad en las operaciones industriales. Por otro lado, se encuentran las Tecnologías de la Información (IT) que proporcionan a una organización la automatización de procesos, almacenamiento y gestión de datos, análisis y reportes y mejoramiento de la productividad, dando lugar al desarrollo de soluciones en forma de sistemas de información logren operar en infraestructuras con altos estándares de servicio, satisfaciendo las necesidades de transacciones lógicas (Isaza, 2024).

No obstante, la incorporación del IIoT también genera desafíos relacionados con la sobrecarga de datos, estandarización de protocolos y compatibilidad entre plataformas. En este contexto, protocolos como OPC UA cobran protagonismo al facilitar la comunicación entre distintos niveles de la cadena productiva, desde sensores hasta sistemas en la nube.

### *Computación en el Borde*

Es un paradigma distribuido que traslada parte del procesamiento, análisis y almacenamiento de datos desde servidores centrales o nubes hacia dispositivos o nodos ubicados lo más cerca posible de la fuente de datos (sensores, controladores, cámaras, servidores locales). El objetivo principal es reducir latencia, ahorrar ancho de banda, mantener la continuidad operativa cuando la conexión a la nube es intermitente y preservar la privacidad y seguridad de datos sensibles al no enviarlos innecesariamente a centros remotos (Satyanarayanan, 2017a).

En términos prácticos, en lugar de enviar todos los datos al centro para procesarlos, el edge filtra, agrega o analiza localmente los datos relevantes y envía solo los resultados o los eventos importantes a la nube para almacenamiento histórico, análisis a gran escala o entrenar modelos (NIST, 2020).

### *Fabricación Inteligente*

Es la aplicación de tecnologías digitales. IIoT, sensores, automatización avanzada, analítica de datos, inteligencia artificial, computación en el borde y la nube, para crear sistemas de producción altamente conectados, adaptativos y orientados a datos que responden en tiempo real a cambios en la demanda, en las condiciones de la planta y en la cadena de suministro. La meta es orquestar de forma integrada los procesos físicos, digitales y de negocio para lograr mayor eficiencia, flexibilidad, calidad y competitividad (NIST, 2023).

Smart manufacturing no es sólo introducir sensores o automatizar tareas: es rediseñar procesos productivos alrededor de datos, adoptando una arquitectura tecnológica y organizativa que permita operaciones autónomas, resilientes y centradas en el valor. Su adopción ofrece ventajas competitivas claras, pero requiere planificación técnica, gobernanza de datos y atención a la seguridad y capacidades humanas.

### *Sistemas CPS*

Los Sistemas Ciber-Físicos son sistemas integrados donde componentes físicos (máquinas, sensores, actuadores, procesos) y componentes computacionales, virtuales (software, redes, algoritmos de control, análisis) interactúan estrechamente en tiempo real. En un CPS la frontera entre lo "físico" y lo "digital" se difumina, los procesos físicos generan datos que el software procesa y, a su vez, el software toma decisiones que modifican el mundo físico mediante actuadores.

Los CPS son el corazón de la Industria 4.0, combinan sensores, control y software para permitir sistemas que perciben, analizan y actúan sobre el mundo físico de forma coordinada. Cuando se diseñan bien, ofrecen mejoras sustantivas en eficiencia y capacidad; cuando se descuidan, especialmente en seguridad o en requisitos de tiempo real, pueden introducir riesgos operacionales y de seguridad física. En el contexto industrial, su desarrollo exitoso exige una integración cuidadosa de comunicaciones (protocolos adecuados), arquitectura (edge/cloud), y prácticas de ciberseguridad y gobernanza.

### *Big Data Industrial*

El Big Data industrial es el proceso de recolección, almacenamiento, procesamiento y análisis de grandes volúmenes de datos generados por máquinas, sensores, sistemas de control y plataformas digitales dentro de entornos industriales. Su propósito es transformar esos datos en información útil para mejorar la eficiencia, la calidad, la seguridad y la toma de decisiones estratégicas en una empresa, permite que la industria pase de simplemente "medir" a comprender profundamente sus procesos, identificar patrones, predecir fallas y optimizar operaciones.

El Big Data industrial convierte la inmensa cantidad de datos generados por máquinas, sensores y sistemas de control en información valiosa para mejorar procesos, reducir fallas y

aumentar la competitividad. Es un habilitador clave de la Industria 4.0 y un componente esencial de la automatización moderna.

## Conceptos Fundamentales de las Redes Industriales

### *Red Industrial*

Es una infraestructura de comunicación diseñada específicamente para conectar dispositivos y sistemas que monitorean, supervisan y controlan procesos físicos en plantas industriales (PLC, RTU, DCS, HMI, SCADA, sensores, actuadores, etc). Su propósito principal no es el intercambio general de información empresarial, sino garantizar el control fiable, con requisitos de disponibilidad, determinismo y seguridad que sostienen procesos productivos continuos y críticos.

### *Arquitecturas de Comunicación OT*

Son los esquemas organizados (topologías, protocolos y componentes) que permiten que los dispositivos y sistemas de control industrial, PLC, RTU, DCS, HMI, SCADA, sensores, actuadores, sistemas Historian/MES, intercambien información entre sí y con sistemas corporativos. Su finalidad principal no es el intercambio general de información de oficina, sino garantizar control fiable y determinista de procesos físicos, con requisitos estrictos de latencia, disponibilidad y seguridad.

### *Latencia*

Es el tiempo que tarda un paquete de datos (o una señal) en viajar desde su origen hasta su destino. En redes se suele hablar de round trip time (RTT), tiempo de ida y vuelta, o tiempo de un solo sentido. La latencia condiciona la capacidad de una red para soportar aplicaciones en tiempo real: controles, sincronización, visión artificial, etc.

La latencia es una magnitud crítica en redes industriales: no solo importa su valor medio, sino la consistencia (jitter). Comprender sus componentes (propagación, transmisión, procesamiento, colas) permite estimarla y reducirla mediante diseño (edge, TSN, QoS, hardware especializado). En proyectos industriales define requisitos claros (máximos y percentiles) y verifica con mediciones reales en condiciones de carga.

***Determinismo***

En el contexto de los sistemas de comunicación industrial, el determinismo se refiere a la capacidad de una red o sistema de garantizar que un evento, dato o mensaje ocurrirá dentro de un tiempo conocido, fijo y predecible. Esto significa que no solo se espera que la comunicación sea rápida, sino que siempre ocurrirá dentro del mismo intervalo de tiempo, sin variaciones significativas.

En otras palabras, un sistema determinista entrega datos con tiempos de respuesta constantes y garantizados, esenciales para procesos industriales donde el sincronismo y la precisión temporal impactan directamente la seguridad, calidad del producto y continuidad de la operación.

Autores como (Zurawski, 2015), señalan que el determinismo es el principio que diferencia redes industriales de redes tradicionales, ya que en entornos de control automático se debe asegurar que la comunicación no dependa de aleatoriedad ni congestión como ocurre en redes IT convencionales.

***Interoperabilidad***

En el contexto de la automatización industrial, la interoperabilidad es la capacidad que tienen distintos dispositivos, sistemas, protocolos o plataformas, fabricados por diferentes proveedores o basados en tecnologías distintas, para comunicarse, intercambiar datos y operar

conjuntamente de manera efectiva, sin requerir adaptaciones manuales o configuraciones complejas.

Según la International Electrotechnical Commission (IEC), la interoperabilidad implica que los sistemas pueden entender, procesar y utilizar la información enviada por otros sistemas de forma coherente y estandarizada (IEC, 2019a)

En términos prácticos, la interoperabilidad permite que un sensor, un PLC, un sistema SCADA, un software MES o una plataforma en la nube interactúen sin importar el fabricante o el protocolo de comunicación.

### *Topologías Industriales*

La topología describe la forma en que están conectados físicamente (o lógicamente) los nodos de una red y cómo circula la información entre ellos. En entornos industriales la topología condiciona la latencia, la disponibilidad, la facilidad de diagnóstico, el coste de cableado y la posibilidad de implementar redundancia. Las decisiones sobre topología deben alinearse con requisitos de control, seguridad y continuidad operacional.

Para efectos de esta investigación a continuación se dará descripción de los tres tipos de topología más relevantes.

**Topología Estrella.** Todos los dispositivos se conectan a un punto central. En Ethernet moderna esto equivale a una red conmutada donde cada nodo tiene un enlace dedicado al switch.

**Topología Bus**. Todos los nodos comparten un mismo medio físico (bus), históricamente típica de fieldbuses serie (RS-485/Modbus RTU, Profibus DP) donde los dispositivos se conectan en cadena a un cable común. En Ethernet actual el “bus” suele ser más una topología lógica que física.

**Topología Anillo.** Los nodos se conectan formando un lazo cerrado; el tráfico circula por lazo y existen mecanismos de conmutación para mantener la comunicación ante fallo. En la industria se usan variantes con protocolos de recuperación rápida (MRP, PRP/HSR, REP) para alta disponibilidad.

## Conceptos de Seguridad Industrial

### *Ciberseguridad OT*

Es el conjunto de políticas, procesos, tecnologías y controles aplicados específicamente para proteger los sistemas de control industrial (ICS), los controladores lógicos programables (PLC), sistemas SCADA, RTU y demás elementos de la tecnología operacional frente a amenazas digitales y físicas que puedan comprometer la disponibilidad, integridad o seguridad física de procesos industriales. Su objetivo prioriza la continuidad operacional y la seguridad física, además de la protección de la información.

### *Ataque MITM*

Ocurre cuando un adversario se posiciona entre dos partes que creen comunicarse directamente, con la capacidad de interceptar, leer, modificar o reenviar los mensajes que se intercambian. En esencia el atacante crea dos canales separados y los hace parecer como una única conexión legítima para las víctimas.

Desde el punto de vista técnico, un MITM puede ser pasivo o activo. Para realizarlo el atacante típicamente necesita capacidad para redirigir o interceptar tráfico (control de un router, estar en la misma subred, manipular entradas DNS o ARP), y a partir de ahí puede aplicar lectura, modificación, reenvío o repetición de mensajes (OWASP, 2025).

***Criptografía***

Es la disciplina científica y técnica que se dedica a diseñar y aplicar métodos para transformar información de forma que solo las partes autorizadas puedan acceder a su contenido. Básicamente convierte un mensaje legible en un formato codificado o cifrado, y solo quien posee la clave correcta puede descifrarlo para recuperar el mensaje original. Esta técnica busca proteger la confidencialidad de los datos frente a posibles interceptores (IBM, 2025).

***Infraestructura Crítica***

Se refiere a todos los sistemas, activos, instalaciones y servicios esenciales cuya interrupción o afectación puede generar un impacto grave en la seguridad nacional, la economía, la salud pública o el bienestar de una sociedad. Estos incluyen sectores como energía, transporte, agua potable, telecomunicaciones, salud, finanzas y servicios gubernamentales. La característica principal de estas infraestructuras es que su funcionamiento continuo es indispensable para el desarrollo de un país y para la protección de la vida humana (CISA, 2023).

# Marco Teórico

Antes de la aparición de redes industriales modernas, la automatización dependía de señales analógicas (4-20 mA) para transmitir información de sensores y actuar sobre dispositivos. Esto implicaba cableado extenso, limitada flexibilidad y poca interoperabilidad. Con el avance de la electrónica y los primeros controladores lógicos programables (PLC), surgió la necesidad de digitalizar la comunicación entre dispositivos de control y campo. Es así como comienzan los primeros desarrollos orientados a comunicaciones más estructuradas en la industria (Campo, 2020).

Es imperativo explicar conceptos fundamentales con la finalidad de entender la transición hacia las redes de comunicación moderna.

## Historia y Evolución de las Redes Industriales

### *Evolución de las Redes Industriales*

En la primera etapa, las investigaciones se centraron en los protocolos de buses de campo (Fieldbus, DeviceNet, Profibus), cuyo objetivo era reemplazar sistemas cableados punto a punto con redes más organizadas y eficientes. Según la (IEC, 2019), la Norma IEC 61158 estableció las bases para la estandarización de protocolos de comunicación industrial, generando un marco de interoperabilidad básica en la automatización, sistemas de control como, computadoras o robot, para manejar procesos industriales y maquinaria con el fin de mejorar la eficiencia, productividad y calidad.

Las redes industriales permiten que los datos circulen entre PLCs, HMIs y servidores. La infraestructura física ha evolucionado, además del bus campo tradicional se usan redes Ethernet deterministas y enlaces de alto ancho de banda que soportan video, teleasistencia y sincronización en tiempo real.

Este concepto es la base para entender la integración de redes y protocolos que permiten la comunicación entre diferentes dispositivos y sistemas. Las redes industriales son infraestructuras de comunicación diseñadas específicamente para entornos industriales, en las cuales se interconectan dispositivos, controladores, sensores y sistemas de supervisión. A diferencia de las redes convencionales, deben responder a altos requisitos de confiabilidad, baja latencia y resistencia a interferencias electromagnéticas y condiciones ambientales adversas.

Con la expansión de Ethernet industrial, surgieron investigaciones que evaluaron la capacidad de este estándar para soportar aplicaciones en tiempo real. (García, 2019b) destaca que el uso de Ethernet permitió incrementar la velocidad de transmisión, pero también exigió nuevas arquitecturas y técnicas de priorización del tráfico para garantizar la estabilidad de los procesos críticos.

***Buses de Campo Tradicionales a Ethernet Industrial***

La etapa inicial de la comunicación industrial partió de señales analógicas (4-20 mA, 0-10 V) y cableado punto a punto para sensores y actuadores; estas soluciones eran robustas pero rígidas y costosas en cableado y mantenimiento, lo que motivó la necesidad de digitalizar las comunicaciones en planta para facilitar diagnóstico, expansión y control distribuido.

En respuesta a esa necesidad surgieron los fieldbuses (buses de campo) desde finales de los años 70 y durante los 80-90, protocolos como Modbus, Profibus y otros permitieron multiplexar señales digitales sobre un solo medio, reducir cableado y unificar la comunicación entre PLCs, I/O remota y dispositivos de instrumentación. Estas tecnologías estandarizaron capas de servicio y perfiles de dispositivo, facilitando la interoperabilidad dentro de sus respectivos ecosistemas.

La maduración de los fieldbuses también mostró límites: proliferaron muchos estándares, cada uno optimizado para ciertas aplicaciones, lo que generó fragmentación y complicó la interconexión multiplataforma a nivel planta, empresa; además, los requisitos crecientes de datos y conectividad hicieron evidentes las limitaciones de ancho de banda y escalabilidad de muchos buses serie.

La llegada y madurez de Ethernet y la pila TCP, IP, abrieron la posibilidad de aprovechar una infraestructura de red global, con mayor ancho de banda, herramientas de gestión y compatibilidad con TI; sin embargo, Ethernet tradicional debía adaptarse para cumplir requisitos industriales, lo que impulsó el desarrollo de variantes industriales como PROFINET, EtherNet/IP, EtherCAT y Ethernet con soporte para comunicación en tiempo real.

***Limitaciones Históricas***

Los primeros protocolos industriales se diseñaron en una era en la que las redes estaban aisladas dentro de la planta y la principal preocupación era reemplazar cableado punto a punto por comunicaciones digitales sencillas.

Otra limitación frecuente fue el ancho de banda y la velocidad, protocolos serie y varios fieldbus ofrecen tasas relativamente bajas y, en consecuencia, no soportan fácilmente grandes volúmenes de telemetría, streaming o aplicaciones de visión analítica en tiempo real. Esa restricción condicionó su uso a lectura,escritura periódica de registros y a E/S no masivas, siendo insuficiente para escenarios modernos de Big Data/IIoT sin arquitecturas adicionales de agregación.

Para profundizar en la compresión de la evolución de las redes industriales, a continuación, se presenta la siguiente tabla comparativa.

**Tabla 1**

*Evolución de las Redes Industriales*

| Etapa, Periodo | Acontecimiento tecnológico, conceptual | Descripción y aporte principal | Notas relevantes |
|---|---|---|---|
| Predigital, Señales analógicas (antes 1970) | Señales punto a punto (4–20 mA, 0–10 V). | Comunicación directa sensor, control; muy robusta pero costosa en cableado y sin posibilidad de integración o diagnóstico avanzado. | Base histórica: control cableado tradicional; limitaciones en escalabilidad y flexibilidad. |
| Fieldbus, Buses de campo (1970–1990) | Protocolos Fieldbus: Modbus, Profibus, DeviceNet, FOUNDATION Fieldbus. | Reemplazan cableado punto a punto por redes compartidas; reducen cableado, permiten E/S distribuida y diagnósticos locales; aparecen iniciativas de estandarización. | Estándar IEC 61158 como referencia para estandarizar fieldbus; interoperabilidad básica entre dispositivos. |
| Proliferación de estándares, (1980–1990) | Multiplicidad de protocolos y perfiles de dispositivo. | Fragmentación del mercado con protocolos optimizados por sector; impulsó interoperabilidad vía gateways y herramientas de integración. | Ventaja: innovación; Desventaja: complejidad para integraciones multiplataforma. |
| Transición a Ethernet industrial (finales 1990–2010) | Industrial Ethernet (PROFINET, EtherNet,IP, EtherCAT). | Adopción de Ethernet,TCP,IP adaptada a OT: mayor ancho de banda, mejor integración IT,OT, diagnóstico avanzado; creación de switches gestionables y topologías modernas. | Requiere diseño para determinismo; habilita transmisión de video, teleasistencia y tráfico de mayor volumen. |
| Determinismo sobre Ethernet y mejora de sincronía (2010) | Tecnologías de tiempo real y TSN; PROFINET IRT; EtherCAT. | Aparecen mecanismos para garantizar latencias y jitter bajos sobre Ethernet; posibilitan control de movimiento y aplicaciones de alta sincronización. | Aumenta la aptitud de Ethernet para lazos críticos; demanda hardware y configuración especializados. |
| IIoT, interoperabilidad semántica y modelos de información (2010–2020) | OPC UA, MQTT, edge computing, modelos de información. | Surgen capas de interoperabilidad y seguridad (OPC UA) y arquitecturas edge/cloud que permiten analítica, gemelos digitales y gestión centralizada de datos. | Facilita IIoT y convergencia IT,OT; requiere PKI, gobernanza de datos y adaptación de legacy. |
| Conectividad avanzada y movilidad industrial (2018–2025) | Redes inalámbricas industriales, LoRa, Wi-Fi industrial, 5G privado. | Habilitan servicios de baja latencia y movilidad (teleasistencia, video en tiempo real, sensores remotos) en entornos industriales; permiten nuevos casos de uso. | Ejemplo: pruebas de 5G en refinería (Ecopetrol,Barrancabermeja) para asistencia remota; exige gestión de seguridad y cobertura. |
| Actualidad,redes seguras y convergentes (2020) | Seguridad integrada, zonificación (IEC 62443), TSN, OPC UA combinados. | La tendencia actual combina determinismo, interoperabilidad semántica y seguridad por diseño; el foco está en arquitecturas híbridas y gobernanza. | Desafíos: gestión de parches en OT, migración incremental y formación de talento. |

*Nota*. Esta tabla muestra la evolución de las redes industriales.

## Tendencias Tecnológicas Globales

Hoy en día hay muchas tendencias tecnológicas globales que aportan innovación, desarrollo y cambios generalizados, a continuación, se explican las más relevantes para la industria, redes y automatización.

### *Integración de Datos, Big Data y IIoT*

Con el volumen creciente de datos generados por sensores, máquinas, sistemas de control y plataformas digitales, la capacidad de almacenar, procesar y extraer valor se ha vuelto crítica. Tendencias como Big Data, analítica avanzada, machine learning y IoT permiten optimizar operaciones, hacer mantenimiento predictivo, mejorar eficiencia y anticipar fallos (Observatorio, 2024).

Las redes de comunicación industrial han experimentado una notable transformación en las últimas décadas, impulsada por la convergencia entre tecnologías de la información (IT) y tecnologías de operación (OT). Esta evolución responde a las crecientes demandas de eficiencia, flexibilidad, interoperabilidad y seguridad en el marco de la Industria 4.0, donde la integración de sistemas ciberfísicos y el Internet Industrial de las Cosas (IIoT) han redefinido la forma en que los procesos industriales se gestionan y supervisan (Fernández, 2020; Kagermann y otros, 2018).

Las redes de comunicación industrial han evolucionado, pasando de sistemas basados en buses de campo como Profibus o DeviceNet a arquitecturas soportadas en Ethernet industrial y protocolos orientados a servicios como OPC UA. Este cambio responde a la necesidad de mayor velocidad de transmisión, interoperabilidad entre equipos de distintos fabricantes y capacidad para integrarse con tecnologías emergentes, que impulsa la transición hacia entornos productivos más inteligentes y conectados (Fernández, 2020; Sauter, 2021).

### *Inteligencia Artificial (IA) y Automatización Inteligente*

La IA se ha consolidado como el motor principal de transformación tecnológica a nivel global. Muchas empresas ya adoptan IA, no solo para análisis de datos, sino para automatización de tareas, mantenimiento predictivo, optimización de procesos y toma de decisiones. Según un reporte reciente, la IA continúa liderando las inversiones tecnológicas en 2025 (Computing, 2025).

Por su parte, la automatización avanzada (robótica, sistemas ciber-físicos, control inteligente) permite que industrias logren mayor eficiencia, menor error humano y flexibilidad operativa, lo cual es clave en entornos industriales modernos (Rivas, 2023).

## Modelos de Referencia en Redes de Comunicación

Los modelos de referencia son esenciales para comprender los principios que rigen la transmisión de datos en sistemas industriales, el estudio de las comunicaciones industriales requiere partir de modelos conceptuales que faciliten la comprensión de cómo los datos son transmitidos, procesados y recibidos en distintos entornos. Entre los más relevantes se encuentran.

### *Modelo OSI (ISO/IEC 7498)*

Es un marco conceptual estándar de siete capas definido por la norma ISO/IEC 7498-1. Cada capa desempeña funciones específicas en la transmisión de datos: desde la conexión física hasta las aplicaciones de usuario. La separación en niveles permite la interoperabilidad: los protocolos distintos pueden comunicarse siempre que respeten las funciones asignadas a cada capa. Las siete capas que maneja este modelo son las siguientes:

Capa física (nivel 1): Define las características mecánicas y eléctricas del medio de transmisión y la manera de enviar bits por el canal físico. Establece topologías y parámetros eléctricos.

Capa de enlace de datos (nivel 2): Organiza los bits en tramas y controla el acceso al medio.

Capa de red (nivel 3): Determina la ruta óptima para enviar paquetes a su destino y maneja la congestión, permitiendo la interconexión de redes.

Capa de transporte (nivel 4): Garantiza la comunicación fiable extremo a extremo.

Capa de sesión (nivel 5): Establece y controla sesiones de comunicación entre aplicaciones.

Capa de presentación (nivel 6): Se encarga del formato, codificación y cifrado de los datos.

Capa de aplicación (nivel 7): Ofrece servicios finales al usuario y las aplicaciones (correo electrónico, transferencia de archivos, navegadores web).

***Modelo TCP/IP***

Es la arquitectura práctica usada en Internet y la mayoría de las redes actuales, el modelo TCP/IP surge de implementaciones reales: define un conjunto de protocolos estándar que especifican cómo formatear, direccionar, enviar y enrutar datos entre equipos. Esto garantiza conectividad de extremo a extremo en la red. La pila TCP/IP se organiza en cuatro capas principales.

Capa de aplicación: Incluye los protocolos de usuario final que interactúan con las aplicaciones. Proporciona servicios como correo electrónico, web y transferencia de archivos.

Capa de transporte: Gestiona la comunicación fiable entre hosts finales. Aquí actúan TCP.

Capa de internet: Contiene el protocolo IP, que se encarga del direccionamiento y del enrutamiento de paquetes entre redes.

Capa de acceso a la red: Abarca las tecnologías del nivel físico y de enlace (Ethernet, Wi-Fi, etc.) utilizadas para transmitir los paquetes en el medio físico.

***Modelo Purdue***

Es un marco arquitectónico que sistematizar la estructura de redes en plantas industriales. Divide las redes de control industrial (ICS/OT) y las redes corporativas (TI) en niveles jerárquicos basados en su función. El modelo define típicamente 6 niveles.

Nivel 0. Proceso físico: El entorno físico donde se producen bienes (reactores, líneas de montaje).

Nivel 1. Dispositivos inteligentes: Sensores y actuadores que monitorean y actúan sobre el proceso.

Nivel 2. Control de planta: Sistemas de control en tiempo real (PLC, DCS, SCADA) que supervisan y regulan el proceso.

Nivel 3. Operaciones de manufactura (MES): Sistemas de gestión de la producción que organizan el flujo de trabajo, recopilación de datos y control de calidad.

Nivel 4. Logística y planificación (ERP): Sistemas empresariales para planificación de recursos, logística, contabilidad y gestión corporativa.

Nivel 5. Redes corporativas: infraestructura de TI administrativa y de gestión (bases de datos, servidores corporativos, Internet).

### *Modelo ISA-95*

Es un modelo funcional y de integración que describe cómo deben comunicarse los sistemas empresariales y de planta. Su objetivo es definir interfaces y flujos de datos entre niveles operativos (control) y de negocio (empresa).

En términos de jerarquía, ISA-95 suele considerar los siguiente 5 niveles.

Nivel 0: Equipos del proceso (motores, válvulas, máquinas).

Nivel 1: Dispositivos de campo inteligentes (sensores, actuadores).

Nivel 2: Sistemas de control de planta (PLC, DCS, OCS).

Nivel 3: Sistemas de ejecución de manufactura (MES), que conectan la planta con sistemas de negocio.

Nivel 4: Sistemas empresariales (ERP) y de gestión de negocios (logística, finanzas, calidad).

## Ciberseguridad en las Comunicaciones Industriales

La ciberseguridad en entornos industriales comprende el conjunto de estrategias, técnicas y normas destinadas a proteger la infraestructura de comunicación contra accesos no autorizados, manipulación de datos y ataques cibernéticos. Normas internacionales como la IEC 62443 establecen directrices específicas para garantizar la protección de infraestructuras críticas.

Las redes industriales interconectan numerosos dispositivos críticos (PLC, RTU, HMI, SCADA) con sistemas corporativos e Internet, ampliando su superficie de ataque, estos entornos suelen carecer de medidas de seguridad integradas ya que fueron diseñados originalmente para la disponibilidad de procesos.

Diversos estudios han propuesto estrategias como segmentación de redes, cifrado de datos y monitoreo en tiempo real para reducir riesgos. La tendencia apunta hacia arquitecturas de

defensa en capas, en donde la seguridad debe ser considerada desde la fase de diseño de las redes.

***ISA/IEC 62443***

Es un conjunto de estándares internacionales diseñados específicamente para la ciberseguridad de los sistemas de automatización y control industrial (IACS/OT). Su enfoque es holístico, cubre desde requisitos organizacionales y de proceso hasta requisitos técnicos para sistemas y componentes, y promueve prácticas basadas en evaluación de riesgo para proteger activos industriales a lo largo de su ciclo de vida (Isa, 2025).

IEC 62443 está organizada en varias partes dirigidas a distintos públicos y propósitos: partes que abordan conceptos generales y terminología, requisitos de gestión para propietarios de activos, requisitos de proceso para integradores y proveedores de servicios, requisitos de sistema y requisitos de producto componente (cómo desarrollar dispositivos y softwares seguros). Esto permite aplicar la norma en distintos niveles (IEC, 2023).

***NIST SP 800-82***

Es una guía práctica publicada por NIST que ofrece orientación para proteger sistemas de control industrial (SCADA, DCS, PLC, RTU, etc.). El documento describe topologías típicas, amenazas y vulnerabilidades relevantes en entornos ICS, y proporciona recomendaciones y contramedidas adaptadas a las restricciones operativas de OT (NIST, 2015)

NIST SP 800-82 cubre aspectos como modelos de arquitectura de red para ICS, controles recomendados (segmentación, control de acceso, monitorización, gestión de parches con precauciones), planeamiento de respuesta a incidentes, y la adaptación de controles IT al contexto OT. El documento insiste en aplicar un enfoque basado en riesgos y en equilibrar seguridad con requisitos de disponibilidad y seguridad funcional de los procesos.

# Resultados de la Investigación

## Caracterización de los Principales Protocolos de Comunicación Industrial

La evolución de la comunicación industrial ha ido del serial a soluciones basadas en Ethernet e IoT, adaptándose a las demandas de velocidad, flexibilidad y seguridad. En este contexto.

### *Modbus*

Desarrollado en 1979 por la empresa estadounidense Modicon, en 1996 Modicon fue adquirida por Schneider Electric, que hoy mantiene el protocolo a través de la Modbus Organization creada en 2002 para gestionar sus especificacioneses, desde su origen está diseñado para uso industrial es uno de los protocolos más utilizados por su simplicidad y amplia disponibilidad, aunque carece de mecanismos avanzados de seguridad y presenta limitaciones en velocidad de transmisión, sigue siendo empleado en sistemas de supervisión y control básico. Ha sido descrito como un protocolo simple y robusto, ideal para aplicaciones de monitoreo, pero con limitaciones en seguridad y escalabilidad (Stallings, 2017c).

El propósito de este protocolo es trasmitir información entre diferentes tipos de equipos electrónicos que estén conectados a un mismo bus, es un protocolo de comunicación maestro, esclavo. Una gran cantidad de dispositivos de campo lo utilizan para lograr comunicarse con SCADA’s y PLC’s. La comunicación en Modbus lo dictamina el propio protocolo. En este caso, siempre existe un maestro que consulta datos a uno o múltiples esclavos al mismo tiempo. Se debe tener en cuenta desventajas relevantes tales como que no cuenta con características de seguridad, sin tiempo reales garantizados ni sincronizados, datos numéricos simples y limitados (16 bits) y una escalabilidad restringida por su arquitectura maestro, esclavo.

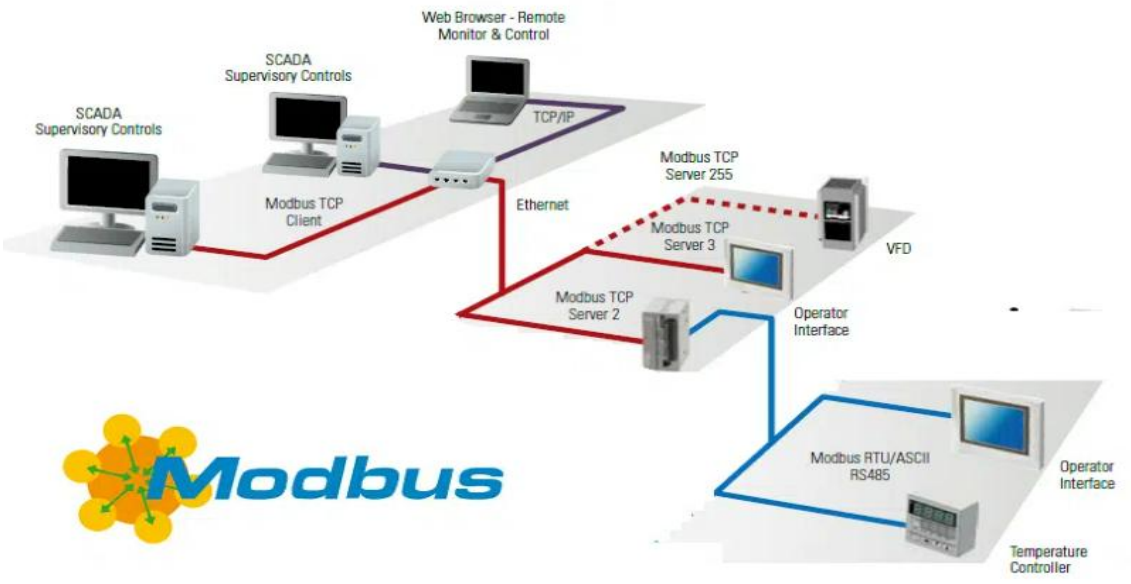
Modbus se emplea principalmente en la instrumentación de procesos continuos, el protocolo permite la lectura de variables esenciales como presión, temperatura, caudal y nivel, así como la escritura de parámetros de control asociados a bombas, válvulas y actuadores. Su implementación en sistemas SCADA ha permitido consolidar arquitecturas de supervisión robustas y de bajo costo.

Sin embargo, pese a su amplia adopción, el protocolo carece de mecanismos nativos de autenticación, cifrado o verificación de integridad. Esta característica limita su idoneidad en entornos donde la ciberseguridad constituye un requisito primario.

En consecuencia, Modbus continúa siendo crítico en aplicaciones donde se prioriza la interoperabilidad con dispositivos existentes y la economía de implementación, aunque requiere medidas compensatorias de seguridad a nivel de arquitectura.

**Figura 1**

*Protocolo Modbus*




*Nota.* Figura que explica el protocolo Modbus. Tomado Vester Training.

***Profinet***

Es un protocolo de comunicación desarrollado por la organización PROFIBUS & PROFINET International (PI) surgió a principios de los años 2000 para llevar Ethernet a la automatización, PROFIBUS & PROFINET International fue la organización que desarrolló el estándar, con el propósito original de unir las redes de automatización existentes con las arquitecturas Ethernet, mejorando el rendimiento y la integración con TI.

Está diseñado para conectar dispositivos industriales con varios tipos de equipamiento productivo, como motores, sensores y otros dispositivos electrónicos. Es un protocolo de Ethernet industrial en tiempo real para automatización de plantas, fue diseñado para ser independiente del fabricante, lo que significa que los dispositivos de diferentes marcas pueden funcionar juntos sin problemas. Además, el protocolo se ha optimizado para proporcionar un rendimiento óptimo a través de soluciones innovadoras como la detección automática de equipamiento, herramientas de diagnóstico avanzadas y recuperación rápida en caso de fallas. Estas características hacen que las redes basadas en PROFINET sean ideales para los entornos industriales modernos. (Profibus-Profinet, 2024).

Es ideal para aplicaciones críticas como robótica y control de movimiento, su implementación requiere mayor complejidad de configuración, hardware especializado, su seguridad depende de complementos (no está cifrado por defecto), es menos flexible para tratar datos complejos o cloud sin pasarela requiere OPC UA u otros protocolos superiores para IIoT, pero permite escalabilidad y alta confiabilidad.

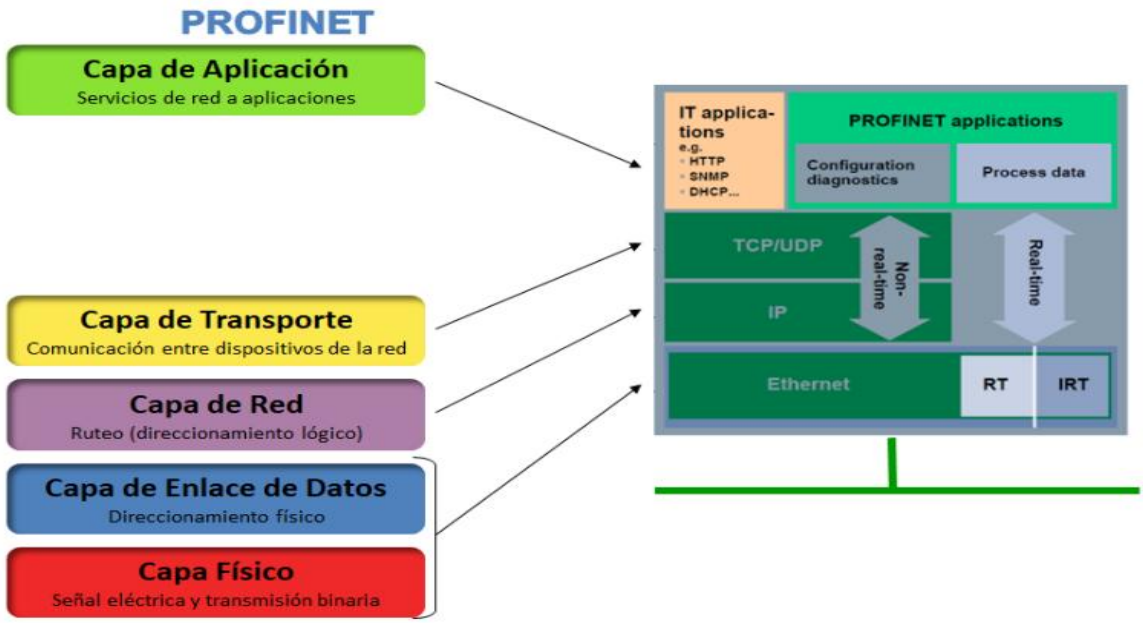
PROFINET facilita la integración de PLC, variadores de frecuencia, servomotores y dispositivos de seguridad funcional, su arquitectura distribuida permite reducir el cableado,

mejorar la capacidad de diagnóstico y habilitar configuraciones flexibles propias de la Industria 4.0.

No obstante, las implementaciones tradicionales del protocolo no incorporan cifrado extremo a extremo ni autenticación fuerte por defecto, lo que obliga a complementar su uso mediante segmentación de red, firewalls industriales y esquemas de seguridad definidos en arquitecturas como el modelo Purdue o el marco normativo IEC 62443. Así, PROFINET resulta especialmente crítico en aplicaciones donde el tiempo real determinista es un requisito operacional fundamental.

**Figura 2**

*Protocolo Profibus*




*Nota.* Figura que explica el protocolo Profinet. Tomado de profibus.

***OPC UA***

Fue desarrollado a mediados de los años 2000 como sucesor independiente de OPC clásico, tras varios años de trabajo de especificación, la Fundación OPC publicó la primera versión de OPC UA en 2006, se diseñó el estándar OPC UA para mejorar el servicio orientado a la conexión, permitiendo crear nuevas y fáciles formas de comunicarse entre diferentes sistemas operativos. Todo esto, sumado a la cuantiosa mejora en la seguridad de las conexiones, marcada por la autenticación de los usuarios en los clientes y servidores, la autorización dentro de las relaciones de comunicación OPC y la integridad de los datos, hacen del estándar OPC UA, tenga todas las especificaciones y funcionalidades de OPC Classic, pero simplificando y solucionando en gran medida los problemas de configuración conocidos del protocolo primario junto con la falta de interoperabilidad y de seguridad (Incibe, 2024).

Se caracteriza por su orientación a servicios, interoperabilidad y escalabilidad. La OPC lo reconoce como el protocolo con mayor proyección en la Industria 4.0, ya que integra dispositivos de diferentes fabricantes y soporta conexión con la nube y sistemas IIoT. plataformas de comunicación orientada a servicios que garantizan la interoperabilidad entre diferentes sistemas y dispositivos, aportando seguridad y escalabilidad, es señalado como el estándar con mayor proyección, al permitir interoperabilidad entre sistemas de distintos fabricantes y facilitar la integración con el IIoT y la nube.

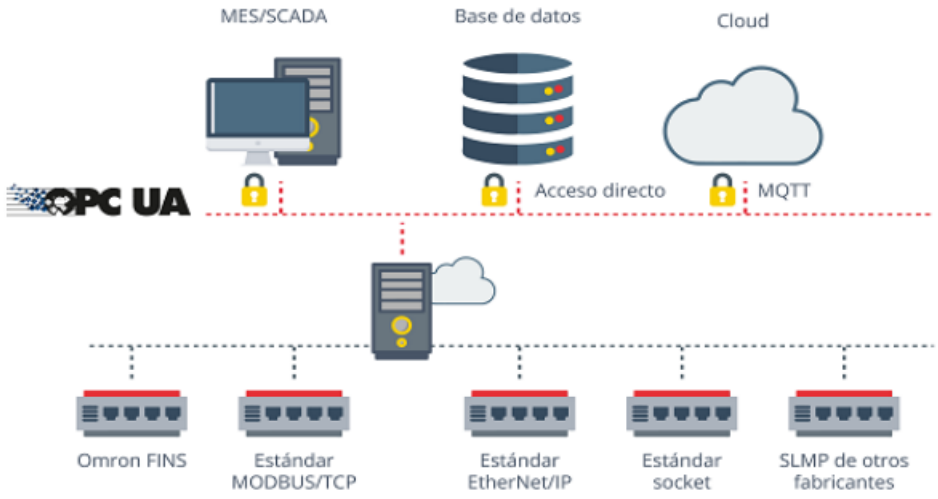
El protocolo es fundamental en estrategias de mantenimiento predictivo y digitalización industrial, ya que permite transmitir no solo valores de proceso, sino también metadatos asociados, calidad del dato y estructuras de modelado de activos. Su arquitectura cliente, servidor, junto con la incorporación de mecanismos de seguridad integrados y control de acceso

basado en roles, lo posicionan como uno de los protocolos más robustos en términos de ciberseguridad industrial.

Sin embargo, OPC UA no está diseñado para reemplazar protocolos deterministas de control de movimiento, sino para operar en niveles superiores de integración y análisis. Por ello, su papel crítico radica en la convergencia IT/OT y en la habilitación de entornos de Industria 4.0, más que en el control directo de procesos en tiempo real, se debe tener en cuenta que es un protocolo complejo y pesado; implementarlo exige recursos computacionales y configuración de PKI, su adopción requiere de inversiones en actualización de equipos y capacitación.

**Figura 3**

*Protocolo OPC UA*




*Nota.* Figura que explica el protocolo OPC UA. Tomado de incibe**.**

## Análisis de las Ventajas y Limitaciones de los Protocolos

Modbus, PROFINET y OPC UA, son protocolos ampliamente implementados representan distintas generaciones tecnológicas y responden a necesidades operativas diferenciadas dentro de la arquitectura industrial. Mientras algunos fueron concebidos para entornos de control de campo con requerimientos limitados de procesamiento y baja complejidad estructural, otros emergieron como respuesta a la necesidad de sincronización de alta precisión, modelado de información avanzada o integración semántica de datos empresariales.

En consecuencia, el presente análisis examina las ventajas y limitaciones de los protocolos en entornos industriales, evaluando su desempeño, interoperabilidad.

### *Ventajas de los Protocolos*

Modbus TCP/IP es popular por su simplicidad, apertura y bajo costo; al ser libre de derechos de autor, resulta fácil de desplegar y mantiene muy pocas restricciones de formato de datos, su estructura de mensajes y modelo de registros hacen que la implementación y depuración sean muy directas; por ello es el “lenguaje” más común en dispositivos legacy y en integraciones rápidas.

Profinet comparado con Modbus, ofrece un conjunto de funciones más robustas para automatización de alto rendimiento, integra además perfiles para diferentes dispositivos (drive, energía, proceso) y soporta TSN, lo que mejora la eficiencia de la red y la interoperabilidad entre equipos heterogéneos, ofrece latencia y jitter controlados, apto para monitoreo, control y sincronización, soporta diagnóstico a nivel dispositivo, autoconfiguración y perfiles de dispositivo, lo que facilita el mantenimiento predictivo.

OPC UA por su parte, facilita la interoperabilidad a alto nivel, al abstraer protocolos propietarios mediante servidores, cliente. OPC, permite integrar dispositivos diversos y sistemas

de planta con aplicaciones IT, OPC UA prioriza la seguridad y la portabilidad sobre el rendimiento extremo. A diferencia de Profinet, no es determinista ni orientado a I/O rápidos, sino que mueve información de forma más lenta y genérica (Profibus, 2020). Esto significa que para operaciones críticas de E/S directas, OPC UA por sí solo no reemplaza los buses de campo; en cambio, complementa estas redes, llevando datos a sistemas de nivel superior (SCADA, MES, nube).

***Limitaciones de los Protocolos***

Modbus, tiene prestaciones limitadas (mensajes simples, sin mecanismos avanzados) lo hacen menos adecuado para sistemas muy densos o con altísimos requerimientos de rendimiento, las tramas clásicas no ofrecen autenticación ni cifrado; sin compensaciones (VPN, firewalls, listas blancas) el tráfico puede ser leíble y manipulable, carece de semántica, lo que obliga a documentar y mapear manualmente cada tag en integraciones superiores, en topologías grandes el modelo maestro, esclavo y el polling secuencial generan latencias acumuladas; no es apto para ciclos de control rápidos ni para sincronización.

Profinet, al presentar mayor capacidad y conjunto de funciones, implica una complejidad y costo de infraestructura superiores (switches industriales, configuración de red) que deben justificarse según la aplicación, tiempo de sincronización y diseño de la topología exige personal calificado y pruebas exhaustivas. PROFINET priorizó rendimiento sobre cifrado; por tanto, suele requerir segmentación, firewalls industriales y controles perimetrales adicionales.

OPC AU debido a su cifrado y autenticación integrados desde el origen, cosa que otros protocolos carecen, su implementación es más compleja. De hecho, diversos autores señalan que OPC UA puede ser complejo de configurar y menos flexible en entornos muy heterogéneos (Hexa, 2024).

Requiere gestión de certificados (PKI), políticas de seguridad y, en general, más pasos de configuración inicial, en dispositivos con recursos escasos el cifrado y modelado pueden requerir hardware o firmware actualizado.

Para mayor compresión se organiza la información en la siguiente tabla comparativa, donde se muestra un análisis más visible y explicito.

**Tabla 2**

*MODBUS (RTU/TCP) · PROFINET · OPC UA*

| Atributo | MODBUS (RTU / TCP) | PROFINET | OPC UA |
|---|---|---|---|
| Velocidad (enlace físico típico) | RTU: hasta 115.2 kbps (RS-485). Modbus TCP: depende de Ethernet → 100 Mbps / 1 Gbps típico. | Ethernet industrial: 100 Mbps común; 1 Gbps posible en switches y controladores modernos. | Capa de aplicación sobre TCP/UDP, depende del enlace (Ethernet 100 Mbps / 1 Gbps). |
| Latencia (característica típica) | RTU: ms, decenas de ms (depende de tasa y número de esclavos). Modbus TCP: ~1–10 ms en LAN no congestionada. | PROFINET RT: sub-ms a 1 ms para ciclos típicos; PROFINET IRT: sub-ms/µs para motion control. | Cliente-servidor clásico: decenas a cientos de ms (no determinista). Pub/Sub, TSN: puede alcanzar ms o sub-ms niveles deterministas. |
| Seguridad (por diseño / opciones) | Baja en Modbus clásico (RTU, TCP): sin cifrado ni autenticación nativos; requiere túneles/TLS o pasarelas seguras para endurecer. | Seguridad incremental: histórico sin cifrado por defecto; prácticas modernas recomiendan segmentación, firewalls y uso de perfiles seguros; algunas implementaciones admiten autenticación y medidas complementarias. | Alta, diseñada con seguridad integrada: autenticación mutua, firmas, cifrado (TLS), políticas de certificados; requiere PKI para gestión de claves. |
| Interoperabilidad (semántica, facilidad de integración) | Técnica/básica: intercambio de registros y coils; simple y ampliamente soportado, pero pobre semántica (datos sin contexto). | Buena entre dispositivos de automatización; perfiles y GSD/EDT permiten interoperabilidad a nivel de I/O y control; menor riqueza semántica que OPC UA. | Muy alta: modelo de información orientado a objetos (types, nodes), excelentes capacidades semánticas y mapeo directo a MES/ERP/IIoT. |
| Mejor uso para. | Integración legacy, | Lazos de control en planta, | Conexión |

| Atributo | MODBUS (RTU / TCP) | PROFINET | OPC UA |
|---|---|---|---|
| | sensores, actuadores simples, telemetría básica. | monitor, control, comunicación determinista entre PLC y E/S. | Planta, empresa, interoperabilidad entre fabricantes, IIoT, historización y servicios seguros. |
| Limitación principal. | Falta de seguridad y semántica; escala y velocidad en RTU. | Requiere infraestructura Ethernet industrial y configuración para determinismo; menor semántica comparada con OPC UA. | No determinista en su forma básica cliente, servidor; depende de red subyacente para requisitos de tiempo real. |

*Nota.* Esta tabla realiza una comparación y análisis de los protocolos.

**Vulnerabilidades, Riesgos y Medidas de Ciberseguridad en Redes Industriales**

Actualmente, con el avance de la tecnología aplicada en los procesos industriales se maneja gran cantidad de información mediante los diferentes tipos de redes, las cuales permiten de manera rápida la administración de la información en los diferentes campos. La evolución tecnológica ha permitido el uso de herramientas de hardware y software necesario para centralizar los datos obtenidos por medio de los diferentes captadores y sensores utilizados en la industria (Caicedo-Erasoa y otros, 2015), pero también se han generado vulnerabilidades y riesgos a nivel de ciberseguridad, los cuales se presentan a continuación. Para una mejor compresión se aclara la diferencia entre los conceptos de vulnerabilidad y riesgo en ciberseguridad.

Vulnerabilidad, es una debilidad, falla o configuración incorrecta en un sistema, hardware, software, procedimiento o control que puede ser explotada por una amenaza para provocar un impacto negativo sobre la confidencialidad, integridad o disponibilidad de la información o del proceso controlado.

Riesgo, en términos generales, es la combinación de la probabilidad de que ocurra un evento adverso y el impacto o consecuencia que dicho evento produciría sobre los objetivos, activos o procesos de una organización. Es decir, no es solo la amenaza o la vulnerabilidad por separado, sino la relación entre la posibilidad de que algo suceda y el daño que causaría si efectivamente ocurre.

### *Vulnerabilidades*

**Carencia de Autentificación y Cifrado**. Modbus y Profibus no incluyen autenticación ni cifrado, al no contar con mecanismos robustos de autenticación, se permite el acceso no autorizado a un atacante en la red, que puede enviar, escuchar, modificar y obtener información sobre las diferentes operaciones del sistema.

Para mitigar estos riesgos, la literatura recomienda aplicar controles fuertes sobre el tráfico industrial. Instalar IDS, IPS especializados o firewalls industriales que filtren estrictamente Modbus, TCP, permitiendo solo los mensajes previamente autorizados, también conviene monitorizar los puertos y protocolos sospechosos y bloquear comandos peligrosos mediante listas blancas.

OPC UA, incluye un modelo de seguridad con certificados y cifrado extremo a extremo, los servidores OPC deben bastionarse y supervisarse activamente para detectar cualquier acceso no autorizado

En general, las medidas de ciberseguridad propuestas incluyen la segmentación de la red, el uso de VLAN y DMZ para aislar las redes OT, la autentificación robusta en todos los dispositivos, y la monitorización continua del tráfico industrial, estas prácticas, junto con la selección de protocolos con características seguras (como OPC UA), son fundamentales para reducir los riesgos en las redes de control industrial.

Software Desactualizado. otros vectores críticos incluyen vulnerabilidades en dispositivos (controladores o sensores) que muchas veces operan con software desactualizado o con credenciales por defecto. Se refiere a sistemas, firmware o aplicaciones que operan con versiones antiguas que no incluyen parches de seguridad, actualizaciones de firmware o correcciones de vulnerabilidades conocidas, en un entorno industrial, esto afecta, PLC, HMI, RTU, variadores de frecuencia, SCADA. En entornos IT, OT, las actualizaciones no se aplican con frecuencia, los equipos operan 24/7, los mantenimientos son limitados, muchos equipos y dispositivos tienen ciclos de vida de 10-20 años, es un fenómeno común en plantas, el problema es que muchos ataques a infraestructura crítica se deben a software sin parches.

**Carencia de Seguridad Nativa**. Muchos protocolos industriales nacieron en entornos cerrados, donde la seguridad no era una prioridad, sin autenticación fuerte, cifrado de datos, integridad criptográfica, gestión segura de identidad.

Los equipos Profinet fueron diseñados para funcionar en, tiempo real, alta velocidad, determinismo, comunicación con PLC, I/O, no fue diseñado inicialmente para operar en redes expuestas a internet, también carecen de seguridad nativa en el endpoint, por lo que cualquier enlace Profinet debe asegurarse mediante segmentación de red y firewalls perimetrales.

***Riesgos***

**Alteración del Sistema.** Es la modificación intencional del comportamiento de controladores, lógica de PLC, setpoints, o valores de actuadores, sensores mediante inyección o modificación de mensajes válidos del protocolo, reescritura de programas de control o manipulación de parámetros operativos, esto ocurre en entorno industriales porque protocolos como legacy (Modbus, PROFIBUS) y muchos endpoints no implementan autenticación ni cifrado, redes OT a menudo están planas o mal segmentadas, facilitando el acceso lateral tras una

intrusión inicial, políticas de parcheo laxas y firmware desactualizado que permiten exploits remotos o locales, un atacante que conozca las direcciones de dispositivos y códigos de función válidos puede enviar mensajes maliciosos sin obstáculos.

**Suplantación de Identidad.** La suplantación de identidad ocurre cuando un actor malicioso consigue que la red o un dispositivo acepte a un emisor falso como legítimo, un controlador, un sensor o una puerta de enlace. La suplantación permite interceptar, alterar o inyectar tráfico como si proviniera de un nodo de confianza.

Las principales causas que pueden originar este riesgo se deben a, redes OT con conmutación y poca verificación de identidades, ausencia de autenticación por endpoint en muchos protocolos legacy, dispositivos con credenciales por defecto o sin gestión de claves, falta de PKI o de gestión de certificados a escala en plantas.

**Ataques de Repetición.** Consiste en capturar mensajes válidos en la red y retransmitirlos posteriormente para provocar acciones repetidas o fuera de tiempo, si los protocolos no incorporan mecanismos de frescura o integridad con protección contra replay, esta técnica es viable, protocolos industriales con mensajes simples y sin protección de integridad, time, stamps, redes con tráfico sin cifrar donde un atacante en la LAN puede capturar paquetes pasivamente, sistemas que aceptan mensajes sin verificar la secuencia o el contexto operacional.

### *Medidas de Ciberseguridad*

Los protocolos clásicos de automatización no fueron diseñados con seguridad cibernética inherente, separar física o lógicamente las redes operativas (OT) de las corporativas (IT) es crucial. Se recomienda configurar DMZ industriales y utilizar redes dedicadas con firewalls de grado industrial, la literatura técnica concuerda en un enfoque por capas (defensa en profundidad) para minimizar estas amenazas. Entre las más nombradas están.

**Firewalls Industriales y Perímetros Seguros.** Los firewalls diseñados para entornos OT filtran tráfico basándose en protocolos ICS, permitiendo solo comunicaciones autorizadas (CYBOLT, 2024). En Colombia las guías sectoriales exigen perímetros de seguridad claros con firewalls frente al exterior, estos dispositivos actúan como primera línea de defensa entre TI y OT, impidiendo accesos no autorizados a las sub redes de control.

**Control de Acceso Robusto.** Se debe imponer autenticación multifactor (MFA) y gestión de cuentas estricta incluso en entornos OT. Herramientas como servidores y gestión centralizada de usuarios garantizan que sólo el personal autorizado acceda a los equipos industriales.

**Monitoreo y Detección Continua.** Implantar sistemas IDS, IPS adecuados para OT permite detectar tráfico anómalo en tiempo real. Soluciones modernas pueden monitorizar desde la red SCADA hasta los controladores, alertando de patrones maliciosos, además, análisis de amenazas y ICS ayudan a anticipar ataques.

**Formación y Gobernanza.** Capacitar al personal operativo en buenas prácticas OT es tan importante como la tecnología, las organizaciones deben nombrar un responsable de ciberseguridad industrial y difundir la cultura de seguridad en todo el equipo de operaciones (Colombia, 2018). La concienciación es un componente esencial para evitar errores humanos que abran brechas de seguridad.

A medida que OT se conecta a redes empresariales y a internet, aparecen riesgos. Por eso es crítico implementar marcos de ciberseguridad específicos para entornos industriales (IEC 62443) y prácticas como segmentación de red, DMZ para sistemas IIoT, gestión de parches y control de accesos.

**Evidencia Documentada y Estudios de Caso Comparados**

Con base en la investigación realizada, la revisión de literatura técnica especializada y el análisis de reportes industriales publicados, se identifican varios casos de adopción real de los protocolos Modbus, PROFINET y OPC UA que permiten validar sus impactos operativos

***Caso 1***

Implementación de PROFINET en una línea de ensamblaje automotriz (BMW Group, Alemania).

Contexto del caso: La planta de ensamblaje de BMW en Ratisbona operaba con redes basadas en Profibus DP y variaciones de Ethernet propietario. La digitalización impulsada por Industria 4.0 exigía una red determinista, de alta disponibilidad y con capacidad de diagnóstico avanzado.

Problema identificado: Latencia variable en los buses tradicionales, dificultad para integrar robots, sistemas de visión y celdas modulares, y limitaciones para implementar mantenimiento predictivo.

Protocolo implementado: PROFINET IRT (Isochronous Real Time).

Datos técnicos reportados según Siemens & BMW (2019): Latencia garantizada: ≤1 ms para comunicación de control. Jitter menor a 50 µs, adecuado para sincronización de robots. Disponibilidad de red superior al 99.99% mediante topologías redundantes MRP. Reducción del tiempo de diagnóstico y calibración en 30–40%.

Impacto en la operación: Integración fluida de PLCs, robots KUKA y sistemas MES. Optimización del tiempo de ciclo en la línea de montaje. Mayor capacidad de auto-diagnóstico de fallos en tiempo real. Migración escalonada sin detener la producción.

Conclusión del caso: PROFINET IRT permitió lograr sincronización precisa, alto rendimiento y escalabilidad, cumpliendo con los requisitos de manufactura inteligente del sector automotriz (Siemens & BMW, 2019).

***Caso 2***

Migración a OPC UA para integración IT/OT en planta de energía (Danfoss, Dinamarca).

Contexto del caso.

Danfoss, fabricante global de soluciones para energía y refrigeración, operaba múltiples líneas con PLC de diversos fabricantes, bases de datos independientes y sistemas SCADA no estandarizados.

Problema identificado: Falta de interoperabilidad entre PLC Siemens, Beckhoff y ControlLogix, datos dispersos, imposibilidad de análisis centralizado, barreras para implementar IIoT y analítica avanzada.

Protocolo implementado: OPC UA como estándar unificado para comunicación vertical (PLC, MES, Cloud).

Datos técnicos reportados: Según OPC Foundation (2020) y Danfoss (2021):

Reducción de 80% del tiempo para integrar nuevos dispositivos.

Operación segura mediante cifrado TLS y certificados X.509.

Capacidad de transmisión de modelos completos de información (Address Space Model).

Conectividad con plataformas cloud como Azure IoT y AWS IoT.

Impacto en la operación: Implementación exitosa de mantenimiento predictivo en motores y compresores, con reducción de fallos críticos del 25%.

Integración nativa con dashboards corporativos y sistemas ERP.

Escalabilidad: incorporación de más de 400 nodos OPC UA en la planta.

Conclusión del caso: OPC UA resolvió la heterogeneidad tecnológica y habilitó una infraestructura de datos unificada, segura y escalable, esencial para la Transformación Digital (OPC & Danfoss, 2020; 2021).

***Caso 3***

Implementación de Modbus TCP en planta petroquímica para modernización de instrumentación (Chevron.  EE.UU.).

Contexto del caso: Una refinería de Chevron utilizaba sistemas legacy basados en Modbus RTU y telemetría serial para instrumentación crítica. La expansión de la planta requería integrar sensores inteligentes, sistemas SCADA modernos y analítica en tiempo real.

Problema identificado: Limitaciones del bus serial RS-485.

Imposible transportar grandes volúmenes de datos (vibración, presión dinámica).

Dificultad para integrar sistemas de distintos fabricantes.

Protocolo implementado: Modbus TCP sobre Ethernet industrial redundante.

Datos técnicos documentados: Según ISA (International Society of Automation) y Chevron (2018). Aumento del ancho de banda: de 19.2 kbps (RTU), hasta 100 Mbps (Ethernet).

Integración inmediata con sistemas SCADA Wonderware y Honeywell Experion.

Reducción del tiempo de configuración de dispositivos en 50%.

Mayor confiabilidad gracias a enlaces redundantes en topología anillo.

Impacto en la operación: Monitoreo en tiempo real de instrumentación crítica (válvulas, caudalímetros, analizadores).

Disminución del tiempo de diagnóstico de fallas en 40%.

Migración sin reemplazar todos los dispositivos legacy.

Limitación observada: Modbus TCP no incorpora mecanismos de seguridad nativos. Chevron implementó: Firewalls industriales, segmentación Purdue, capas de inspección profunda de paquetes (DPI).

Conclusión del caso: Modbus TCP fue una solución efectiva y económica para integrar sistemas legacy con tecnologías modernas, aunque requiere reforzamiento en ciberseguridad OT (Chevron & ISA, 2018; 2019).

Los casos comparados permiten observar cómo cada protocolo responde de manera diferenciada a los requerimientos específicos del sector industrial manufactura discreta, procesos continuos, energía o infraestructura crítica evidenciando que su impacto no depende únicamente de sus características técnicas intrínsecas, sino también del contexto arquitectónico en el cual se implementa.

A continuación, se presenta una tabla, la cual permite comparar las experiencias documentadas y obtener lecciones aprendidas de los casos anteriormente expuestos.

**Tabla 3**

*Implementación de Protocolos*

| Dimensión | PROFINET IRT (BMW, Alemania) | OPC UA (Danfoss, Dinamarca) | Modbus TCP (Chevron, EE.UU.) |
|---|---|---|---|
| Contexto industrial y necesidad tecnológica | En la industria automotriz se requieren sistemas altamente sincronizados, para producción de alto volumen. BMW se apoyó PROFINET como Ethernet industrial unificado para enfrentar las limitaciones de los buses de campo tradicionales y acelerar la | Se busca conectividad inteligente en el nivel de control y nube. Necesitaba un protocolo moderno que garantizara intercambio de datos seguro desde PLC/HMI hasta los drives, y permitiera gestión de activos y actualizaciones remotas sin hardware adicional. | El desafío era integrar equipos antiguos basados en tecnología de bus serie hacia redes IP; por eso Chevron empleó Modbus TCP, que extiende el protocolo Modbus serial a Ethernet, conectando miles de dispositivos industriales distintos. |

| Dimensión | PROFINET IRT (BMW, Alemania) | OPC UA (Danfoss, Dinamarca) | Modbus TCP (Chevron, EE.UU.) |
|---|---|---|---|
| | integración de componentes de diferentes proveedores. | | |
| Problema identificado antes de la implementación | Antes del PROFINET IRT, BMW lidiaba con redes heterogéneas y buses de campo con ancho de banda limitado, lo cual impedía una sincronización precisa de alta velocidad. La falta de un protocolo común provocaba altos costos de integración y riesgos de fallo. | Danfoss enfrentaba dificultades para acceder y actualizar sus drives distribuidos. Los métodos anteriores eran complejos y vulnerables. Se requería una solución unificada para facilitar la recolección de datos en nube y asegurar la transferencia con integridad y confidencialidad. | El problema era consolidar datos de campo en sus sistemas corporativos. Modbus TCP ofrecía un camino de migración sobre Ethernet/IP, aunque sin resolver los problemas de seguridad innatos del protocolo tradicional. |
| Protocolo implementado | PROFINET IRT Permite comunicación determinista usando conmutación y reserva de ancho de banda especiales. Se implementa en dispositivos PROFINET CC-C que cumplen los requisitos de IRT | **Se** integró OPC UA directamente en sus drives iC7-Automation. Usa modelo cliente, servidor con seguridad embebida que ofrece un árbol de información estandarizado. Permite lectura, escritura de parámetros y flujos de publicación, facilitando acceso a datos de campo desde controladores superiores, nubes o SCADA. | Modbus TCP, IP, versión Ethernet del popular Modbus. Funciona en modelo maestro, esclavo simple, el maestro envía consultas y los esclavos responden. Fue implementado en gabinetes SCADA y racks para conectar equipos de control de proceso y de suministro de energía. |
| Beneficios técnicos | PROFINET IRT Logra comunicación determinista usando conmutación y reserva de ancho de banda especiales. Se implementa en dispositivos. | OPC UA incorporado en los drives Danfoss ofrece seguridad y conectividad avanzada sin hardware extra. Los drives pueden ser accedidos como sensores inteligentes tanto desde la planta como desde la nube, eliminando la necesidad de | Modbus TCP se destaca por su sencillez y compatibilidad universal. Prácticamente cualquier dispositivo industrial admite Modbus TCP, simplificando la integración de equipos heterogéneos. No |

| Dimensión | PROFINET IRT (BMW, Alemania) | OPC UA (Danfoss, Dinamarca) | Modbus TCP (Chevron, EE.UU.) |
|---|---|---|---|
| | | pasarelas externas. Esto mejora el ancho de banda efectivo. Técnicamente, la modelización de la información y acceso unificado reduce la carga de configuración manual. | requiere licencias ni membrecías, lo que abarata el despliegue. En términos de rendimiento, provee anchos de banda suficientes para tareas de monitoreo no crítico. |
| Impacto operativo | Gracias a la sincronización precisa se mejoró la productividad, la línea evita tiempos muertos sin interrupciones imprevistas. La estandarización Ethernet simplifica mantenimiento e ingeniería, agilizando reconfiguraciones de líneas. | Se logró operaciones más flexibles, supervisión en tiempo real y mantenimientos remotos seguros. Los ingenieros pueden actualizar firmware y respaldar parámetros de los drives de forma centralizada. Esto reduce considerablemente el tiempo de inactividad por reemplazos o calibraciones. | Se consiguió visualizar datos de forma centralizada sin interfaces costosas. Operativamente, el ancho de banda limitado de Modbus no impide las tareas rutinarias, pero su naturaleza secuencial puede alargar los ciclos de sondeo en redes muy |

*Nota.* Esta tabla realiza una comparación de la implementación de los protocolos.

## Lineamientos para Redes Industriales Seguras y Eficientes

Diseñar redes industriales seguras requiere un enfoque integral basado en estándares como IEC 62443 e NIST SP 800-82. En general, se recomienda aplicar defensa en profundidad escalonando controles de seguridad en múltiples capas (red, perímetro, dispositivo), la segmentación de la red es fundamental, debe dividirse en dominios o zonas funcionales con flujos controlados entre ellas. Esto implica usar firewalls industriales dedicados y VLANs en los bordes de cada zona, controlando estrictamente qué protocolos se permiten.

La implementación de estas medidas debe alinearse con los principios de IEC 62443 que define la defensa en profundidad como escalar múltiples capas de protección para dificultar la

penetración de atacantes. NIST SP 800-82 complementa este enfoque y provee una guía práctica, recomienda segmentar el ICS en dominios de confianza, separar física o lógicamente redes OT y Snormas abogan por un diseño de red jerárquico y modular, vigilado constantemente y adaptado a la criticidad de cada activo.

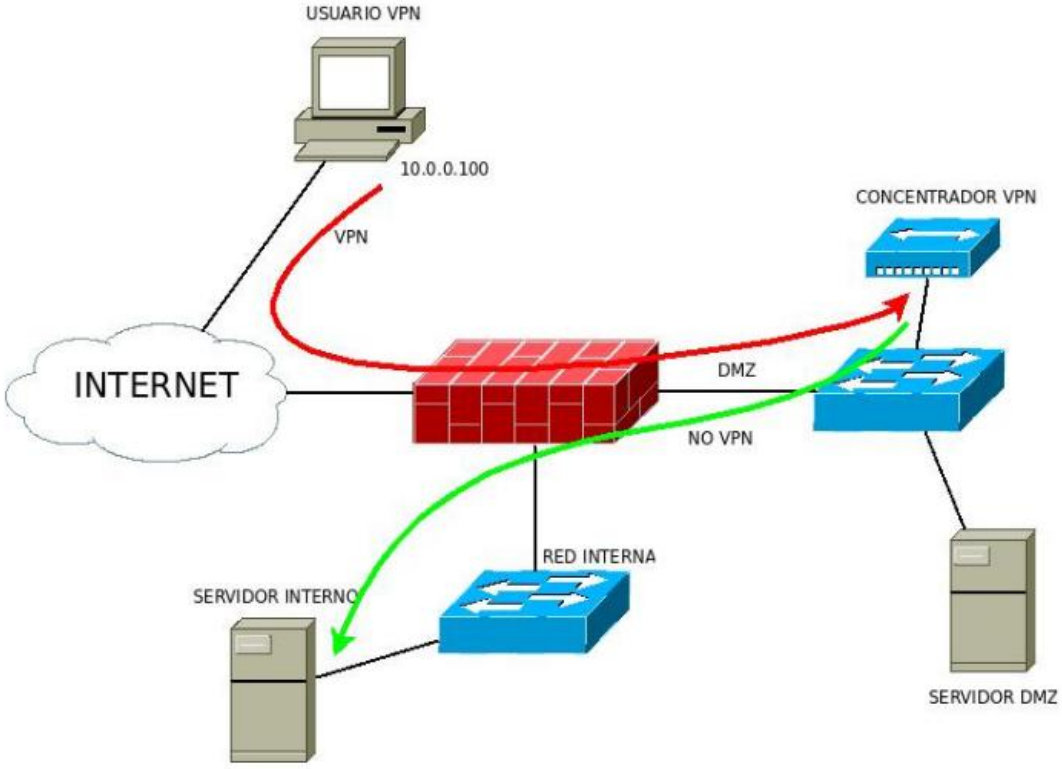
La modernización combina cambios físicos en la red con actualizaciones de protocolo y monitoreo continuo, aunque una transformación total puede ser costosa, estos pasos modulares permiten mejorar la seguridad paso a paso, priorizando los activos más críticos. El Decreto 338 de 2022 colombiano enfatiza este enfoque de gradualidad, ordenando que la implementación de estrategias de seguridad sea progresiva y acorde a los recursos disponibles.

Las mejores prácticas combinan principios de arquitectura y seguridad, en primer lugar, se recomienda segmentar la red siguiendo el modelo Purdue.

Separar los niveles de campo (sensores/actuadores), control (PLC, HMI), DMZ y red corporativa, la zona DMZ es clave para aislar tráfico OT e IT y evitar acceso directo entre redes de control y la empresa. Además, debe implementarse una defensa en profundidad en capas, control físico de accesos, políticas estrictas, segmentación de red, diodos de datos o firewalls industriales entre zonas, y endurecimiento de dispositivos.

**Figura 4**

*Red DMZ*




*Nota.* Figura que explica la red DMZ. Tomado de securityartwork.

En cuanto a la configuración de la red y los dispositivos, las políticas de firewall se sugieren “denegar por defecto”: se bloquea todo el tráfico salvo que esté explícitamente autorizado, cada regla de acceso debe especificar origen, destino, puerto y servicio permitidos, documentando el flujo y asignando responsables. Todo tráfico de la red de control hacia la corporativa debe pasar por la DMZ, y no debe haber rutas directas ICS, Internet ni ICS, IT sin filtro, asimismo, las conexiones de administración deben realizarse por canales seguros con autenticación fuerte.

Es esencial monitorear y actualizar el sistema, activar registros de eventos, usar IDS, IPS industriales para detectar anomalías, y mantener actualizados los firmwares. Estas medidas, unidas a la elección de protocolos seguros (OPC UA sobre OPC clásico, SSH en lugar de Telnet, TLS en redes de SCADA, etc.), conforman un diseño de red industrial que maximiza la robustez y seguridad sin sacrificar la eficiencia operativa.

Se explica y propone de forma clara ocho lineamentos para redes industriales segura y eficientes:

***Segmentación por Niveles y DMZ***

Diseñar la red siguiendo el modelo Purdue permite separar claramente los dominios de campo (sensores, actuadores), control (PLC, HMI), supervisión, DMZ y red corporativa. La creación de una DMZ entre OT e IT evita accesos directos entre redes de control y la empresa, mantiene interfaces auditables y actúa como punto controlado para la transferencia de datos hacia MES, ERP o la nube; esto reduce el riesgo de movimiento lateral de amenazas y facilita la aplicación de controles ajustados por zona.

***Defensa en Profundidad en Capas***

Adoptar una estrategia de defensa en profundidad implica combinar controles físicos (control de acceso a salas de control y gabinetes), controles de red (segmentación, VLANs, firewalls industriales, diodos de datos) y controles de aplicación (listas blancas, hardening de servicios). La redundancia de controles en múltiples capas asegura que la falla de una medida no resulte automáticamente en la exposición total del sistema, lo cual es crítico en entornos donde la disponibilidad operativa es prioritaria.

### *Políticas de Firewall y Reglas Explícitas Documentadas*

Implementar políticas de firewall exige que todo tráfico sea bloqueado salvo que exista una regla explícita que autorice origen, destino, protocolo, puerto y propósito operativo; cada regla debe registrarse, justificarse, y asignarse a un responsable. Esta práctica minimiza superficies de ataque y facilita auditorías, además de forzar la definición clara de flujos de datos entre zonas OT/IT y hacia la DMZ.

### *Gestión de Accesos y Administración Segura*

Todas las cuentas, conexiones y canales de administración deben regirse por el principio de mínimo privilegio, uso de cuentas únicas, control de sesiones administrativas mediante jump hosts o bastion servers, autenticación multifactor para accesos remotos, y registros de sesiones con retención definida. Además, debe prohibirse el uso de credenciales por defecto y debe existir rotación, control de contraseñas y gestión de identidades (IAM) adaptada a OT.

### *Endurecimiento de Dispositivos y Gestión de Parches con Enfoque de Riesgo*

Endurecer controladores, HMI, gateways y switches implica deshabilitar servicios no necesarios, cerrar puertos innecesarios, aplicar configuraciones seguras de fábrica y mantener inventario de firmware, modelos. La gestión de parches en OT debe planificarse con pruebas en entornos de staging y, cuando el parcheo inmediato no sea viable, implementarse mitigaciones compensatorias hasta completar la validación.

### *Monitorización Continua, Logging y Detección de Anomalías*

Permite detectar movimientos laterales, comandos anómalos o cambios en patrones de tráfico antes de que generen daños. La correlación de logs OT, IT en un SIEM adaptado y la definición de indicadores clave mejora la capacidad de respuesta y la trazabilidad ante incidentes.

### *Uso de Protocolos Seguros y Cifrado de Comunicaciones*

Siempre que sea posible, preferir protocolos con seguridad integrada (OPC UA sobre OPC clásico, OPC UA con certificados y TLS, SSH en vez de Telnet, MQTT sobre TLS) y habilitar cifrado en tránsito y autenticación mutua (mTLS) para enlaces críticos. Además, gestionar una infraestructura de clave pública industrial para emitir, renovar y revocar certificados es esencial para mantener confianza entre dispositivos y servicios.

### *Arquitectura Resiliente y Planes de Continuidad*

Diseñar la red con redundancia (topologías anillo o PRP/HSR donde aplique), tolerancia a fallos en controladores y caminos de comunicación, copias de seguridad de configuraciones y procedimientos claros de recuperación (backups, playbooks de DR). Es imprescindible realizar ejercicios periódicos (simulacros, pruebas de conmutación, pruebas de restauración) para validar que las medidas no comprometen la operación y que los equipos saben actuar bajo incidentes reales.

## Discusión Final

La caracterización comparativa realizada revela que MODBUS, PROFINET y OPC UA cumplen roles diferenciados en la automatización industrial. MODBUS (RTU, TCP) es un protocolo maestro, esclavo abierto, sencillo y de bajo costo, ampliamente adoptado debido a su simplicidad y gratuidad, sin embargo, esta simplicidad implica limitaciones. MODBUS carece de confirmaciones de seguridad y opera principalmente en arquitecturas pequeñas. PROFINET, en cambio, es un estándar Ethernet industrial determinista de alto rendimiento, al usar tecnologías IT como TCP, IP, permite transmisión de datos en tiempo real con latencias muy bajas, esta rapidez y fiabilidad determinista es esencial en plantas modernas, aunque PROFINET no es enrutable más allá de la LAN local.

OPC UA surge como una solución orientada a la interoperabilidad y a la Industria 4.0, es independiente de plataforma, orientado a objetos, y proporciona seguridad integrada, su arquitectura “unificada” permite crear un “lenguaje universal” entre máquinas de distintos fabricantes.

La literatura técnica y las guías prácticas coinciden en varios puntos. NIST y documentos industriales recomiendan segmentación, defensa en profundidad y medidas adaptadas al contexto OT (NIST SP 800-82); autores y estudios de rendimiento muestran que OPC UA es adecuado para IIoT aunque su rendimiento depende de la infraestructura subyacente; y los organismos del ecosistema PROFINET. Siemens indican que PROFINET, IRT o PROFINET, TSN permiten ciclos deterministas para control avanzado.

Coinciden en que no existe “un único protocolo que lo haga todo”, la práctica recomendada es combinar protocolos según la función (control vs. supervisión vs. integración). También coinciden en que la seguridad debe integrarse por diseño y que la migración debe ser

incremental. Las normas y guías (IEC 62443, NIST) enfatizan zonificación y gestión de riesgos como ejes transversales.

Difieren en la prioridad de adopción, algunos estudios académicos promueven una adopción más acelerada de Ethernet/OPC UA, mientras que literatura sectorial y guías de campo advierten que, por la realidad operativa, muchas plantas seguirán conservando buses tradicionales y requerirán soluciones híbridas y mitigaciones temporales. Además, las evaluaciones de desempeño de OPC UA muestran variabilidad, en entornos no optimizados puede no ser apto para lazos críticos sin TSN o configuración Pub, Sub adecuada.

En Colombia existen barreras concretas, baja adopción de digitalización en PYMES industriales, limitaciones en infraestructura de conectividad en algunas zonas, y presupuestos restringidos para modernización masiva. Estudios locales y encuestas evidencian una adopción relativamente baja de soluciones 4.0 en PYMES y una brecha en talento especializado para OT, IIoT. Es decir, la infraestructura y la capacitación son factores que inciden directamente en la velocidad de adopción.

El análisis comparado indica ventajas y limitaciones en cada protocolo. PROFINET garantiza desempeño determinista con jitter de décimas de milisegundo, mientras que OPC UA opera en modo best,effort con latencias del orden de decenas a centenares de milisegundos, así, PROFINET es idóneo para lazos de control locales de alta velocidad y precisión, mientras que OPC UA se orienta a reportes de estado y datos de monitoreo, en particular, PROFINET no es enrutable fuera de la red local, pero OPC UA es ruteable y alcanza la nube o intranets, ofreciendo flexibilidad de conectividad, a pesar de sus diferencias, ambos protocolos pueden coexistir.

Por lo general PROFINET cubre la comunicación de campo y OPC UA el puente a sistemas de supervisión. De hecho, se observan tendencias donde los controladores PROFINET incluyen servidores OPC UA para exponer datos de planta, difuminando los roles jerárquicos clásicos, en consecuencia, la interconexión entre dispositivos industriales es cada vez más heterogénea: por ejemplo, un HMI o sistema SCADA puede conectarse directamente a un sensor de campo mediante OPC UA, usando PROFINET para lazos de control y OPC UA para datos históricos. Esta estrategia híbrida optimiza la eficiencia operativa al tiempo que amplía interoperabilidad.

Aunque OPC UA incorpora seguridad, los protocolos industriales clásicos presentan severas debilidades. Estudios recientes destacan que los estándares OT legados fueron diseñados sin mecanismos de autenticación o cifrado, de modo similar, PROFINET y EtherNet, IP no ofrecen integridad o confidencialidad obligatorias; su seguridad es en muchos casos opcional, Estas vulnerabilidades se ven agravadas porque gran parte del equipamiento industrial carece de actualizaciones regulares y se apoya en software obsoleto, mientras tanto, aunque la especificación de OPC UA fue diseñada “con la seguridad en mente” la práctica ha demostrado que una configuración deficiente puede dejar a los sistemas expuestos.

La literatura técnica coincide en que los protocolos ICS sin mecanismos de seguridad nativos facilitan ataques, por ello, cualquier brecha de red o acceso no autorizado puede traducirse en control malicioso de procesos físicos, en base a los hallazgos y la información recopilada se recomienda lineamientos para el diseño y modernización de las redes industriales.

Se definieron conceptos que permiten estructurar análisis donde convergen la automatización, las redes industriales, los protocolos de comunicación, el IIoT, la ciberseguridad y la Industria 4.0. Su comprensión integral es indispensable para evaluar las características y

limitaciones de los protocolos de comunicación industrial, así como lineamientos que fortalezcan la resiliencia y eficiencia de las infraestructuras en entornos productivos modernos.

En Colombia la convergencia ya está en marcha, grandes compañías han mostrado casos concretos y las políticas públicas apoyan el desarrollo de capacidades. El verdadero desafío para la industria es escalar estas experiencias hacia las PYMEs, mantener la seguridad frente a nuevas amenazas y formar talento híbrido OT, TI que haga sostenible la transformación. Con planificación técnica, gobernanza de ciberseguridad y pilotos con retorno claro, la industria colombiana puede consolidar la promesa de Industria 4.0 con beneficios medibles en productividad, seguridad y sostenibilidad.

Elegir y justificar protocolos y medidas de seguridad para comunicaciones industriales en un marco alcanzable. Queda respondido, la monografía entrega criterios técnicos (latencia, determinismo, interoperabilidad), evidencia (casos) y lineamientos prácticos que permiten a tecnólogos y responsables técnicos tomar decisiones informadas y escalables para modernizar redes manteniendo la continuidad operativa.

Este trabajo es una revisión documental; por tanto, no incluye experimentación empírica ni pruebas de campo controladas que cuantifiquen latencias o rendimiento en condiciones reales particulares. Esto limita la capacidad de ofrecer valores medidos aplicables a una planta específica.

A pesar de la existencia de proyectos puntuales y consultorías, la literatura pública y los casos de estudio formales en Colombia son relativamente escasos y a menudo no documentan métricas técnicas ni aspectos de seguridad de manera detallada; por ello la sección de casos colombianos queda menos robusta que la internacional. Esto dificulta generalizar hallazgos para todos los sectores industriales nacionales.

No se realizaron pruebas comparativas ni ensayos de penetración controlados. Para validar empíricamente los lineamientos propuestos sería necesario ejecutar pilotos, ni evaluar comportamientos bajo carga y probar estrategias de mitigación en entornos de laboratorio o planta.

Los hallazgos muestran que la modernización de comunicaciones industriales debe entenderse como un proceso híbrido y por fases, aprovechar la robustez y el bajo coste de soluciones legacy cuando corresponde (MODBUS), usar Ethernet industrial determinista para control de alta velocidad (PROFINET, EtherCAT, TSN) y adoptar OPC UA como el estándar de interoperabilidad y seguridad para IIoT y enlace a IT. La seguridad no es opcional, la evidencia y avisos documentados obliga a integrar controles compensatorios y una gobernanza de parches adaptada a OT.

La presente discusión sintetiza los hallazgos de la revisión documental y los conecta de manera explícita con los cinco objetivos. Su propósito es dejar claro qué se aprendió en cada objetivo, cómo esos aprendizajes responden al problema inicial sobre la elección y justificación de protocolos y medidas de seguridad alcanzables, y cuáles son las implicaciones prácticas y limitaciones del estudio.

Discusión en relación con el objetivo 1.

La revisión confirmó que cada protocolo cumple una función técnica distinta en la arquitectura industrial. MODBUS (RTU, TCP) permanece como la opción más extendida en escenarios legacy por su simplicidad y bajo coste, aunque carece de mecanismos de seguridad y de semántica rica; PROFINET aporta determinismo y bajo jitter para lazos de control en planta, pero está pensado para redes locales y requiere infraestructura Ethernet industrial; OPC UA actúa como la capa de interoperabilidad y exposición de datos, con modelos de información y

seguridad integrada que facilitan la conectividad hacia MES, ERP y la nube. Este resultado satisface el objetivo 1 al ofrecer una caracterización técnica y funcional que permite diferenciar claramente cuándo y por qué usar cada protocolo en función del requerimiento operativo.

Discusión en relación con el objetivo 2.

El análisis de desempeño mostró un patrón claro. PROFINET garantiza latencias muy bajas y determinismo (por tanto, mejor para control crítico), OPC UA ofrece interoperabilidad semántica y ruteabilidad (adecuado para IIoT y supervisión) y MODBUS ofrece simplicidad operativa a costa de seguridad y semántica. Asimismo, emergió la necesidad de soluciones híbridas, la combinación PROFINET (control), OPC UA (exposición de datos) maximiza eficiencia y compatibilidad. Este objetivo queda satisfecho porque la monografía cuantifica (conceptualmente) las ventajas y limitaciones, latencia, determinismo, semántica, seguridad, que permiten evaluar trade, offs técnicos al diseñar una red.

Discusión en relación con el objetivo 3.

Las fuentes consultadas coinciden en que gran parte de los protocolos legacy fue diseñado sin seguridad nativa (ausencia de cifrado, autenticación y control de integridad), lo que aumenta el riesgo de intrusión y de control malicioso de procesos. Incluso PROFINET,EtherNet,based soluciones pueden quedar expuestas si no se aplican controles. OPC UA ofrece mecanismos de seguridad potentes, pero su efectividad depende de una implementación y gestión correcta (certificados, configuración TLS, gobernanza de keys). De este modo el objetivo 3 se cumple aportando un mapa de riesgos y acciones precautorias, identificación de vectores, factores de exposición y controles compensatorios, que son imprescindibles para cualquier plan de modernización.

Discusión en relación con el objetivo 4.

Los casos revisados (migraciones PROFIBUS, PROFINET, adopciones OPC UA) muestran que la modernización suele hacerse por fases, con pasarelas y DMZ como elementos transicionales. Los estudios de caso confirman beneficios operativos, mayor visibilidad, mejora en diagnóstico, potencial reducción de desperdicios y capacidad analítica, sin embargo, también evidencian limitaciones prácticas (costos de reingeniería, dependencia de proveedor, necesidad de PKI a escala, riesgo de single points of failure). El objetivo 4 queda satisfecho en la medida en que la evidencia documentada valida los patrones técnicos y de gestión identificados en los objetivos previos.

Discusión en relación con el objetivo 5.

A partir de los resultados anteriores se elaboraron lineamientos que integran criterios de rendimiento (determinismo, latencia) y de seguridad, ofreciendo un marco práctico y alcanzable para la modernización incremental. Por tanto, el objetivo 5 se cumple entregando recomendaciones operativas que enlazan directamente con las limitaciones detectadas en los otros objetivos: priorizar uso de PROFINET para lazo crítico, usar OPC UA para exposición semántica, mantener MODBUS para legacy solo con compensaciones de seguridad, y aplicar DMZ y monitoreo continuo.

## Conclusiones

A partir de la metodología documental y cualitativa aplicada, basada en la revisión sistemática de literatura técnica, normas internacionales y estudios de caso industriales, se concluye que la automatización electrónica industrial y la Industria 4.0 demandan redes de comunicación robustas y protocolos estandarizados para integrar dispositivos desde sensores hasta sistemas de gestión. La convergencia de tecnologías OT e IT permite combinar el control de procesos local con la gestión en la nube, optimizando la productividad y la toma de decisiones en tiempo real, sin embargo, esta integración conlleva nuevos desafíos de ciberseguridad e interoperabilidad. En este contexto, protocolos abiertos avanzados (OPC UA) favorecen la escalabilidad e interoperabilidad de los sistemas, mientras que un marco normativo de seguridad resulta esencial para proteger las redes industriales y los datos críticos.

El estudio documental permitió identificar que los protocolos industriales cumplen roles diferenciados, mientras que soluciones deterministas como PROFINET son idóneas para el control en tiempo real, protocolos orientados a la interoperabilidad como OPC UA resultan fundamentales para la integración de datos, la escalabilidad y el enlace con sistemas superiores. Los resultados muestran que el uso de protocolos abiertos avanzados, junto con la aplicación de marcos normativos de seguridad como IEC 62443 y NIST SP 800-82, constituye un elemento clave para proteger las redes industriales y los datos críticos, confirmando que la seguridad debe ser incorporada desde la fase de diseño y no como un complemento posterior.

En Colombia, la adopción de tecnologías de Industria 4.0 e IIoT es todavía incipiente debido a barreras como la insuficiente infraestructura, los altos costos de inversión y desafíos en ciberseguridad y financiamiento. No obstante, programas nacionales de digitalización han evidenciado los beneficios de estas tecnologías. Empresas que han implementado soluciones

avanzadas de automatización, inteligencia artificial o blockchain han reportado mejoras en ventas, productividad y calidad de producto. Estos casos sugieren que la automatización avanzada está comenzando a reducir costos operativos y errores en sectores como la manufactura.

En conclusión, la automatización electrónica industrial junto con la Industria 4.0 se perfilan como motores de desarrollo futuro para la industria colombiana. No obstante, su éxito dependerá de superar las barreras técnicas, de infraestructura y de capacitación, así como de aprovechar las estrategias nacionales de digitalización y apoyo tecnológico, de lograrse esto, las empresas podrán optimizar sus cadenas productivas, mejorar la calidad de sus productos y fortalecer su competitividad en el mercado global.

## Recomendaciones

Uno de los pilares fundamentales para la adopción de la Industria 4.0 en Colombia es la capacitación continua y la formación técnica especializada de los profesionales. Para ello, se debe promover la creación de programas educativos y talleres especializados en tecnologías emergentes (Internet de las Cosas, inteligencia artificial, robótica, entre otras), dirigidos tanto a profesionales activo como a nuevos talentos.

La formación continua en estas áreas fortalecerá el capital humano necesario para implementar y mantener sistemas avanzados de comunicación industrial. Paralelamente, es esencial fomentar la innovación y las alianzas multisectoriales como estrategia clave, la colaboración entre empresas, centros de investigación, universidades y entidades gubernamentales puede acelerar la transferencia de conocimiento y la generación de soluciones adaptadas al contexto nacional.

Iniciativas de investigación conjunta, la creación de laboratorios de pruebas y la participación en redes internacionales de innovación tecnológica permitirán desarrollar proyectos de Industria 4.0 más sólidos y competitivos. Asimismo, estas alianzas facilitan la adopción de buenas prácticas globales y la adaptación de la industria colombiana a las tendencias mundiales.

En segundo lugar, se recomienda impulsar la estandarización de protocolos y la interoperabilidad de los sistemas industriales. Adoptar estándares internacionales de comunicación (OPC UA, MQTT u otros protocolos abiertos) y desarrollar marcos normativos comunes permitirá integrar distintos dispositivos y plataformas, reduciendo la complejidad en los procesos de automatización. En paralelo, es necesario robustecer la infraestructura digital y mejorar la conectividad, garantizando redes de alta velocidad (banda ancha fija y móvil, 5G) en los parques industriales y zonas de producción.

Una conectividad confiable y de bajo retardo es crucial para soportar aplicaciones críticas de Industria 4.0, como el control remoto de procesos o la analítica en tiempo real.

Finalmente, la ciberseguridad industrial debe recibir especial atención dentro de este conjunto de acciones. Se sugiere implementar buenas prácticas de seguridad (segmentación de redes, cifrado de comunicaciones, monitoreo continuo de sistemas) y formar especialistas en protección de redes de control industrial.

La certificación de dispositivos frente a amenazas cibernéticas y la elaboración de protocolos de respuesta a incidentes fortalecerán la resiliencia de las infraestructuras industriales. En conjunto, la ejecución coordinada de estas estrategias entre empresas, academia y gobierno permitirá a Colombia superar los retos actuales y aprovechar las oportunidades de productividad y competitividad que ofrece la automatización avanzada.

## Referencias Bibliográficas

Caicedo-Erasoa, J. C., Varón-Serna, D. R., & Arango, F. O. (02 de 03 de 2015). *Unesca-intra.* Unesca-intra.metabiblioteca.org: https://unesca-intra.metabiblioteca.org/cgi-bin/koha/opac-search.pl?q=au:%22Caicedo%20Eraso%2C%20Julio%20C%C3%A9sar%20%3B%22

Campo, B. d. (29 de 02 de 2020). *Bus de campo*. pt.wikipedia.org: https://pt.wikipedia.org/wiki/Fieldbus?utm_source.com

Chevron, C., & ISA. (2018; 2019). *Migration to Modbus TCP in Petrochemical Instrumentation Systems; Best Practice for Ethernet-base Industrial comunication in Pretrochemical Plants*. ISA Industrial Automation Proceedings; ISA Publishing: https://www.isa.org/

Chong, I. (2007). *investigacion documental*. repositorio-uapa.cuaed.unam.: https://repositorio-uapa.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1516/mod_resource/content/3/contenido/index.html

CISA. (25 de 10 de 2023). *Seguridad por diseño* . cisa.gov: https://www.cisa.gov/resources-tools/resources/secure-by-design

Colombia, E. s. (2018). *Ciberseguridad-industrial-en-colombia-2018*. fedetec.org: https://fedetec.org/wp-content/uploads/2019/06/Ciberseguridad-Industrial-en-Colombia-2018.pdf#:~:text=de%20las%20organizaciones%20encuestadas%20utilizan,seguridad%20en%20la%20automatizaci%C3%B3n%20y

Computing. (17 de 09 de 2025). *Tendencias tecnológicas que se consolidan en 2025*. computing.es: https://www.computing.es/cio/las-tendencias-tecnologicas-que-se-consolidan-en-2025/?utm_source.com

CYBOLT. (2024). *CYBOLT US*. Ciberseguridad en sistemas de control industrial sin interrupciones : https://cybolt.com/latam/ciberseguridad-en-sistemas-de-control-industrial-sin-interrupciones/#:~:text=

Fernández. (2020). *Internet industrial de las cosas: Desafíos y oportunidades.* Editorial Innovación Industrial. https://doi.org/https://repository.ucc.edu.co/server/api/core/bitstreams/af057b8d-891f-4668-8101-9aeab9f73dda/content

Galvis, O. L., & Palacio, G. J. (30 de 12 de 2018). *Impato de las nuevas tecnologías de "industry 4.0" en Colombia*. resvistas.sena.edu.co: https://revistas.sena.edu.co/index.php/LOG/article/view/2007

García. (2019). *Redes industriales y comunicaciones en la industria 4.0.* Editorial Técnica Industrial. https://doi.org/https://alinin.org/wp-content/uploads/2020/12/La-industria-40-33-45.pdf

García, M. C. (01 de 03 de 2025). *GUÍA DIDÁCTICA de INVESTIGACIÓN DOCUMENTADA*. rodin.uca.es: https://rodin.uca.es/handle/10498/36110

Hexa. (2024). *Hexa*. hexaingenieros.com: https://hexaingenieros.com/en/que-es-opc-ua-diferencias-con-opc/#:~:text=

IBM. (2025). *ibm.com*. ¿Qué es la criptografía?: https://www.ibm.com/es-es/think/topics/cryptography?utm_source.com

IEC. (2019). https://webstore.iec.ch,

Incibe. (11 de 01 de 2024). *incibe.es*. incibe.es: https://www.incibe.es/incibe-cert/blog/opc-ua-equilibrio-entre-ciberseguridad-y-rendimiento

Isa. (2025). *Serie de normas ISA/IEC 62443-ISA*. isa.org: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards?utm_source=chatgpt.com

Isaza, J. L. (2024). *Ciberseguridad en la convergencia entre redes IT y OT.* bibliotecadigital.econ.uba.ar: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1367_MoraIsazaJL.pdf

Kagermann, Wahlster, & Helbig. (2018). *Recommendations for implementing the strategic initiative Industrie 4.0. Springer.* https://doi.org/10.1007/978-3-662-62371-0

Kagermann, Wahlster, & Helbig. (26 de 4 de 2022). *Diez años de Industria 4.0*. researchgate.net: https://www.researchgate.net/publication/367188088_Ten_Years_of_Industrie_40

Observatorio, I. (2024). *Informe-Smart-Industry-4.0*. observatorioindustrial.org: https://observatorioindustria.org/wp-content/uploads/2024/11/2024-11-Informe-Smart-Industry-4.0-2024.pdf?utm_source=chatgpt.com

OPC, F., & Danfoss, G. (2020; 2021). *Danfoss adopts OPC UA for industrial data strategy; OPC UA Interoperability in Industrial Energy Systems*. OPC technical Case Studies Repository; Technical White Paper: https://opcfoundation.org/wp-content/uploads/2023/05/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf

OWASP. (2025). *Ataque de manipulador en el medio*. owasp.org: https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack?utm_source.com

Profibus. (4 de 08 de 2020). *Profinet*. us.profinet.com: https://us.profinet.com/profinet-versus-opc-2/#:~:text=PROFINET%20mueve%20datos%20r%C3%A1pidamente%3B%20OPC,mueve%20la%20informaci%C3%B3n%20m%C3%A1s%20lentamente

Profibus-Profinet. (2024). *profibus*. profibus. com: https://profibus.com.ar/profinet-que-es-y-como-funciona/

Reyes-Ruiz, L. &. (2020). *bonga.unisimon.edu.co.* bonga.unisimon.edu.co: https://bonga.unisimon.edu.co/server/api/core/bitstreams/2af35a4b-2abf-4f78-a550-0a4e4764e674/content

Rivas, L. (30 de 12 de 2023). *10 tendencias tecnológicas importantes para el 2024*. republica.com: https://republica.com/tecnologia/10-tendencias-tecnologicas-importantes-para-el-2024-2023121316530?utm_source=chatgpt.com

Satyanarayanan. (01 de 2017a). *El surgimiento de la computación de borded*. researchgate.net: https://www.researchgate.net/publication/312109957_The_Emergence_of_Edge_Computing

Sauter, M. (2021). *John Wiley & Sons.* From 3G to 5G: The revolution of wireless communications. : https://doi.org/10.1002/9781119715530

Siemens, & BMW. (2019). *Real-time Industrial Ethernet in Automitive Assembly Systems*. Munich: Technical Report: https://cache.industry.siemens.com/dl/files/465/27069465/att_106101/v1/SYH_IE-Net_76.pdf

UNAD. (03 de 08 de 2019). *noticias.unad.edu.co/index.php*. noticias.unad.edu.co: https://noticias.unad.edu.co/index.php/noticias-unad/las-organizaciones-colombianas-estan-preparadas-para-asumir-los-retos-que-trae-la-revolucion-4-0

VANEGAS, L. H. (2024). *studocu.com.* studocu.com: https://www.studocu.com/co/document/universidad-nacional-abierta-y-a-

distancia/automatizacion-industrial/fase-4-comunicaciones-industriales-avanzadas-y-su-impacto-en-la-industria-40/127765521

Zurawski, R. (2015). *Industrial Communication Technology Handbook.* Taylor & Francis Group. https://doi.org/https://api.pageplace.de/preview/DT0400.9781482207330_A25890586/preview-9781482207330_A25890586.pdf

# Apéndices

## Apéndice A

*Glosario*

Automatización Industrial: Aplicación de sistemas electrónicos y de control para operar máquinas y procesos sin intervención humana continua. La automatización busca mejorar la eficiencia, la repetibilidad y la calidad en la producción industrial, mediante sensores, actuadores y redes de control que regulan variables de proceso en tiempo real.

Bus de campo: Red de comunicación utilizada en planta para conectar directamente sensores, actuadores, válvulas y otros dispositivos de instrumentación con controladores. Los buses de campo reemplazan cableados punto a punto, permitiendo enviar datos digitales y comandos de control con un único canal compartido.

DCS (Sistema de Control Distribuido)**:** Plataforma de control industrial en la que las funciones de control se distribuyen en varios nodos interconectados por red. Un DCS suele utilizarse en procesos continuos y permite gestionar cientos de variables de forma integrada. Se diferencia de un PLC en que el DCS es una solución centralizada para grandes plantas, mientras que los PLC suelen emplearse por separado en estaciones discretas.

Ethernet Industrial**:** Adaptación de la tecnología Ethernet estándar al entorno industrial. Incluye protocolos sobre Ethernet tales como PROFINET (Siemens) o EtherNet/IP (Rockwell). Estas redes usan cables robustecidos y switches industriales para cumplir requisitos de tiempo real y durabilidad. Ethernet Industrial permite altos anchos de banda y conecta controladores, paneles HMI, robots y sistemas SCADA dentro de una planta.

Fábrica Inteligente**:** Concepto de planta de producción altamente integrada y automatizada, donde máquinas, sensores y sistemas de control colaboran de forma autónoma. En una fábrica inteligente los procesos se autorregulan y optimizan en tiempo real usando datos

masivos y algoritmos avanzados. El resultado es una producción más flexible, personalizada y eficiente en recursos.

HMI (Interfaz Hombre-Máquina)**:** Dispositivo o software (pantalla táctil, panel gráfico) que muestra datos del proceso industrial (valores de sensores, alarmas, diagramas) al operario y le permite enviar comandos (arrancar/parar equipos, ajustar parámetros). El HMI traduce la compleja operación de sistemas de control en elementos gráficos intuitivos, facilitando el monitoreo y la supervisión de procesos.

ICS (Sistemas de Control Industrial)**:** Conjunto de sistemas encargados de controlar y automatizar procesos industriales. Incluye equipos como PLC, DCS, SCADA y sus redes asociadas. Un ICS abarca la estructura completa de control en fábricas, plantas y redes de servicios públicos. Su misión es asegurar el funcionamiento continuo de operaciones críticas (energía, agua, manufactura), integrando hardware, software y comunicaciones especializadas.

IIoT (Internet Industrial de las Cosas)**:** Aplicación del Internet de las Cosas (IoT) en el ámbito industrial. Consiste en conectar máquinas, equipos y sensores de planta a internet o redes privadas de datos, para recopilar información en tiempo real. El IIoT permite el monitoreo remoto de activos, mantenimiento predictivo (basado en datos de sensores) y la optimización de procesos mediante análisis de grandes volúmenes de datos industriales.

IoT (Internet de las Cosas)**:** Red global de objetos físicos (sensores, actuadores, dispositivos inteligentes) que se comunican entre sí y con sistemas centrales mediante Internet. En el IoT industrial, estos objetos envían datos sobre su estado o entorno, posibilitando monitoreo remoto y control a gran escala. El IoT incluye aplicaciones en hogares inteligentes, pero en el contexto industrial (IIoT) se focaliza en la productividad y operación de plantas.

Nube Industrial**:** Servicios de computación en la nube adaptados para entornos industriales. Incluyen almacenamiento de datos, análisis remoto y plataformas de gestión escalables para información de plantas. Mediante la nube industrial, las empresas pueden acceder a herramientas de análisis avanzado sin necesidad de infraestructura local masiva.

PLC (Controlador Lógico Programable)**:** Es Computador industrial diseñado para el control automático de máquinas y procesos en tiempo real. Un PLC lee entradas digitales/analógicas, ejecuta un programa lógico y activa las salidas. Son robustos para entornos ruidosos y proporcionan fiabilidad en la ejecución de ciclos de control repetitivos, siendo el elemento básico de la automatización de líneas de producción.

SCADA (Supervisory Control and Data Acquisition)**:** Sistemas informáticos de supervisión que recopilan en tiempo real datos de planta de múltiples ubicaciones. Con interfaces gráficas, permiten a operadores monitorear y controlar procesos, integra controladores locales, presenta alarmas, gráficos históricos y posibilidades de control remoto, siendo clave para la gestión de infraestructuras extensas.