REVISIÓN DE ALCANCE SOBRE LA CONECTIVIDAD PLC-CLOUD EN LA EVOLUCIÓN HACIA EL IIOT: FUNDAMENTOS, CARACTERÍSTICAS TÉCNICAS Y DESAFÍOS EN LA AUTOMATIZACIÓN INDUSTRIAL

Karol Dayana Marcelo M.[1]
Karol Gisselle Aponte M.[2]
John Henry Bautista S.[3]

RESUMEN

Este artículo es una revisión de alcance cualitativa que busca comprender, interpretar y sintetizar información sobre la conectividad PLC-Cloud en la evolución hacia el Internet Industrial de las Cosas (IIoT**)** en la automatización industrial. Utiliza una metodología sistemática con criterios de inclusión/exclusión y técnicas de representación visual, como diagramas de Venn y mapas conceptuales. Resultados demuestran una inclinación hacia Edge y Fog computing para reducir la latencia, y el uso de protocolos como OPC UA, MQTT y Modbus. Se observa un creciente interés en la temática desde 2022, con Europa y Asia liderando la investigación. El estudio identifica ejes temáticos clave como protocolos de comunicación y arquitectura IIoT, pero también importantes vacíos. Estos incluyen la ciberseguridad específica para IIoT, la integración robusta de IA/ML, soluciones de bajo costo para PYMES, la interoperabilidad, el diseño de arquitecturas descentralizadas, y desafíos metodológicos en la investigación práctica.

PALABRAS CLAVE
Conectividad PLC-Cloud, IIoT, Automatización Industrial, Edge Computing, Ciberseguridad.

SCOPING REVIEW ON PLC-CLOUD CONNECTIVITY IN THE EVOLUTION TOWARD IIOT: FUNDAMENTALS, TECHNICAL FEATURES, AND CHALLENGES IN INDUSTRIAL AUTOMATION

ABSTRACT

This article is a qualitative scoping review that seeks to understand, interpret, and synthesize information on PLC-Cloud connectivity in the evolution towards the Industrial Internet of Things (IIoT) in industrial automation. It utilizes a systematic methodology with inclusion/exclusion criteria and visual representation techniques, such as Venn diagrams and conceptual maps. Results demonstrate a leaning towards Edge and Fog computing to reduce latency, and the use of protocols like OPC UA, MQTT, and Modbus. A growing interest in the topic has been observed since 2022, with Europe and Asia leading the research. The study identifies key thematic areas such as communication protocols and IIoT architecture, but also significant gaps. These include specific cybersecurity for IIoT, robust AI/ML integration, low-cost solutions for SMEs, interoperability, the design of decentralized architectures, and methodological challenges in practical research.

KEYWORDS

PLC-Cloud Connectivity, IIoT, Industrial Automation, Edge Computing, Cybersecurity.

INTRODUCCIÓN

La constante evolución de la automatización industrial hacía el internet industrial de las cosas (IIoT), requiere una comprensión de los avances tecnológicos clave. Este articulo presenta una revisión de alcance para mapear fundamentos, características técnicas y desafíos relacionados con la conectividad PLC-Cloud dentro del panorama de transición. La convergencia entre las tecnologías de la información (IT) y las Tecnologías de Operación (OT) es una tendencia significativa, que impulsa el desarrollo de arquitecturas hibridas como Edge y Fog Computing para reducir la latencia y optimizar la gestión de grandes volúmenes de datos en tiempo real Además abordar los desafíos críticos como la ciberseguridad, la integración de Inteligencia Artificial (IA) y el aprendizaje automático (ML) y la necesidad de soluciones estandarizadas y accesibles para pequeñas y medianas empresas (PYMES), son aspectos primordiales para el despliegue de los sistemas IIoT.

El objetivo general de este artículo es elaborar una revisión de alcance sobre la evolución tecnológica de la conectividad PLC con plataformas

Cloud en la automatización industrial basada en IIoT. Para lograrlo, los objetivos específicos son:

• Describir la evolución de los fundamentos conceptuales, contextos industriales y características técnicas relacionadas con la conectividad entre PLC y plataformas Cloud en entornos de automatización industrial basados en IIoT.

• Identificar vacíos o desafíos tecnológicos en la implementación de la conectividad PLC-Cloud en sistemas de automatización industrial.

• Sintetizar la información seleccionada en la literatura para el reconocimiento de tendencias evolutivas y patrones de cambio en la conectividad PLC-Cloud.

MÉTODOLOGIA

Para este artículo de revisión, se define un enfoque metodológico cualitativo, debido a que tiene como finalidad que se comprenda, interprete y sintetice la información que se deriva de distintos estudios, con base en lo anterior, se desarrolló bajo el enfoque de revisión de alcance, el cual es adecuado ya que permite mapear de manera sistemática la literatura técnica y científica disponible sobre la evolución tecnológica de la conectividad entre PLC y plataformas Cloud en el entorno de la automatización industrial con IIoT, además busca llevar a cabo la síntesis de resultados provenientes de estudios individuales con el objetivo de responder a una pregunta especifica.

Para la recolección de información y la construcción de la pregunta problema se seleccionó la metodología TCCM (Teoría, contexto, características y metodología).

La estrategia de búsqueda de información se llevó a cabo en bases de datos relevantes para ingeniería, como: Scopus, ScienceDirect, Elsevier, Springerlink, Scielo y Google Scholar, posteriormente, se elaboró una lista de palabras claves y se formularon ecuaciones de búsqueda utilizando operadores booleanos como AND y OR las cuales se ingresaron en las bases de datos anteriormente mencionadas.

Para la selección de información se establecieron ciertos criterios de inclusión y exclusión, dentro de los que se tuvieron en cuenta características tales como: Idioma, tipo de publicación, relevancia temática, tecnologías obsoletas entre otras.

Principalmente se emplearon diversas técnicas de representación visual como un diagrama de Venn el cual permitió mostrar relaciones de intersección, exclusividad o coincidencia entre dos o más temas, seguidamente, se realizó la organización de información por medio de conceptos claves y relaciones jerárquicas mediante un mapa conceptual; finalmente para visualizar como la tecnología ha avanzado cronológicamente se tuvo en cuenta la cantidad de publicaciones por año y por

categoría, con base en esto se desarrolló un gráfico de evolución.

Posteriormente, se sistematizó y analizó la información recolectada a través de una matriz de análisis en la que se registraron características claves de cada articulo (Titulo, Tipo de documento, autores, palabras clave, año y país de publicaciones), con base en estos se realizó un gráfico de distribución geográfica que permitió identificar las regiones lideres en la investigación e implementación de tecnologías de conectividad PLC-Cloud

RESULTADOS

I. Pregunta problema

Teniendo en cuenta el modelo metodológico TCCM, se planteó la siguiente pregunta problema.

¿Cómo ha evolucionado tecnológicamente la conectividad PLC-Cloud en la automatización industrial basada en IIoT, fundamentos, contextos industriales, características técnicas, enfoques metodológicos y desafíos de implementación?

II. Resultados de la búsqueda y selección

Con el fin de validar la pertinencia, accesibilidad y calidad de la literatura considerada, se establecieron criterios específicos de inclusión y exclusión. Estos criterios permitieron delimitar la búsqueda de documentos académicos, técnicos y científicos relacionados directamente con la evolución tecnológica de la conectividad PLC-Cloud. En la Tabla 1 se detallan los criterios de inclusión y exclusión aplicados para la selección de literatura.

Tabla 1 Criterios de inclusión y exclusión

Categoría	Inclusión	Exclusión
Idioma	Documentos en inglés y español	Publicaciones en otros idiomas sin traducción disponible.
Tipo de publicación	Artículos revisados por pares, revisiones de literatura, tesis o proyectos de grado, capítulos de libros e informes técnicos.	Documentos sin sustento académico o respaldo científico, blogs, paginas comerciales.
Año de publicación	Publicaciones a partir del 2010, priorizando las posteriores a 2018, debido a que es una tecnología en constante evolución	Publicaciones anteriores a 2010 a excepción caso relevantes históricos o normativos.

Relevancia temática	Documentos que aborden directamente la conectividad PLC-Cloud en entornos industriales.	Artículos enfocados únicamente en IOT, sin mención específica al PLC ni conexión con Cloud.
Vigencia tecnológica	Tecnologías actuales o en desarrollo	Tecnologías obsoletas o en desuso, en entornos industriales
Aplicación industrial	Casos aplicados o relacionados explícitamente a sectores de producción.	Estudios netamente teóricos sin aplicaciones prácticas o sin mención al entorno industrial.
Conexión con PLC	Debe incluir componentes relacionados con PLC y la conectividad con plataformas Cloud	IIoT sin integración con PLC, o enfocado en sensores/redes sin incluir controladores.
Acceso	Publicaciones en acceso abierto (Open Access)	Documentos sin acceso al texto completo o restringidos por pago o suscripción

Fuente: Propia

- **Estrategia de búsqueda**

Teniendo en cuenta los criterios previamente definidos, se diseñaron ecuaciones de búsqueda utilizando operadores booleanos junto con palabras clave relacionadas con la conectividad PLC- Cloud, IIoT, protocolos de comunicación y ciberseguridad.

Las búsquedas se realizaron en diferentes bases de datos como Scopus, ScienceDirect, SciELO SpringerLink, y Google Scholar. En la Tabla 2 se muestran algunas de las ecuaciones de búsqueda utilizadas.

Tabla 2 Ecuaciones de búsqueda

Tema	Ecuación
Conectividad y protocolos	"PLC" OR "programmable logic controller" AND "cloud connectivity" OR "IIoT" AND "OPC UA" OR "MQTT" OR "REST API"
	"PLC" OR "Programmable Logic Controller" AND "cloud" OR "cloud computing" AND "Industrial Internet of Things" OR "IioT"
Evolución IIoT	“Industrial Internet of Things" AND "evolution"
Ciberseguridad industrial	"cybersecurity" AND "PLC" " AND "cloud connectivity" OR "IIoT" AND ("OPC UA" OR "MQTT" AND "firewall" OR "VPN"

Desafíos y aplicaciones	“PLC” AND “ Cloud” AND “Application” AND “ challenge"

Fuente: Propia

Al realizar la búsqueda de información con las respectivas ecuaciones en las diferentes bases de datos, se obtuvieron 333 artículos relevantes, de los cuales se seleccionaron 50 artículos para el análisis. La tabla 3 presenta la cantidad de artículos elegidos por tema.

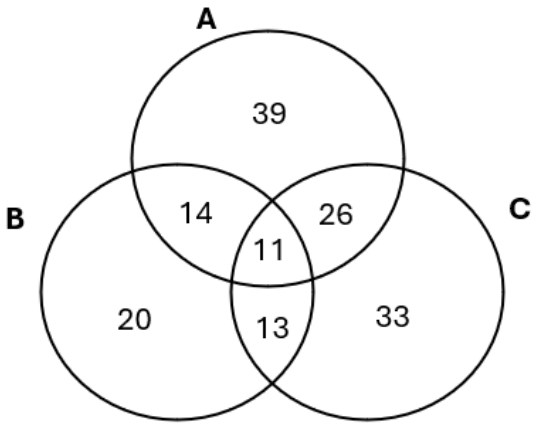
Tabla 3 Selección de artículos

Tema	Artículos encontrados	Artículos seleccionados
Conectividad y protocolos	170	20
Evolución IIoT	80	10
Ciberseguridad industrial	65	12
Desafíos y aplicaciones	18	8

Fuente: Propia

Después de seleccionar los artículos, se elaboró un Diagrama de Venn. Esta representación gráfica permitió identificar y clasificar la información en temas generales y en común, con el fin de organizar y analizar las intersecciones temáticas en la literatura encontrada. La figura 1 presenta la categorización obtenida, adicionalmente, la Tabla 4 especifica los temas generales y la Tabla 5 detalla las características de cada intersección.

Figura 1 Diagrama de Venn



Fuente: Propia

Tabla 4 Definición de conjuntos

Conjunto	Tema	Descripción
A	IIoT/ Cloud	Artículos que traten tecnologías de monitoreo remoto, protocolos de comunicación, etc.
B	Ciberseguridad en automatización industrial	Redes, amenazas, integridad de datos, privacidad, etc.
C	Integración PLC	Implementación de PLC en sistemas industriales.

Fuente: Propia

Tabla 5 Intersección entre temas

Intersección	Descripción
$A \cap B$	Artículos de abarquen IIoT/Cloud y ciberseguridad
$A \cap C$	Artículos que tratan IIoT/Cloud e implementación de PLC
$B \cap C$	Artículos que contienen ciberseguridad y PLC
$A \cap B \cap C$	Artículos que abordan los tres temas IIoT/Cloud, Ciberseguridad y PLC

Fuente: Propia

III. Panorama general de la literatura revisada

Dentro de la literatura revisada se evidencio una inclinación hacia el uso de arquitecturas como Edge computing y Fog computing ya que estas tecnologías posibilitan un procesamiento eficiente, debido a que

disminuyen la latencia, simplifican el análisis del origen de datos y mejoran la respuesta en tiempo real en sistemas industriales.

Los protocolos de comunicación más utilizados en la conectividad PLC-Cloud son OPC UA establecido como el estándar más completo por sus capacidades de modelado y seguridad,

MQTT debido a su ligereza y operatividad en contextos con bajo ancho de banda y finalmente, Modbus, que actualmente continúa empleándose en la industria tradicional por su compatibilidad y sencillez.

Con el fin de estructurar y visualizar las relaciones entre conceptos clave documentados en la información seleccionada, se utilizó un mapa conceptual, el cual permitió organizar jerárquicamente y desglosar el tema general de conectividad entre PLC y plataformas Cloud. En la Figura 2 se evidencia la jerarquía y las relaciones temáticas identificadas.

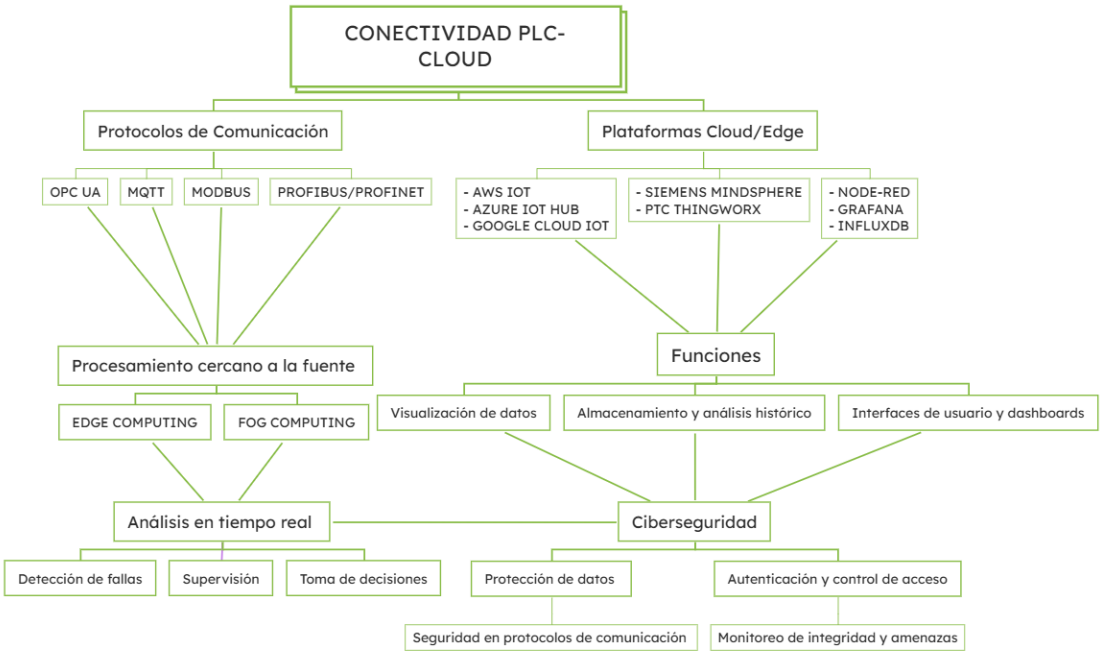


Figura 2 Estructura y jerarquía de conceptos clave
Fuente: Propia

Con el objetivo de comprender la evolución de la documentación enfocada en la conectividad PLC-Cloud en entornos industriales con IIoT, se analizó la cantidad de publicaciones realizadas por año, en un intervalo del 2015 al 2025. Este análisis permitió identificar tendencias, avances tecnológicos y los periodos con mayor producción académica. La figura 3 detalla la cantidad de publicaciones por año.

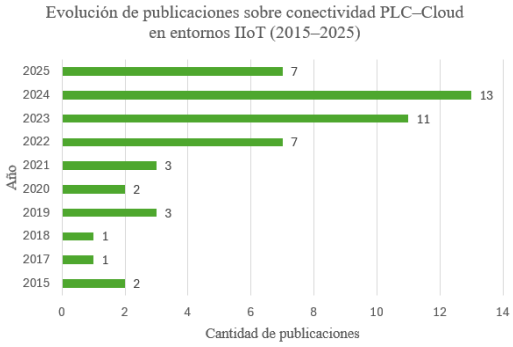


Figura 3 Cantidad de publicaciones por año
Fuente: Propia

En la Figura 3 se evidencia un incremento progresivo de publicaciones a partir del año 2022, lo cual demuestra un creciente interés en la temática de la conectividad PLC-Cloud y IIoT en entornos industriales.

Para identificar las regiones lideres en publicaciones referentes al tema, se analizó la cantidad de artículos provenientes de diferentes zonas geográficas a nivel mundial. Esto permitió visualizar la distribución global de áreas con mayor contribución académica. La Figura 4 presenta la cantidad de publicaciones por región.

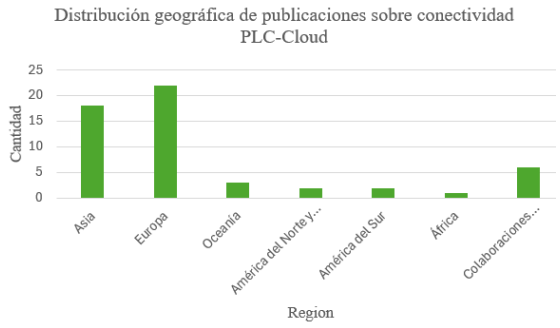


Figura 4 Distribución geográfica de publicaciones
Fuente: Propia

La mayoría de las publicaciones son provenientes de Europa y Asia, lo cual evidencia la actividad investigativa en países como España, China y Alemania, demostrando que estas regiones se encuentran liderando el desarrollo y la aplicación de tecnologías PLC-Cloud en entornos industriales, Asimismo, se identificaron colaboraciones internacionales relevantes como Asia y Oceanía

IV. Ejes temáticos

El Internet Industrial de las cosas (IIoT) es un tema bastante amplio que se encuentra en constante evolución, potenciado por la incorporación de diferentes tecnologías y enfocado en la automatización y optimización de procesos industriales. Dentro de la literatura revisada se identificaron los siguientes ejes temáticos:

i. Protocolos de comunicación

Los protocolos de comunicación son fundamentales para la operatividad del Internet Industrial de las Cosas (IIoT) (Lalaoui Hassani et al., 2021). Se utilizan protocolos OT (Tecnología de Operación) y estándares IT (Tecnología de la Información) para garantizar la comunicación efectiva y confiable en entornos industriales (Lalaoui Hassani et al., 2021). La implementación de protocolos personalizados es crucial para una comunicación efectiva y fiable

en sistemas IIoT (Torres Ventura et al., 2023).

Protocolos OT/Industriales:

- Modbus es un protocolo industrial fundamental, patentado en 1979 (Torres Ventura et al., 2023). OPC (Object Linking and Embedding for Process Control), evolucionado de DCOM, también es clave (Torres Ventura et al., 2023). La Open Platform Communications Unified Architecture (OPC UA) es ampliamente utilizada para la integración de datos en entornos IIoT, incluyendo la agregación **de datos y la** comunicación en la nube (Gilles et al., 2022; Torres Ventura et al., 2023). Se considera que OPC UA facilita la convergencia de protocolos OT e IT (Gilles et al., 2022).
- **S7COMM** es un protocolo de comunicación propietario de Siemens utilizado por los Controladores Lógicos Programables (PLC) (Ruiz-Villafranca et al., 2023; Folgado et al., 2024).

Protocolos IT/Internet:

- **El Message Queuing Telemetry Transport (MQTT) y JSON (JavaScript Object Notation)** son estándares IT comunes utilizados para la comunicación de datos y comandos (Singh et al., 2024).
- **MQTT** es particularmente relevante para el monitoreo y control de robots industriales y la construcción de sistemas IIoT (Wojtulewicz & Chaber, 2025; MacHeso et al., 2022).
- **REST API** también se utiliza para la transmisión de datos a sistemas en la nube (Chen et al., 2025).
- **El protocolo TLS (Transport Layer Security)** es mencionado para la seguridad de las comunicaciones (Gilles et al., 2022).
- **CoAP (Constrained Application Protocol) y AMQP (Advanced Message Queuing Protocol)** son otros protocolos de IoT aplicados en IIoT (Singh et al., 2024; Homaei et al., 2024).

Gestión y Flexibilidad:

- **Node-RED,** un gestor de protocolos de código abierto

desarrollado por IBM, se integra perfectamente en el IIoT por ser multiplataforma, consumir pocos recursos y ofrecer alta capacidad de procesamiento y gestión de comunicación, además de ser fácil de usar por personal no especializado (Torres Ventura et al., 2023; MacHeso et al., 2022).

ii. Sectores industriales

Con el objetivo de identificar los entornos de aplicación de las tecnologías asociadas con IIoT y conectividad PLC-Cloud, se analizó la cantidad de artículos que mencionaban los sectores industriales donde se implementaron estas tecnologías. La Figura 5 ilustra la cantidad de aplicaciones por sector

Figura 5 Implementación por sector industrial
Fuente: Propia

Los sectores industriales con mayor implementación son manufactura, Automatización industrial y aplicaciones en entornos 4.0, demostrando una tendencia hacia la modernización de procesos mediante la conectividad PLC-Cloud.

iii. Conceptos fundamentales y arquitectura IIoT

Oñate y Sanzs (2023) proponen que las arquitecturas IIoT deben contar con una integración eficaz entre IT y OT, y deben ser soportadas por plataformas en la nube y en el borde. Resaltan la importancia de incluir sistemas ciberfísicos (CPS), monitoreo inteligente y mecanismos de seguridad. Salis et al. (2023). Plantean una arquitectura escalable y modular para la industria 4.0 basada en software de código abierto, con la capacidad de análisis en tiempo real y soporte para machine learning, que se adapta a cualquier tipo de planta (Nueva o antigua).

iv. Amenazas y vulnerabilidades en IIoT

Mekala et al. (2023), destacan que las amenazas cibernéticas son un reto critico en IIoT, especialmente por la integración con sistemas antiguos, señalan que muchas

de las soluciones actuales no se adaptan al entorno industrial.

v. **Computación Edge y Cloud en IIoT**

Chamola et al. (2017) hace énfasis en la importancia del Edge computing para reducir la latencia y mejorar la eficiencia en entornos industriales.

Al-Hawawreh et al. (2024). Propone un marco que integra la computación en el borde, nube privada y gemelos digitales para mejorar la seguridad, detección de ciberataques y eficiencia energéticamente en redes IIoT.

V. Identificación de vacíos y áreas emergentes

A partir del análisis de los estudios seleccionados, se identificaron varias brechas temáticas que limitan la comprensión y aplicación extendida de las soluciones PLC-Cloud en la industria:

Ciberseguridad y Privacidad Especifica para IIoT:

Como lo menciona (Mekala et al., 2023), existe una escasez en los mecanismos de prevención de riesgos actuales para mitigar la aparición de amenazas para plataformas IIoT, ya que las soluciones de seguridad existentes están diseñadas para el uso de plataformas IoT de consumo y no abordan correctamente la complejidad y diversidad del IIoT.

Las normas y directrices de seguridad de IIoT no cuentan con las suficientes implementaciones practicas (Mekala et al., 2023). Y la investigación en esta área es limitada ya que la mayoría de los marcos se encuentran en etapas iniciales. Se resalta que no existe un marco sistemático integral que satisfaga las necesidades de seguridad en IIoT (Abdullahi & Lazarova-Molnar, 2025), igualmente, también menciona que existe una ausencia de manuales guía detallados sobre la implementación de mecanismos de protección.

Integración y robustez de Inteligencia artificial (IA) y Aprendizaje Automático (ML)

Algunos de los vacíos mencionados por diferentes autores son:

Los modelos de aprendizaje automático existentes para la detección de ataques en IIoT, comúnmente se entrenan fuera de línea, por ende, se genera un retraso en la detección y una tensión en los recursos (Al-Hawawreh & Hossain, 2024), igualmente, se presentan desafíos en el manejo de datos heterogéneos, de alta dimensión y desequilibrados (Al-Hawawreh & Hossain, 2024)

Gran cantidad de modelos IA/ML están diseñados únicamente para IoT de consumo y carecen de robustez

necesaria para la complejidad de los entornos IIoT (Mekala et al., 2023).

También se resalta que las soluciones con IA son costosas debido a que requieren gran cantidad de datos de alta calidad y la participación intensiva de expertos para la curación y el etiquetado de datos (Salis et al., 2023).

Implementación en pequeñas y medianas empresas (PYMES) y soluciones de bajo costo

Uno de los principales desafíos en la implementación de IIoT en las PYMES, radica en las limitaciones estructurales y tecnológicas, Según Kolla et al., 2022, muchas de estas empresas aún no se encuentran en las condiciones para el tratamiento adecuado de datos.

Ante estos retos, el retrofitting tecnológico aparece como una solución inicial clave, ya que permite integrar capacidades de recolección de datos en maquinaria antigua sin la necesidad de remplazarla. Sin embargo, los autores mencionan que no existe una solución que unifique todos los casos, debido a que las aplicaciones industriales cuentan con gran diversidad de condiciones y necesidades específicas.

Otra limitante identificada en la literatura revisada es el alto costo de los sistemas on-premises, por ende, representan una barrera para organizaciones con recursos limitados (Briatore & Braggio, 2025). Teniendo en cuenta lo anterior, se evidencia el requerimiento de soluciones económicas y accesibles, que tengan una inversión inicial más baja y minimicen el riesgo para aquellas empresas que buscan iniciar su transición hacia la industria 4.0.

Asimismo, los Gateway IIoT ofrecidos por fabricantes de PLC tienen costos elevados, por ende, se ha motivado la incorporación de alternativas económicas, Por ejemplo, Boonmeeruk et al, (2024), señala el uso de microcontroladores como el ESP32 como una opción accesible para implementar la conectividad en aplicaciones industriales a bajo costo.

Interoperabilidad y estandarización

La heterogeneidad de dispositivos, redes y protocolos en IIoT, generan dificultades para una interoperabilidad avanzada, principalmente en entornos industriales complejos (Mekala et al., 2023). Actualmente, continua la desconexión significativa entre los diversos nieles del sistema, lo cual restringe la integración fluida de datos y componentes (García et al., 2023; Oñate & Sanz, 2023). Además, los dispositivos IoT de distintos fabricantes por lo general, utilizan protocolos propietarios, lo que dificulta la comunicación abierta (Mishra & Reddy, 2024). La convergencia IT/OT sigue siendo empírica y fragmentada (Kampa et al., 2024), lo que retrasa el despliegue de sistemas IIoT integrados.

Arquitecturas descentralizadas y gestión de recursos en Edge/Cloud

El diseño de arquitecturas descentralizadas adaptadas las condiciones del entorno industrial continúa siendo un reto (Mekala et al., 2023). Aunque existen avances en la investigación sobre Edge y Fog computing aun es incipiente y presenta limitaciones como el bajo poder de cómputo y el almacenamiento de sensores, así como la gestión de recursos en Edge-PLCs(Peng et al., 2020; Fu et al., 2022). Igualmente, la ubicación de nodos Fog y la adaptación de protocolos continua sin solucionarse completamente (Qayyum et al., 2022; Ruiz-Villafranca et al., 2023).

Gemelos digitales y seguridad

En el uso de gemelos digitales, se ha identificado una falta de evaluación integral, en cuanto a su rendimiento físico como virtual (Al-Hawawreh & Hossain, 2024). Gran cantidad de enfoques se apoyan en reglas predefinidas que no son eficientes ante nuevas amenazas y la ciberseguridad no siempre se integran de forma prioritaria (Homaei et al., 2024), lo que compromete la fiabilidad de las soluciones.

Retos metodológicos en investigación

Se evidencian deficiencias metodológicas en aplicaciones reales, ya que muchas de las investigaciones se centran en simulaciones (Oñate & Sanz, 2023). La terminología relacionada con IIoT e industria 4.0 también es utilizada de manera ambigua, Asimismo, los simuladores actuales no están en la capacidad de representar los entornos industriales con precisión, y la explotación de datos generados en planta es limitada por sistemas cerrados y falta de estandarización (Salis et al., 2023; Guarda et al., 2022).

DISCUSIÓN

Realizando la revisión que llevo a cabo la exploración de la conectividad entre los controladores lógicos programables (PLC) y la nube, analizando la transición hacia el Internet industrial de las cosas (IIoT) y la evolución de los sistemas de automatización industrial, se evidencia el fortalecimiento en las tendencias tecnológicas, pero allí también se presentan ciertas contraindicaciones que llegan a ser importantes y algunos de los vacíos que no han sido abordados adecuadamente.

Uno de los patrones más importantes teniendo en cuenta el enfoque dado al artículo, es la convergencia que se presenta entre las tecnologías de la información (IT) y tecnologías de operación (OT), ya que esta ha promovido al desarrollo de arquitectura hibridas mediante Edge y Fog computing. El enfoque escogido, se respaldó con estudios previos, donde se percibe como un continuo que llega a

complementar la nube centralizada, esto hace que se reduzca la latencia, se gestionen y optimicen en tiempo real grandes volúmenes de datos en tiempo real.

La ciberseguridad es uno de los puntos con una prioridad crítica y obligatoria en los entornos del internet industrial de las cosas (IIoT), esto se establece debido a que en múltiples estudios señalan la creciente exposición a diversas amenazas, en las que se incluyen los ataques de denegación de servicio (DDoS), el robo de identidad y la manipulación maliciosa de datos. Se resalta la necesidad de incluir un enfoque proactivo con respecto a las estrategias de seguridad, realizando la implementación de estándares como el IEC 62443 que se ha generalizado, principalmente en lo que respecta a la segmentación de redes.

Paralelo a la creciente preocupación por la ciberseguridad, también se confirma el uso extendido de inteligencia artificial (IA) y el aprendizaje automático (ML), las cuales son tecnologías fundamentales para desarrollar tareas fundamentales como lo es la detección de anomalías, diagnóstico de fallas e identificar intrusiones tanto en redes IIoT como SCADA. Aunque se hace uso de modelo de redes neuronales avanzados que han demostrado mejoras que son sustanciales frente a enfoques tradicionales, aun se debe reconocer que existen ciertas limitaciones que requieren de investigación.

Existe un claro acuerdo respecto a la importancia de los estándares industriales, destacándose con OPC UA como un protocolo clave, el cual tiene como principal rol asegurar la interoperabilidad y una comunicación confiable entre los distintos componentes que se encuentran en los sistemas industriales. Adicionalmente, existe una necesidad de facilitar loa adopción de este tipo de tecnologías emergentes en las PYMES donde se ha impulsado el desarrollo de soluciones a un bajo costo apoyándose en hardware más accesibles como lo son Raspberry Pi o ESP32 y herramientas de código abierto como Node-RED teniendo un poco más de probabilidad de acceso a la automatización avanzada**.**

REFERENCIAS BIBLIOGRÁFICAS

Abdullahi, S. M., & Lazarova-Molnar, S. (2025). On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances. *International Journal of Information Security*, *24*(1). https://doi.org/10.1007/s10207-024-00951-8

Al-Hawawreh, M., & Hossain, M. S. (2024). Digital twin-driven secured edge-private cloud Industrial Internet of Things (IIoT) framework. *Journal of Network and Computer Applications*, *226*. https://doi.org/10.1016/j.jnca.2024.103888

Behnke, I., & Austad, H. (2024). Real-Time Performance of Industrial IoT Communication Technologies: A Review. *IEEE Internet of Things Journal*, *11*(5), 7399–7410. https://doi.org/10.1109/JIOT.2023.3332507

Boonmeeruk, P., Palrat, P., & Wongsopanakul, K. (2024). Cost-Effective IIoT Gateway Development Using ESP32 for Industrial Applications. *Engineering Journal*, *28*(10), 93–108. https://doi.org/10.4186/ej.2024.28.10.93

Briatore, F., & Braggio, M. (2025). Edge, Fog and Cloud Computing framework for flexible production. *Procedia Computer Science*, *253*, 2206–2218. https://doi.org/10.1016/j.procs.2025.01.281

Chalapathi, G. S. S., Chamola, V., Vaish, A., & Buyya, R. (2019). *Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing: A Review and Future Directions*. http://arxiv.org/abs/1912.00595

Chaudhari, S. S., Bhole, K. S., & Rane, S. (2024). An application of IIoT framework in system design, performance monitoring and control for industrial process heater. *International Journal on Interactive Design and Manufacturing*, *18*(10), 6965–6981. https://doi.org/10.1007/s12008-023-01235-6

Chen, W. C., Ji, B. Y., & Chen, H. H. (2025). A case study on implementing a flexible IIoT service framework for the integration of machine tools. *Journal of Industrial Information Integration*, *47*. https://doi.org/10.1016/j.jii.2025.100908

Chohan, B. S., Xu, X., & Lu, Y. (2022). MES Dynamic interoperability for SMEs in the Factory of the Future perspective. *Procedia CIRP*, *107*, 1329–1335. https://doi.org/10.1016/j.procir.2022.05.153

Cindrić, I., Jurčević, M., & Hadjina, T. (2025). Mapping of Industrial IoT to IEC 62443 Standards. In *Sensors* (Vol. 25, Issue 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s25030728

de Barrena Sarasola, T. F., García, A., & Ferrando, J. L. (2024). IIoT Protocols for Edge/Fog and Cloud Computing in Industrial AI: A High Frequency Perspective. *International Journal of Cloud Applications and Computing*, *14*(1), 1–30. https://doi.org/10.4018/IJCAC.342128

Folgado, F. J., Calderón, D., González, I., & Calderón, A. J. (2024). Review of Industry 4.0 from the Perspective of Automation and Supervision Systems: Definitions, Architectures and Recent Trends. In *Electronics (Switzerland)* (Vol. 13, Issue 4). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13040782

Fu, L., Zhang, Z., Tan, L., Yao, Z., Tan, H., Xie, J., & She, K. (2023). Blockchain-enabled device command operation security for Industrial Internet of Things. *Future Generation Computer Systems*, *148*, 280–297. https://doi.org/10.1016/j.future.2023.06.004

Fu, T., Peng, Y., Liu, P., Lao, H., & Wan, S. (2022). Distributed reinforcement learning-based memory allocation for edge-PLCs in industrial IoT. *Journal of Cloud Computing*, *11*(1). https://doi.org/10.1186/s13677-022-00348-9

Garcia, A., Oregui, X., Franco, J., Arrieta, U., Ferreres, J., & Valencia, J. A. (2024). Time Series Manufacturing Data Edge Monitoring and Visualization to Support Industrial Maintenance Teams. *SN Computer Science*, *5*(1). https://doi.org/10.1007/s42979-023-02442-4

Gavlas, A., Zwierzyna, J., & Koziorek, J. (2018). *Possibilities of transfer process data from PLC to Cloud platforms based on IoT*. *51*(6), 156–161. https://doi.org/10.1016/j.ifacol.2018.07.146

Gilles, O., Gracia Pérez, D., Brameret, P. A., & Lacroix, V. (2023). Securing IIoT communications using OPC UA PubSub and Trusted Platform Modules. *Journal of Systems Architecture*, *134*. https://doi.org/10.1016/j.sysarc.2022.102797

Gutierrez-Guerrero, J. M., & Holgado-Terriza, J. A. (2019). Automatic configuration of OPC UA for industrial internet of things environments. *Electronics (Switzerland)*, *8*(6). https://doi.org/10.3390/electronics8060600

Hassani, H. L., Bahnasse, A., Martin, E., Roland, C., Bouattane, O., & Mehdi Diouri, M. el. (2021). Vulnerability and

security risk assessment in a IIoT environment in compliance with standard IEC 62443. *Procedia Computer Science*, *191*, 33–40. https://doi.org/10.1016/j.procs.2021.07.008

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. C., Ávila, M., & Caro, A. (2024). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*, *57*(8). https://doi.org/10.1007/s10462-024-10805-3

Jayanthi, G., Aaradhika, S., Swathy, S., & Mathumitha, N. (2019). Automation using plc and iiot monitoring in jaggery preparation. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 5227–5230. https://doi.org/10.35940/ijitee.A9236.119119

Kampa, T., Müller, C. K., & Großmann, D. (2024). Interlocking IT/OT security for edge cloud-enabled manufacturing. In *Ad Hoc Networks* (Vol. 154). Elsevier B.V. https://doi.org/10.1016/j.adhoc.2023.103384

Karacayılmaz, G., & Artuner, H. (2024). A novel approach detection for IIoT attacks via artificial intelligence. *Cluster Computing*, *27*(8), 10467–10485. https://doi.org/10.1007/s10586-024-04529-w

Keshav Kolla, S. S. V., Lourenço, D. M., Kumar, A. A., & Plapper, P. (2022). Retrofitting of legacy machines in the context of Industrial Internet of Things (IIoT). *Procedia Computer Science*, *200*, 62–70. https://doi.org/10.1016/j.procs.2022.01.205

Liu, P., Liu, K., Fu, T., Zhang, Y., & Hu, J. (2021). A privacy-preserving resource trading scheme for Cloud Manufacturing with edge-PLCs in IIoT. *Journal of Systems Architecture*, *117*. https://doi.org/10.1016/j.sysarc.2021.102104

Mallia, J., Francalanza, E., Xuereb, P., & Refalo, P. (2024). The development of a generic IIOT framework for an industrial pneumatic system. *Procedia CIRP*, *126*, 277–282. https://doi.org/10.1016/j.procir.2024.08.339

Mathias, S. G., Schmied, S., & Grossmann, D. (2021). A framework for monitoring multiple databases in industries using OPC UA. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 47–56. https://doi.org/10.1007/s12652-020-02850-x

Mekala, S. H., Baig, Z., Anwar, A., & Zeadally, S. (2023). Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. In *Computer Communications* (Vol. 208, pp. 294–320). Elsevier B.V. https://doi.org/10.1016/j.comcom.2023.06.020

Mishra, M., & Reddy, S. R. N. (2024). Performance assessment and comparison of lightweight D2D-IoT communication protocols over resource constraint environment. *Multimedia Tools and Applications*, *83*(26), 67569–67598. https://doi.org/10.1007/s11042-024-18132-z

Mozaryn, J., Bogusz, K., & Juszczynski, S. (2022). Development of PLC Based Fault Isolation and Remote IIoT Monitoring of Three Tank System. *IFAC-PapersOnLine*, *55*(6), 175–180. https://doi.org/10.1016/j.ifacol.2022.07.125

Nguyen, V. H., Jeanmougin, A., Lecointe, V., & Hammer, B. (2024). Hybrid edge–cloud energy management system for an industrial-scale green hydrogen refilling station: Lessons learned and findings. *International Journal of Hydrogen Energy*, *85*, 360–373. https://doi.org/10.1016/j.ijhydene.2024.08.151

Olakanmi, O. O., & Odeyemi, K. O. (2021). Faster and efficient cloud-server-aided data de-duplication scheme with an authenticated key agreement for Industrial Internet-of-Things. *Internet of Things (Netherlands)*, *14*. https://doi.org/10.1016/j.iot.2021.100376

Oñate, W., & Sanz, R. (2023). Analysis of architectures implemented for IIoT. In *Heliyon* (Vol. 9, Issue 1). Elsevier Ltd. https://doi.org/10.1016/j.heliyon.2023.e12868

Peng, Y., Liu, P., & Fu, T. (2020). Performance analysis of edge-PLCs enabled industrial Internet of things. *Peer-to-Peer Networking and Applications*, *13*(5), 1830–1838. https://doi.org/10.1007/s12083-020-00934-1

Qayyum, T., Trabelsi, Z., Waqar Malik, A., & Hayawi, K. (2022). Mobility-aware hierarchical fog computing framework for Industrial Internet of Things (IIoT). *Journal of Cloud Computing*, *11*(1). https://doi.org/10.1186/s13677-022-00345-y

Ruiz-Villafranca, S., Carrillo-Mondéjar, J., Castelo Gómez, J. M., & Roldán-Gómez, J. (2023). MECInOT: a

multi-access edge computing and industrial internet of things emulator for the modelling and study of cybersecurity threats. *Journal of Supercomputing*, *79*(11), 11895–11933. https://doi.org/10.1007/s11227-023-05098-2

Sri Harsha Mekala, Zubair Baig, Adnan Anwar, Sherali Zeadally,(2023), Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions, Computer Communications, Volume 208, Pages 294-320, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2023.06.020.

Sajiddanwar, T., & Filipeejorgeemotaapintoo, M. (n.d.). *EAI/Springer Innovations in Communication and Computing Information and Knowledge in Internet offThings*. http://www.springer.com/series/15427

Salis, A., Marguglio, A., de Luca, G., Razzetti, S., Quadrini, W., & Gusmeroli, S. (2022). An Edge-Cloud based Reference Architecture to support cognitive solutions in Process Industry. *Procedia Computer Science*, *217*, 20–30. https://doi.org/10.1016/j.procs.2022.12.198

Savaglio, C., Mazzei, P., & Fortino, G. (2024). Edge Intelligence for Industrial IoT: Opportunities and Limitations. *Procedia Computer Science*, *232*, 397–405. https://doi.org/10.1016/j.procs.2024.01.039

Sha, L., Xiao, F., Chen, W., & Sun, J. (2018). IIoT-SIDefender: Detecting and defense against the sensitive information leakage in industry IoT. *World Wide Web*, *21*(1), 59–88. https://doi.org/10.1007/s11280-017-0459-8

Torres Ventura, J., Ruelas Puente, A. H., & Herrera García, J. R. (2023). PERFORMANCE FOR INTEROPERABILITY BETWEEN RASPBERRY PI AND ESP8266 WITH A PLC IN A NODE-RED SERVER FOR IIOT. *Ingenius*, *2023*(29), 90–97. https://doi.org/10.17163/ings.n29.2023.08

Cortijo Leyva, R., Quintero, Y., Suntaxi, A. (2024). Supervisión remota por IoT de la bobinadora de láminas plásticas en la empresa Empaqplast S.A. [Tesis de maestría, UISRAEL-EC-MASTER-ELEC-AUTOM-PRO-378.242-2024-028. (n.d.). http://repositorio.uisrael.edu.ec/handle/47000/4253

Wojtulewicz, A., & Chaber, P. (2025). Industrial Robot Control System with a Predictive Maintenance Module Using IIoT Technology. *Sensors*, *25*(4). https://doi.org/10.3390/s25041154

Wu, G., Zhang, Y., Zhang, H., Yu, S., Yu, S., & Shen, S. (2024). SIHQR model with time delay for worm spread analysis in IIoT-enabled PLC network. *Ad Hoc Networks*, *160*. https://doi.org/10.1016/j.adhoc.2024.103504

Wu, W., Fouzi, H., Benamar, B., Sidi-Mohammed, S., & Ying, S. (2025). Deep learning-based stacked models for cyber-attack detection in industrial internet of things. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-025-11418-9

Zhang, X., Ma, L., Peng, K., Zhang, C., & Shahid, M. A. (2024). A cloud–edge collaboration based quality-related hierarchical fault detection framework for large-scale manufacturing processes. *Expert Systems with Applications*, *256*. https://doi.org/10.1016/j.eswa.2024.124909

Zhang, X., Ma, L., Peng, K., Zhang, C., Shahid, M. A., & Wang, Y. (2025). A cloud–edge collaborative hierarchical diagnosis framework for key performance indicator-related faults in manufacturing industries. *Journal of Process Control*, *152*. https://doi.org/10.1016/j.jprocont.2025.103462

Zolotová, I., Bundzel, M., & Lojka, T. (2015). Industry IoT gateway for cloud connectivity. *IFIP Advances in Information and Communication Technology*, *460*, 59–66. https://doi.org/10.1007/978-3-319-22759-7_7