



Compás
capacitación e investigación



© Luis Orlando Philco Asqui
Bryan Ivan Barahona Montalvan
Bryan Orlando Velez San Martin
Hamilton Francisco Villamar Barros

© Editorial Grupo Compás, 2025
Guayaqui, Ecuador
www.grupocompas.com
<http://repositorio.grupocompas.com>

Primera edición, 2025

ISBN: 978-9942-33-926-3

Distribución online

 Acceso abierto

Cita

Philco, L., Barahona, B., Velez, B., Villamar, H. (2025) La industria conectada: Casos de entornos industriales y agointeligentes. Editorial Grupo Compás

Este libro ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad de la publicación. El copyright estimula la creatividad, defiende la diversidad en el ámbito de las ideas y el conocimiento, promueve la libre expresión y favorece una cultura viva. Quedan rigurosamente prohibidas, bajo las sanciones en las leyes, la producción o almacenamiento total o parcial de la presente publicación, incluyendo el diseño de la portada, así como la transmisión de la misma por cualquiera de sus medios, tanto si es electrónico, como químico, mecánico, óptico, de grabación o bien de fotocopia, sin la autorización de los titulares del copyright.

ÍNDICE GENERAL

INDICE DE FIGURAS.....	8
INDICE DE TABLAS	10
PRÓLOGO.....	11
INTRODUCCIÓN	12
PLATAFORMAS TECNOLÓGICAS INDUSTRIALES INALÁMBRICAS	12
CAPÍTULO I:	14
PANORAMA DE LAS COMUNICACIONES INDUSTRIALES INALÁMBRICAS	14
MERCADO DE PLATAFORMAS DE AUTOMATIZACIÓN INDUSTRIALES .	15
DE LA INDUSTRIA 4.0 A LA 5.0	21
INTELIGENCIA ARTIFICIAL EN PLANTA	23
CAPÍTULO II:	28
DATOS, PROTOCOLOS Y SEGURIDAD EN REDES INDUSTRIALES.....	28
DESAFIOS EN WSN	30
MODELO DE ARQUITECTURA DE CAPAS.....	32
APLICACIONES DE WSN.....	33
ARQUITECTURA DE UNA WSN.....	33
PROCESO DE IMPLEMENTACIÓN DE UNA WSN	35
TOPOLOGÍA DE UNA WSN	37
TÉCNICAS DE PROTOCOLO DE ENRUTAMIENTO EN WSN	38
TENDENCIAS Y AVANCES RECIENTES	40
REDES DE SENSORES INALÁMBRICAS INDUSTRIALES.....	41
PRINCIPALES CARACTERÍSTICAS	41
APLICACIONES INDUSTRIALES.....	41
REQUERIMIENTOS PARA UNA IWSN	44
REQUERIMIENTOS DE IWSN FRENTE A BUSES DE CAMPO DIGITALES.	47
Interoperabilidad.....	47
Resistencia al ruido y coexistencia	48
Consumo energético.....	48

Autoorganización	49
Robustez y tolerancia a fallos	50
Confiabilidad de enlace	50
Bajo retardo	51
Diferenciación de servicios.....	51
Calidad de Servicio (QoS)	51
Escalabilidad	51
Fuente múltiple y múltiples sumideros	52
Comportamiento predecible.....	52
Protocolos específicos de la aplicación.....	52
Agregación de datos.....	52
Seguridad.....	53
RED DE SENSORES Y ACTUADORES INALÁMBRICOS (WSAN)	54
CARACTERÍSTICAS PRINCIPALES DE WSAN	54
MODELO DE COMUNICACIÓN EN WSAN	56
USO DEL PROTOCOLO MQTT EN WSAN	57
TECNOLOGÍAS DE COMUNICACIÓN EN IWSN.....	57
ESTÁNDAR ZIGBEE	58
CARACTERÍSTICAS	58
ZIGBEE PRO Y SU EVOLUCIÓN	59
ESTÁNDAR WIRELESSHART	59
CARACTERÍSTICAS CLAVE DE WIRELESSHART	59
EJEMPLO DE APLICACIÓN: WIRELESSHART EN UNA PLANTA QUÍMICA	60
ARQUITECTURA OSI EN WIRELESSHART	62
TOPOLOGÍA DE RED EN WIRELESSHART	64
SEGURIDAD EN WIRELESSHART	65
HART IP	66
CARACTERÍSTICAS PRINCIPALES:	67
ISA 100 WIRELESS,	68
CARACTERÍSTICAS PRINCIPALES:	68

SEGURIDAD EN CONTROL CRÍTICO.....	70
ESTÁNDAR WIA-PA PARA AUTOMATIZACIÓN DE PROCESOS	72
CARACTERÍSTICAS PRINCIPALES:	73
CARACTERÍSTICAS PRINCIPALES:	74
MODELO OSI EN WIA-PA	74
DISPOSITIVOS DE RED WIA-PA	77
ESTÁNDAR WIA-FA PARA AUTOMATIZACIÓN DE FÁBRICAS	78
CARACTERÍSTICAS PRINCIPALES	78
PRIORIDAD DE DATOS EN WIA-FA.....	80
OTROS ESTANDARES	81
CAPÍTULO III:	84
LOS DATOS EN LA FÁBRICA DIGITAL.....	84
CASO: TRANSMISIÓN DE DATOS INDUSTRIALES.....	87
DETALLE DE CONEXIÓN DE UN ESQUEMA INDUSTRIAL	87
COMPONENTES Y DATOS	88
ENVÍO DE DATOS DESDE PLC HACIA LA NUBE	90
FLUJO DE DATOS	90
VISUALIZACIÓN EN TIEMPO REAL EN UN DISPOSITIVO MÓVIL	92
HARDWARE Y SOFTWARE PARA LA VLAN	93
CAPÍTULO IV:.....	98
ESCENARIO DE AGROMÁTICA	98
CASO: CULTIVO INTELIGENTE.....	99
HARDWARE BÁSICO.....	99
CONEXIÓN DE SENSORES A RASPBERRY PI (GPIO).....	100
CÓDIGO PYTHON PARA LECTURA DE SENSORES.....	102
MOTOR DE VISIÓN ARTIFICIAL.....	110
MOTOR IA CON JETSON NANO DE NVIDIA	110
SISTEMA OPERATIVO Y SOFTWARE	111
CONFIGURACIÓN PASO A PASO	112
MODELO DE IA PARA DETECTAR PLAGAS Y CRECIMIENTO.....	114
ENVÍO DE RESULTADOS A RASPBERRY PI O NUBE	116

VISUALIZACIÓN Y SUPERVISIÓN REMOTA.....	117
CONSIDERACIONES FINALES.....	118
REFERENCIAS.....	119
GLOSARIO	123

INDICE DE FIGURAS

Figura 1. Proyección de uso de tecnologías industriales (2023–2025).....	17
Figura 2. Escenario de conectividad industrial.....	19
Figura 3. Escenario Industrial en proceso de ensamblaje de autos	20
Figura 4. Diferencias entre industria 4.0 y 5.0.....	22
Figura 5. Uso de la AI Edge	24
Figura 6. Empresas con Edge AI	24
Figura 7. Integración de tecnologías en Industria inteligente.....	25
Figura 8. Partes principales de una mota	29
Figura 9. Esquema de mota de una WSN	30
Figura 10. Red WSN típica	30
Figura 11. Arquitectura de cinco capas en IoT.....	32
Figura 12. Ejemplos de las aplicaciones de WSN	33
Figura 13. Arquitectura de una WSN distribuida	35
Figura 14. Proceso de implementación general de una WSN	36
Figura 15. Topología estrella.....	37
Figura 16. Topología malla.....	37
Figura 17. Topología árbol.....	38
Figura 18. Un escenario de agrupamiento de clústeres.....	39
Figura 19. Esquema de conexión con tolerancia a fallos	50
Figura 20. Escalabilidad en red	51
Figura 21 Seguridad en la red.....	53
Figura 22. Escenario de IWSN básico	53
Figura 23. Lazo de control de una WSAW	55
Figura 24 Tipos de automatización a. Automatización parcial y b. Automatización total	56
Figura 25. Estándares de comunicación inalámbrica utilizadas a nivel industrial	57
Figura 26. Red WirelessHART típica.....	60
Figura 27. Conexiones WirelessHART	61
Figura 28. Pila de protocolo HART y WirelessHART	62
Figura 29. Topologías de red en WirelessHART	64
Figura 30 Seguridad en WirelessHART	65
Figura 31. Comunicación de HART-IP y Ethernet-APL.....	67
Figura 32 Flexibilidad de la red ISA100.11a	69
Figura 33. Red ISA 100.11a.....	72
Figura 34. Topología malla y estrella de red WIA-PA	73
Figura 35. Arquitectura del protocolo WIA-PA	74
Figura 36. Estructura de super trama de WIA-PA	75

Figura 37. Dispositivos de red industrial con estándar WIA-PA.....	77
Figura 38. Máquinas y equipos conectados.....	85
Figura 39. Esquema conectividad inalámbrica industrial	88
Figura 40. Configuración del switch	89
Figura 41. Configuración del Cisco IOS	89
Figura 42. Configuración del PLC	90
Figura 43. Códigos para envío de datos de temperatura	90
Figura 44. Esquema de comunicación inalámbrica industrial	92
Figura 45, Configuración VLAN.....	93
Figura 46. Configuración básica: del router con salida a internet.....	94
Figura 47. Publicación de datos del PLC a la nube	94
Figura 48. Configuración de router	95
Figura 49. SCADA en Paraguay.....	95
Figura 50. Topología resumida	95
Figura 51. VLAN entre dos países	96
Figura 52. Esquema de Agromática	98
Figura 53, Configuración de pines GPIO	100
Figura 54. Escenario para cultivo inteligente de tomate.....	100
Figura 55. Pines de conexión de Raspberry Pi con sensores	102
Figura 56. Código en Python para sensor DTH22	102
Figura 57. Código Python para sensor Humedad del suelo	104
Figura 58. Conexión de sensor YL-69	104
Figura 59. Código en Python para sensor TSL2561	105
Figura 60. Código Python para control de actuadores y relés.....	105
Figura 61. Código para activar una bomba de agua	106
Figura 62.Código en Python para OpenCV	108
Figura 63. Código para capturar imagen y detectar manchas.....	109
Figura 64 Escenario con motor IA Jetson Nano.....	110
Figura 65. Código para conectar cámara.....	112
Figura 66. Código para captura de imágenes con OpenCV.....	113
Figura 67, Código para Inferencia con Jetson Nano	115
Figura 68. Código para publicación con MQTT.....	117
Figura 69. Esquema de la visión artificial en cultivo inteligente.....	117

INDICE DE TABLAS

Tabla 1. Características entre la Industria 4.0 y 5.0	21
Tabla 2. Comparación de ISA-100 con otras tecnologías	42
Tabla 3. Comparación de características técnicas de estándares IWSN	76
Tabla 4. Comparativa de arquitectura OSI y WIA.FA	80
Tabla 5. Ejemplos de herramientas de dashboards	91
Tabla 6. Hardware para la VLAN	93
Tabla 7. Software requerido	93
Tabla 8, Hardware para invernadero inteligente	99
Tabla 9. Tipo de comunicación de los sensores.....	101
Tabla 10. Opciones de motor para visión artificial	110
Tabla 11. Descripción de componentes para motor Jetson Nano.....	111
Tabla 12. Descripción de interfaz y protocolos	111

PRÓLOGO

Los autores en este libro describen protocolos y estándares de las redes inalámbricas industriales. Así como los avances en las tecnologías que comprende la industria 5.0, expresión que engloba la interacción equilibrada entre humanos y máquinas inteligentes. El intercambio de datos va ganado espacio entre el desarrollo tecnológico industrial. La industria es la parte de una economía que genera o crea productos materiales utilizando la mecanización y la automatización.

A medida que las industrias evolucionan hacia entornos cada vez más conectados, el dominio de las redes industriales y la automatización programable se vuelve crucial. Hoy en día se puede integrar la teoría de protocolos industriales (como Modbus, Profinet, OPC UA) y la aplicación práctica de casos en Automatización y Agromática mediante lenguajes de programación modernos como Python.

Los autores examinan el paradigma de la Internet de las Cosas Industriales (IIoT), detallando la convergencia entre tecnologías OT (tecnología operativa) e IT (tecnología de la información), así como su impacto en la reconfiguración de procesos productivos. Finalmente detallan un contexto de la Agromática con un caso de aplicación de estas tecnologías en el sector agroindustrial.

INTRODUCCIÓN

PLATAFORMAS TECNOLÓGICAS INDUSTRIALES INALÁMBRICAS

Se está acelerando la transformación digital en la Industria 5.0 (la quinta revolución industrial). En conjunto con la implementación del Industrial of Things (IIoT), en español denominado IoT industrial establecen para equipos, sistemas y entornos industriales el escenario con plataformas que prioriza la co-creación y personalización masiva (fabricación inteligente), no solo eficiencia.

La industria es uno de los sectores de la sociedad más necesitados del ahorro de energía, ya que su logro supone una mayor competitividad. En los procesos industriales automatizados los buses de campo digitales con su cableado tradicional basadas en Ethernet industrial pueden proporcionar una alta confiabilidad de las comunicaciones, pero no pueden cumplir por completo los requisitos identificados en términos de flexibilidad, re-configurabilidad rápida y soporte de máquinas móviles y robots, y otros desafíos de la Industria 5.0.

Las fábricas modernas utilizan muchos tipos de equipos, incluidos brazos robóticos en la línea de producción, una variedad de sensores y actuadores para la automatización e incluso vehículos no tripulados para aumentar la eficiencia. La implementación de redes privadas 5G dentro de entornos industriales, conocido como 5G NR–New Radio, permiten una conectividad confiable, de baja latencia (menor a 1 milisegundo) y altamente segura, lo cual es crítico para procesos en tiempo real y operaciones autónomas.

La inteligencia artificial (IA) permite que las máquinas tomen decisiones sin necesidad de intervención humana. Gracias al aprendizaje de máquina, los sistemas pueden aprender de la experiencia y mejorar con el tiempo. La infraestructura de comunicación y decisión en la industria conectada revoluciona eficientemente entornos Industriales hasta entornos prioritarios como la Agromática por la seguridad alimentaria, pilar fundamental de los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas.

"La Industria 5.0 es una reintegración estratégica entre operadores humanos y sistemas ciberfísicos avanzados para potenciar la personalización, la resiliencia y la eficiencia de los procesos productivos".

Los autores. 2025

CAPÍTULO I:

PANORAMA DE LAS COMUNICACIONES INDUSTRIALES INALÁMBRICAS

El uso de la comunicación inalámbrica en las fábricas se dedica especialmente a tareas de inspección remota y de operación de los equipos facilitan el monitoreo de variables en un campo de interés. Las tecnologías digitales dependen en gran medida, de una forma u otra, de la disponibilidad de sistemas de comunicación inalámbrica. (Robayo, 2019). Durante la pandemia, la conectividad fue imprescindible y trascendental, pues permitió que la fuerza laboral trabaje de forma remota y que los servicios y negocios electrónicos satisfagan las necesidades básicas, entre otras cosas más.

Si bien las empresas se esfuerzan por hacer que su proceso de producción sea inteligente, deben considerar qué tecnología de comunicación tiene las cualidades para lograrlo. 5G, la red móvil de quinta generación promete superar las deficiencias de los otros sistemas inalámbricos. Un estudio, sobre si está preparada la industria, realizado con profesionales de la industria manufacturera, concuerda que la tecnología inalámbrica más utilizada hoy en los entornos de producción industrial es la Wi-Fi, seguida por la de redes celulares y Bluetooth (Robayo, 2019).

El acceso y la supervisión remota proporciona a los grandes fabricantes como a los técnicos de máquinas y equipos a examinar el rendimiento de la máquina o equipo. Realizar actualizaciones programadas y solucionar problemas sin tener que desplazarse al sitio. También permite la capacitación remota, donde el instructor puede usar la realidad aumentada u otras herramientas para capacitar al personal de mantenimiento en el sitio. En industrias donde el tiempo de actividad es crítico, esto ahorra una increíble cantidad de tiempo y costo.

Esta mayor conectividad entre máquinas y equipos conocida como IoT o una red de objetos conectados entre sí a través de internet y capaces de interactuar se está aplicando a ciertos procesos de la industria formando el IoT Industrial (IIoT). Las ventajas que ofrecen las redes inalámbricas en procesos industriales resultan útiles. Se indica que a pesar que existe cables de red en categoría (Cat.) 7, y también (Cat.) 8, que son superiores en velocidad y frecuencia. Ambas categorías de cable de red, no pueden superar al 5G en velocidad en distancias cortas, no ofrece la movilidad, baja latencia ni escalabilidad que el 5G proporciona en entornos industriales.

Aunque hay desafíos como en seguridad y fiabilidad, se requieren redundancia de medios para lograr determinados niveles de fiabilidad. Se deben otorgar canales inalámbricos libres o que superen todo tipo de interferencias que afecten las comunicaciones sin cables. La sustitución del cableado de comunicación entre dispositivos y equipos de un proceso industrial, deben ser fiables, robustos y seguros, incluso en entornos hostiles (temperaturas altas por cercanía a calderas, hornos, las vibraciones de las máquinas eléctricas, etc.), Garantizar los aspectos antes mencionados constituyen un auténtico reto que debe resolverse (Moosavi, Bakhshi, & Martek, 2021).

MERCADO DE PLATAFORMAS DE AUTOMATIZACIÓN INDUSTRIALES

Tradicionalmente, los sistemas de automatización industrial (compuestos por un sensor, un control y un actuador) se han implementado a través de arquitecturas conectadas por cable. Gracias a los estándares de compatibilidad impuestos por la industria y al despliegue de hardware de red inalámbrica ligero se pueden poner en marcha redes inalámbricas para entornos industriales. Si bien en la actualidad existen aplicaciones para el monitoreo de procesos automatizados industrial; muchas de ellas operan con

protocolos propietarios de los fabricantes, por lo que en la mayoría de los casos no facilitan la conectividad directa con otras tecnologías.

Los estándares de tecnologías inalámbricas no pueden cumplir con la solidez requerida y la baja latencia que necesitan las aplicaciones industriales inalámbricas de máquina a máquina (M2M, *Machne to Machine*). Por tanto, se están sub-utilizando principalmente para el monitoreo en aplicaciones no críticas. El estándar más utilizado es el 802.11 aprobado por el Instituto de Ingenieros Eléctricos y Electrónicos (*IEEE, Institute of Electrical and Electronics Engineers*), la cual es una organización mundial para normalizaciones y desarrollo de áreas técnicas. Los estándares industriales en tecnologías inalámbricas permitirán que los diferentes fabricantes o desarrolladores de tecnologías establecieran mecanismos que garanticen la operatividad de un sistema, o una red.

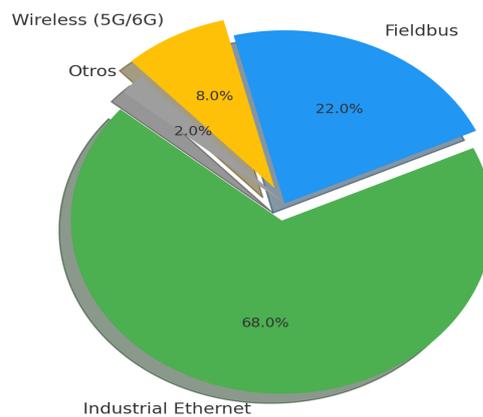
Las comunicaciones inalámbricas industriales cuentan con aplicaciones en los ámbitos de las plantas de producción de todo tipo, la automoción, la generación, transmisión y distribución de energía, etc. El hardware de los dispositivos en las redes inalámbricas requiere el uso de tecnología que se ocupa de las frecuencias de radio y de la transmisión de datos, por consiguiente, en un enlace de radio frecuencia se originan alteraciones de la señal, particularmente por: las largas longitudes de transmisión, paredes y obstáculos impenetrables. Por lo tanto, es vital que se ofrezcan niveles de disponibilidad del enlace.

Según proyecciones de la empresa sueca Hardware Meet Software (HMS) líder mundial en comunicación industrial e IloT y del análisis con matriz McKinsey (2023), se estima que el uso de Ethernet Industrial seguirá consolidándose como la tecnología dominante, impulsado por la incorporación de Time Sensitive Networking (TSN), redes convergentes y la conectividad a Edge AI.

Las tecnologías inalámbricas, incluyendo 5G y las primeras pruebas de 6G, comienzan a ganar terreno, especialmente en entornos donde la movilidad y la flexibilidad son claves.

En la figura 1, se presenta una proyección estimada del uso de tecnologías de comunicación industrial para el periodo 2023–2025:

Figura 1. Proyección de uso de tecnologías industriales (2023–2025).



Fuente: HMS Networks y McKinsey, 2023.

La organización Foundation Fieldbus (FF) tiene su protocolo de comunicación industrial para una red de área local (LAN) con sensores, actuadores y dispositivos de control de procesos. Esto es una red digital, bidireccional y multipunto, diseñada para reemplazar las redes propietarias que conectan los controladores lógicos programables (PLC) de muchas grandes empresas. En los sistemas tradicionales, una computadora o una costosa unidad controladora proporciona el control de la red de dispositivos.

En los últimos años, algunas empresas han desarrollado sistemas de instrumentación con mayor inteligencia integrada. La principal desventaja de estos sistemas es que son propietarios y, por lo tanto, no son interoperables. Existen otros estándares de instrumentación abiertos, como PROFIBUS y HART, pero estos protocolos no implementan el control; aún se requiere un

controlador independiente. FF es un estándar abierto que permite que los dispositivos de campo ejecuten tanto la entrada/salida como el control (National Instrument, 2024).

A diferencia de los sistemas tradicionales de 4-20 mili Amperios (Ma), FF ofrece interoperabilidad, diagnóstico remoto y continuidad operativa incluso si se pierde conexión con el sistema central. Ante escenarios convencionales, las soluciones IIoT actuales permiten la creación de potentes métricas y secciones de control sin necesidad de ser un experto en TI. Esto le permite tomar decisiones informadas, mejorar la eficiencia operativa y promover la sostenibilidad en toda la cadena de valor. (HMS Networks, 2025)

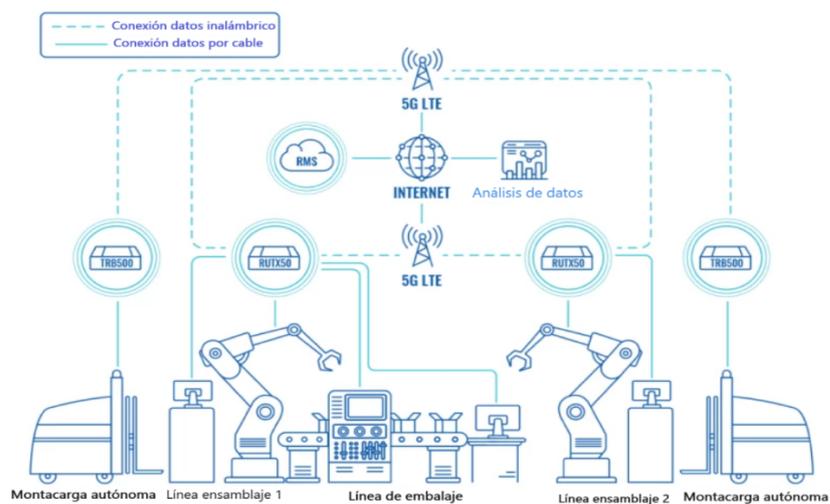
Una aplicación común de redes industriales inalámbricas utiliza puntos de acceso (hotspots) que operan con el estándar Wi-Fi 802.11n en las bandas de 2,4 GHz o 5 GHz. Este estándar permite el roaming, facilitando la conectividad continua cuando un dispositivo se desplaza entre distintas áreas de cobertura. Así, los datos pueden transmitirse de manera inalámbrica hacia otros sensores o unidades de procesamiento y control. Sin embargo, estas redes enfrentan limitaciones en el manejo de grandes volúmenes de datos, debido al ancho de banda y la capacidad insuficientes que ofrece la infraestructura Wi-Fi actual en entornos industriales. Por lo tanto, se necesita una nueva infraestructura de red para cumplir con los mayores requisitos de velocidad, ancho de banda, latencia y calidad.

Según un informe de Ericsson (2023), más del 35% de las empresas manufactureras medianas y grandes están migrando hacia redes privadas 5G para gestionar operaciones en plantas de producción con robots colaborativos, vehículos autónomos y monitoreo predictivo. Este salto tecnológico permite reducir los tiempos de inactividad en un 40% y aumentar la eficiencia energética hasta un 20%. La aceleración de la digitalización, complementada con la automatización y la electrificación, cobrará un gran

impulso en los próximos cinco a diez años, generando un impacto profundo y duradero en la sociedad y las industrias. Esta interacción intersectorial se sustentará en rápidos avances tecnológicos en tres tecnologías clave: IA, nube y movilidad. (Ericsson, 2025).

Ejemplo de ello pueden ser la automatización de procesos y el control remoto de maquinaria y vehículos industriales en fábricas, el mantenimiento preventivo y la monitorización de activos en parques de aerogeneradores con el uso de cámaras y drones, las operaciones y el mantenimiento en puertos con trazabilidad de contenedores y vehículos, la detección de plagas en explotaciones agrícolas, la conexión de miles de sensores para Smart Cities, la mejora de la seguridad para empleados en almacenes, soluciones de telemedicina o la asistencia remota apoyada en tecnologías de realidad virtual o aumentada (Bustán, 2024).

Figura 2. Escenario de conectividad industrial



Fuente: Digitalización 5G en la fabricación (Teltonika, 2023)

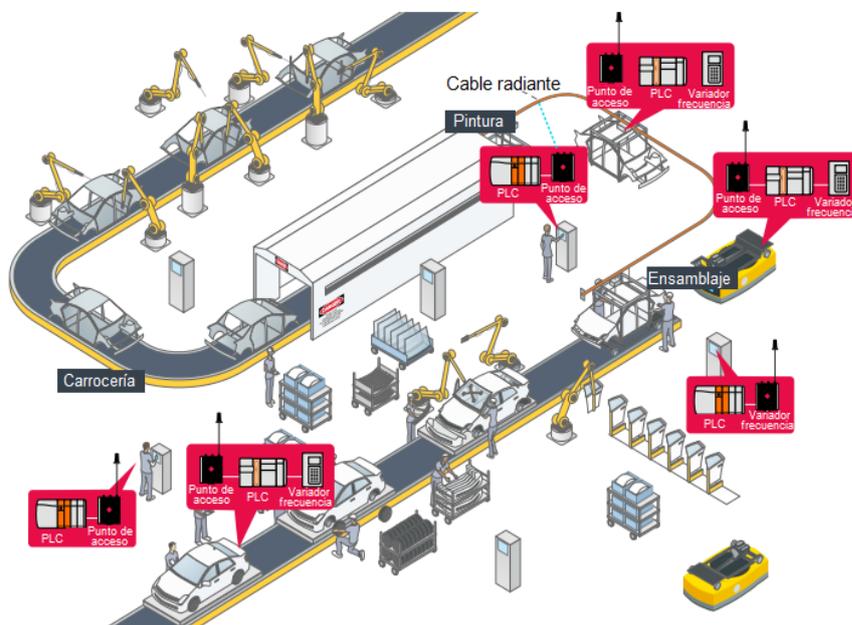
Pero el cambio a 5G también genera desafíos para las pequeña y mediana industria (PYMES) ya que deben invertir en nueva infraestructura tecnológica y adaptarse a los cambios de los procesos incluyendo actualización de equipos, capacitación del personal y replanteamiento de modelos de negocio

aprovechando al máximo lo que puede ofrecer la tecnología 5G (Paliz, Ruales, & Recalde, 2025)..

El despliegue de la tecnología 5G facilitará que fabricantes pongan a disposición equipamiento de conexión a internet para la industria inteligente; por tanto, la tecnología 5G proporciona conectividad de alta velocidad y flexibilidad que ayuda a mejorar todo el sistema de fabricación. Con tiempo de reacción de hasta 1 milisegundo, lo que permite respuestas y transmisiones de datos en tiempo real. Aparte ofrece conectividad masiva, es decir, un sinnúmero de conexiones y mayores velocidades de transacción puede admitir aplicaciones relacionadas con la inteligencia artificial, realidad aumentada, etc.

En la figura 3, se muestran líneas de ensamblaje de autos y en el cual la comunicación inalámbrica, conecta equipos y máquinas que forman parte de procesos automatizados de carrocería, soldadura, pintura, etc.

Figura 3. Escenario Industrial en proceso de ensamblaje de autos



Fuente. (ProSoft, Wireless Functional Safety Application Guide. 2020, p.7)

Las soluciones inalámbricas son cada vez más comunes en entornos industriales ya que permiten una producción más eficaz, pues permite mover

maquinaria o reconfigurar líneas de producción sin necesidad de re-cablear, lo que reduce costos y tiempos de parada.

DE LA INDUSTRIA 4.0 A LA 5.0

La transición de la Industria 4.0 a la 5.0 incorpora una convergencia hacia una mayor integración de trabajo o colaboración entre humanos (obreros, técnicos, profesionales, científicos) y las máquinas, enfocándose en la sostenibilidad, la personalización y la asistencia en lugar de la “pura automatización”. La Industria 4.0, aunque ha sido fundamental en la digitalización y automatización, se centra en la eficiencia y la optimización. La Industria 5.0, por otro lado, busca re-introducir el factor humano, promoviendo la colaboración, la sostenibilidad y la personalización. En lugar de reemplazar a los trabajadores, los robots y la IA están delineados para trabajar junto a ellos, aprovechando la creatividad y habilidades humanas con la precisión y velocidad de la automatización.

En la tabla 1 se realiza una comparativa entre industria 4.0 y 5.0.

Tabla 1. Características entre la Industria 4.0 y 5.0

Aspecto	Industria 4.0	Industria 5.0
Enfoque	Digitalización y automatización avanzada.	Colaboración entre humanos y máquinas.
Automatización y eficiencia	Robots y sistemas automatizados realizan tareas repetitivas y precisas.	Cobots apoyan en tareas creativas y de toma de decisiones.
IoT y Big Data	Dispositivos conectados comparten datos en tiempo real.	Dispositivos conectados comparten datos en tiempo real.
Inteligencia artificial	Algoritmos optimizan procesos y predicen fallos.	Algoritmos optimizan procesos y predicen fallos.
Colaboración humano-robot	N/A	Robots colaborativos trabajan junto a humanos.
Centrado en las personas	N/A	Mejora de la experiencia y bienestar del trabajador.

Sostenibilidad	N/A	Prácticas industriales sostenibles.
Desafíos clave	Alta inversión inicial, adaptación de infraestructura, ciberseguridad.	Integración de tecnología avanzada, capacitación continua, gestión de colaboración hombre-máquina.

La Industria 5.0 representa una evolución sobre la Industria 4.0, enfocándose no solo en eficiencia y automatización, sino también en el impacto humano, ambiental y sistémico. De forma gráfica se puede diferenciar esta asociación entre las máquinas y las personas

Figura 4. Diferencias entre industria 4.0 y 5.0



Fuente: Autores

Desde el aspecto de sostenibilidad, implicará el uso eficiente de recursos, reducción de emisiones, energías limpias y economía circular. La resiliencia será la capacidad de los sistemas industriales para adaptarse, recuperarse y continuar operando ante interrupciones, como crisis sanitarias, fallos tecnológicos o desastres naturales. Ambas características permiten mantener la productividad sin comprometer el medio ambiente ni depender de condiciones externas estables. Por ejemplo. Una planta industrial equipada con sensores IoT que monitorean en tiempo real:

- ❖ Consumo energético,
- ❖ Emisiones de CO₂,
- ❖ Eficiencia de máquinas.

Esta planta además funciona con un sistema híbrido de energía (solar y red eléctrica), y está conectada a una plataforma en la nube que aplica machine learning para optimizar el consumo. Si se origina una interrupción del suministro eléctrico externo (por ejemplo, por una sequía que afecta a una central hidroeléctrica), el sistema resiliente:

- ❖ Cambia automáticamente al respaldo solar más baterías,
- ❖ Reajusta procesos menos críticos para priorizar tareas esenciales,
- ❖ Mantiene la producción operativa sin pérdidas ni parada total.

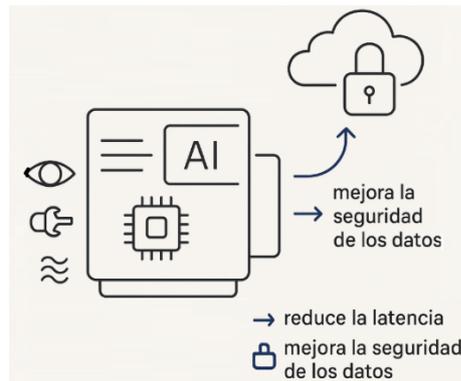
A la vez, los datos recolectados permiten evaluar qué procesos generan más emisiones, proponiendo ajustes para ser más sostenibles, como:

- Cambiar horarios de producción para coincidir con horas pico de radiación solar.
- Mantener equipos solo en operación cuando se detecta presencia de operarios (sensores de proximidad + IA).
- Prolongar la vida útil de equipos y máquinas, el reemplazo fortuito (mantenimiento correctivo) de una máquina antes de tiempo trae costos y pérdida de tiempo por paradas o suspensiones en la producción, aquí juega un papel importante el mantenimiento predictivo.

INTELIGENCIA ARTIFICIAL EN PLANTA

El uso de inteligencia artificial distribuida en el borde (*Edge AI*) es parte de la industria 5.0. pues permite que los dispositivos industriales tomen decisiones localmente, reduciendo la dependencia de la nube. Esto es especialmente relevante para aplicaciones críticas como control de calidad con visión artificial, mantenimiento predictivo y análisis de vibraciones en motores eléctricos.

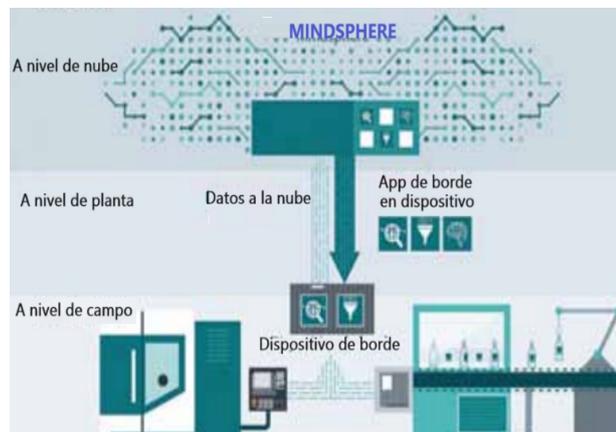
Figura 5. Uso de la AI Edge



Fuente: Autores

Plataformas como Siemens Industrial Edge, Rockwell Automation FactoryTalk Edge y Huawei Edge AI, han reportado aumentos de hasta el 30% en productividad gracias al procesamiento distribuido, según datos de la consultoría global de gestión McKinsey esta tendencia reduce la latencia y mejora la seguridad de los datos al evitar el tránsito constante hacia nubes públicas.

Figura 6. Empresas con Edge AI



Fuente: (Skubacz, 2020)

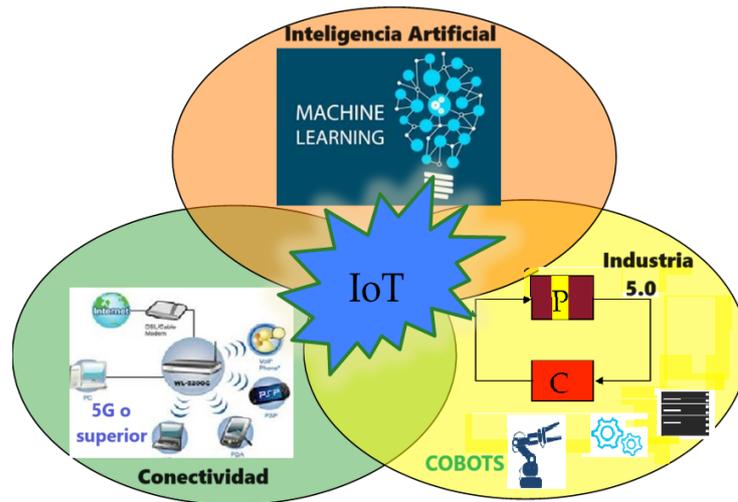
Un ejemplo es el sistema operativo de IoT abierto: MindSphere de Siemens, basado en la nube que permite comprender los datos conectando en tiempo real de productos, sistemas y máquinas al mundo digital. Bajo el escenario con procesamiento distribuido, los procesos controlados por inteligencia artificial no se ejecutan en un solo lugar (como en la nube central), sino que están

repartidos en múltiples nodos o dispositivos locales (dispositivo de borde o edge) (IBM, 2025). Esto significa que sensores, controladores lógicos programables (PLC), cámaras o robots pueden tener algoritmos de inteligencia artificial ejecutándose directamente en ellos, sin depender de un servidor remoto para analizar datos o tomar decisiones.

Un ejemplo de control de calidad con visión artificial, es cuando una cámara con IA integrada examina productos en una línea de ensamblaje y decide en tiempo real si hay defectos. De esta manera se puede mejorar no solo la precisión y la velocidad. Sino que se adapta a los requisitos dinámicos de la producción. El ejemplo de un mantenimiento predictivo, es cuando un sensor montado en un motor detecta vibraciones anormales, y su IA embebida predice una posible falla. Los sensores de los equipos localizan las imperfecciones y notifican rápidamente a la dirección las reparaciones cruciales, lo que permite resolverlas a tiempo y evitar tiempos de inactividad operativos.

Así, se puede detener la máquina antes de que se dañe. Los sistemas de control de calidad basados en IA detectan fallas con mayor precisión, garantizando la consistencia del producto final.

Figura 7. Integración de tecnologías en Industria inteligente



Fuente: Autores

La industria 5.0 se apoya de la conectividad con comunicaciones inalámbricas 5 G o superiores, más la AI y cobots. En síntesis, la conectividad avanzada junto con la Edge Computing habilitan la hiper-conectividad requerida para organizar eficientemente el ecosistema de dispositivos y el procesamiento distribuido de datos en entornos industriales inteligentes.

"Las redes WiFi son más susceptibles a la pérdida de paquetes debido a interferencias de señales externas, saturación del espectro y obstrucciones físicas".

Pandora FMS Team. 2025

CAPÍTULO II:

DATOS, PROTOCOLOS Y SEGURIDAD EN REDES INDUSTRIALES

Los protocolos en redes de sensores y actuadores son fundamentales para garantizar la comunicación eficiente, segura y en tiempo real entre dispositivos en entornos industriales, agrícolas, urbanos, entre otros. Son conjuntos de reglas y estándares que toda red de datos industrial, define cómo sensores, actuadores y otros equipos de red intercambian información. De manera inicial, se define primeramente, que es una red de sensores, estos son nodos¹ con capacidad de detección, se consideran un método de recopilación de datos para construir el sistema de información y comunicación, el cual mejorará en gran medida la confiabilidad y eficiencia de los sistemas de infraestructura.

La Unión Internacional de Telecomunicaciones (ITU-T, International Telecommunication Union), define a una red de sensores como una red compuesta por nodos sensores interconectados, que intercambian datos detectados, usando comunicación inalámbrica o cableada. (UIT-T Recomendación X.1361, 2018) Estas redes de sensores están densamente desplegadas, ya sea dentro del ambiente donde ocurre un fenómeno o muy cerca de él, y se basan en el esfuerzo de colaboración de todos sus nodos para la obtención de los datos (Rueda & Talavera, 2017).

Estos dispositivos son de bajo costo y consumo, las cuales son unidades autónomas que tienen la capacidad de detectar, procesar y comunicar datos a través de enlaces inalámbricos hasta un dispositivo denominado estación base o en su defecto a un nodo sink o sumidero y posteriormente al Gateway

¹ Es un punto de conexión en una red que puede enviar, recibir, crear o almacenar datos. Es cualquier dispositivo de red, como una computadora, impresora, módem, puente o conmutador, que puede procesar y transmitir información a otros nodos.

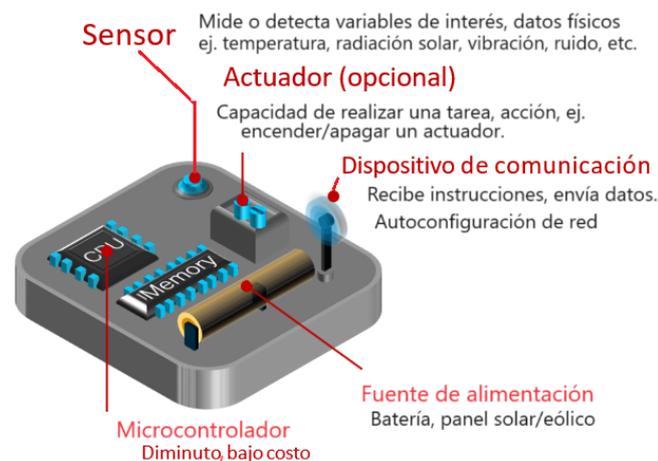
o puerta de enlace. El desarrollo tecnológico de miniaturización de componentes microcontroladores más avanzados convierten a las redes de sensores inalámbricos (Wireless Sensor Network, WSN) en la tecnología clave para IoT.

Existe una terminología que suelen referirse al mismo concepto.

- Sensores inteligentes » Cosas inteligentes
- Dispositivos inteligentes » Dispositivos inteligentes
- Dispositivos de IoT » Objetos inteligentes
- Dispositivos inteligentes » Cosas ubicuas
- Cosas » Productos inteligentes

También existe el término “mota” utilizado para referirse a un sensor en una red de sensores. En la figura 8 se muestra un nodo sensor con sus partes principales.

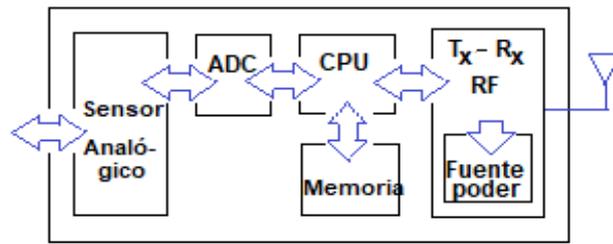
Figura 8. Partes principales de una mota



Fuente: Autores

Los procesadores o más bien microcontroladores toman los datos del sensor a través de sus puertas de datos, y envían la información a la estación base (nodo sumidero o servidor). Por estas capacidades se les denominan “motas”. En la figura 8 se puede ver la compartición interna de una mota WSN.

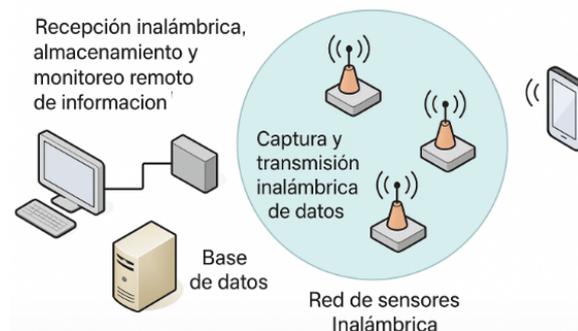
Figura 9. Esquema de mota de una WSN



Fuente: Autores

Como se indicó anteriormente los nodos actúan como elementos de la infraestructura de comunicaciones al reenviar los mensajes transmitidos por nodos más lejanos hacia al centro de coordinación o *gateway*. Los sensores pueden ser fijos o móviles. Estos dispositivos básicamente constan de un microcontrolador, una fuente de energía (casi siempre una batería), un transceptor (Tx-Rx) que transmite y recepta señales de radiofrecuencia (RF) y un sensor analógico (Huma Kamal & Ali Salahuddin, 2015).

Figura 10. Red WSN típica



Fuente: Autores

DESAFIOS EN WSN

Se especifican algunos desafíos que tienen las WSN:

1. **Limitaciones Energéticas:** Los nodos de sensores tienen energía limitada y no suelen poder recargarse o reemplazarse, especialmente en entornos hostiles. Esto impone un estricto presupuesto energético.
2. **Factores de Fallo:** Los nodos pueden fallar por:

- Agotamiento de batería
 - Fallos de hardware
 - Errores de comunicación
 - Interferencias ambientales
 - Ataques maliciosos
3. **Tolerancia a Fallos:** Es esencial que la red mantenga su funcionalidad ante fallos. Esto se logra mediante:
- Protocolos de enrutamiento resilientes
 - Capacidad de auto-restauración y reconfiguración
4. **Cobertura y Agujeros Negros:** La cobertura de red puede verse afectada por nodos inactivos, generando "agujeros negros" que desperdician energía en retransmisiones innecesarias.
5. **Modos de Bajo Consumo:** Los nodos operan en modo "sleep" la mayor parte del tiempo para conservar energía.
6. **Propiedades de Autogestión:** Las WSN modernas incorporan:
- Auto-diagnóstico
 - Auto-configuración
 - Auto-organización
 - Auto-reparación
7. **Optimización Energética y Calidad de servicio (QoS):** La vida útil de la red depende de minimizar el consumo energético sin comprometer:
- Sensado
 - Ruteo
 - Transmisión de datos
 - Calidad de Servicio (QoS)

MODELO DE ARQUITECTURA DE CAPAS

El modelo de arquitectura en el ecosistema del IoT más popularizado, es el modelo de cinco capas.

Figura 11. Arquitectura de cinco capas en IoT



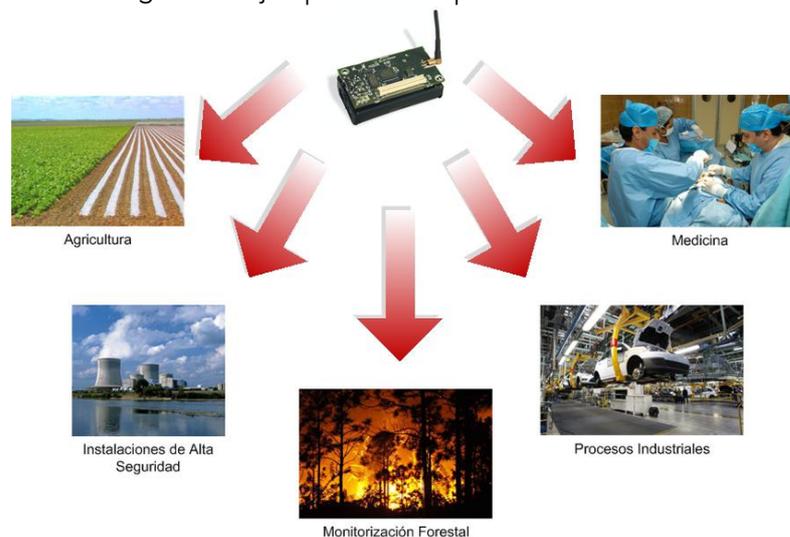
Fuente: Autores

En la primera capa están los dispositivos u objetos conectados, se encuentran sensores, actuadores, electrodomésticos, vehículos, inclusive personas (wearables o dispositivos biométricos), etc. Además de conectividad a redes privadas o a internet para acceder a la nube. La siguiente capa es la de red aunque de manera intermedia, equipos como puertas de enlace transportan los datos recolectados de la primera capa hacia capa, de red, donde switches administrables, no administrables, routers comunican al internet o sistemas de cómputo en la nube. La capa de servicios están aplicaciones de automatización, mantenimiento predictivo, monitoreo ambiental, salud, logística, etc Se integran mediante APIs RESTful, servicios web y plataformas como ThingsBoard, Kaa, ThingSpeak. Puede incluir inteligencia artificial y machine learning para análisis predictivo y toma de decisiones autónoma., finalmente la capa de aplicación suministra los servicios personalizados, según las necesidades de los usuarios. Por ejemplo, Dashboards de monitoreo y control en tiempo real (Grafana, Power BI, aplicaciones móviles/web). Aquí se definen reglas de negocio, KPIs, alertas, reportes, visualización de datos.

APLICACIONES DE WSN

Los escenarios de aplicación de las WSN son varios, se implementan para monitorizar variables de interés en las ciudades inteligentes, la agricultura, de precisión, seguridad en instalaciones, monitorización de incendios forestales, etc. La figura 12 muestra algunos ejemplos de aplicaciones con WSN.

Figura 12. Ejemplos de las aplicaciones de WSN



Fuente: (García. 2010, p. 7)

ARQUITECTURA DE UNA WSN

En diferentes aplicaciones de WSN los dispositivos de control o detección integrados en la red se basan generalmente en diferentes plataformas de hardware, sistemas operativos, bases de datos y middleware. Y no se pueden implementar en una variedad de entornos de red heterogéneos con libre intercambio de información, excepto si son compatibles con sistemas comerciales dedicados y plataformas de administración de aplicaciones.

En términos de diseño de arquitectura, la mayoría de los entornos de aplicación de la red de sensores están diseñados en arquitecturas cerradas estrechamente acopladas. En este sentido, el sistema presenta características de un silo de información y solo es adecuado para el entorno de aplicación en industrias de pequeña escala. Además, es difícil compartir y reutilizar la

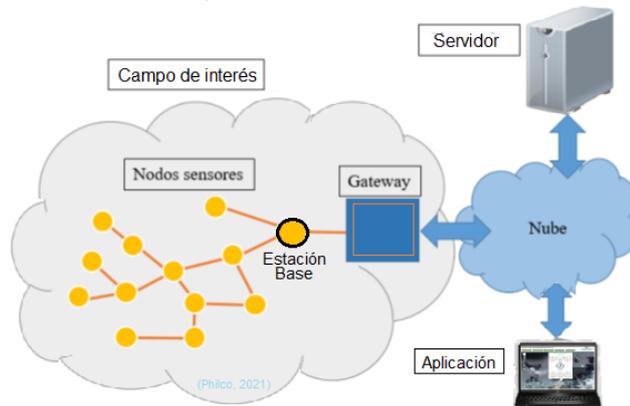
arquitectura y los servicios del sistema de infraestructura. Por tanto, los recursos de terceros son difíciles de integrar de forma rentable en el sistema. Como resultado, la aplicación y promoción de la tecnología de redes de sensores a gran escala es limitada. (Raza, Faheem, & Guenes, 2019).

Sin embargo, existen dos arquitecturas de la red WSN, estas son:

1. Arquitectura centralizada: en la que los nodos se comunican únicamente con el Gateway, equipo único en la red que controla y gestiona requerimientos de dicha red. No procesa los datos más bien depende de una unidad o nodo con capacidad de procesamiento de datos. En otros términos, la inteligencia de la red está centralizada,

2. Arquitectura distribuida: La computación se realiza en la red, no en un nodo central, lo que reduce el consumo de energía y la carga de comunicación hacia la estación base. Esta arquitectura es ideal en entornos donde se requiere escalabilidad, tolerancia a fallos y eficiencia energética. Otro aspecto es el procesamiento distribuido, donde los nodos cooperan y ejecutan algoritmos distribuidos para obtener una única medida global que el nodo coordinador se encarga de comunicar a la estación base. Los nodos no solo captan la información, sino que utilizan su capacidad de cómputo para elaborar historiales gracias al almacenamiento en base de datos de algún servidor.

Figura 13. Arquitectura de una WSN distribuida



Fuente: Autores

Esta arquitectura y los esfuerzos por reducir las dimensiones de sus componentes de hardware han permitido a los nodos sensores alcanzar tamaños que facilitan la implementación de cientos de aplicaciones. Esta reducción del tamaño también ha generado que los nodos sensores posean limitaciones de recursos como la restricción en:

- Alcance de transmisión
- Capacidades de procesamiento
- Capacidades de almacenamiento
- Energía limitada de sus baterías.

Este último factor es determinante al momento de estimar el tiempo de vida de una WSN, ya que si se le acaba la energía o carga de las baterías el nodo literalmente “muere” en la red.

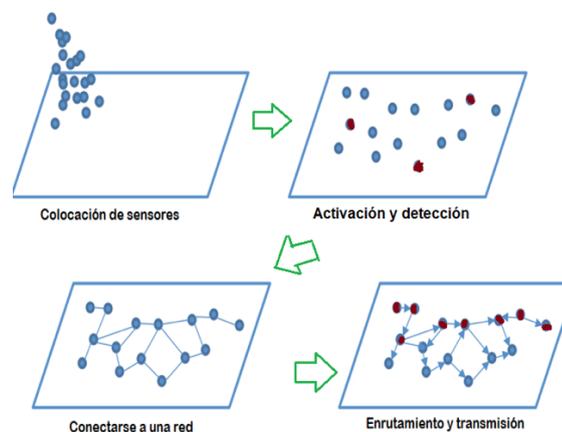
PROCESO DE IMPLEMENTACIÓN DE UNA WSN

Regularmente, los nodos de la red de sensores se despliegan en un campo de interés y el despliegue puede ser determinístico o no determinístico (aleatorio); luego entre los nodos se transmiten su estado (activación o hibernación) a los alrededores y reciben el estado de otros nodos para detectarse entre sí. Posteriormente, los nodos se organizan en una red

conectada de acuerdo con una topología determinada. Finalmente, las rutas adecuadas se calculan en la red construida para transmitir los datos de detección.

El proceso de implementación general de una WSN por lo regular es de forma aleatoria, es decir sin planificar y cumplir estrictamente ubicación y distancias, muchas veces la orografía del terreno o lugar dificultan el despliegue planificado.

Figura 14. Proceso de implementación general de una WSN



Fuente. Autores

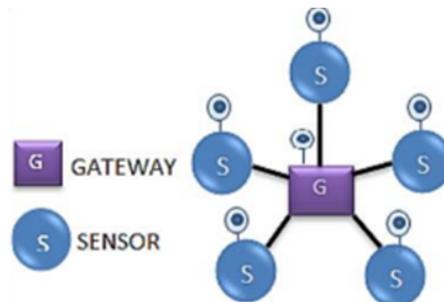
La potencia de los nodos de la red de sensores generalmente la proporcionan las baterías, por lo que la distancia de transmisión de los nodos WSN es corta. La distancia de transmisión puede ser de hasta 800 a 1000 metros en un entorno exterior abierto con línea de visión. Para ampliar la cobertura de una red, se utiliza el modo de transmisión de varios saltos. Es decir, los nodos de la red son tanto transmisores como receptores. El primer nodo de la red, el nodo transmisor, envía datos a un nodo cercano para su transmisión a la puerta de enlace. Así el reenvío pudiese repetirse hasta que los datos llegaran a la puerta de enlace. Los protocolos y algunas técnicas de implementación de las WSNs se pueden adaptar a la arquitectura y las tecnologías maduras de las redes de computadoras inalámbricas.

TOPOLOGÍA DE UNA WSN

Para la comunicación de los diversos nodos en una red WSN, existen tres topologías distintas, los cuales se describen a continuación:

1. **Topología estrella:** Llamado también "sistema de un solo salto", en este tipo de configuración, cada nodo se encuentra directamente comunicado con su nodo base o *gateway*. Una de las ventajas de este tipo de topología es su baja latencia y el bajo consumo de energía de cada nodo. Ideal para aplicaciones en las que el consumo de energía no es esencial y el alcance necesario de la red es corto.

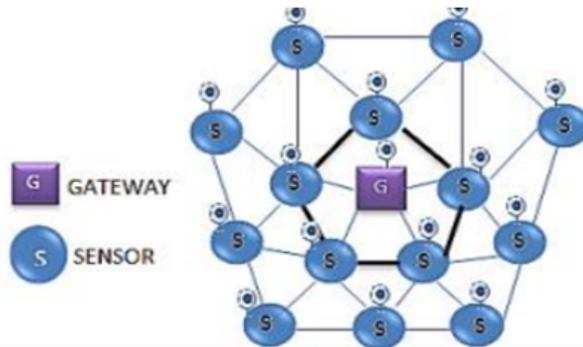
Figura 15. Topología estrella



Fuente: Autores

2. **Topología malla:** Este tipo de configuración se caracteriza por tener nodos intermedios (*routers*) que se encargan de retransmitir la información entre los nodos de la red hasta encontrar el nodo *gateway*. Por eso es un sistema multi saltos. Los nodos son capaces de autoconfigurarse para encontrar el mejor camino, aun en caso de que un nodo se encuentre defectuoso. Es más, se considera una topología robusta, ya que tiene la capacidad de adaptarse a errores originados en los nodos de la red. Además, tiene un mayor alcance que la topología tipo estrella, pero a su vez, tiene una latencia más elevada y un mayor consumo energético.

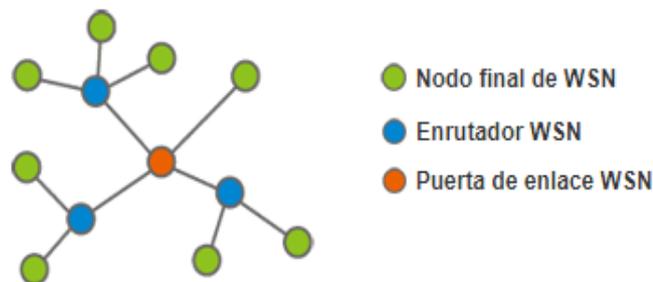
Figura 16. Topología malla



Fuente: autores

3. **Topología árbol:** Cada nodo sensor se conecta a un nodo que se coloca más arriba, jerárquicamente (topología árbol) hasta llegar el nodo sink, nodo coordinador principal o en su defecto al gateway. Para así enlazarse con la estación base o red externa (cloud, servidor, etc.). Sus principales ventajas se basan en la capacidad de expansión de la red y alta eficiencia energética si los nodos intermedios hacen agregación de datos (Chasi, 2018).

Figura 17. Topología árbol



Fuente: Autores

TÉCNICAS DE PROTOCOLO DE ENRUTAMIENTO EN WSN

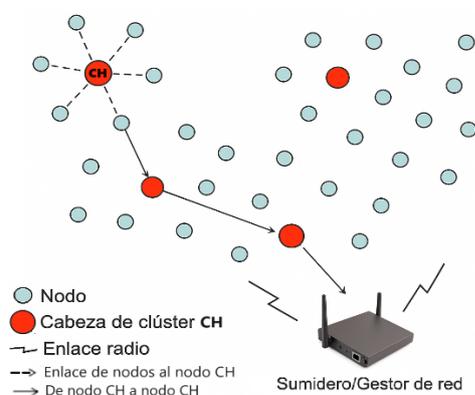
Se definen algunos enfoques basados en la estructura de la red:

- **Enrutamiento plano:** En este enfoque todos los nodos tienen capacidades y funcionalidades iguales, es decir son redes homogéneas. En esta clase se enumeran los protocolos de enrutamiento guiados por consultas centradas en datos. Esta técnica es adecuada para aplicaciones que necesitan un gran número de nodos de sensores y donde los nodos ubicados en una

región pequeña registran datos iguales o similares. La estación base envía una consulta a una región de interés y dependiendo de la solicitud de datos, los nodos responden a través de paquetes de datos. Los protocolos importantes en esta clase son:

- SAR (Sequential Allocation Routing) que asigna rutas en función de la prioridad de los datos y la energía disponible en los nodos.
- Difusión directa: aquí la estación base envía consultas a una región de interés y los nodos responden con paquetes de datos relevantes.
- **Enrutamiento jerárquico.** En este esquema, los nodos sensores se organizan en clústeres (agrupaciones lógicas), donde cada grupo está coordinado por un nodo especializado denominado cabeza de clúster (*Cluster Head, CH*). Estos nodos CH asumen funciones avanzadas, como la agregación de datos, gestión del tráfico intra-clúster y la comunicación directa con el nodo *sink* o con otros CHs en niveles superiores de la jerarquía. A diferencia de los nodos miembros, los CH poseen mayores responsabilidades computacionales y de comunicación, actuando como nodos de control locales en la arquitectura de red. Este enfoque permite una reducción significativa en el volumen de datos transmitidos, mejora la eficiencia energética global y proporciona escalabilidad a la red.

Figura 18. Un escenario de agrupamiento de clústeres



Fuente: Autores

Las técnicas de enrutamiento jerárquico son usualmente basadas en acceso múltiple por división de tiempo (TDMA, Time Division Multiple Access). Las principales técnicas de enrutamiento jerárquico son: Jerarquía de agrupamiento adaptable de baja energía (LEACH, Low Energy), Red de sensores de eficiencia energética sensibles al umbral Clustering Hierarchy (TEEN Threshold Sensitive Energy Efficient Sensor Network), Red de sensores de eficiencia energética sensible al umbral adaptativo (APTEEN Adaptive TEEN) y mucho otros más.

- **Enrutamiento basado en ubicación:** Utiliza información geográfica para determinar las rutas de transmisión. Algunos protocolos destacados son:
 - GPSR (Greedy Perimeter Stateless Routing): Un protocolo que selecciona la ruta más corta basada en coordenadas geográficas.
 - GAF (Geographic Adaptive Fidelity): Optimiza el consumo energético al desactivar nodos redundantes en la red.

TENDENCIAS Y AVANCES RECIENTES

Los protocolos de enrutamiento en WSN han incorporado nuevas técnicas para mejorar la eficiencia y la seguridad:

- **Enrutamiento basado en inteligencia artificial:** Algoritmos de aprendizaje automático optimizan la selección de rutas y la gestión de energía.
- **Protocolos adaptativos:** Se ajustan dinámicamente a las condiciones de la red, mejorando la resiliencia ante fallos.
- **Integración con IoT:** Las WSN se están integrando con plataformas de Internet de las Cosas (IoT) para mejorar la interoperabilidad y el análisis de datos en tiempo real.

REDES DE SENSORES INALÁMBRICAS INDUSTRIALES

Las redes de sensores inalámbricos industriales (IWSN) han revolucionado la forma en que las industrias monitorean, controlan y optimizan sus operaciones. Tradicionalmente, los sistemas industriales dependían de redes cableadas para conectar dispositivos de control y detección, pero la necesidad de mayor flexibilidad y reducción de costos ha impulsado la adopción de WSN.

PRINCIPALES CARACTERÍSTICAS

Expansión y escalabilidad: La integración de nuevos sensores en redes cableadas es costosa y compleja. Las WSN permiten una expansión más rápida y flexible.

Fiabilidad en la transmisión de datos: Se requieren garantías de entrega de paquetes sin errores, especialmente en aplicaciones críticas como seguridad y mantenimiento predictivo.

Ubicación de nodos: Se pueden desplegar de manera determinista (ubicación planificada) o aleatoria, dependiendo de la aplicación y movilidad de los sensores.

APLICACIONES INDUSTRIALES

Las WSN industriales se utilizan en:

- Monitoreo de condiciones operativas: Detección de fugas, medición de presión en tuberías y niveles de fluidos.
- Automatización de procesos: Control de maquinaria y optimización de producción.
- Seguridad y emergencia: Sistemas de alerta temprana y monitoreo estructural.

- **Mantenimiento predictivo:** Sensores que detectan fallos antes de que ocurran.

Las tendencias actuales han mejorado la eficiencia y seguridad de las WSN:

Recopilación de datos en tiempo real: Permite decisiones más rápidas y precisas.

Eficiencia operativa mejorada: Integración con sistemas de control automatizados para ajustes dinámicos.

Escalabilidad y flexibilidad: Fácil incorporación de nuevos sensores sin interrupciones.

Reducción de costos: Minimización del mantenimiento manual y prevención de fallos en equipos.

Integración con IoT: Conectividad con plataformas en la nube para análisis avanzado

Ante estos escenarios, la International Society of Automation (ISA) ha definido estándares y aplicaciones para redes industriales, especialmente en el ámbito de la automatización y control de procesos. Como para las redes inalámbricas industriales, enfocado en automatización de procesos y control. (International Society of Automation, ISA, 2020). Véase a continuación una comparación del estándar ISA100 con otras tecnologías o estándares.

Tabla 2. Comparación de ISA-100 con otras tecnologías

Tecnología	Características	Ventajas	Aplicaciones
ISA-100	Protocolo inalámbrico para automatización industrial	Alta seguridad, escalabilidad, interoperabilidad	Control de procesos, monitoreo remoto
WirelessHART	Basado en HART, diseñado para sensores inalámbricos	Bajo consumo energético, integración con dispositivos HART	Sensores industriales, monitoreo ambiental

Tecnología	Características	Ventajas	Aplicaciones
PROFIBUS/PROFINET	Redes cableadas para automatización	Alta velocidad, confiabilidad en transmisión	Control de maquinaria, automatización de fábricas
LoRaWAN	Tecnología de largo alcance y baja potencia	Gran cobertura, bajo consumo	Monitoreo de infraestructura, ciudades inteligentes

Fuente: autores

La ISA100 destaca por su seguridad avanzada, baja latencia y compatibilidad con múltiples dispositivos industriales. Además, permite una gestión eficiente de redes inalámbricas en entornos crítico. En la tabla 3 se detalla aspectos de seguridad, control y vigilancia de aplicación junto con estimativo en la latencia.

Tabla 3. Diferentes clases de aplicaciones definidas por ISA-100

Categoría	Rango	Aplicación	Latencia	Descripción
Seguridad	0	Acción de emergencia	10 milisegundos. (determinista)	Siempre crítico, por ej, sistemas de protección/sistemas de protección instrumentados.
	1	Control regulatorio de circuito cerrado.	10 milisegundos.	A menudo crítico, p. ej., Control de bucle de control regular.
Control	2	Control de supervisión de circuito cerrado.	hasta 100 milisegundos.	Por lo general, no es crítico, por ejemplo, manipulación del punto de ajuste para la optimización del sistema de control.
	3	Control de bucle abierto.		Humano en bucle, por ejemplo, acciones humanas manuales en alertas.
Vigilancia	4	Alertando	100 milisegundos. en promedio	Consecuencia operativa a corto plazo, por ejemplo, mantenimiento basado en eventos.
	5	Registro y descarga/carga	100 milisegundos. en promedio	Sin consecuencias operativas inmediatas, por ejemplo, recopilación de historial, secuencia de eventos, mantenimiento preventivo.

Fuente: (Wang & Jiang. 2016, p. 2200)

1. Sistemas de seguridad (Categoría 0)

- Prioridad máxima, con latencias de 10 ms deterministas.
- Aplicaciones incluyen seguridad contra incendios, monitoreo en centrales nucleares y sistemas de protección en entornos industriales críticos.

➤ Integración con monitoreo en tiempo real, permitiendo la supervisión de bomberos y personal de respuesta temprana.

2. Sistemas de control (Categorías 1, 2 y 3)

➤ Control de lazo cerrado (1): Utiliza retroalimentación para regular procesos industriales. Se aplica en automatización de fábricas y control de procesos, con latencias de 2-100 ms.

➤ Supervisión de lazo cerrado (2): Reacciona a eventos específicos, recopilando datos estadísticos para optimización de procesos.

➤ Control de lazo abierto (3): Operado por humanos, donde la WSN recolecta y transmite datos a una base central para análisis y toma de decisiones.

3. Sistemas de monitoreo (Categorías 4 y 5)

➤ Alertas operativas (4): Monitoreo continuo de variables como temperatura en hornos, con respuestas basadas en eventos.

➤ Recolección de información (5): Recopilación de datos ambientales e industriales para análisis a largo plazo, con latencias superiores a 1 segundo.

REQUERIMIENTOS PARA UNA IWSN

La IWSN requiere de protocolos de comunicación eficientes para garantizar confiabilidad, escalabilidad y eficiencia energética. A continuación, se presentan requerimientos en el diseño del protocolo Media Access Control (MAC).

Confiabilidad: La confiabilidad se refiere a la capacidad de la red para asegurar la entrega correcta de los datos, minimizando errores, pérdidas y retrasos. Algunos factores clave que impactan la confiabilidad incluyen: Redundancia o implementación de múltiples rutas de comunicación y nodos de respaldo para evitar fallos en la transmisión. Otro aspecto la tolerancia a fallos donde la red debe seguir operativa en presencia de fallos en dispositivos

o enlaces. Ejemplo: En una red basada en Zigbee, si un nodo falla, la información es redirigida por rutas alternativas.

Corrección de errores: Se emplean códigos de detección y corrección, como CRC (Cyclic Redundancy Check), para verificar la integridad de los paquetes. Se debe garantizar una alta tasa de recepción de paquetes para evitar fallos en el sistema. La confiabilidad está relacionada con la eficiencia energética, asegurando una vida útil adecuada de la red.

Prioridad y heterogeneidad de paquetes: En entornos industriales, se generan distintos tipos de tráfico con diferentes niveles de prioridad. Los comandos de control y actuación tienen mayor prioridad que los datos de sensores. Un retraso en estos paquetes puede causar interrupciones o fallos en la producción. Ejemplo: activación/desactivación de motores, ajuste de válvulas, cambios en parámetros de operación.

Se requiere un protocolo que gestione la prioridad para garantizar respuestas oportunas en caso de fallas. Existen múltiples estándares como Modbus, Profibus², EtherNet/IP³ y MQTT⁴, que presentan distintas estructuras de paquetes y requerimientos de transmisión.

Eficiencia energética y consumo de energía: Los sensores alimentados por batería deben optimizar el consumo energético para prolongar su funcionamiento.

La baja latencia y alta confiabilidad pueden aumentar el consumo de energía, por lo que se deben equilibrar estos factores.

² Conjunto de protocolo de comunicación industrial para la automatización, utilizado principalmente en entornos industriales para la comunicación entre sensores, actuadores y controladores.

³ Es una red Ethernet flexible que permite la interconexión de dispositivos, como sensores, controladores y sistemas de control, en un entorno industrial

⁴ Message Queuing Telemetry Transport, es un protocolo de mensajería ligero, basado en el modelo de publicación/suscripción, que se utiliza para la comunicación entre dispositivos, especialmente en entornos IoT (Internet de las Cosas) y M2M (Máquina a Máquina)

Se requieren protocolos robustos y flexibles que minimicen el gasto energético sin comprometer el rendimiento.

Escalabilidad: Las IWSN deben ser capaces de adaptarse a la adición o eliminación de nodos sin degradar el rendimiento. Los protocolos como WirelessHART e ISA100.11a utilizan acceso múltiple por división de tiempo, lo que impone restricciones en la cantidad de nodos.

Se necesitan protocolos MAC escalables que permitan la expansión de la red sin afectar la calidad del servicio.

Comunicación multisalto: En plantas industriales grandes, los nodos sensores deben transmitir datos a través de múltiples nodos antes de llegar al sumidero. Esto permite flexibilidad en la expansión de la red y agrega redundancia en caso de fallos. Es decir, permite que los datos viajen de un nodo a otro hasta alcanzar el destino final, lo que optimiza la cobertura y reduce el consumo energético en redes inalámbricas. Se usa en entornos donde la comunicación directa no es posible debido a obstáculos o limitaciones de alcance.

En la tabla 4 se muestran los requisitos para distintos tipos de sensores de IWSN, en automatización de procesos.

Tabla 4. Especificaciones de sensores para supervisión de procesos

Aplicaciones de redes de sensores	Retardo	Rango	Tiempo de vida de la batería	Frecuencia de actualización (update)	Nivel de seguridad
Supervisión y monitoreo					
Sensor de vibración	s	100 m	3 años	Segundos - días	bajo
Sensor de presión	ms	100 m	3 años	1 segundo	bajo
Sensor de temperatura	s	100 m	3 años	5 segundos	bajo
Sensor de detección de gas	ms	100 m	3 años	1 segundo	bajo
Control de lazo cerrado					
Válvula de control	ms	100 m	> 5 años	10-500 ms	medio
Sensor de presión	ms	100 m	> 5 años	10-500 ms	medio
Sensor de temperatura	ms	100 m	> 5 años	500 ms	medio

Sensor de flujo	ms	100 m	> 5 años	10-500 ms	medio
Sensor de torque	ms	100 m	> 5 años	10-500 ms	medio
Variador de velocidad	ms	100 m	> 5 años	10-500 ms	medio
Interbloqueo y control					
Sensor de proximidad	ms	100 m	> 5 años	10-250 ms	medio
Motor	ms	100 m	> 5 años	10-250 ms	medio
Válvula	ms	100 m	> 5 años	10-250 ms	medio
Relés de protección	ms	100 m	> 5 años	10-250 ms	medio

Fuente: (Akerberg, Gidlund, & Bjorkman. 2011, p. 412)

Así en aspecto de recolección de datos ambientales o de condición sin necesidad de respuesta inmediata. Para caso del control en tiempo real de procesos industriales, es vital la sincronización precisa y confiable. Y en aspecto de seguridad operativa y control de eventos críticos, la respuesta rápida es esencial.

REQUERIMIENTOS DE IWSN FRENTE A BUSES DE CAMPO DIGITALES

Se indica que los sistemas de comunicación digital utilizados en la automatización industrial (buses de campo) para conectar dispositivos de campo como sensores, actuadores, y controladores. Al respecto una IWSN debe cumplir con una serie de requerimientos técnicos para integrarse eficazmente en entornos industriales dominados por buses de campo digitales cableados. Estos requerimientos son:

Interoperabilidad

Las IWSN deben integrarse con sistemas cableados existentes. Esto requiere pasarelas eficientes y un enfoque estandarizado para facilitar la interoperabilidad con normas de la Comisión Electrotécnica Internacional (IEC). La integración debe ser fluida, permitiendo configuración, despliegue y mantenimiento sencillos.

Resistencia al ruido y coexistencia

Las IWSN operan en entornos ruidosos por lo que deben soportar interferencias y coexistir con otras tecnologías inalámbricas. Se requieren técnicas como:

- Diversidad en tiempo, frecuencia y espacio
- Cancelación de interferencias
- Gestión eficiente del espectro
- Radios definidas por software (SDR)

Consumo energético

Bajo consumo: Uso de baterías y señales de baja potencia para prolongar la vida útil. Imaginemos una planta de fabricación de perfiles de acero que monitorea vibraciones en sus motores mediante sensores inalámbricos. Para optimizar el consumo energético: Los sensores transmiten datos cada 10 segundos en condiciones normales, pero aumentan la frecuencia si se detecta un evento crítico (pico de vibración).

Podrían usarse protocolos de baja energía, como WirelessHART, que permite que los nodos funcionen por más de 5 años con una batería de litio. Además, los sensores entran en modo de suspensión cuando no hay cambios en la vibración, reduciendo el consumo.

La red debe diseñarse con enrutamiento optimizado, evitando retransmisiones innecesarias y maximizando la eficiencia. El aspecto del consumo eficiente: logra balanceo de carga mediante protocolos de enrutamiento energéticamente conscientes.

Autoorganización

Las IWSN deben autoconfigurarse y operar sin intervención humana, especialmente en ubicaciones de difícil acceso. Imaginemos una planta química con sensores inalámbricos distribuidos para monitorear temperatura, presión y concentración de gases peligrosos. Debido a la naturaleza del ambiente, los sensores deben operar con mínima intervención humana.

Se debe tomar en cuenta estos puntos

- **Autoconfiguración:** Al encender los sensores, cada dispositivo detecta los nodos cercanos y establece comunicación con la unidad central. Si un sensor de temperatura se activa, busca automáticamente el mejor camino para enviar datos sin intervención manual.
- **Adaptación a cambios:** Si se instala un nuevo sensor de presión, la red lo incorpora automáticamente y ajusta las rutas de transmisión de datos.
- **Balanceo de carga:** Si un sensor está transmitiendo demasiada información, otros nodos cercanos asumen parte de la carga para evitar congestión.
- **Recuperación ante fallos:** Si un sensor deja de funcionar, los demás redirigen la información por rutas alternativas sin afectar la operación global.

La autoorganización en redes IWSN se basa en varios protocolos de comunicación:

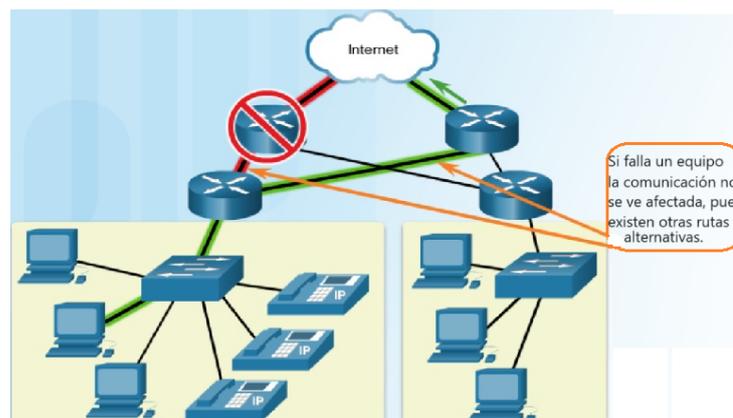
- **RPL (Routing Protocol for Low-Power and Lossy Networks):** Optimiza el enrutamiento en redes con limitaciones energéticas.
- **Zigbee y WirelessHART:** Utilizan topologías en malla que permiten comunicación resiliente entre sensores sin intervención manual.
- **ALOHA y CSMA/CA:** Permiten que los nodos decidan cuándo transmitir datos sin generar colisiones.

La autoorganización mejora la autonomía y eficiencia de las IWSN, reduciendo la necesidad de mantenimiento y mejorando la confiabilidad en ambientes industriales hostiles. Por ejemplo; Cuando varios sensores de un clúster detectan anomalías el CH realiza una agregación de datos, pero si dicho sensor es destruido, los nodos vecinos se reorganizan y eligen un nuevo CH y actualizan rutas sin intervención humana.

Robustez y tolerancia a fallos

Un sistema tolerante a fallas es aquel que puede experimentar una falla (o múltiples fallas) en sus componentes, pero que continúa funcionando correctamente.

Figura 19. Esquema de conexión con tolerancia a fallos



Fuente: (Linares, 2017)

La red debe seguir operando incluso si algunos nodos fallan. Se requieren protocolos de enrutamiento adaptativos y resilientes a cambios de topología.

Confiabilidad de enlace

Los enlaces de baja potencia son menos confiables, lo que puede causar pérdidas de paquetes y retrasos. Se deben implementar:

- Retransmisiones eficientes
- Protocolos de replicación
- Mecanismos de recuperación de fallos

Bajo retardo

Fundamental en sistemas de control en tiempo real, especialmente en lazos cerrados. La red debe garantizar tiempos de respuesta predecibles y rápidos.

Diferenciación de servicios

Los datos de distintos sensores requieren distintos niveles de prioridad. La red debe ofrecer diferenciación a nivel de nodo, paquete y espacial.

Calidad de Servicio (QoS)

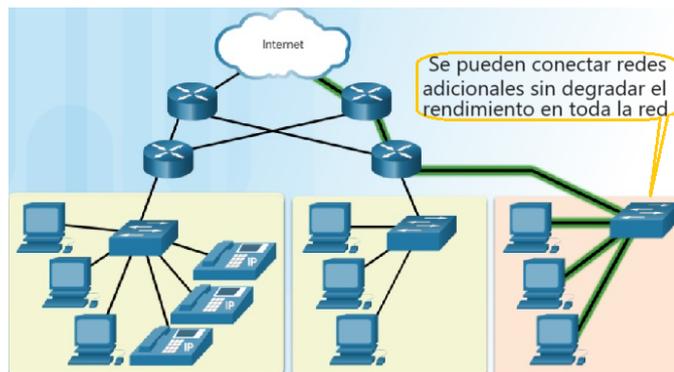
- QoS de aplicación: se refiere al cumplimiento de requisitos específicos del servicio final que la red de sensores proporciona. A diferencia de la QoS de red (retardo, jitter, pérdida de paquetes), la QoS de aplicación considera métricas directamente relacionadas con la utilidad, confiabilidad y cobertura del sistema para cumplir su objetivo funcional. Cobertura mínima, número de sensores activos, precisión.
- QoS de red: se refiere a las características técnicas del tráfico de datos dentro de la red: cómo se transmiten, con qué eficiencia, qué tan rápido y con qué nivel de pérdida o interrupción. Es crítica en aplicaciones tiempo-real, industriales o sensibles, donde las decisiones deben tomarse con datos actuales y confiables. Principales parámetros; ancho de banda, latencia, confiabilidad y disponibilidad.

Escalabilidad

Las IWSN deben adaptarse al crecimiento de la red y a la evolución de las aplicaciones industriales. Esto implica:

- Protocolos y normas escalables.
- Capacidad para añadir o eliminar cientos de nodos sin degradar la QoS.
- Autoorganización como soporte clave para la escalabilidad.

Figura 20. Escalabilidad en red



Fuente: (Linares, 2017)

Fuente múltiple y múltiples sumideros

Las redes deben soportar múltiples aplicaciones simultáneas, lo que implica:

- Uso de múltiples nodos sumideros.
- Soporte para topologías como WSN (Wireless Sensor and Actuator Networks).
- Protocolos de enrutamiento adaptados a múltiples destinos.

Comportamiento predecible

Las soluciones deben ser:

- Analizables antes de su implementación.
- Capaces de cumplir con los requerimientos industriales de forma confiable y eficiente.

Protocolos específicos de la aplicación

Aunque las normas son reutilizables, los protocolos deben adaptarse a:

- Requisitos particulares de cada aplicación industrial.
- Escenarios con necesidades diferenciadas.

Agregación de datos

Para mejorar la eficiencia energética:

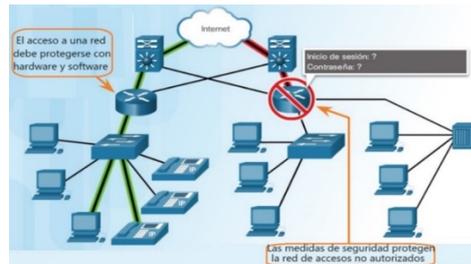
- Se deben reducir datos redundantes.

- Aplicar agregación local o grupal de sensores.
- Minimizar el número de paquetes transmitidos.

Seguridad

La seguridad debe ser prioritaria, incluso en funciones no críticas.

Figura 21 Seguridad en la red



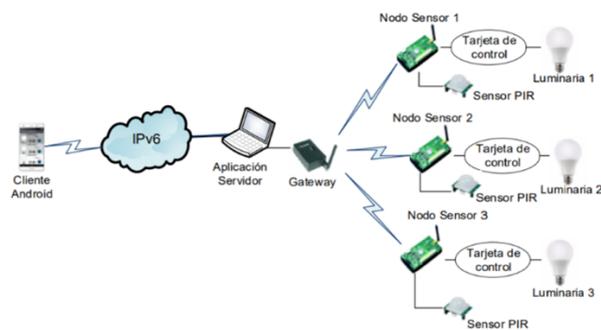
Fuente: (Linares, 2017)

Se requiere:

- Protección contra fallos que puedan causar pérdidas o daños.
- Diseño robusto para evitar situaciones peligrosas o incontroladas.

En la figura 22 se muestra un ejemplo de aplicación IWSN que consta de nodos que recibe señales de un sensor de proximidad infrarrojo (PIR Passive Infrared). Esto último constituye la etapa de detección. Y donde el nodo respectivo tomará la decisión de encendido o apagado de luminarias por la proximidad de intrusos. El gateway permite que un usuario de la aplicación pueda supervisarlo en tiempo real.

Figura 22. Escenario de IWSN básico



Fuente: (Egas, Viracocha, & Rivera. 2019, p. 46)

RED DE SENSORES Y ACTUADORES INALÁMBRICOS (WSAN)

Estos sistemas pueden procesar los datos obtenidos, tomar decisiones y realizar operaciones específicas en el entorno monitoreado, como encender dispositivos (como lámparas o ventiladores), a través de actuadores instalados en los nodos. Los sistemas WSAN pueden considerarse como sistemas distribuidos en tiempo real e integrados (DRE, Distributed, Real-time, and Embedded). Como tal, las WSAN se caracterizan por una alta heterogeneidad con respecto a los requisitos de la aplicación, la tecnología de radio, las capacidades de los nodos y los protocolos de red.

Como se ha indicado están diseñadas para descentralizar la toma de decisiones y operar de manera autónoma, reduciendo la intervención humana en entornos industriales. Este enfoque mejora la confiabilidad de la producción y los beneficios económicos, al permitir que los sistemas inteligentes optimicen procesos.

CARACTERÍSTICAS PRINCIPALES DE WSAN

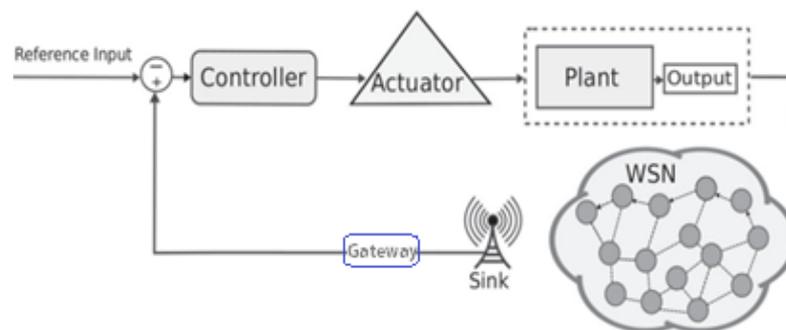
Se indican las siguientes particularidades:

- **Autonomía y descentralización:** Los sensores y actuadores trabajan juntos para detectar cambios y responder sin necesidad de intervención manual.
- **Desafíos ambientales:** Factores como interferencia electromagnética, ruido, calor y polvo afectan la comunicación, requiriendo protocolos robustos.
- **Integración con sistemas ciber-físicos (CPS):** WSAN forma parte de la infraestructura de Industria 4.0, mejorando la producción eficiente y la calidad del producto.

- **Interacción entre sensores y actuadores:** Los sensores recopilan datos del entorno, mientras que los actuadores responden ajustando procesos en tiempo real.
- **Impacto en la confiabilidad y seguridad:** La pérdida de señales puede causar interrupciones costosas en la producción y riesgos para los empleados.

La figura 23 muestra el lazo de control de un proceso o planta que recibe señales o datos de una WSN centralizada.

Figura 23. Lazo de control de una WSN



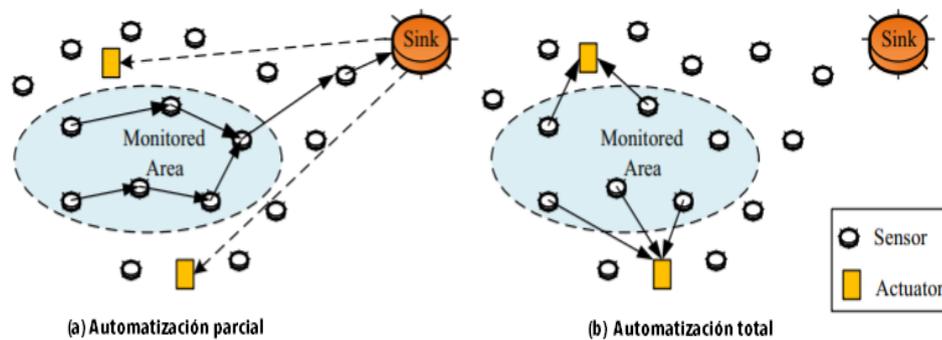
Fuente: Raza, Faheem, & Guenes. 2019, p. 7)

La WSN es un escenario de sensores/actuadores distribuidos donde los sensores tienen comunicación directa con los actuadores y ellos también pueden comunicarse entre sí. Por lo tanto, a diferencia de WSN, donde los sensores siempre comunican los datos detectados al nodo sumidero o estación base, una WSN implica comunicaciones de datos de sensor a actuadores y de actuador a actuador a través de transmisiones de un solo salto o de varios saltos.

Una WSN tiene la capacidad de realizar detección distribuida, fusión de datos, tomar decisiones en colaboración y realizar acciones apropiadas en el entorno físico. Por ejemplo, detectar el nivel o el flujo de agua y enviar datos al actuador, y el actuador controla el nivel o el flujo de agua. De esta manera, la información que se detecta se puede utilizar de manera eficiente para realizar las acciones apropiadas.

En la figura 24 muestra una red WSAN con dos valoraciones de automatización.

Figura 24 Tipos de automatización a. Automatización parcial y b. Automatización total



Fuente: (Sheltami, Al-Roubaiey, & Ashraf. 2015, p. 2050)

En la figura 24 a. la estación base participa en la toma de decisiones que está más centralizada y controlada, pero incurre en más demoras; mientras que, en la interacción es totalmente automatizada. En la figura 24 b. los sensores detectan los datos y los envían directamente a los actuadores para su procesamiento y reacción en respuesta al resultado de análisis de los datos locales. El enfoque totalmente automatizado es más adecuado para aplicaciones en tiempo real, ya que reduce el tiempo y los gastos generales del enfoque centralizado (automatizado parcial). Los actuadores pueden coordinarse entre sí para decidir la acción apropiada y realizar la asignación de tareas o modificar alguna variable en el mundo físico. Debido a la inexistencia de un controlador central, o interacción humana, esta arquitectura se denomina automatizada.

MODELO DE COMUNICACIÓN EN WSAN

Las WSAN se basan en un modelo de comunicación impulsado por eventos, donde el interés se centra en los datos en sí, en lugar de en direcciones específicas. Esto reemplaza el tradicional modelo de solicitud/respuesta, que resulta ineficiente en redes altamente dinámicas. Para resolver este desafío,

las WSN adoptan el modelo publicación/suscripción (pub/sub), que desacopla la comunicación en términos de tiempo, espacio y sincronización.

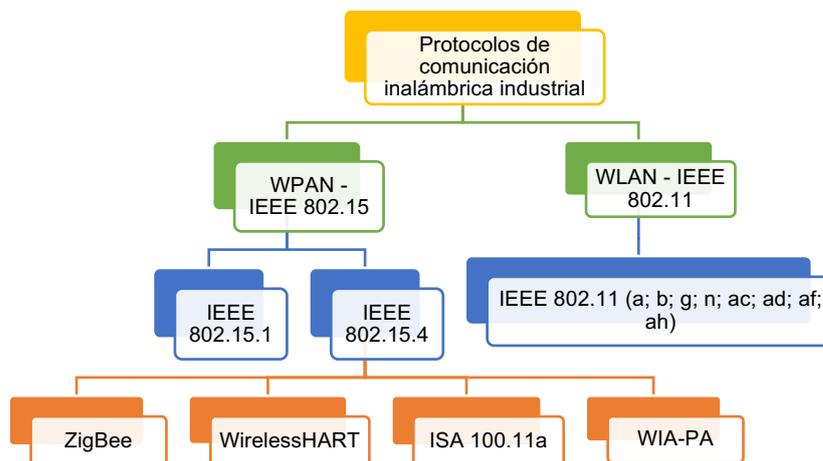
USO DEL PROTOCOLO MQTT EN WSN

El protocolo MQTT es fundamental para la transmisión eficiente de datos en redes de sensores y actuadores industriales. Se utiliza ampliamente en sistemas SCADA para la supervisión y control de procesos a distancia. MQTT opera sobre redes con tráfico elevado, optimizando el intercambio de información mediante una estructura ligera basada en JSON (JavaScript Object Notation). Este modelo de comunicación refuerza la confiabilidad y eficiencia de las WSN en sistemas industriales modernos.

TECNOLOGÍAS DE COMUNICACIÓN EN IWSN

Las tecnologías de comunicación IWSNs son estándares, los cuales se dividen en tres clases principales, de estas tres, dos se utilizan como medio de comunicación para el control en procesos industriales. Véase la figura 25.

Figura 25. Estándares de comunicación inalámbrica utilizadas a nivel industrial



Fuente. Autores

No obstante, varios grupos de trabajo como la Alianza de Redes Inalámbricas (WINA), la Alianza ZigBee, la HCF (HART Communication Foundation), la Sociedad Internacional de Automatización y la China Industrial Wireless Alliance, han establecido normas para IWSN. Los estándares resultantes son

WirelessHART, ZigBee, ISA100.11a y WIA-PA, todos basados en el estándar IEEE 802.15.4.

ESTÁNDAR ZIGBEE

ZigBee es un protocolo de comunicación inalámbrico de bajo consumo y bajo costo, basado en el estándar IEEE 802.15.4, diseñado inicialmente para automatización del hogar y luego adaptado a aplicaciones industriales. Su red de malla mejora la cobertura y la confiabilidad, aunque presenta limitaciones en clases regulatorias y de emergencia debido a la baja fiabilidad de los datos.

CARACTERÍSTICAS

- **Velocidad de datos:** 250 Kbps, adecuada para sensores con transmisión periódica o irregular.
- **Topologías de red:** Soporta configuraciones en malla, estrella y árbol para mejorar la conectividad.
- **Consumo energético:** Optimizado para prolongar la vida útil de la batería en sensores y dispositivos de monitoreo.
- **Interoperabilidad:** Presenta limitaciones al competir con otras tecnologías como Bluetooth y Wi-Fi.
- **Seguridad:** Vulnerable a interferencias y ataques, lo que puede comprometer la integridad de los datos.

Un ejemplo de aplicación: ZigBee es el monitoreo de temperatura en almacenes. Imaginemos un almacén de productos farmacéuticos, donde se requieren mediciones continuas de temperatura: Los sensores ZigBee monitorean la temperatura y transmiten datos cada minuto. La red de malla garantiza cobertura en toda la instalación, incluso en áreas con interferencias. Es decir, si un nodo falla o se interrumpe la comunicación en una ruta, los datos pueden redirigirse automáticamente por otra ruta disponible, asegurando la

continuidad del monitoreo. El bajo consumo energético permite que los sensores operen por años sin reemplazo frecuente de baterías.

ZIGBEE PRO Y SU EVOLUCIÓN

La versión ZigBee PRO, optimizada para IoT, mejora eficiencia energética y permite hasta 64,000 dispositivos conectados, aunque su adopción en automatización industrial es limitada, principalmente para telemetría en procesos con baja movilidad. Este protocolo es una opción viable para monitoreo de sensores en entornos industriales, aunque presenta desafíos de seguridad y rendimiento frente a otras tecnologías. Aunque ZigBee PRO incluye cifrado AES-128, puede ser vulnerable si no se implementan políticas de autenticación y gestión de claves adecuadas.

ESTÁNDAR WIRELESSHART

WirelessHART es un estándar de comunicación inalámbrica para entornos industriales que opera en la frecuencia de 2.4 GHz. Utiliza acceso múltiple por división de tiempo (TDMA) para sincronizar dispositivos y asegurar una red confiable. Se basa en IEEE 802.15.4 y emplea DSSS (Direct Sequence Spread Spectrum) y FHSS (Frequency Hopping Spread Spectrum) para mejorar la seguridad y la resistencia a interferencias.

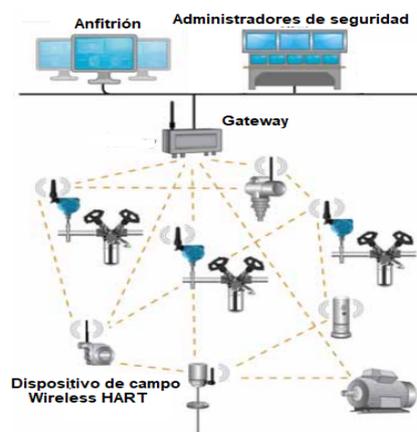
CARACTERÍSTICAS CLAVE DE WIRELESSHART

- **Red tipo malla:** aumenta de esta forma la fiabilidad mediante múltiples rutas de comunicación.
- **Adaptabilidad:** Compatible con dispositivos 4-20 mA/HART mediante adaptadores inalámbricos.
- **Autoorganización y recuperación:** en caso de fallos de nodos.
- **Escalabilidad:** adecuada para pequeñas y grandes plantas industriales.

EJEMPLO DE APLICACIÓN: WIRELESSHART EN UNA PLANTA QUÍMICA

En una planta de procesamiento químico, los sensores monitorean presión y temperatura de reactores: los sensores inalámbricos envían datos en tiempo real al sistema de control. La red en malla garantiza transmisión confiable, evitando interrupciones por interferencias. Sus adaptadores WirelessHART permiten actualizar sensores analógicos a una infraestructura inalámbrica moderna. Así se logra optimización de procesos, reduciendo costos operativos y mejorando la seguridad.

Figura 26. Red WirelessHART típica



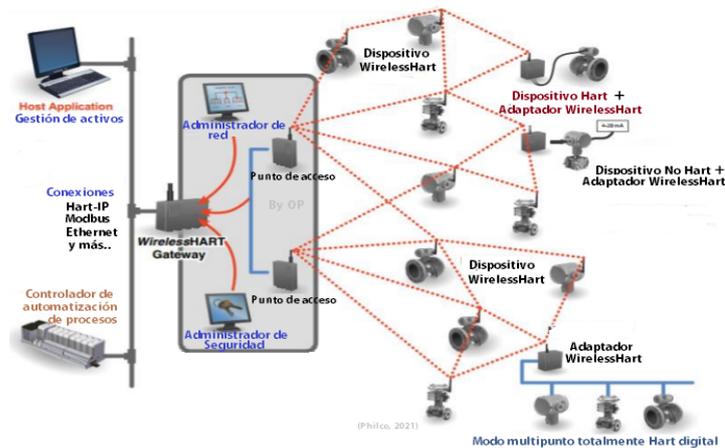
Fuente: FieldComm Group. WirelessHART: User Case Studies. 2019, p. 7)

Los dispositivos conectados de la figura 26 se detallan a continuación:

- Anfitrión: Estación de trabajo que interactúa con el proceso mediante el Gateway WirelessHART, recopilando datos de dispositivos conectados y utilizando protocolos como Profibus y HSE.
- Gateway WirelessHART: Elemento central que convierte datos entre el anfitrión y los dispositivos de campo. Integra el Administrador de Red, el Administrador de Seguridad y el Punto de Acceso, además de poder traducir entre distintos protocolos.
- Administrador de Seguridad: Aplicación dentro del Gateway que gestiona claves de cifrado y autoriza dispositivos a unirse a la red.

- Dispositivos de campo WirelessHART: Sensores que convierten datos analógicos en digitales y pueden retransmitir mensajes dentro de la red

Figura 27. Conexiones WirelessHART



Fuente: (FieldComm Group. 2017, p. 5)

- **Administrador de red;** es el "cerebro" de la red WirelessHART y tiene la responsabilidad de gestionar todo lo relacionado con la red inalámbrica como, por ejemplo, la formación de la red, reconfiguración, configuración de ruta de red, gestionar la distribución de tiempos de acceso, programación de la comunicación de cada dispositivo en la red, etc. Solamente una herramienta de Network Manager puede estar activa en una red WirelessHART, con la posibilidad de tener otro de backup por si el que está activo falla.
- **Adaptador:** unen dispositivos HART cableados a la red WirelessHART en red malla.
- **Terminal:** se utiliza para unir un nuevo instrumento de medición o dispositivo a una red WirelessHART existente. Tiene una conexión con la puerta de enlace y, después, a un instrumento que puede ser utilizado para el diagnóstico.

Aquí los dispositivos de campo están conectados directamente al proceso de una planta industrial en conjunto con los actuadores. En este tipo de red, se utiliza el protocolo de malla sincronizada en tiempo (TSMP, Time Synchronized Mesh Protocol) que fue desarrollado por Dust Networks para control de acceso

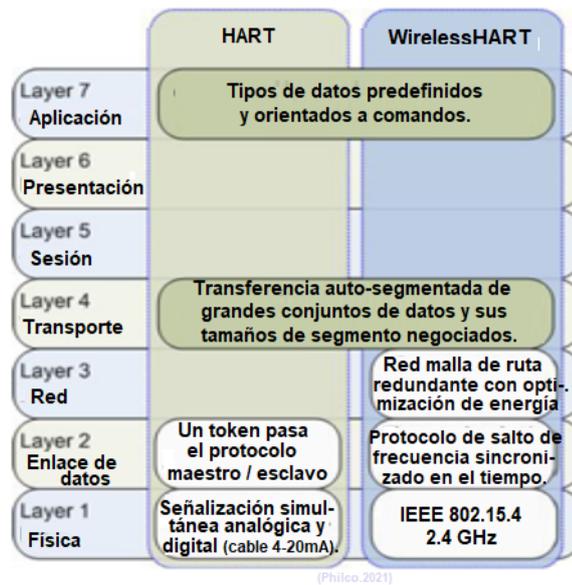
a medios y funciones de capa de red. TSMP utiliza TDMA para el acceso de canal y permite el salto de canal y la lista negra de canales en la capa de red. El salto de canal es una técnica en la que la transferencia de datos sucede a diferentes frecuencias en diferentes períodos de tiempo. También admite el enrutamiento redundante con el fin de mejorar la fiabilidad. Por lo tanto, WirelessHART se considera robusto, eficiente en cuanto a la energía y confiable (Noor-A, Firyaguna, Sherazi, Kushch, & Vijayan, 2023).

El Network Manager (administrador de red) de WirelessHART es responsable de planificar las rutas, asignar slots de tiempo (TDMA) y frecuencias de salto (*Frequency Hopping*) para garantizar la integridad de la comunicación (IEC 68512, 2016).

ARQUITECTURA OSI EN WIRELESSHART

La pila de protocolo de WirelessHART comprende cinco capas: la capa física (PHY) que se basa en el estándar IEEE 802.15.4, la capa de enlace (incluyendo MAC), la capa de red, la capa de transporte, y la capa de aplicación. Véase a continuación la pila de protocolos de HART y WirelessHART. (FieldComm Group, 2017)

Figura 28. Pila de protocolo HART y WirelessHART



Fuente. (Núñez. 2016, p. 2)

WirelessHART (IEEE 802.15.4), opera en la banda ISM de 2.4 GHz con 15 canales y una velocidad de transmisión de hasta 250 Kbps. Su capa física utiliza la técnica de modulación en espectro ensanchado por secuencia directa (DSSS) empleado en comunicaciones inalámbricas para reducir la interferencia y mejorar la resistencia a la multi-trayectoria de la señal en la transmisión y el espectro ensanchado por salto de frecuencia (FHSS) para minimizar interferencias, garantizando comunicación robusta.

La capa de enlace de datos emplea TDMA, sincronizando todos los dispositivos en intervalos de tiempo predefinidos, lo que optimiza la comunicación y el consumo energético. Además, incorpora *Clear Channel Assessment (CCA)* y *Blacklisting* para evitar conflictos con otros sistemas inalámbricos.

Las capas de red y transporte soportan una topología de malla, permitiendo el reenvío de paquetes entre dispositivos. Existen dos mecanismos de enrutamiento: *graph routing*, que asigna rutas redundantes para evitar fallos, y *source routing*, utilizado para diagnóstico de red.

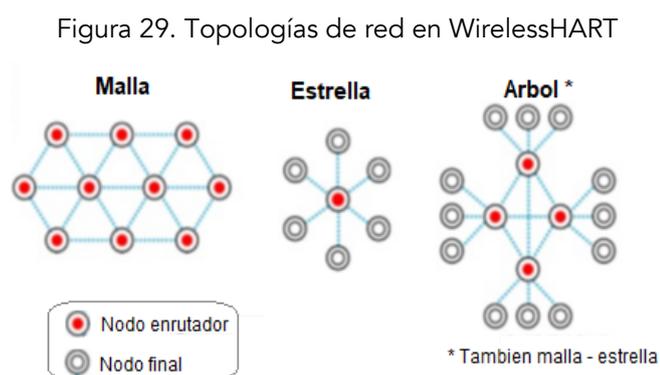
La capa de aplicación mantiene la estructura de comandos del estándar HART cableado, facilitando la comunicación entre dispositivos. En cuanto a costos,

los dispositivos WirelessHART son más caros que los cableados debido a su electrónica de baja potencia, protección contra explosiones y componentes de alta frecuencia

TOPOLOGÍA DE RED EN WIRELESSHART

Normalmente los dispositivos WirelessHART tienen una topología de red en malla, donde todos los dispositivos deben tener la capacidad de enrutamiento, es decir, pueden ser tratados por igual en términos de capacidad de red, instalación, formación y expansión, lo que amplía el alcance de la red y proporciona rutas de comunicación redundantes para aumentar la fiabilidad. Esto proporciona rutas redundantes que permite que los mensajes sean encaminados evitando obstáculos físicos, enlaces rotos e interferencias. Sin embargo, en WirelessHART existen otras configuraciones que no son red en malla.

También se puede conectar en topologías de árbol o en estrella, tal como aparece en la figura 29, aunque no son recomendadas ya que en entorno por datos críticos resulta confiable por la capacidad del enrutamiento en red malla.



Fuente: (Núñez. 2016, p. 3)

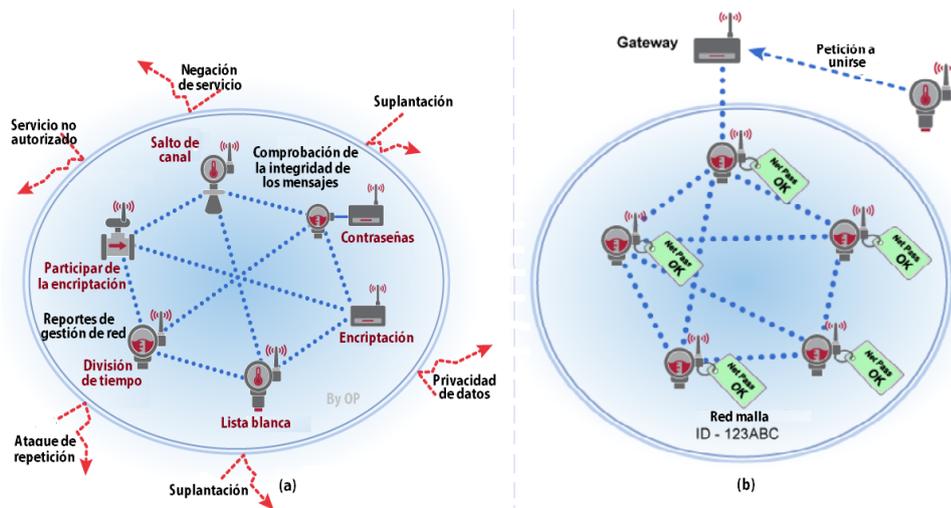
SEGURIDAD EN WIRELESSHART

WirelessHART implementa medidas de seguridad avanzadas para garantizar la integridad y confidencialidad de la comunicación en redes industriales. Sus principales características incluyen:

- **Cifrado AES-128:** Utiliza el estándar de encriptación avanzada basado en FIPS-197, asegurando protección contra accesos no autorizados mediante claves de red, sesión e integridad.
- **Protección contra ataques:** Bloquea amenazas como man-in-the-middle (interceptación de datos) y sink-hole (dispositivos maliciosos que redirigen el tráfico de la red).
- **Autenticación y encriptación de mensajes:** Emplea seguridad de salto simple en la capa de enlace de datos y end-to-end en la capa de red para evitar alteraciones en la comunicación.
- **Cipher Block Chaining Message Authentication Code (CCM):** Método que refuerza la seguridad de los mensajes combinando AES-128 con autenticación para la protección de datos.
- **Gestión de claves y restricciones:** La seguridad es obligatoria en WirelessHART y no puede ser desactivada, lo que garantiza una red confiable ante posibles ataques.

Estas medidas hacen de WirelessHART una solución robusta para la seguridad en redes de automatización industrial.

Figura 30 Seguridad en WirelessHART



Fuente: (FieldComm Group. WirelessHART Security. 2021, p. 1)

WirelessHART implementa controles de acceso para proteger la red contra amenazas internas y externas. Los ataques pueden comprometer dispositivos insertando troyanos, simulando redes falsas para obtener datos o interrumpiendo el servicio mediante técnicas como la denegación de servicio (DoS), que interfieren con las comunicaciones inalámbricas.

La seguridad de la red depende de claves cifradas:

- **Clave de acceso a la red:** Necesaria para que nuevos dispositivos se unan.
- **Clave de sesión:** Autentica la comunicación extremo a extremo entre dispositivos.
- **Clave de red:** Autentica mensajes en la capa de enlace de datos mediante un salto (one hop).
- **Administrador de Seguridad** gestiona las claves y las distribuye a los dispositivos a través del Administrador de Red, asegurando una infraestructura protegida mediante autenticación, autorización y detección de ataques.

HART IP

HART-IP es una extensión del protocolo HART que integra direccionamiento IP para facilitar la comunicación en redes industriales mediante Ethernet.

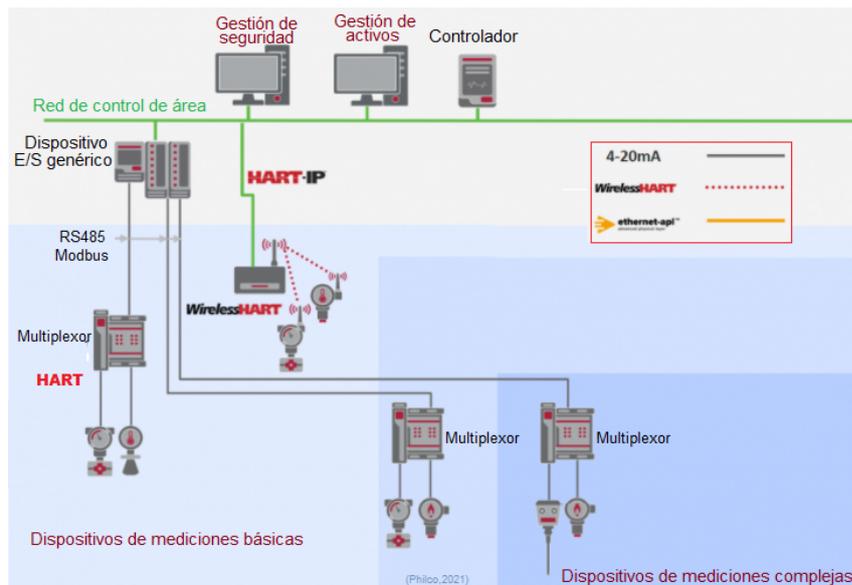
Desarrollado por FieldComm Group en 2012, permite una comunicación bidireccional eficiente entre dispositivos de campo inteligentes y sistemas anfitriones. (FieldComm Group, 2025).

Aunque HART-IP no define una capa física inalámbrica nativa, puede integrarse con tecnologías inalámbricas a nivel de red IP mediante infraestructura intermedia. Se conectará a un gateway HART-IP (con puerto Ethernet) a un punto de acceso Wi-Fi industrial. El dispositivo cliente (ej. tablet, HMI, SCADA, servidor) se comunica con el gateway a través de Wi-Fi utilizando protocolo HART-IP sobre TCP/IP.

CARACTERÍSTICAS PRINCIPALES:

- Interfaz basada en IP: Sustituye el esquema de direccionamiento HART tradicional por direcciones IP, simplificando la gestión de dispositivos.
- Encapsulación de datos: Multiplexores y gateways WirelessHART convierten datos HART 4-20 mA en paquetes IP para transmisión de alta velocidad.
- Compatibilidad con Ethernet APL: La capa física avanzada (Advanced Physical Layer) permite conectividad en redes de dos cables, mejorando la integración de HART-IP en sistemas de campo.

Figura 31. Comunicación de HART-IP y Ethernet-APL



Fuente: (FieldComm Group. Transitioning to HART-IP. 2020, p. 1)

ISA 100 WIRELESS,

ISA100.11a, también conocido como ISA 100 Wireless, es un estándar de comunicación inalámbrica para automatización industrial basado en IEEE 802.15.4, diseñado para aplicaciones como monitoreo, alarmas y supervisión, con tiempos de respuesta no críticos (~100 ms).

CARACTERÍSTICAS PRINCIPALES:

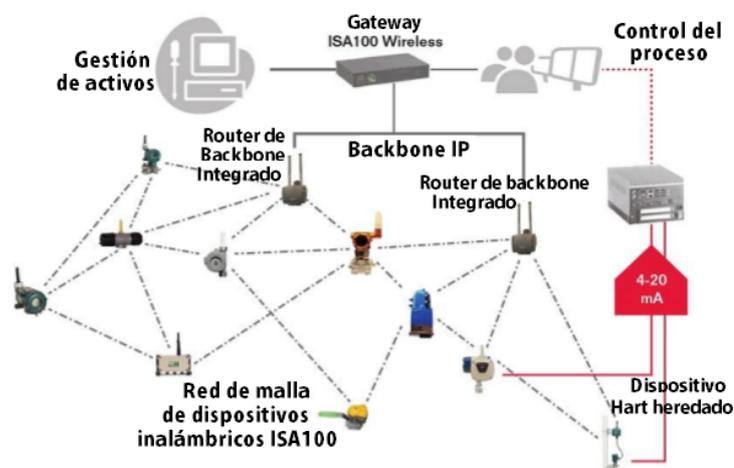
- Compatibilidad con IPv6 y 6LoWPAN, facilitando la conectividad a Internet en entornos industriales.
- Métodos de salto de canal (lento, rápido y mixto) para mejorar la eficiencia de transmisión.
- Capa de enlace de datos híbrida, combinando TDMA y CSMA para optimizar el acceso a la red.
- Topologías de red estrella y malla, con integración de protocolos heredados como HART cableado y coexistencia con WirelessHART.
- Certificación ISA100 Wireless Compliant, garantizando interoperabilidad entre dispositivos industriales.

El estándar busca adaptarse a la Industria 4.0, ofreciendo baja latencia y coexistencia con redes inalámbricas industriales y dispositivos como smartphones. Además, la ISA y la Hart Communication Foundation (HCF) exploran la convergencia de WirelessHART e ISA100.11a para un futuro estándar global.

A través del direccionamiento IPv6 se facilita la segmentación de dispositivos en subredes, similar a VLANs, mejorando la gestión del tráfico y la seguridad.. Por consiguiente, existen mejoras de ciberseguridad en el entorno industrial, Además, se han desarrollado soluciones para reducción de costos operativos y optimización de procesos, como la implementación de ISA100 Wireless en aplicaciones de monitoreo de grandes instalaciones industriales. En la industria, las fábricas pueden recopilar información automática sobre el estado de las máquinas, la producción y el mantenimiento. Por ejemplo, si una máquina detecta que está a punto de fallar, puede enviar una alerta para que los técnicos la revisen antes de que ocurra un problema grave. Esto ayuda a mejorar la eficiencia y a reducir costos operativos. (CESA, 2025)

Estas mejoras refuerzan su papel en la Industria 5.0, asegurando una comunicación robusta y adaptable a futuras necesidades

Figura 32 Flexibilidad de la red ISA100.11a



Fuente: (ISA 100 ISA100. Wireless Applications, Technology, and Systems, 2014, p- 19)

Los dos dispositivos HART heredados, conectados a un controlador, envía simultáneamente datos digitales HART a la red inalámbrica ISA100 a través de adaptadores respectivos. La ISA100 Wireless define dos clases de dispositivos: dispositivos de campo y dispositivos backbone, además de dos administradores dedicados:

1. Administrador del sistema: Gestiona los recursos de la red y la comunicación.
2. Administrador de seguridad: Implementa medidas de seguridad basadas en la política de la red.

Los dispositivos de campo pueden ser inalámbricos con o sin capacidad de enrutamiento. Un ejemplo sin enrutamiento sería un teléfono inteligente, que se asocia con un dispositivo de red para monitoreo o transmisión de datos. En contraste, los dispositivos *backbone* tienen alto suministro de energía, por lo que operan de manera constante.

ISA100 Wireless emplea una topología de malla TDMA, lo que garantiza mayor confiabilidad y gestión eficiente de interferencias, ideal para Industria 4.0. Aunque se admite la topología en estrella, la malla es preferible por su robustez y capacidad de adaptación ante fallas mediante enrutamiento dinámico y sincronización temporal.

SEGURIDAD EN CONTROL CRÍTICO

Los desafíos sobre la seguridad en la red desembocan en reaccionar ante posibles fallas de los nodos sensores y, por lo tanto, se garantizará la confiabilidad de la operación. Ejemplos de ataques y amenazas en las redes inalámbricas son la manipulación de nodos, el control de nodos, la denegación de servicio y las interferencias de radio. Un objetivo básico del diseño es implementar una administración de seguridad eficaz, teniendo en cuenta las débiles capacidades del hardware restringido que se utiliza habitualmente y la

eficiencia energética requerida. La administración de la seguridad es un pilar fundamental de las principales normas industriales y, en muchos casos, se maneja con la misma importancia en comparación con otros requisitos (Raptis, Passarella, & Conti, 2020). Las opciones de seguridad suelen oscilar entre:

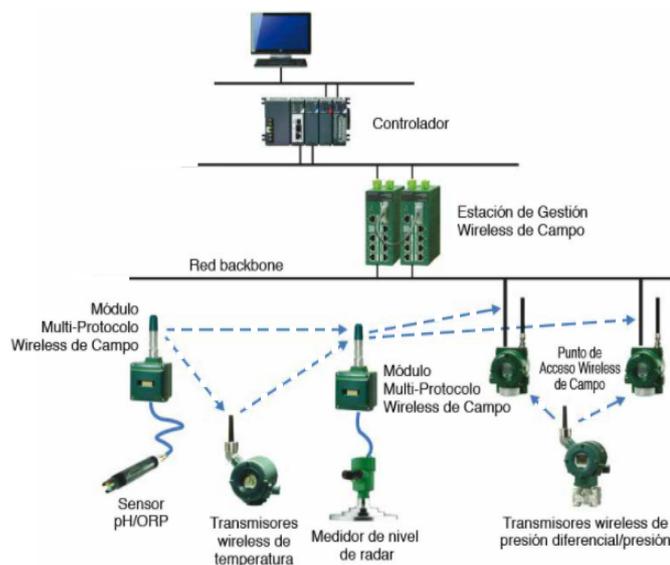
- Redes no seguras (que no se recomiendan).
- Redes protegidas simétricamente
- Redes protegidas asimétricamente.

La administración de seguridad de ISA100.11a se implementa en las capas de enlace y transporte. En particular, los datos se autentican en la capa de enlace, mientras que la carga útil de los datos se cifra mediante el algoritmo estándar de cifrado avanzado. ISA100.11a también puede proteger y asegurar el transporte y el encabezado de carga útil, en la capa de transporte.

El control en tiempo real en redes industriales inalámbricas permite gestionar múltiples lazos de control, mejorando la eficiencia y reduciendo costos. La confiabilidad de estas redes depende de una comunicación estable y de baja latencia, fundamental para evitar fallas operativas y accidentes (Innova Tech, 2025).

En entornos críticos como refinerías de petróleo, es necesario monitorear constantemente variables como niveles de líquidos para prevenir derrames. Sin embargo, factores como ancho de banda limitado, interferencias electromagnéticas y obstáculos físicos pueden afectar la comunicación inalámbrica.

Figura 33. Red ISA 100.11a



Fuente: (Editorial Control. 2018, p. 1)

En la figura 33 se muestra que es importante instalar un módulo de gestión multi-protocolo de campo inalámbrico, ya que admite convertir instrumentos y actuadores de válvula inteligentes compatibles con HART cableado ya existentes en dispositivos Wireless o inalámbricos, reduciendo así costos de instalación de cableado y mantenimiento. También amplía la gama de tipos de sensores inalámbricos disponibles y simplifica la instalación de dispositivos. Con la adopción de ISA100.11.a las funcionalidades de monitoreo y control de procesos se han vuelto capaces de lograr confiabilidad y comunicación inalámbrica en tiempo real a través de diversidad espacial y de espectro.

ESTÁNDAR WIA-PA PARA AUTOMATIZACIÓN DE PROCESOS

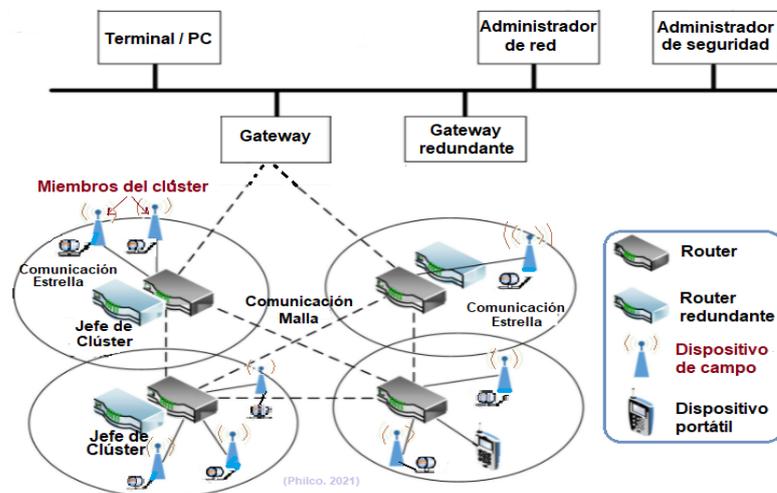
Es un estándar industrial chino propuesto por la Chinese Industrial Wireless Alliance. WIA-PA (Wireless Networks for Industrial Automation - Process Automation) es una solución de comunicación industrial aprobada como IEC 62601 en 2011, diseñada para ofrecer alta fiabilidad, eficiencia energética y

capacidad de auto-reparación en redes inalámbricas de automatización de procesos.

CARACTERÍSTICAS PRINCIPALES:

- Compatibilidad con IEEE 802.15.4, utilizando una combinación de CSMA, TDMA y FDMA para optimizar el acceso a la red.
- Soporte para IPv6, facilitando la integración con redes industriales modernas.
- Soporte para 16 canales en la banda de 2.4 GHz, con mecanismos avanzados de salto de frecuencia para minimizar interferencias.
- Interoperabilidad con protocolos heredados, incluyendo HART cableado, Profibus, Modbus y WirelessHART.
- Topología híbrida: emplea malla para la comunicación entre enrutadores y estrella para la conexión con dispositivos de campo.

Figura 34. Topología malla y estrella de red WIA-PA



Fuente. Autores

Según la figura 34, cada enrutador funciona de manera similar, como jefe o cabezal de un clúster (CH) que proporciona una mejor comunicación. Ya que este mecanismo de jefe de clúster (CH) selecciona un nodo con alta energía residual y ubicación óptima para mejorar la comunicación en la red.

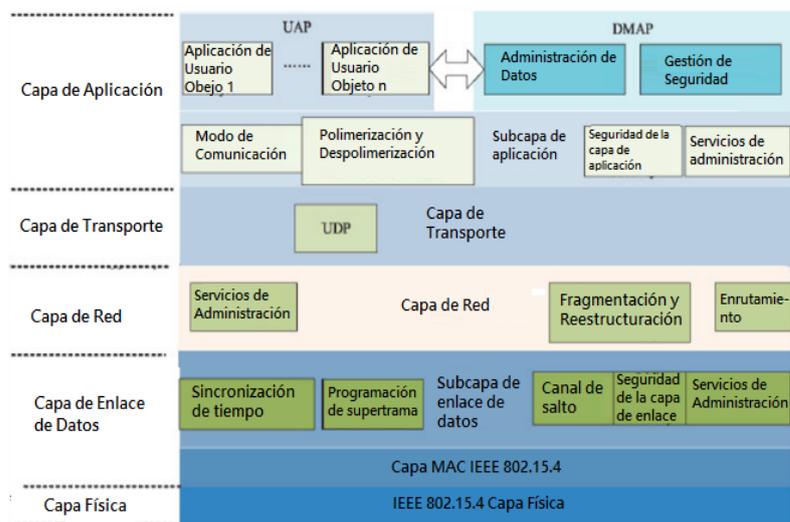
CARACTERÍSTICAS PRINCIPALES:

- Topología de malla en estrella o malla de clúster, favoreciendo interacciones eficientes.
- Puertas de enlace encargadas de la administración y seguridad de la red.
- Reglas de seguridad: configuración de claves, verificación de dispositivos y análisis de mensajes transmitidos.
- Reglas de administración: supervisión de dispositivos, gestión de programación y asignación de canales de comunicación.

MODELO OSI EN WIA-PA

Se muestra el modelo OSI del estándar WIA-PA con su pila de protocolos organizada.

Figura 35. Arquitectura del protocolo WIA-PA



Fuente: (Das Neves, Künzel, Müller, & Pereira. 2018. P. 176)

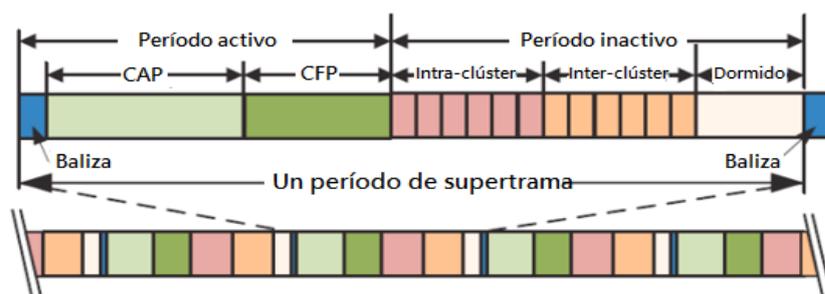
La capa física usa radiofrecuencia estandarizada por IEEE 802.15.4 y hay 14 canales disponibles. La capa de enlace también se basa en IEEE 802.15.4 pero tiene algunas características adicionales, como el salto de frecuencia adaptivo (AFH, Adaptive Frequency Hopping), que busca minimizar la interferencia externa en el sistema. La capa de red tiene la responsabilidad de direccionamiento, enrutamiento y administración de paquetes. La capa de

transporte utiliza el (UDP, User Datagram Protocol) o Protocolo de datagramas de usuario como base de trabajo. Además, la capa de aplicación sigue la orientación de mapeo de dispositivos y servicios, con el propósito de estandarizar los métodos. Finalmente, la capa de aplicación tiene la responsabilidad de hacer que el protocolo sea compatible con las tecnologías heredadas WIA-PA. (Neves, Künzel, Müller, & Pereira, 2018).

Para asegurar la fiabilidad de la comunicación entre los distintos dispositivos de la red, así como la sincronización entre ellos, el protocolo WIA-PA utiliza una estructura de super trama compatible con el estándar IEEE 802.15.4. A través de las tramas de baliza (comprende los datos de red requeridos por una estación antes de transmitir una trama). Las tramas de baliza se utilizan para sincronizar dispositivos y anunciar la existencia de dispositivos en una conexión WLAN. Por consiguiente, dichas tramas de baliza son enviadas entre el mensaje por los dispositivos de puerta de enlace periódicamente.

En la figura 36 se muestra la estructura de super trama de WIA-PA.

Figura 36. Estructura de super trama de WIA-PA



Fuente. (Wang & Jiang. 2016, p. 16)

Los dispositivos de campo monitorean los canales disponibles bajo el período de acceso a contención (CAP, Contention Access Period), que se utiliza para verificar y administrar todos los dispositivos. En cambio, el período libre de contención (CFP, Contention-Free Period) se utiliza para la comunicación entre dispositivos de campo móviles. El período inactivo se usa para la comunicación entre sub-redes y para la comunicación dentro de cada subred, y puede usarse

como un período inactivo del propio protocolo. La duración total de la super trama se define como 32 intervalos de tiempo de la base de tiempo de comunicación de la red (Wang & Jiang, 2016).

Utilizando la topología híbrida y la super trama, el administrador del sistema puede realizar una gestión unificada de los recursos de comunicación de toda la red. Es decir, los recursos serán asignados a cada dispositivo según las demandas de la topología de la red y la comunicación del dispositivo. A partir de entonces, el dispositivo de red se comunicaría a intervalos de tiempo y canales específicos en la superestructura.

En la tabla 3 se muestran características disponibles en los estándares WirelessHART e ISA100.11a, y comparándolos con el WIA-PA.

Tabla 3. Comparación de características técnicas de estándares IWSN

Capa	Parámetro	Wireless HART	ISA 100.11a	WIA-PA
Física	Número de canales	15 (Banda de 2,4 GHz)	16 (Banda de 2,4 GHz)	16 (Banda de 2,4 GHz)
	Balizamiento	No	No	Si
	Estructura de super trama	Colección de intervalos de tiempo	Colección de intervalos de tiempo	Super trama de IEEE 802.15.4
Enlace de datos / MAC	Salto de frecuencia	Salto ranurado	Salto ranurado/Lentado/Híbrido	Salto adaptable/Ranurado. Conmutador de frecuencia adaptable.
	Duración del intervalo de tiempo	10 ms	Flexibles y Configurables	Configurables
	Estándar de tiempo	UTC	TAI	UTC opcional
Enlace de datos / Red	Enrutamiento	Enrutamiento de super trama/fuente y gráfico	Enrutamiento de super trama/Enrutamiento Gráfico y de origen.	Enrutamiento Estático
Red	Topología de la red	Estrella, Malla	Estrella, Malla	Malla + Estrella
Aplicación	Capa de APP nativa	HART	ISA 100.11a	Profibus / FF / HART

Fuente: (Wang & Jiang. Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards. 2016, p. 14)

DISPOSITIVOS DE RED WIA-PA

Las soluciones de infraestructura para la industria inteligente se encuentran en medio de un período de expansión de nuevas soluciones de red, desde el nivel de dispositivo hasta la nube, que permitirán nuevos niveles de innovación digital con el objetivo de transformar la fabricación global. Por consiguiente, las redes industriales y de TI deben estar abiertas para canalizaciones de datos en toda la infraestructura de la empresa, incluidos los entornos de TI y OT y, por supuesto, la infraestructura de la nube. Sin embargo, a medida que se avanza hacia una automatización industrial más basada en datos, los equipos y dispositivos exigen cada vez más soluciones que puedan proporcionar los niveles más altos de energía necesarios para admitir más datos.

Existen algunos fabricantes que desarrollan dispositivos como *routers*, *gateways* y repetidores bajo el estándar WIA-PA. La mayoría de los fabricantes son de China sin embargo existen fabricantes de otros países como Emerson, Yokogawa, que fabrican dispositivos con este estándar.

Figura 37. Dispositivos de red industrial con estándar WIA-PA



Fuente: (Pond Technical. Wireless Field Network Instrument & Valve Products. 2019, p. 1)
Incluso si los dispositivos cumplen con el estándar, aún puede ser necesario adaptar los dispositivos de campo existentes del antiguo sistema de bus de campo o de otro estándar a una versión WIA-PA. De esta forma, es posible utilizar un adaptador inalámbrico para transformar la señal del sensor

incompatible en una señal compatible con el protocolo. Este adaptador tiene una radio estandarizada que consta de antena, circuito de filtro, circuito de acondicionamiento de señal, transceptor, microcontrolador e interfaz, circuitos con protocolos como el transceptor asíncrono universal (UART Universal Asynchronous Receiver/Transmitter) e interface de comunicación serial (SPI Serial Peripheral Interface). (Sharma, 2023)

El microcontrolador del adaptador realiza toda la gestión necesaria creando celdas de protocolo para la comunicación por radiofrecuencia, realizando toda la interfaz de comunicación entre la entrada de datos del dispositivo de campo y el transceptor y supervisando el acondicionador de señal y el adaptador.

ESTÁNDAR WIA-FA PARA AUTOMATIZACIÓN DE FÁBRICAS

El estándar WIA-FA (Wireless Industrial Automation - Factory Automation) define la arquitectura y el protocolo de comunicación para redes inalámbricas en la automatización de fábricas. (Neves, Künzel, Müller, & Pereira, 2018).

Se basa en la capa física IEEE 802.11-2012 (Wi-Fi) y está diseñado para la medición, seguimiento y control de procesos industriales de alta velocidad.

CARACTERÍSTICAS PRINCIPALES

- Topología de red: Se estructura en una red de dispositivos de acceso conectados a dispositivos de campo en una configuración de estrella, con redundancia opcional.
- Protocolo de comunicación: Utiliza TDMA y FDMA para evitar colisiones y garantizar transmisión en tiempo real.
- Gestión de red: Un único administrador de red asigna direcciones, mantiene la topología y supervisa el estado de los dispositivos y canales.

Por último, la capa de aplicación está compuesta por una subcapa (ASL, Application SubLayer) y el proceso de aplicación de usuario (UAP), donde la ASL proporciona servicios de comunicación para UAP. Una UAP es una unidad utilizada para implementar aplicaciones industriales distribuidas. Cada UAP se compone de uno o más objetos de aplicación de usuario (UAO) que se definen de acuerdo con diferentes funciones. En la práctica, UAO recopila y procesa los datos de aplicación (velocidad, par y aceleración) de los procesos industriales.

Los UAOs pueden estar ubicados en el mismo dispositivo o en diferentes dispositivos, donde diferentes UAOs pueden interactuar entre sí a través del ASI. Por ejemplo, un sistema de monitoreo de motores industriales en una planta de producción. En este caso, la capa de aplicación de WIA-FA se estructura de la siguiente manera:

1. Application SubLayer (ASL): Actúa como intermediario entre los dispositivos de campo y el proceso de aplicación de usuario (UAP), asegurando la comunicación eficiente.
2. Proceso de aplicación de usuario (UAP): Implementa la lógica de monitoreo y control de los motores industriales.
3. Objetos de aplicación de usuario (UAO): Cada motor tiene un UAO que recopila y procesa datos clave como velocidad, par y aceleración.

Funcionamiento

- Cada UAO en los motores recopila datos en tiempo real.
- Los UAOs pueden estar en el mismo dispositivo o en diferentes dispositivos, comunicándose entre sí a través de la ASL.
- La ASL transmite los datos al UAP, que analiza la información y ajusta parámetros de operación si es necesario.

- Si un motor detecta una anomalía en su velocidad, su UAO puede enviar una alerta a otro UAO en un dispositivo diferente, permitiendo ajustes automáticos en la producción

Véase la comparación de la arquitectura OSI y WIA-FA

Tabla 4. Comparativa de arquitectura OSI y WIA.FA

OSI	Función	WIA-FA
Aplicación	Proporciona al usuario una aplicación compatible con la red.	Servicios de aplicaciones distribuidas
Presentación	Convierte entre los datos de la capa de aplicación y los formatos de datos de la capa inferior	
Sesión	Servicios de gestión de conexiones	
Transporte	Proporciona transferencia de mensajes transparente independiente de la red	
Red	Resolución de direcciones de red, enrutamiento de paquetes de extremo a extremo	Comunicación basada en acceso de múltiples dispositivos, DLL, TDMA, FDMA
Enlace de red	Establece paquetes de datos, estructura de tramas, detección de errores, arbitraje de bus.	
Física	Transmite flujo de bits sin formato. Conexión mecánica/eléctrica.	Física IEEE 802.11-2012

Nota: Las flechas indican que la funcionalidad de esta capa, cuando esté presente, puede incluirse en la capa de protocolo más cercana en la dirección de la flecha. Por lo tanto, la funcionalidad de red y transporte puede incluirse en la capa de enlace de datos o en la capa de aplicación, no en la capa de enlace de datos.

PRIORIDAD DE DATOS EN WIA-FA

WIA-FA admite cinco tipos de prioridad de datos transferidos entre el dispositivo de puerta de enlace y los dispositivos de campo. Así el orden descendente de prioridad se da como datos urgentes (RT0, Real Time 0), luego RT 1, RT 2, RT3 y un NRT (No en tiempo real) o de prioridad baja. Se detallan estos niveles de prioridad a continuación:

- Comandos urgentes periódicos, como comandos de arranque y parada con prioridad de datos RT0. Por ejemplo, el comando de la computadora central para desactivar el actuador, la alarma urgente de notificación de falla o error y los servicios críticos de administración de red de la computadora principal.
- Datos de entrada periódicos (Valores de medición del sensor, estado del interruptor, valores de retroalimentación del actuador) y datos de salida periódicos (puntos de ajuste del actuador, valores establecidos del interruptor) con prioridad de datos RT1.
- Informes de alarma periódicos con prioridad de datos RT2. Por ejemplo, informes de alarmas aperiódicas, como las alarmas no urgentes provocadas por eventos.
- Datos de gestión periódica (prioridad RT3) para monitorizar datos y mensajes de estado de la red. Por ejemplo, los datos de gestión periódicos para las condiciones del dispositivo y el estado del canal, como los datos de monitoreo y los mensajes de condición de la red.
- NRT, con la prioridad más baja, se refiere a solicitudes y respuestas no periódicas para accesos de lectura y escritura de atributos y reconocimientos de alarmas. La transmisión NRT no debe interferir con ninguna transmisión en tiempo real.

OTROS ESTANDARES

Además de ISA 100, WirelessHART, WIA-PA y WIA-FA, existen otros estándares relevantes en redes industriales que están impulsando la evolución hacia Industria 5.0. Uno de los más destacados es LoRaWAN, un estándar de comunicación de baja potencia y largo alcance que está siendo adoptado en aplicaciones industriales.

- **LoRaWAN:** Se ha convertido en un estándar importante para la conectividad en IIoT (Internet Industrial de las Cosas), permitiendo la comunicación eficiente entre dispositivos en entornos industriales.
- **OPC UA:** Facilita la interoperabilidad entre sistemas industriales, permitiendo la integración de datos en tiempo real.
- **5G Industrial:** La implementación de redes 5G en la industria mejora la conectividad y la baja latencia en procesos de automatización avanzada.
- **TSN (Time-Sensitive Networking):** Proporciona comunicación determinista en redes Ethernet industriales, asegurando sincronización precisa y transmisión confiable.

“La tecnología inalámbrica es un factor clave para la automatización industrial. Con mayor fiabilidad y velocidad, la conectividad inalámbrica ofrece más posibilidades para conectar y automatizar diversas aplicaciones”

Andrea Orioli

Director de Gestión de Productos, IIoT Wireless,

Cisco Systems, 2025

CAPÍTULO III:

LOS DATOS EN LA FÁBRICA DIGITAL

A medida que aumenta la automatización en las fábricas para mejorar la productividad, la calidad, la seguridad y reducir costos, las tecnologías de comunicación inalámbricas son esenciales. Las redes de área local (LAN) inalámbricas industriales basadas en Wi-Fi, 5G industrial o ambas abren un amplio abanico de posibilidades para la industria. Al respecto, la tecnología inalámbrica presenta requisitos estrictos.

Cualquier fallo en la red operativa podría provocar la parada de la línea de producción, lo que se traduce en pérdida de ingresos y desperdicio de materiales. Los vehículos autónomos, las herramientas móviles y otras aplicaciones críticas requieren conectividad inalámbrica ininterrumpida para una respuesta en tiempo real. Los retrasos o la interrupción de las comunicaciones con estos activos afectan la seguridad de las operaciones y del personal. (FutuRed, 2024).

Desde una perspectiva tecnológica, se han producido avances significativos que están transformando la fabricación. Algunos ejemplos incluyen la fusión de sensores, gracias a un mayor despliegue de sensores en activos y equipos de fabricación, para generar conjuntos de datos completos que pueden utilizarse para optimizar las máquinas y aumentar la efectividad del equipo operativo. La automatización definida por software se está implementando para aumentar los niveles de productividad, flexibilidad y escalabilidad en la fabricación, lo que permite una configuración y validación más rápidas.

Últimamente, la inteligencia artificial (IA) se está dirigiendo hacia el "borde" (cerca del sensor o actuador), donde se generan los datos. La IA de borde (*Edge Computing*) transformará los datos de fabricación en información valiosa mediante la toma de decisiones basada en datos. Cuando los datos generados

se analizan de forma adecuada, los tomadores de decisiones —ya sean operadores industriales o responsables de planta— pueden identificar oportunidades para mejorar la calidad del producto y optimizar los índices de producción. En escenarios donde es necesario reubicar maquinaria o modificar la disposición de equipos, tradicionalmente se requeriría una nueva instalación de cableado. Sin embargo, con la implementación de redes 5G industriales, es posible reducir significativamente la dependencia del cableado físico, facilitando una mayor flexibilidad operativa y reduciendo tiempos de inactividad

El 5G ofrece mejor transferencia, baja latencia, mejor destino de los dispositivos, mayor número de dispositivos y mejor cobertura. Todos estos elementos permiten al personal de planta ser más creativo en el diseño y en la implementación del concepto de fábrica inteligente

Figura 38. Máquinas y equipos conectados



Fuente: (Industrial Ethernet Book, 2023)

A medida que el Wi-Fi mejora con las versiones 6/6E y 7 los fabricantes de dispositivos para la conexión inalámbrica (módulos como Gateway, switches, routers) siguen integrando procesamiento y Radio Frecuencia (RF) en los módulos y añadiendo certificaciones a diferentes formatos. Esto permite a los

desarrolladores añadir procesamiento de aplicaciones al módulo RF y reducir la complejidad del dispositivo final.

Los proveedores de dispositivos y puertas de enlace (*gateways*) siguen creando dispositivos con diferentes formatos para facilitar la integración de la tecnología inalámbrica industrial en diversos productos. Esto permite al cliente usar la misma puerta de enlace y añadir diferentes tecnologías inalámbricas según la aplicación.

Las soluciones más recientes son la conectividad de alta velocidad del borde a la nube para la transmisión de datos en tiempo real y una cobertura confiable para soluciones de inteligencia artificial y aprendizaje automático alojadas en la nube, Transferir datos desde la planta al departamento de TI para optimizar el negocio sigue siendo un buen caso de uso para la tecnología inalámbrica industrial. Los trabajadores conectados que utilizan teléfonos y tabletas inalámbricos industriales (compatibles con 5G) pueden acceder a aplicaciones móviles. Entre ellas se incluyen análisis, gemelos digitales, reparación de máquinas y aplicaciones de activos móviles (MES).

Las aplicaciones de activos móviles, en particular los vehículos de guiado automático (AGV) y los robots móviles autónomos (AMR), requieren movilidad y una entrega rápida y fiable. La tecnología inalámbrica industrial permite a los AMR y AGV coordinar y mapear mejor la planta.

La liberación de activos industriales fijos y de baja latencia aumenta la agilidad operativa y reduce el tiempo necesario para reequipar el taller. En el contexto industrial, la "liberación de activos fijos" hace referencia a la desvinculación de los equipos de producción de una infraestructura física rígida, como cableado fijo, estaciones estáticas o áreas delimitadas. Es decir, se liberan del anclaje físico para que operen de forma más dinámica, portátil o flexible. Se lo puede determinar de dos maneras:

1. **Antes (activo fijo):**

- Maquinaria conectada por cables a una red Ethernet industrial.
- Limitada a un solo punto en la planta.
- Difícil de mover o reconfigurar sin tiempo de inactividad.

2. **Después (activo liberado):**

- Equipos como robots móviles autónomos (AMR) o vehículos guiados automáticamente (AGV) usan Wi-Fi industrial o 5G privado.
- Pueden desplazarse por distintas áreas manteniendo conectividad y sincronización.
- Permite que la configuración del taller sea reconfigurable, ideal para producción flexible

CASO: TRANSMISIÓN DE DATOS INDUSTRIALES

Se plantea el caso de una industria automatizada en algún lugar del Ecuador y en el cual existen procesos con maquinas y robot manipuladores en una línea de montaje. La supervisión de l proceso engloba transmisión de datos, uso de una red privada virtual para enlazar una sucursal en otro país (Paraguay).

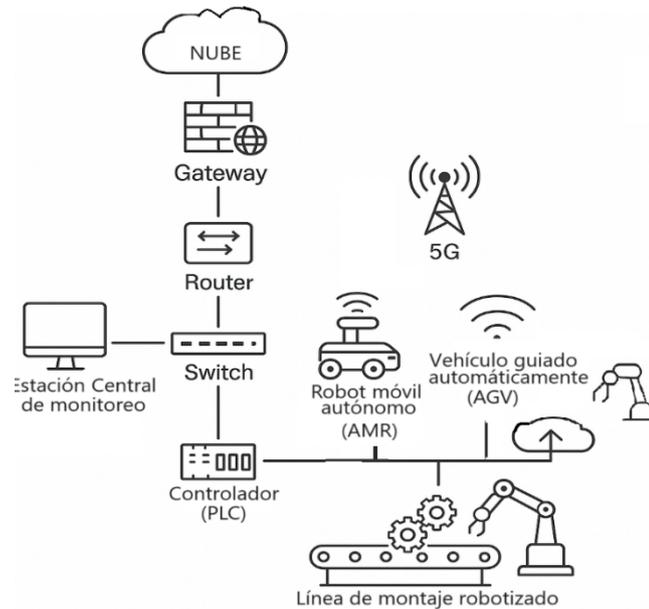
DETALLE DE CONEXIÓN DE UN ESQUEMA INDUSTRIAL

Se indica el equipamiento principal para una conexión inalámbrica de la planta automatizada en Ecuador.

- Router Industrial: Se conecta a la red externa y a la red local. Administra el tráfico, seguridad y direccionamiento.
- Firewall/Gateway: Protege la red interna, segmenta tráfico y gestiona acceso remoto.
- Switch Core: Administra todo el tráfico cableado: PLCs, SCADA, estaciones fijas.

- Controlador Wi-Fi: Distribuye señal Wi-Fi industrial (2.4 y 5 GHz robustos) a equipos portátiles.
- Antena 5G privada: Cubre áreas amplias con baja latencia y alta disponibilidad. Ideal para AGVs o AMRs con requerimientos críticos.

Figura 39. Esquema conectividad inalámbrica industrial



Fuente: Autores

COMPONENTES Y DATOS

Se detalla técnicamente el hardware necesario para el escenario de la figura 39.

1. PLC (Controlador Lógico Programable)

- Modelo: Siemens S7-1200
- Dirección IP asignada: 192.168.10.10/24
- Protocolo: Modbus TCP/IP o MQTT over TCP (para IoT)
- Interfaz: Ethernet RJ45

2. Switch Industrial

- Modelo: Cisco IE-3000 o Hirschmann RSP
- VLAN de producción: VLAN 10

- Puertos configurados en modo acceso (PLC) y trunk (hacia router)
- QoS habilitado para tráfico en tiempo real.

Figura 40. Configuración del switch

```
interface FastEthernet0/1
  switchport mode access
  switchport access vlan 10
!
interface FastEthernet0/24
  switchport mode trunk
```

3. Router Industrial

- Modelo: Cisco IR1101 o Teltonika RUTX11
- IP LAN: 192.168.10.1
- IP WAN: asignada por el proveedor o estática (200.100.50.10)
- NAT activado: Traducción de IP privada del PLC a IP pública
- Rutas estáticas o dinámicas configuradas para alcanzar la nube.

Figura 41. Configuración del Cisco IOS

```
interface GigabitEthernet0/0
  description LAN hacia planta
  ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
  description WAN hacia Internet
  ip address dhcp
!
ip nat inside source static 192.168.10.10 200.100.50.10
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
```

4. Firewall / Gateway

- Control de tráfico de salida (puerto 8883 si MQTT)
- VPN opcional para canal seguro
- IDS/IPS habilitado para seguridad de datos

5. Nube (Ejemplo: AWS IoT Core o Azure IoT Hub)

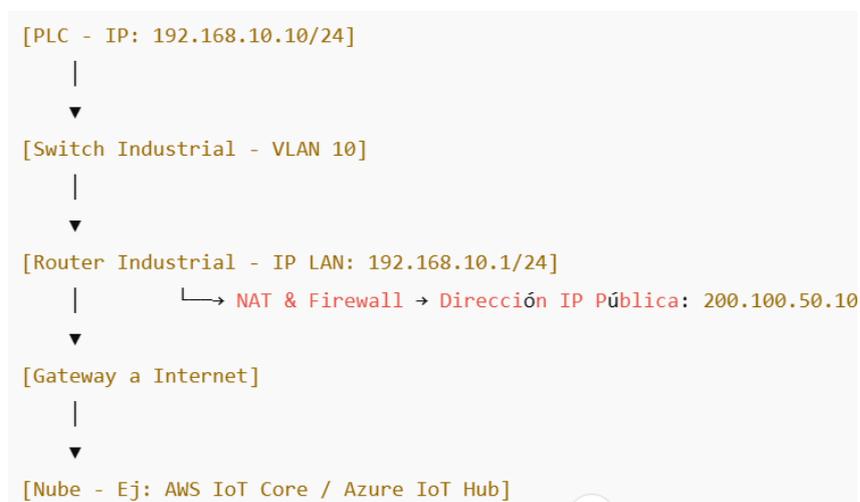
- El router o el PLC envía datos vía MQTT o HTTPS con certificados TLS

- Se requiere endpoint como:
`mqtt://a2v3dfmn.cloudiot.amazonaws.com:8883`
- Autenticación: certificado X.509 o token JWT

ENVÍO DE DATOS DESDE PLC HACIA LA NUBE

Se muestra la configuración para el Controlador Lógico Programable (PLC) hacia la nube.

Figura 42. Configuración del PLC



FLUJO DE DATOS

- El PLC recoge datos del proceso (temperatura, presión). Mediante un diccionario: `dato_sensor`
- Las claves ("sensor", "valor", "unidad") permiten acceder a los datos asociados.
- Este tipo de estructura es muy común para representar datos de sensores en aplicaciones de IoT o telemetría.
- Publica el mensaje:

Figura 43. Códigos para envío de datos de temperatura

```

# Diccionario que representa una lectura de sensor
dato_sensor = {
    "sensor": "temp",
    "valor": 75.5,
    "unidad": "C"
}

# Acceder a Los valores
print(f"Tipo de sensor: {dato_sensor['sensor']}")
print(f"Valor medido: {dato_sensor['valor']} {dato_sensor['unidad']}")

```

- Lo envía vía MQTT a través del router; {"sensor": "temp", "valor": 75.5, "unidad": "C"}
- El router realiza la NAT (Network Address Translation) que traduce la IP privada del dispositivo a una IP pública para que pueda comunicarse con servidores externos. Entonces se enruta el paquete a la IP pública de la nube.
- La nube lo recibe, analiza, guarda o visualiza en dashboards (Grafana, PowerBI, etc.).

Un dashboard es una herramienta de visualización de datos que muestra métricas clave (KPIs), gráficos, tablas y alertas en una sola pantalla. Su objetivo es ofrecer una visión rápida y accionable del estado de un sistema, proceso o negocio.

Tabla 5. Ejemplos de herramientas de dashboards

Herramienta	Características principales	Uso típico
Grafana	Código abierto, ideal para monitoreo en tiempo real, integración con bases de datos de series temporales como Prometheus, InfluxDB.	IoT, DevOps, monitoreo industrial
Power BI	Plataforma de Microsoft, potente para análisis de datos empresariales, integración con Excel, SQL Server, Azure.	Inteligencia de negocios, reportes financieros
Tableau	Visualizaciones interactivas, análisis avanzado, integración con múltiples fuentes de datos.	Análisis de datos corporativos
Kibana	Visualización de datos de Elasticsearch, ideal para logs y análisis de eventos.	Seguridad, monitoreo de sistemas

Fuente: Autores

Se debe indicar que el broker MQTT en la nube recibe el mensaje y lo reenvía a:

- Un servicio de almacenamiento (como InfluxDB, Firebase, DynamoDB, etc.).
- Un motor de análisis (como Node-RED, Python, o servicios de IA).
- Un dashboard en tiempo real

VISUALIZACIÓN EN TIEMPO REAL EN UN DISPOSITIVO MÓVIL

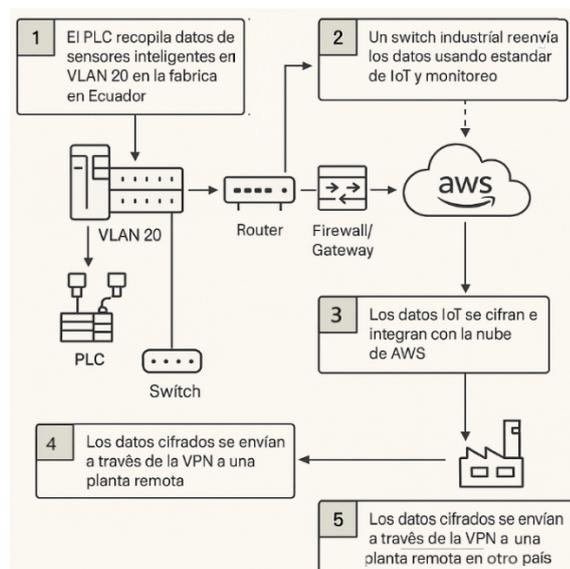
- El dashboard está alojado en la nube y es accesible desde cualquier navegador o app móvil.
- El usuario accede a una interfaz web responsiva o una aplicación móvil que se conecta al backend.

Se pueden usar tecnologías como:

- WebSocket o MQTT sobre WebSocket para actualizaciones en tiempo real.
- Notificaciones push si se detectan valores fuera de rango.
- Gráficas interactivas para visualizar tendencias.

Se muestra el esquema de conexiones de la planta automatizada en Ecuador.

Figura 44. Esquema de comunicación inalámbrica industrial



A continuación, se diseña una VLAN industrial para el caso anterior, la fábrica se localiza en Ecuador, y tiene conectado el equipamiento con sensores con el PLC, se enrutará datos a la nube (ej. AWS o Azure), y se enviará datos cifrados a una sucursal industrial en Paraguay mediante la VPN.

HARDWARE Y SOFTWARE PARA LA VLAN

Se detallan equipamiento y software para la VLAN, véase las tablas 5 y 6

Tabla 6. Hardware para la VLAN

Componente	Modelo recomendado
PLC industrial	Siemens S7-1200 o Allen-Bradley Micro820
Switch gestionable	Cisco IE-3000 / Hirschmann RS20
Router industrial VPN	Teltonika RUTX11 / Cisco IR1101
Servidor en la nube	AWS EC2 (MQTT Broker) / Azure IoT Hub
Gateway industrial	Moxa UC-8100 / Advantech Uno-2271G

Tabla 7. Software requerido

Software	Función
TIA Portal / Studio 5000	Configuración PLC
Cisco IOS / WinBox	Configuración de red y VLAN
Mosquitto MQTT / Node-RED	Publicación y suscripción de datos
OpenVPN / IPsec	VPN segura Ecuador ↔ Paraguay
Wireshark / Grafana	Análisis de red y visualización

Paso 1: Crear VLAN en switch industrial (en Ecuador)

Objetivo: Separar tráfico industrial en VLAN 20.

Configuración en Cisco Switch (modo CLI)

Figura 45, Configuración VLAN

```

enable
configure terminal
vlan 20
 name Industria
exit
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 20
!
interface FastEthernet0/24
 switchport mode trunk
 switchport trunk allowed vlan 20

```

Conectar el PLC (IP: 192.168.20.10) al puerto Fa0/1.

Paso 2: Configurar router con salida a Internet y NAT

- Router industrial: Teltonika RUTX11
- IP LAN: 192.168.20.1
- IP WAN pública: 200.100.50.2
- Red VLAN 20: 192.168.20.0/24

Figura 46. Configuración básica: del router con salida a internet

```

interface GigabitEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 description LAN VLAN20
!
interface GigabitEthernet0/1
 ip address dhcp # 0 IP fija del ISP
 description WAN
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
access-list 1 permit 192.168.20.0 0.0.0.255

```

Paso 3: Publicar datos del PLC a la nube (AWS o Azure)

PLC publica datos vía MQTT (Broker Mosquitto en AWS):

Figura 47. Publicación de datos del PLC a la nube

```

{
  "sensor": "temperatura",
  "valor": 72.5,
  "unidad": "C"
}

```

Configuración básica en Node-RED (instalado en nube):

- Suscripción al topic: /ecuador/fabrica/temperatura
- Dashboard para monitoreo

- MQTT over TLS (puerto 8883)

Paso 4: Configurar VPN IPsec entre Ecuador y Paraguay

- En el router de Ecuador (Cisco):

Figura 48. Configuración de router

```
crypto isakmp policy 10
encr aes
hash sha
authentication pre-share
group 2
!
crypto isakmp key ParaguaySecretKey address 186.80.50.12
!
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
set peer 186.80.50.12
set transform-set TSET
match address 100
!
access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
!
interface GigabitEthernet0/1
crypto map VPN-MAP
```

- Router en Paraguay (red remota):

IP LAN: 192.168.30.1/24

Mismo procedimiento, invirtiendo IPs y claves.

Paso 5: Envío de datos cifrados a la planta en Paraguay

- Nodo suscriptor en Paraguay se conecta al mismo topic MQTT
- Firewall permite tráfico solo por VPN
- Datos fluyen encriptados y autenticados

Ejemplo: En Paraguay, un sistema SCADA suscribe:

Figura 49. SCADA en Paraguay

```
Broker MQTT: 10.8.0.1 (vía túnel VPN)
Topic: /ecuador/fabrica/temperatura
```

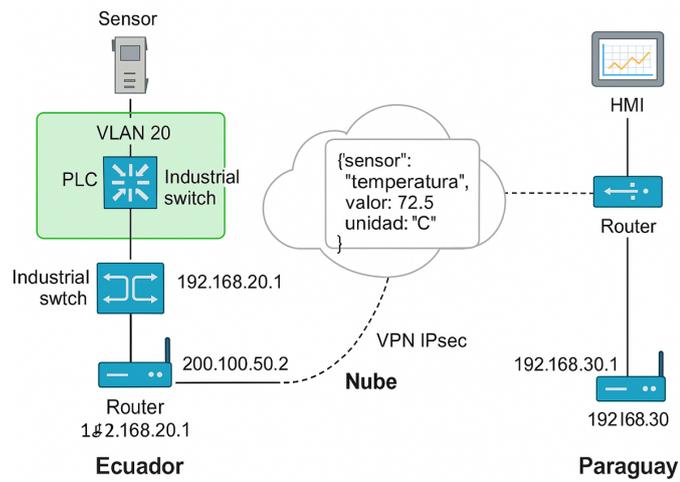
Resultado: el SCADA muestra en tiempo real la temperatura de sensores en Ecuador.

Figura 50. Topología resumida



En la figura 51 se muestra el esquema de la VLAN entre dos países con envío de datos por un proceso industrial

Figura 51. VLAN entre dos países



Fuente: Autores

"La convergencia entre IA, IoT y visión artificial, es esencial disponer de una arquitectura distribuida y escalable que garantice la interoperabilidad entre sensores, actuadores y motores de inferencia, permitiendo una supervisión autónoma, segura y en tiempo real del entorno agrícola".

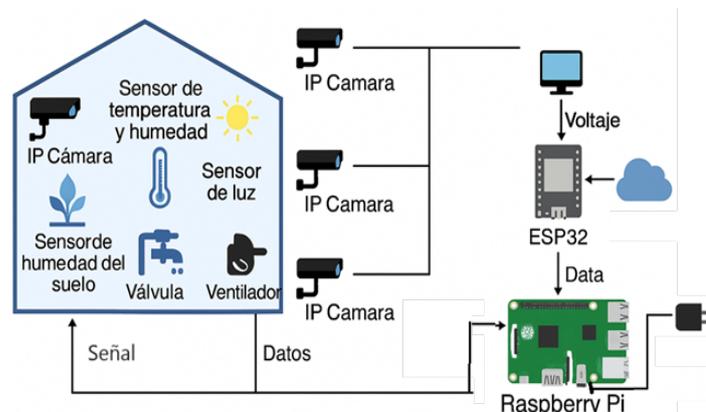
Los autores. 2025

CAPÍTULO IV:

ESCENARIO DE AGROMÁTICA

Un sistema de cultivo inteligente permite emplear diversos sensores en la toma de datos o supervisión de variables de interés de dicho cultivo, cada sensor debe enviar las señales de las variables medidas hacia la estación base y ésta a un equipo controlador (en muchos casos puede ser un solo equipo controlador que deberá contar con el dispositivo Gateway para enviar la información donde el usuario lo requiera. El uso de la computación en la nube para almacenamiento, procesamiento y analítica de datos, junto con la visión artificial revolucionan la agricultura de precisión. La figura 52 muestra un invernadero que a través de tecnologías TI más visión con IA integra diversos sensores y actuadores.

Figura 52. Esquema de Agromática



Fuente: Autores

Los cultivos inteligentes representan la convergencia entre inteligencia artificial, sistemas embebidos y redes de sensores, permitiendo una supervisión autónoma, eficiente y en tiempo real del entorno agrícola mediante arquitecturas interoperables y escalables.

Los sensores adecuados para el monitoreo de crecimiento o desarrollo de plantas o árboles pueden utilizar sensores para la humedad, radiación, etc. Asimismo, los actuadores o máquinas pueden activarse, según el programa

instalado previamente en un servidor local para la supervisión y control del cultivo o de los invernaderos. Por ejemplo, se encendería de forma automática una bomba de riego, uno o varios ventiladores o extractores de aire. El uso la inteligencia artificial en una opción importante y podría aplicarse en el escenario de cultivo inteligente. Una o varias cámaras para visión artificial (software de IA, instalado en un servidor local o remoto), en su operación del reconocimiento por imágenes podría identificar o detectar el estado de madurez de las frutas, o la afectación de la misma por incidencia de plagas.

CASO: CULTIVO INTELIGENTE

Se detalla aspectos como hardware y software para agricultura de precisión en invernadero con medida de 50 metros x 100 metros. El cultivo es de tomate.

Nombre científico: *Solanum lycopersicum*

Requisitos:

- Temperatura. óptima: 22–28 °C
- Humedad Relativa H.R.: 65–85%
- Luz solar: alta radiación ($\geq 300 \text{ W/m}^2$)
- Riego: por goteo, controlado por humedad del suelo
- Necesario: monitoreo de plagas, hongos, manchas foliares

HARDWARE BÁSICO

Se muestra equipamiento básico necesario en la siguiente tabla.

Tabla 8, Hardware para invernadero inteligente

Componente	Función
Raspberry Pi 4B	Nodo central de control y supervisión
Sensor DHT22	Temperatura y humedad ambiente
Sensor FC37 o YL-69	Humedad del suelo
Sensor LDR + fotodiodo	Radiación solar (o TSL2561 I2C)
Módulo de relé 5V	Activación de bomba de agua y ventiladores
Cámara Pi + OpenCV	Visión artificial para plagas y crecimiento

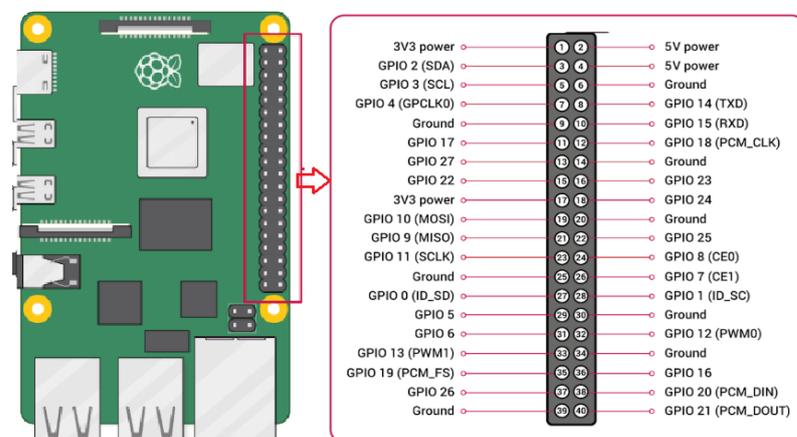
Componente	Función
Ventiladores / Extractores	Control de clima interno
Bomba de agua DC o 220V	Activación por humedad baja

CONEXIÓN DE SENSORES A RASPBERRY PI (GPIO)

Para conectar sensores a la placa controladora Raspberry Pi a través de los pines GPIO (General Purpose Input/Output) es fundamental entender la numeración de los pines y el tipo de sensor que se va a utilizar. Para controlar GPIO con Python, primero se debe importar una librería de código escrito previamente. Los GPIO son pines de propósito general que pueden configurarse como entrada o salida, y la Raspberry Pi ofrece una variedad de pines para diferentes tipos de sensores.

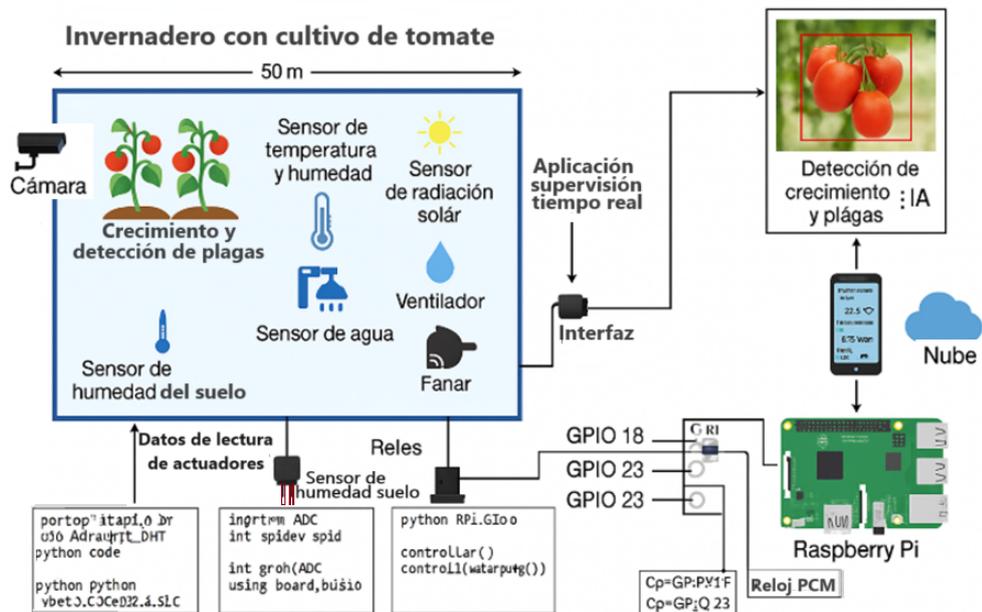
En el siguiente enlace web se puede obtener un [tutorial para GPIO](#) Raspberry Pi.

Figura 53, Configuración de pines GPIO



Los sensores suelen tener pines para alimentación (3.3V o 5V), tierra (GND) y datos. Es importante conectar estos pines a los correspondientes en la Raspberry Pi, siguiendo la documentación del sensor y la configuración de la Raspberry Pi.

Figura 54. Escenario para cultivo inteligente de tomate



En la tabla 9, se muestran los tipos de comunicación para cada uno de los sensores definidos.

Tabla 9. Tipo de comunicación de los sensores

Dispositivo	Conexión / Comunicación	Tipo de comunicación
DHT22	GPIO 4	Digital directa (1-Wire)
YL-69 (sensor humedad suelo)	ADC + GPIO 17 (requiere MCP3008)	SPI (Serial, vía MCP3008)
TSL2561 (sensor de luz)	I2C (SDA → GPIO 2, SCL → GPIO 3)	I2C (Serial)
Relé bomba	GPIO 18	Digital directa
Relé ventilador	GPIO 23	Digital directa
Cámara Pi	CSI port	CSI (Camera Serial Interface)

El sensor de temperatura DHT22, y relés: usan pines GPIO con señales digitales simples (alta/baja). El sensor de luz TSL2561 usa I2C, que es un tipo de comunicación serial. La cámara Pi usa CSI, que también es serial pero específica para video.

El sensor de humedad YL-69 requiere un convertidor ADC como el MCP3008, que se comunica por SPI, otro tipo de comunicación serial.

Figura 55. Pines de conexión de Raspberry Pi con sensores

DHT22	→ GPIO 4
YL-69	→ ADC + GPIO 17 (requiere convertidor ADC como MCP3008)
TSL2561	→ I2C (SDA → GPIO 2, SCL → GPIO 3)
Relé bomba	→ GPIO 18
Relé vent.	→ GPIO 23
Cámara Pi	→ CSI port (nativo en Raspberry Pi)

CÓDIGO PYTHON PARA LECTURA DE SENSORES

Se establecen códigos en Python para leer datos desde los sensores físicos conectados a la placa Raspberry Pi, La lectura de datos: lo establece el código que determina los valores como temperatura, humedad del suelo, luz, etc.

Sensor de Temperatura y Humedad – DHT22: Se detallan los siguientes pasos:

- Se importa la librería necesaria para trabajar con sensores DHT.
- Luego se declara el tipo de sensor que se está utilizando (DHT22).
- Luego se define el número del pin GPIO de la Raspberry Pi al que está conectado el sensor (en este caso, el GPIO 4).
- Se intenta leer los valores de humedad y temperatura desde el sensor. `read_retry` hace varios intentos si la lectura falla.
- Se muestra los valores leídos con una cifra decimal de precisión.

Figura 56. Código en Python para sensor DTH22

```
import Adafruit_DHT

sensor = Adafruit_DHT.DHT22
gpio = 4

humidity, temperature = Adafruit_DHT.read_retry(sensor, gpio)
print(f"Temperatura: {temperature:.1f} C, Humedad: {humidity:.1f} %")
```

Sensor Humedad del suelo – YL-69 con ADC: Se efectúan los siguientes pasos:

Importar librerías:

- `spidev`: permite la comunicación SPI entre la Raspberry Pi y dispositivos como el ADC MCP3008.
- `time`: se puede usar para pausas o temporización (aunque en este código no se usa directamente).

Luego:

- Crea un objeto SPI para iniciar la comunicación con el bus SPI de la Raspberry Pi.
- Abre la conexión SPI en el bus 0, dispositivo 0. Esto corresponde a los pines SPI por defecto en la Raspberry Pi.
- Define (*def*) una función llamada *read_channel* que recibe como parámetro el número de canal del convertidor analógico-digital ADC (por ejemplo, canal 0 para el sensor de humedad).
- Envía una solicitud al ADC (chip MCP3008) para leer el canal especificado. El parámetro de entrada (*channel*): permite especificar qué canal del ADC se desea leer (por ejemplo, canal 0 para humedad del suelo).
- `xfer2` envía y recibe datos SPI.
- `[1, (8 + channel) << 4, 0]` es la secuencia de 3 bytes que el MCP3008 espera para iniciar la lectura.
- Procesa la respuesta del ADC para obtener el valor digital (entre 0 y 1023) correspondiente a la señal analógica del sensor.
- Devuelve el valor leído del canal.
- Llama a la función para leer el canal 0 del ADC, donde está conectado el sensor de humedad del suelo.
- Muestra en pantalla el valor leído del sensor, en formato de texto.

Se indica que se utiliza comunicación serial SPI para leer datos desde un convertidor ADC como el MCP3008, que a su vez está conectado a un sensor analógico como el YL-69.

Figura 57. Código Python para sensor Humedad del suelo

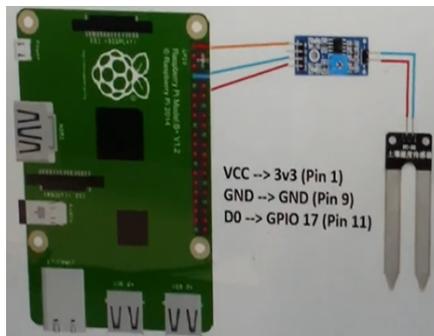
```
import spidev
import time

spi = spidev.SpiDev()
spi.open(0, 0)

def read_channel(channel):
    adc = spi.xfer2([1, (8 + channel) << 4, 0])
    data = ((adc[1] & 3) << 8) + adc[2]
    return data

humedad_suelo = read_channel(0)
print(f"Humedad del suelo (ADC): {humedad_suelo}")
```

Figura 58. Conexión de sensor YL-69



Sensor de Radiación solar (TSL2561): Se establecen los siguientes pasos:

- Se importa el módulo board, que permite acceder a los pines físicos de la placa (como board.SCL y board.SDA para I2C).
- Se importa el módulo busio, que permite crear interfaces de comunicación como I2C, SPI, etc.
- Se importa la librería específica para el sensor TSL2561, que mide la intensidad de luz en unidades de lux.
- Crea un objeto I2C usando los pines SCL (reloj) y SDA (datos) de la Raspberry Pi.
- Esto establece la comunicación serial I2C con el sensor.
- Crea una instancia del sensor TSL2561 y lo conecta al bus I2C previamente definido.
- Lee el valor de iluminancia (radiación solar) en lux desde el sensor y lo guarda en la variable lux.

- Muestra en pantalla el valor leído, con un mensaje descriptivo.

Este código utiliza el protocolo I2C, que es un tipo de comunicación serial muy común para sensores digitales.

Figura 59. Código en Python para sensor TSL2561

```
import board
import busio
import adafruit_tsl2561

i2c = busio.I2C(board.SCL, board.SDA)
sensor = adafruit_tsl2561.TSL2561(i2c)

lux = sensor.lux
print(f"Radiación solar: {lux} lux")
```

Control de actuadores y relés: Se detallan los siguientes pasos:

- Importa la librería RPi.GPIO, que permite controlar los pines GPIO (General Purpose Input/Output) de una Raspberry Pi.
- Importa la librería time, que proporciona funciones relacionadas con el tiempo, como pausas o retrasos en la ejecución del programa.
- Configura el modo de numeración de pines. GPIO.BCM indica que se usarán los números de los pines según la numeración del chip Broadcom (no la física del conector).
- Configura el pin 18 como salida. Este pin se usará para controlar una bomba
- Configura el pin 23 como salida. Este pin se usará para controlar un ventilador.
- Define una función llamada activar_bomba() que enciende la bomba al poner el pin 18 en estado alto (HIGH).
- Define una función llamada desactivar_bomba() que apaga la bomba al poner el pin 18 en estado bajo (LOW).

Figura 60. Código Python para control de actuadores y relés

```

import RPi.GPIO as GPIO
import time

GPIO.setmode(GPIO.BCM)
GPIO.setup(18, GPIO.OUT) # Bomba
GPIO.setup(23, GPIO.OUT) # Ventilador

def activar_bomba():
    GPIO.output(18, GPIO.HIGH)

def desactivar_bomba():
    GPIO.output(18, GPIO.LOW)

```

Ejemplo: activar bomba si humedad suelo < umbral. Se emplea una estructura condicional **if** para controlar una bomba de riego en función de la humedad del suelo.

- Se evalúa **si** el valor de la variable humedad_suelo es menor que 400.
- Se asume que humedad_suelo es un valor numérico obtenido de un sensor de humedad del suelo.
- Si el valor es menor que 400, significa que el suelo está seco y necesita riego.
- Si la condición anterior se cumple (el suelo está seco), se llama a la función `activar_bomba()`, que enciende la bomba de agua para regar el suelo.
- **else** indica una alternativa: si la condición del *if* no se cumple (es decir, si humedad_suelo es mayor o igual a 400), se ejecutará el bloque de código dentro del *else*.
- Si el suelo no está seco, se llama a la función `desactivar_bomba()`, que apaga la bomba de agua para evitar el riego innecesario.

Figura 61. Código para activar una bomba de agua

```

if humedad_suelo < 400:
    activar_bomba()
else:
    desactivar_bomba()

```

Visión artificial con OpenCV: Para la detección de plagas o crecimiento del tomate.

OpenCV (Open Source Computer Vision Library) ofrece herramientas para:

- ❖ Detección de objetos: Localizar objetos específicos en una imagen o video.
- ❖ Reconocimiento facial: Identificar rostros en una imagen o video.
- ❖ Seguimiento de objetos: Seguir el movimiento de objetos a través de secuencias de imágenes o video.
- ❖ Análisis de movimiento: Estudiar el movimiento de objetos o escenas en una imagen o video.
- ❖ Extracción de características: Identificar patrones o características relevantes en una imagen para tareas de clasificación o reconocimiento.
- ❖ Calibración de cámaras: Ajustar los parámetros de una cámara para obtener imágenes precisas.

Se indican la instalación necesaria de herramientas, como:

sudo

- Significa "superuser do".
- Permite ejecutar el comando con privilegios de administrador.
- Es necesario para instalar software o hacer cambios importantes en el sistema.

apt-get

- Es una herramienta de línea de comandos para manejar paquetes en sistemas basados en Debian (como Ubuntu o Raspberry Pi OS).
- Se usa para instalar, actualizar o eliminar programas.

install

- Especifica que se desea instalar un paquete.

python3-opencv

- Es el nombre del paquete que deseas instalar.

- Contiene la librería OpenCV (Open Source Computer Vision Library) para Python 3. Esta librería es de código abierto con una amplia gama de algoritmos y funciones que facilitan estas tareas.
- OpenCV se usa para procesamiento de imágenes y visión por computadora.

Figura 62. Código en Python para OpenCV

```
bash
sudo apt-get install python3-opencv
```

Código: capturar imagen y detectar manchas: Se detallan los siguientes pasos:

- Importa la biblioteca OpenCV, que se usa para procesamiento de imágenes y visión por computadora.
- Inicia la cámara. El parámetro 0 indica que se usará la cámara predeterminada del sistema.
- Captura un fotograma desde la cámara.
 - ret es un valor booleano que indica si la captura fue exitosa.
 - frame contiene la imagen capturada.
- Verifica si la captura fue exitosa (ret es True). Si no lo fue, el resto del bloque no se ejecuta.
- Convierte la imagen a escala de grises, lo cual es útil para simplificar el análisis de la imagen
- Aplica un umbral binario invertido:
 - Los píxeles con valor mayor a 130 se vuelven negros (0).
 - Los píxeles con valor menor o igual a 130 se vuelven blancos (255).
 - Esto ayuda a resaltar manchas u objetos oscuros sobre un fondo claro.
- Muestra la imagen procesada en una ventana llamada 'Plagas o manchas'.

- Guarda la imagen procesada como un archivo llamado deteccion.png
- Libera la cámara, cerrando el acceso a ella para que otros programas puedan usarla.

Figura 63. Código para capturar imagen y detectar manchas

```
import cv2

cam = cv2.VideoCapture(0)
ret, frame = cam.read()
if ret:
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    _, thresholded = cv2.threshold(gray, 130, 255, cv2.THRESH_BINARY_INV)
    cv2.imshow('Plagas o manchas', thresholded)
    cv2.imwrite('deteccion.png', thresholded)
cam.release()
```

Opcional: Se puede modificar el código para que ahora:

- ❖ Detectar contornos en la imagen umbralizada. (o umbralización, del inglés thresholding) es una técnica fundamental en procesamiento de imágenes y visión artificial, especialmente útil en aplicaciones agrícolas como la detección de plagas, madurez de frutos o análisis del crecimiento vegetal.
- ❖ Dibujar los contornos sobre la imagen original. Proceso en visión artificial y procesamiento de imágenes con OpenCV (u otras librerías), donde:
 - Se detectan los contornos (líneas que delimitan objetos) en una imagen.
 - Luego se superponen (dibujan) esos contornos sobre la imagen original en color, para identificar visualmente las regiones de interés.
- ❖ Contar las manchas detectadas.
- ❖ Mostrar y guardar la imagen con los contornos resaltados.

Lógica del código:

- ❖ Se convierte la imagen a escala de grises.
- ❖ Se aplica un umbral binario invertido para resaltar manchas oscuras.
- ❖ Se detectan contornos con cv2.findContours.
- ❖ Se dibujan los contornos con cv2.drawContours.
- ❖ Se imprime el número total de manchas detectadas.

- ❖ Se guarda la imagen como `deteccion_con_contornos.png`.

Modelo avanzado (opcional): Para detección de plagas específicas como Tuta absoluta o mildiu, se puede entrenar un modelo CNN (con TensorFlow/Keras) y ejecutarlo en Raspberry Pi o moverlo a un Jetson Nano para más potencia.

MOTOR DE VISIÓN ARTIFICIAL

Se denomina motor de visión artificial (o motor de visión por computadora) cuando se refiere a un conjunto de hardware y software optimizado para procesar imágenes o video en tiempo real, con el objetivo de interpretar visualmente el entorno.

Tabla 10. Opciones de motor para visión artificial

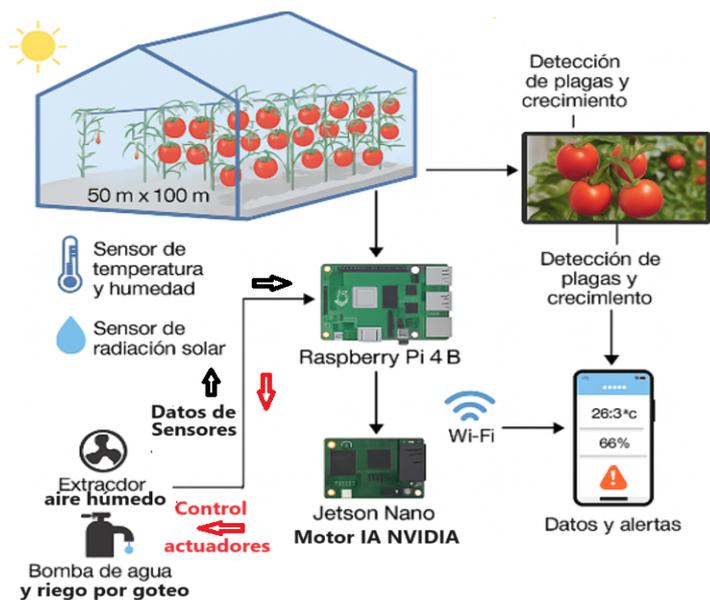
Dispositivo	Características
Raspberry Pi + Pi Cam	Adecuado para tareas básicas de visión
Jetson Nano	Ideal para inferencia de IA en borde
Coral USB + Pi	Acelera inferencia de modelos TensorFlow Lite

A continuación, se detalla cómo configurar un sistema robusto de IA.

MOTOR IA CON JETSON NANO DE NVIDIA

Funciona de forma autónoma o embebida, como un "motor" que impulsa una función específica dentro de un sistema mayor (por ejemplo, un robot, un dron o un sistema de seguridad). Ideal por su GPU integrada y soporte nativo a modelos de IA en tiempo real, Jetson Nano es más potente que la Raspberry Pi para tareas de visión profunda.

Figura 64 Escenario con motor IA Jetson Nano



En las tablas siguientes se detalla componentes, interfaz y protocolos para motor IA con Jetson Nano

Tabla 11. Descripción de componentes para motor Jetson Nano

Componente	Descripción técnica
Jetson Nano	4-core ARM CPU, 128-core GPU CUDA, 4 GB RAM
Cámara CSI (IMX219) o USB	Para capturar imágenes de plantas
Módulo WiFi o Ethernet	Para enviar datos a Raspberry Pi, servidor o la nube
Fuente de alimentación	5V 4A mínimo (USB-C o jack barrel)
MicroSD 64 GB clase 10	Sistema operativo JetPack y entorno de entrenamiento

Tabla 12. Descripción de interfaz y protocolos

Dispositivo	Interfaz física	Protocolo usado
Cámara IMX219	CSI (MIPI-CSI)	VideoStream/OpenCV
Raspberry Pi / Red	Ethernet / WiFi	HTTP, MQTT, TCP/IP
Cloud	Internet vía MQTT o API REST	JSON/HTTPS

SISTEMA OPERATIVO Y SOFTWARE

El sistema Operativo Base es JetPack SDK. El JetPack es el entorno oficial de desarrollo de NVIDIA para sus dispositivos Jetson (Nano, Xavier, Orin, etc.). Está basado en Ubuntu 18.04 o 20.04 LTS el cual es un sistema operativo Linux estable y ampliamente soportado, ideal para desarrollo embebido.

JetPack incluye de forma preinstalada y optimizada, las siguientes librerías importantes:

- OpenCV: captura y procesamiento de imágenes
- TensorFlow o PyTorch: para inferencia del modelo
- MQTT o HTTP: para enviar datos a Raspberry o nube

CONFIGURACIÓN PASO A PASO

1. Instalar JetPack

Desde <https://developer.nvidia.com/embedded/jetpack>

Conectar cámara y verificar: Se detalla el procedimiento:

Se emplea el comando en Bash que utiliza GStreamer, una herramienta para el procesamiento de medios (audio y video), y está orientado al uso con cámaras en dispositivos NVIDIA Jetson (como Jetson Nano).

Figura 65. Código para conectar cámara

```
bash
gst-launch-1.0 nvarguscamerasrc ! nvoverlaysink
```

Componentes:

- **gst-launch-1.0**

Es la herramienta de línea de comandos de GStreamer para construir y ejecutar tuberías multimedia.

- **nvarguscamerasrc**

Es el plugin fuente que accede a la cámara CSI (como la cámara oficial de Raspberry Pi) usando el ARGUS Camera API de NVIDIA.

Este plugin está optimizado para Jetson y permite capturar video desde la cámara.

- !

Es el operador de enlace en GStreamer. Conecta la salida de un elemento con la entrada del siguiente.

- **nvoverlaysink**

Es el plugin de salida (sink) que muestra el video directamente en la pantalla usando la aceleración por hardware de NVIDIA.

Permite una visualización eficiente y de baja latencia.

Este comando captura video en vivo desde la cámara CSI conectada a un Jetson Nano y lo muestra en pantalla en tiempo real usando la aceleración de GPU.

Captura de imagen con OpenCV: Se detallan los siguientes pasos:

- Importa la biblioteca OpenCV, que permite trabajar con imágenes y video.
- Inicia la captura de video desde la cámara predeterminada (índice 0).
- En un sistema como Jetson Nano, esto puede ser una cámara CSI o USB.
- Captura un fotograma (frame) de la cámara.
- `ret` indica si la captura fue exitosa.
- `frame` contiene la imagen capturada.
- Guarda la imagen capturada como un archivo llamado "tomate.png".
- Esta imagen puede ser usada para análisis posterior (por ejemplo, detección de madurez del tomate).
- Libera el recurso de la cámara.

Figura 66. Código para captura de imágenes con OpenCV

```
import cv2

cam = cv2.VideoCapture(0)
ret, frame = cam.read()
cv2.imwrite("tomate.png", frame)
cam.release()
```

Al respecto se indica que se capturan imágenes periódicamente del cultivo de tomates.

Se analizan con modelos de IA (por ejemplo, CNNs) para:

- ❖ Detectar el tamaño del fruto.
- ❖ Estimar el grado de madurez.
- ❖ Identificar enfermedades o plagas.

MODELO DE IA PARA DETECTAR PLAGAS Y CRECIMIENTO

- Entrenar un modelo CNN con imágenes etiquetadas de:
 - Tomates verdes, maduros, en flor
 - Hojas con plagas (mosca blanca, mildiu, etc.)
- Framework: TensorFlow o PyTorch
- Exportar como **TensorFlow Lite (.tflite)** o **ONNX** para inferencia optimizada

INFERENCIA EN JETSON NANO: Se realiza inferencia con un modelo de IA en Jetson Nano usando TensorFlow Lite:

Carga de librerías

- TensorFlow: biblioteca de aprendizaje automático.
- OpenCV (cv2): para procesamiento de imágenes.
- tflite_runtime: versión ligera de TensorFlow para ejecutar modelos .tflite en dispositivos embebidos como Jetson Nano.

Carga del modelo

- Carga el modelo entrenado en formato TensorFlow Lite (.tflite), optimizado para dispositivos con recursos limitados.
- `allocate_tensors()` prepara los tensores de entrada y salida.

Preprocesamiento de la imagen

- Carga la imagen del tomate.
- La redimensiona al tamaño requerido por el modelo (224x224 píxeles).
- Normaliza los valores de píxeles a un rango de 0 a 1.
- Ajusta la forma del tensor para que sea compatible con el modelo (batch size de 1, 3 canales RGB).

Inferencia

- Se establece el tensor de entrada con la imagen preprocesada.
- `invoke()` ejecuta la inferencia.
- Se obtiene el resultado del modelo (por ejemplo, la probabilidad de presencia de plagas).

Salida

- Muestra el resultado de la inferencia, que puede ser una clasificación, una probabilidad o una etiqueta.

Figura 67, Código para Inferencia con Jetson Nano

```

import tensorflow as tf
import cv2
from tflite_runtime.interpreter import Interpreter

interpreter = Interpreter(model_path="modelo_plagas.tflite")
interpreter.allocate_tensors()

# Preprocesamiento
frame = cv2.imread("tomate.png")
frame = cv2.resize(frame, (224, 224))
input_data = frame.astype('float32') / 255.0
input_data = input_data.reshape(1, 224, 224, 3)

# Ejecutar inferencia
interpreter.set_tensor(interpreter.get_input_details()[0]['index'], input_data)
interpreter.invoke()
output = interpreter.get_tensor(interpreter.get_output_details()[0]['index'])
print("Resultado:", output)

```

ENVÍO DE RESULTADOS A RASPBERRY PI O NUBE

Uso de MQTT para enviar resultado de la inferencia: Sse indican los siguientes pasos a seguir:

Código para publicar un mensaje MQTT

- Importar la biblioteca Paho MQTT, que permite a Python comunicarse usando el protocolo MQTT (Message Queuing Telemetry Transport), ideal para IoT.
- Crea una instancia del cliente MQTT.
- Este objeto se usará para conectarse al broker y enviar mensajes.
- Establece conexión con el broker MQTT ubicado en la IP 192.168.1.10.
- El puerto 1883 es el puerto estándar para MQTT sin cifrado.
- 60 es el tiempo de keep-alive en segundos (frecuencia con la que el cliente envía señales para mantener la conexión activa).
- Publica un mensaje en el topic invernadero/vision.
- El mensaje "Tomate maduro detectado" puede haber sido generado por un modelo de visión artificial que analizó una imagen del cultivo.
- Cierra la conexión con el broker MQTT de forma segura.

Figura 68. Código para publicación con MQTT

```
import paho.mqtt.client as mqtt

client = mqtt.Client()
client.connect("192.168.1.10", 1883, 60)
client.publish("invernadero/vision", "Tomate maduro detectado")
client.disconnect()
```

VISUALIZACIÓN Y SUPERVISIÓN REMOTA

- Plataforma en nube (ej. ThingSpeak, Node-RED + MQTT)
- Visualización en dispositivo móvil de datos ambientales y alertas IA
- Panel con info: temperatura, humedad, estado de riego, alerta por plagas

El motor Jetson Nano con la cámara IA detecta tomates maduros y envía alertas en tiempo real a un sistema de monitoreo o aplicación móvil. Este sistema ofrece un enfoque autónomo, escalable y basado en IA para optimizar la producción de tomates en invernadero mediante supervisión visual y ambiental

Figura 69. Esquema de la visión artificial en cultivo inteligente



CONSIDERACIONES FINALES

- Asegurar calibración de sensores
- Mantener el dataset de entrenamiento actualizado
- Usar un UPS para tolerancia a fallos en el sistema

Los datos obtenidos de sensores ubicados planificadamente en un invernadero de dimensiones 50 m x 100m ha hecho posible que los datos se transmitan a la nube: Los datos se envían a un servidor o plataforma en la nube para análisis, almacenamiento y visualización. La supervisión móvil: Dashboard accesible desde dispositivos móviles para monitoreo en tiempo real y recepción de alertas. Un factor clave y eficiente fue la comunicación mediante MQTT.

El proyecto de cultivo inteligente si es implementado de forma real se recomienda un motor IA robusto, para hacer el proceso de Inferencia local con modelos optimizados en TensorFlow Lite o TensorRT. La visualización de datos y alertas son en tiempo real. se tiene bajo consumo energético y alta escalabilidad.

Se concluye así con una aplicación directa en agricultura de precisión y automatización agroindustrial.

REFERENCIAS

- Automática e Instrumentación. (2014). *ISA100.11a se convierte en estándar oficial de ISA para comunicaciones wireless*. Obtenido de <https://www.automaticaeinstrumentacion.com/texto-diario/mostrar/2739683/isa10011a-convierte-estandar-oficial-isa-comunicaciones-wireless>
- Bustán, J. (2024). *El 5G marca el camino en el desarrollo de las industrias*. Obtenido de <https://www.revistazonalibre.ec/2024/07/06/el-5g-marca-el-camino-en-el-desarrollo-de-las-industrias/>
- CESA. (2025). *De la Industria 4.0 a la Industria 5.0: un nuevo paradigma basado en la ética y la sostenibilidad*. Obtenido de <https://www.cesa.edu.co/news/de-la-industria-40-a-la-industria-50-un-nuevo-paradigma-basado-en-la-etica-y-la-sostenibilidad/>
- Chasi, E. (2018). *Diseño, simulación y despliegue de Redes Inalámbricas de Sensores (WSN) con contiki*. Obtenido de https://oa.upm.es/55239/1/TFG_EDISON_LUIS_CHASI_TOMALO.pdf
- Electrónica Fácil. (2019). *Sensor de humedad y temperatura con Arduino y DHT22*. Obtenido de <https://mielelectronicafacil.com/proyectos/arduino/sensor-dht22/>
- Ericsson. (2025). *Tendencias intersectoriales que desencadenan la próxima ola de innovación*. Obtenido de <https://www.ericsson.com/en/next-wave-of-mobile>
- FieldComm Group. (2017). *Intrinsically Secure WirelessHART® Field Device Networks and the Industrial Internet of Things (IIoT)*. Obtenido de http://fieldcommdev.prod.acquia-sites.com/sites/default/files/imce_files/technology/documents/WirelessHART%20security%20v1.0.pdf
- FieldComm Group. (2021). *WIRELESSHART SECURITY*. Obtenido de <https://www.fieldcommgroup.org/wirelesshart-security>
- FieldComm Group. (2025). *Explicación de HART-IP*. Obtenido de <https://www.fieldcommgroup.org/technologies/HART-IP/explained>
- FutuRed. (2024). *Comunicaciones Futured*. Madrid: FutuRed. Disponible en: https://futured.es/wp-content/uploads/2025/01/AF_LIBRO-COMUNICACIONES-FUTURED-2024_CALIDAD-MEDIA-comprimido_1.pdf. Obtenido de https://futured.es/wp-content/uploads/2025/01/AF_LIBRO-COMUNICACIONES-FUTURED-2024_CALIDAD-MEDIA-comprimido_1.pdf

- HMS Networks. (2025). *Tome decisiones basadas en datos con IIoT*. Obtenido de <https://www.hms-networks.com/machine-data-monitoring>
- Huma Kamal, Z., & Ali Salahuddin, M. (2015). *Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications*. Obtenido de http://dx.doi.org/10.1007/978-1-4939-2468-4_1
- IBM. (2025). *Qué es Edge AI?* Obtenido de <https://www.ibm.com/mx-es/topics/edge-ai>
- IEC 68512. (2016). *Industrial networks - Wireless communication network and communication profiles - WirelessHARTTM*. Obtenido de <https://webstore.iec.ch/publication/68512>
- Industrial Ethernet Book. (2023). *Actualización de tecnología inalámbrica industrial*. Obtenido de <https://iebmedia.com/technology/iiot/2023-industrial-wireless-technology-update/>
- Innova Tech. (2025). *Manual de Operacion*. Obtenido de https://innova.tecnm.mx/documentos/local/Manual_de_Operacion_InnovaTecNM_2025_Of.pdf
- International Society of Automation, ISA. (2020). *Informe ISA: el 63 por ciento de los profesionales de la ingeniería de automatización encuestados creen que los estándares de la industria serán 'extremadamente importantes' en el futuro*. Obtenido de <https://www.isa.org/news-press-releases/2020/july/63-percent-of-automation-engineering-professionals>
- Linares, K. (2017). *Red confiable*. Obtenido de [Cursos Cisco-CCNA V6.0: https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-La-red-como-plataforma-Red-confiable.html](https://kevin-linares.blogspot.com/2017/05/exploracion-de-la-red-La-red-como-plataforma-Red-confiable.html)
- Moosavi, J., Bakhshi, J., & Martek, I. (2021). *The application of industry 4.0 technologies in pandemic management: Literature review and case study*. Obtenido de <https://www.sciencedirect.com/science/article/pii/S2772442521000071>
- National Instrument. (2024). *Comparación de FOUNDATION Fieldbus y sistemas tradicionales*. Obtenido de <https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/comparison-of-foundation-fieldbus-and-traditional-systems.html?srsId=AfmBOoo6nWS-TYZPh87Zhk219J96xqjyco0zZzRJKxYrQnPjbrS6a4Dx>
- Neves, Y., Künzel, G., Müller, I., & Pereira, C. (2018). *Industrial Wireless Automation: Overview and Evolution of WIA-PA*. Obtenido de <file:///C:/Users/Orlando/Downloads/1-s2.0-S2405896318305779-main.pdf>

- Noor-A, R., Firyaguna, J., Sherazi, H., Kushch, S., & Vijayan, A. (2023). *Comunicaciones inalámbricas para la fabricación inteligente y la IoT industrial: tecnologías existentes, 5G y más allá*. Obtenido de Journal. Sensors , 23 (1), 73.: <https://doi.org/10.3390/s23010073>
- Núñez, G. (2016). "Redes Inalámbricas en la Industria: Comparación WirelessHART y ZigBee", Páginas: 1-8, *Redes Locales en la Industria. Máster en Automática, Robótica y Telemática Camino de los Descubrimientos*. Obtenido de https://www.academia.edu/26019792/Redes_Inal%C3%A1mbricas_en_la_Industria_Comparaci%C3%B3n_WirelessHART_y_ZigBee
- Paliz, A., Ruales, E., & Recalde, H. (2025). *Impacto de las redes 5G en la transformación digital de las pequeñas y medianas empresas*. Obtenido de <https://editorialscientificfuture.com/index.php/rpca/article/view/114>
- Raaz, J. (2024). *Industria 5.0 vs. Industria 4.0: Principales diferencias y beneficios*. Obtenido de <https://inspenet.com/articulo/industria-5-0-vs-industria-4-0-beneficios/>
- Raptis, T., Passarella, A., & Conti, M. (2020). *A Survey on Industrial Internet With ISA100 Wireless*. Obtenido de IEEE Access V, 8 p.p: 157-177: <https://ieeexplore.ieee.org/document/9178359>
- Raza, S., Faheem, M., & Guenes, M. (2019). *Future Research Challenges in Wireless Sensor and Actuator Networks Targeting Industrial Automation*. Obtenido de *Redes industriales inalámbricas de sensores y actuadores en la industria 4.0: exploración de requisitos, protocolos y desafíos: una encuesta MAC. Revista Internacional de Sistemas de Comunicación*; doi:10.1002/dac.4074
- Robayo, L. (2019). *5G para la comunicación entre equipos de la planta, ¿está la industria preparada?* Obtenido de <https://www.mundopmmi.com/automatizacion/redes-y-conectividad/article/14039543/5g-para-la-comunicacin-entre-equipos-de-la-planta-est-la-industria-preparada>
- Rueda, J., & Talavera, J. (2017). *Similitudes y diferencias entre Redes de Sensores Inalámbricas e Internet de las Cosas: Hacia una postura clarificadora*. Obtenido de RCC. *Revista Colombiana de Computación*, Vol. 18, No. 2, pp. 58–74: <https://revistas.unab.edu.co/index.php/rcc/article/view/3218/2781>
- Sharma, S. (2023). *UART vs SPI: Una comparación completa para sistemas integrados*. Obtenido de <https://www.wevolver.com/article/uart-vs-spi-a-comprehensive-comparison-for-embedded-systems>

- Skubacz, M. (2020). *Edge computing industrial: lo mejor de dos mundos*. Obtenido de Siemens Argentina: https://www.editores-srl.com.ar/sites/default/files/aa11_skubacz.pdf
- Teltonika. (2023). *Conectividad de equipos madrinado y fresado*. Obtenido de <https://teltonika-networks.com/es/newsroom/5g-digitization-in-manufacturing>
- UIT-T Recomendación X.1361. (2018). *Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela*. Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1361-201809-I!!PDF-S&type=items
- Wang, Q., & Jiang, J. (2016). "Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards", Vol. 18, No. 3,. Obtenido de IEEE Communications Surveys & Tutorials, IEEE Journals & Magazines.: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7448365>

GLOSARIO

AES Advanced Encryption Standard

APL Application Layer

ASL, Application SubLayer

CCA Clear Channel Assessment

CCM Cipher block Chaining Message authentication code

CPS Cyber-Physical System

CSMA-CA Carrier Sense Multiple Access with Collision Avoidance

DRE, Distributed, Real-time, and Embedded

DSSS Direct Sequence Spread Spectrum

FHSS Frequency Hopping Spread Spectrum

HTTP Hypertext Transfer Protocol

IEEE Institute of Electrical and Electronics Engineers

IEC International Electrotechnical Commission

IoT Internet of Things

IIoT Industrial Internet of Things

ISA International Society of Automation

ISM Industrial, Scientific, and Medical

ITU International Telecommunication Union

IWSN Industrial Wireless Sensor Network

JSON JavaScript Object Notation

MAC Medium Access Control

M2M Machine to Machine

PHY Physical Layer

QoS Quality of Service

MQTT Message Queuing Telemetry Transport

SCADA supervisory Control and Data Acquisition

TCP Transmission Control Protocol

TDMATime Division Multiple Access
TSMP Time Synchronized Mesh Protocol
UAP User Application Process
UAO User Application Objects
VLAN Virtual Local Area Network
WSN Wireless Sensor Network

Luis Orlando Philco Asqui

Doctor en Ciencias Informáticas; Universidad Nacional de la Plata, Argentina
Docente Investigador; Universidad Agraria del Ecuador
lphilco@uagraria.edu.ec
orcid: <https://orcid.org/0000-0001-5312-3563>

Bryan Iván Barahona Montalván

Ingeniero en Computación; UAE. Magister en Matemáticas
Docente Investigador; Universidad Agraria del Ecuador
bbarahona@uagraria.edu.ec
orcid: <https://orcid.org/0009-0006-2223-4387>

Bryan Orlando Vélez San Martín

Ingeniero en Computación; UAE.
Magister en Educación con mención Entornos Digitales
Magister en desarrollo de Software y Devops.
Docente Investigador; Universidad Agraria del Ecuador
bvelez@uagraria.edu.ec
orcid:
<https://orcid.org/0009-0003-0678-7828>

Hamilton Francisco Villamar Barros

Ingeniero en Sistemas Computacionales; UNEMI
Magister en Tecnología de la Información; UNEMI
Docente Investigador; Universidad Agraria del Ecuador
hvillamar@uagraria.edu.ec

ISBN: 978-9942-33-926-3



Compás
capacitación e investigación