UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Sistema de supervisión y acceso remoto ciberseguro para procesos industriales mediante tecnología IIoT

TESIS

Que para obtener el título de

Ingeniero Eléctrico Electrónico

P R E S E N T A

Diego Sarmiento Sosa

DIRECTOR DE TESIS

Dr. Hoover Mujica Ortega

Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado SISTEMA DE SUPERVISION Y ACCESO REMOTO CIBERSEGURO PARA PROCESOS INDUSTRIALES MEDIANTENTE IIOT que presenté para obtener el titulo de INGENIERO ELÉCTRICO ELECTRÓNICO es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.

DIEGO SARMIENTO SOSA
Número de cuenta: 317117707

Jurado asignado

Presidente:	Mtra. Gloria Correa Palacios
Secretario:	Ing. David Quintanar Villalba
Vocal:	Dr. Hoover Mujica Ortega
1^{er} suplente:	M.I. Ivan de Jesús Osio Chávez
2^{do} suplente:	M.I. Carlos Alberto Peréz Juárez

Ciudad Universitaria, Departamento de Control y Robótica, Laboratorio de Automatización.

Ciudad de México.

Director de tesis

Dr. Hoover Mujica Ortega

Dedicatoria

A todas las personas que confiaron en mi.

Agradecimientos

A mis padres; por su esfuerzo, apoyo y amor incondicional.
A mis amigos y compañeros; que sin ellos mi vida academica no sería la misma.
A la empresa HMS Networks por brindarme el equipo industrial para la realización de este trabajo
A las personas que me dejaron aprender de ellas.
Al Dr. Hoover Mujica Ortga por el apoyo en la relización en este documento.

Resumen

En la actualidad, la industria enfrenta el reto de adaptarse a los cambios que demanda la transformación digital, impulsada por la Industria 4.0 y el Internet industrial de las cosas (IIoT, por sus siglas en inglés). Esta evolución tecnológica busca optimizar los procesos productivos mediante la interconexión de dispositivos, la supervisión remota de operaciones y la gestión inteligente de datos en tiempo real. Sin embargo, el incremento en la conectividad trae consigo nuevos desafíos, especialmente en el ambito de la ciberseguridad, asi como la integridad de la información y disponibilidad de los sistemas de control.

Este trabajo tiene como objetivo implementar un sistema de supervisión y acceso remoto basado en tecnologías IIoT, capaz de integrar y monitorear distintos procesos industriales bajo un enfoque ciberseguro. Para ello, se desarrolló una arquitectura que permite la comunicación entre diferentes familias de Controlador lógico programable (PLC, por sus siglas en inglés), uno dedicado al control de flujo en tanques atmosféricos mediante un lazo Control proporcional integral derivativo (PID) y otro encargado del control secuencial de un proceso de embotellado. Estos controladores fueron conectados a través de un módulo *gateway* IIoT que actúa como nodo central para la recopilación y transmisión de datos hacia una plataforma de monitoreo remoto.

La configuración del sistema se realizó apegado los lineamientos de la norma *IEC 62443*, la cual establece principios y requerimientos de seguridad en Sistemas de automatización y control industrial (IACS, por sus siglas en inglés). Se implementaron medidas como autenticación de usuarios y control de acceso por niveles de privilegio. Estas acciones garantizan la integridad de la información y la protección frente a posibles accesos no autorizados con la ayuda de túneles Red Privada Virtual (VPN, por sus siglas en inglés).

Asimismo, se desarrolló un *dashboard* que integra Indicadores claves de desempeño (KPI, por sus siglas en inglés) de rendimiento, disponibilidad, calidad, así como sus respectivos Eficiencia general de los equipos (OEE, por sus siglas en inglés), permitiendo visualizar en tiempo real el estado operativo de cada proceso. Esta interfaz facilita la interpretación de datos mediante gráficas de tendencia, indicadores visuales y alertas configurables, lo que contribuye a la toma de decisiones informadas en los procesos.

Durante la fase de validación, se comprobó la estabilidad de la comunicación entre los PLC y el módulo IIoT, así como la actualización en tiempo real de las variables supervisadas. Los resultados obtenidos demostraron que el sistema propuesto cumple con los requisitos funcionales de supervisión remota, también ofrece un nivel adecuado de ciberseguridad, al minimizar vulnerabilidades en la comunicación y el acceso a los datos.

Índice general

Índice de figuras

Acrónimos

IIoT Internet industrial de las cosas, por sus siglas en inglés. IX, XIII, XIV, 1, 2, 3, 4, 5, 6, 8, 9, 12, 15, 20, 22, 23, 27, 35, 37, 41, 43, 44, 45, 47

PLC Controlador lógico programable,por sus siglas en inglés. IX, XIII, XIV, 1, 2, 3, 4, 6, 7, 16, 17, 18, 20, 22, 23, 24, 25, 26, 27, 35, 37, 39, 40, 47

PID Control proporcional integral derivativo. IX, 3, 16

IACS Sistemas de automatización y control industrial, por sus siglas en inglés. IX, 10, 12

VPN Red privada virtual ,por sus siglas en inglés. IX, XIII, XIV, 6, 8, 9, 16, 20, 29, 37, 38, 39, 41, 45, 47

KPI Indicadores claves de desempeño, por sus siglas en inglés. IX, XIV, 3, 4, 11, 12, 39, 40, 45, 47

OEE Eficiencia general de los equipos, por sus siglas en inglés. IX, XIII, XIV, 3, 4, 12, 26, 29, 36, 40, 47

SCADA Control de supervision y adquisicion de datos, por sus siglas en inglés. XIII, 4, 6, 7, 8

Tags Nomenclaturas de etiquetas. XIII, 20, 22, 23, 25, 26, 27, 28, 31, 35, 36

HMI Interfaz humano máquina, por sus siglas en inglés. 6, 7

TLS Seguridad de la capa de transporte, por sus siglas en inglés. 8, 9

Capítulo 1

Introducción

1.1. Antecedentes

En los ultimos años el monitoreo y control remoto de sistemas industriales mediante el uso de tecnologías basadas en el IIoT ha ganado relevancia debido a su capacidad para mejorar la eficiencia, reducir costos y minimizar la intervención humana en procesos críticos. Un ejemplo de su aplicacion dentro de las subestaciones eléctricas es el de [Bagyaveereswaran, *et al.*, 2023], donde propusieron un esquema modular basado en IIoT para monitorear y controlar la distribución de energía en un modelo de subestación. Este sistema utiliza un *gateway Flexy 205* y un enrutador de acceso remoto para controlar un modelo de subestación que incluye áreas urbanas y rurales. El control se realiza mediante un PLC *Siemens S7-300*, y donde además se desarrolló una interfaz gráfica de usuario utilizando el software *ViewON* para el acceso remoto. Esta aplicación demostró ser efectiva para la automatización de subestaciones, reduciendo la necesidad de intervención manual y mejorando la eficiencia en la distribución de energía.

Otro trabajo que realiza la implementación de un sistema de monitoreo de consumo de vapor es el de [Moscol y Sánchez, 2021], en donde desarrollaron un sistema basado en IIoT para medir y optimizar el uso de vapor, agua y diésel en una planta de producción de *Nestlé* en Ecuador. Esta aplicación hizo uso de instrumentos de medición como el flujo másico y contadores volumétricos, junto con un PLC *Allen Bradley* y un *gateway Flexy 205*, con esto lograron enviar datos a la nube mediante la plataforma *Talk2M*. Este sistema permitió la generación de indicadores de energía, alarmas y reportes automáticos, lo que agilizó la toma de decisiones en tiempo real y la reducción de pérdidas energéticas.

Otro ámbito en el que esta esta implementeando esta tecnología IIoT es en la gestión de recursos hídricos dentro de la industria, mas especificamente en [Jadhav, *et al.*, 2018] se presenta un sistema de monitoreo del uso de agua en una planta de procesamiento de leche utilizando IIoT. Este sistema emplea sensores de flujo y nivel para medir el consumo de agua en diferentes secciones de la planta, enviando los datos a la nube para su análisis. La implementación de este sistema permitió a la planta generar informes sobre el consumo de agua, facilitando la planificación para la conservación del recurso y reduciendo los costos relacionados.

Un punto crucial dentro de las apliaciones de esta tecnología IIoT es la ciberseguridad, en [Juárez, 2019] se analizaron los desafíos y herramientas para proteger sistemas que adoptan esta tecno-

logía. El estudio concluye con la importancia de estándares y modelos de evaluación para garantizar la seguridad en dispositivos IIoT. Además este estudio propuso el uso de herramientas de evaluación de ciberseguridad, como el *SecureGrid Hacking Tool Box*, para realizar pruebas de penetración y detectar vulnerabilidades en sistemas IIoT.

Con ayuda de los trabajos anteriores podemos ver la relevancia que comienza a cobrar el IIoT y la automatización en diversos sectores industriales. La implementación de estas tecnologías no solo permite un monitoreo y control en tiempo real más eficiente, sino que también contribuye a la reducción de costos operativos. Además, la ciberseguridad en entornos industriales se ha convertido en un aspecto crítico, especialmente con la creciente adopción de dispositivos IIoT en infraestructuras industriales, lo que requiere la implementación de estándares y herramientas de evaluación para garantizar la protección de los sistemas con la intencion de mantener la seguridad de la información.

1.2. Motivación

La Industria 4.0 ha transformado la manera en que se supervisan y controlan los procesos industriales, gracias a la adopción del IIoT. Sin embargo aún existen muchas empresas que no han implementado estas soluciones debido a los costos de implementación y a los retos que implica cibersegurdad con respecto a la integridad de la información .

Es por eso que este proyecto de tesis se motiva en la necesidad de demostrar cómo el IIoT puede mejorar la eficiencia operativa y la toma de decisiones en procesos industriales. Además de aborda otro desafíos en la industria como lo es la integración de sistemas diversos, que permita una mayor flexibilidad y escalabilidad en entornos industriales con multiples procesos.

Otro aspecto clave de este trabajo es la ciberseguridad. Debido a la creciente conectividad de los sistemas industriales, los riesgos de ciberataques han aumentado significativamente. Este proyecto no solo busca implementar un sistema de supervisión remota, sino también garantizar que sea seguro, siguiendo las normativas internacionales como la *IEC 62443*.

1.3. Formulación del problema

Partiendo de lo expuesto en los antecedentes, se puede observa que existen problemáticas que podemos abordar en el desarrollo de este proyecto, se pueden destacar los siguientes puntos:

- La integración de diferentes procesos, es decir, sistemas de control en los cuales se suelen involucrar PLC de diferentes fabricantes. Esta diversidad de tecnologías y protocolos de comunicación dificulta la creación de un sistema de supervisión unificado y escalable, lo que genera ineficiencias y aumenta los costos de implementación.

- Existen empresas que carecen de herramientas para monitorear y controlar sus procesos de manera remota y en tiempo real. Esto nos brinda la oportunidad de implementar un sistema que los apoye en la capacidad para tomar decisiones informadas y en tiempo real, especialmente en procesos críticos. La falta de una supervisión remota no solo reduce la productividad, sino que también aumenta el riesgo de fallos operativos y tiempos de inactividad presentes en cualquier área industrial.

- La creciente conectividad de los sistemas industriales los expone a riesgos de ciberseguridad ante ciberataques cada vez más sofisticados. Un ciberataque puede tener consecuencias devastadoras, como la interrupción de operaciones, la pérdida de datos críticos o incluso daños a la infraestructura física y mas grave aún daños fisicos a operadores.

1.4. Objetivos

1.4.1. Objetivo general

Implementar un sistema IIoT para la supervisión y acceso remoto de procesos industriales, integrando PLC de diferentes fabricantes como lo son el *ControlLogix L81E* de la empresa *Rockwell Automation* y el *S7-1500* de la empresa *Siemens*, garantizando la ciberseguridad del sistema, de forma que se pueda monitorear y supervisar los procesos en tiempo real, utilizando tecnologías como el módulo *Flexy 205* y el *software ViewON* para el diseño de la plataforma de visualización y análisis de datos.

1.4.2. Objetivos específicos

- Diseñar la arquitectura del sistema IIoT, incluyendo la integración de PLC *ControlLogix L81E* y *S7-1500* mediante el módulo *Flexy 205*, para la comunicación y adquisición de datos en tiempo real.
- Implementar un *dashboard* en el *software ViewON* que permita visualizar y analizar datos de los procesos industriales, incluyendo la presentación de KPI y OEE para evaluar el rendimiento de cada proceso.

- Validar el acceso remoto en procesos industriales reales, como el control de tanques atmosféricos con sistemas PID y el prototipo de planta embotelladora controlados por diferentes PLC que tomaremos como caso de estudio.

1.5. Contribuciones

- Se implementó un sistema IIoT que integra PLC de diferentes fabricantes mediante el módulo *Flexy 205*, resolviendo el desafío de la interoperabilidad en entornos industriales diversos.

- Se desarrolló un *dashboard* en *ViewON* para visualizar y analizar datos en tiempo real, incorporando KPI como el rendimiento, la disponibilidad y la calidad de los proceso, así como el cálculo del OEE. Esta herramienta permite monitorear el rendimiento de los procesos industriales de manera eficiente.

- Se configuraron las conexiones necesarias para integrar el sistema IIoT con los PLC, se implementaron rutinas de adquisición de datos en el módulo *Flexy 205*, asegurando la compatibilidad con el *software ViewON* para el desarrollo de un *dashboard* de visualización y análisis de datos.

1.6. Organización de la tesis

El contenido de esta tesis se organiza en cinco capítulos que abarcan desde los fundamentos teóricos hasta la validación del sistema propuesto.

- En el Capítulo 1 se presenta la introducción, donde se expone el contexto industrial, los objetivos y la justificación del proyecto, enfocado en la implementación de un sistema de supervisión y acceso remoto basado en la tecnología IIoT.

- El Capítulo 2 desarrolla el marco teórico, abordando los conceptos de Industria 4.0, digitalización industrial, y sistemas SCADA, así como los fundamentos de conectividad y seguridad con énfasis en las comunicaciones remotas seguras, las amenazas en entornos IIoT y la norma *IEC 62443*. Finalmente, se incluyen los principios del análisis de datos industriales, la generación de KPI y el uso de *dashboards*.

- En el Capítulo 3 se describe el sistema propuesto, su estructura general, los procesos industriales involucrados, la integración de equipos, la configuración del módulo IIoT y las medidas de ciberseguridad aplicadas para garantizar la protección del sistema.

- El Capítulo 4 presenta la evaluación y validación, donde se documentan las pruebas de comunicación, supervisión remota y seguridad, además de incluir una discusión sobre los resultados obtenidos y las oportunidades de mejora.

- En el Capítulo 5 se exponen las conclusiones del trabajo, orientadas en los resultados obtenidos.

Capítulo 2

Fundamento teórico

2.1. Industria 4.0 y digitalización industrial

Antes de proceder a la realizacion de la arquitectura del sistema IIoT se explicaran los conceptos necesarios para de la digitalización industrial y los sistemas de monitoreo industrial además de la preocupación y la importancia acerca de la ciberseguirdad de la información dentro de los procesos industriales, asi como las tecnologías que permiten las conexiones remotas.

2.1.1. Internet Industrial de las Cosas

La transformación digital en entornos industriales representa un cambio de paradigma profundo de los modelos tradicionales de producción. Este cambio está motivado por la necesidad de mejorar la eficiencia, flexibilidad, trazabilidad y capacidad de respuesta de las operaciones, adoptando una visión completa de la industria conectada y automatizada.

Esta transformación implica más que la automatización, busca una optimización inteligente basada en datos. Según [Cartuche-Calva, 2020] esta digitalización requiere no solo de nuevas tecnologías, sino de un rediseño de los procesos de negocio que contemple la integración de sensores, redes, plataformas y estándares de seguridad adaptados al nuevo contexto digital.

En este nuevo modelo, el ciclo de vida de los datos industriales, desde su adquisición, procesamiento y análisis, hasta su visualización y toma de decisiones se vuelve un tema central. La infraestructura digital debe garantizar que estos datos estén disponibles en todo momento, con integridad y protección adecuada. Para lograrlo, se requieren arquitecturas escalables y seguras, donde cada elemento aporte a la visión global del sistema productivo [Cartuche-Calva, 2020].

Dentro del proceso de transformación digital, el IIoT y el *cloud computing* se posicionan como tecnologías esenciales. El IIoT puede definirse como una red de objetos inteligentes y sistemas conectados que, mediante comunicaciones estandarizadas, permiten recolectar, intercambiar y analizar datos industriales en tiempo real, promoviendo así operaciones más autónomas y eficientes.

Los dispositivos IIoT incluyen sensores, actuadores, controladores y plataformas de comunicación que funciona para supervisar y optimizar procesos industriales. Una de sus principales virtudes es la capacidad de habilitar decisiones automatizadas basadas en el análisis de datos, reduciendo la intervención humana y mejorando la capacidad de respuesta del sistema. Esta visión coincide con la de [Boyes, *et al.*, 2018], quienes destacan que el IIoT se sustenta en la integración inteligente de

componentes físicos con plataformas digitales distribuidas, como la computación en la nube y el *edge computing*.

Por su parte, el *cloud computing* proporciona una infraestructura para almacenar, procesar y visualizar datos desde ubicaciones remotas, lo cual resulta clave en sistemas de supervisión industrial distribuidos. Según [Campoverde, *et al.*, 2015] , este modelo permite no solo acceder a información en tiempo real desde cualquier punto autorizado, sino también reducir la dependencia de servidores locales y mejorar la respuesta del sistema ante fallos.

No obstante, esta conectividad también introduce nuevos metodós de ciberataques, por lo que debe acompañarse de mecanismos de seguridad, como el uso de VPN, cifrado de datos, autenticación multifactor y segmentación de redes industriales [Cartuche-Calva, 2020].

2.2. Sistemas de monitoreo industrial

Para profundizar en las bases conceptuales de los sistemas de supervisión industrial, resulta fundamental iniciar con el estudio de uno de los enfoques más consolidados y extendidos en el sector: los sistemas SCADA. Estos sistemas han constituido, durante décadas, la columna vertebral del monitoreo y control de procesos, proporcionando visibilidad operativa, registro histórico y herramientas de gestión en tiempo real. Analizar su estructura, funcionamiento y limitaciones permite comprender el papel que desempeñan dentro de las arquitecturas industriales convencionales. Asimismo, este análisis abre la puerta a identificar cómo la incorporación de tecnologías IIoT introduce nuevas oportunidades de mejora en términos de conectividad, escalabilidad, supervisión remota y seguridad.

2.2.1. Arquitectura básica de sistemas SCADA

Para [Rockwell Automation, 2015] los sistemas SCADA representan una de las herramientas fundamentales para la supervisión y control de procesos industriales. Su principal objetivo es recopilar, procesar y visualizar datos provenientes de diferentes dispositivos de campo, permitiendo a los operadores supervisar el estado del sistema en tiempo real, detectar anomalías y tomar decisiones informadas.

La arquitectura básica de un sistema SCADA se compone de varios elementos distribuidos que trabajan en conjunto:

- Dispositivos de campo: Su objetivo es recopilar variables físicas del proceso y ejecutar acciones de control.
- PLC: Se encargan de la adquisición de datos y del control automático del proceso. Actúa como intermediarios entre los dispositivos de campo y el sistema SCADA.
- Red de comunicación: Permite la transmisión de datos entre los dispositivos de campo, los controladores y el centro de control.
- Servidor SCADA: Se encarga del procesamiento de datos, almacenamiento histórico, gestión de alarmas y comunicaciones con la red de dispositivos.
- Estaciones de trabajo o Interfaz humano máquina (HMI, por sus siglas en inglés): Proporcionan a los operadores una visualización gráfica del sistema en tiempo real, acceso a los registros históricos, alarmas, tendencias y herramientas de análisis.

La arquitectura puede ser escalada desde una configuración simple de un solo PLC conectado a una HMI local, hasta sistemas distribuidos con múltiples estaciones de control, redundancia de servidores, acceso remoto y almacenamiento en la nube. En la Figura 2.1 se muestra un ejemplo de la vista general de un sistema SCADA.

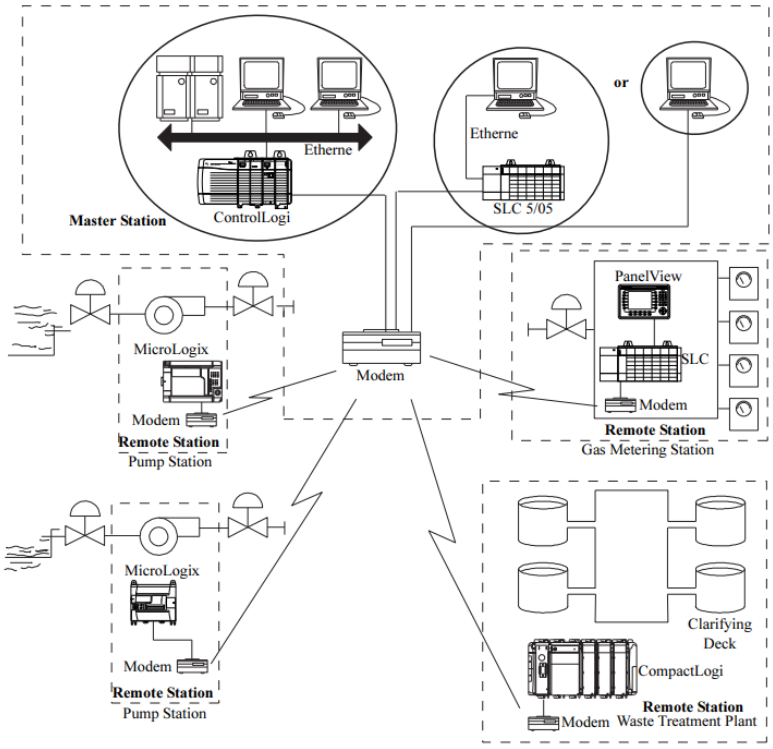

Figura 2.1 .
Ejemplo de arquitectura general de un sistema SCADA.[1]

Los sistemas SCADA ofrecen multiples beneficios para la supervisión y el control. Una de sus principales ventajas es la capacidad de centralizar en tiempo real la información proveniente de distintos dispositivos de campo, permitiendo así una gestión de la planta desde una única plataforma. Esto mejora la eficiencia operativa al facilitar la toma de decisiones con base en datos en vivo y tendencias históricas. Además, los sistemas SCADA permiten una visualización gráfica del proceso, alarmas en tiempo real, análisis de eventos y reportes automáticos, lo cual contribuye a una mejor respuesta ante fallos o situaciones anómalas. También pueden incluir funciones avanzadas como control remoto, registro de datos históricos y generación de reportes personalizados, lo que se traduce en una mejora de la productividad, la trazabilidad. Rockwell Automation, 2015.

Sin embargo, a pesar de sus múltiples beneficios, los sistemas SCADA presentan también ciertas limitaciones y riesgos. Uno de los principales desafíos radica en los altos costos de implementación y mantenimiento, ya que requieren *hardware* especializado, licencias de *software*, infraestructura de red y personal capacitado para su operación. Además, muchos sistemas SCADA tradicionales fueron concebidos para operar en entornos cerrados y seguros, lo que los hace vulnerables si se conectan a redes abiertas o a internet sin las medidas de ciberseguridad adecuadas. Estas debilidades en la protección de datos y accesos representan un riesgo considerable en la actualidad, donde la conectividad es una necesidad. Otro aspecto a considerar es la complejidad para escalar o integrar nuevos dispositivos con

[1] Tomada de Rockwell Automation, 2015.

escasa compatibilidad entre fabricantes. Asimismo, en sistemas centralizados, una falla en el servidor del sistema SCADA puede afectar la supervisión de toda la planta, generando problemas críticos en la continuidad operativa. [Boyes, *et al.*, 2018].

Cabe recalcar que para [Manral, 2020] los sistemas SCADA están evolucionando hacia arquitecturas más abiertas y conectadas, integrando tecnologías de IIoT para responder a los desafíos de interoperabilidad, conectividad. Menciona que, estos sistemas SCADA han ofrecido funciones clave como visualización, alarmas, registro de datos e intervención en tiempo real sobre los procesos, pero su arquitectura cerrada ha limitado históricamente su capacidad de conexión e integración con otros sistemas distribuidos y plataformas digitales. Tambien menciona que el IIoT no pretende reemplazar a estos sistemas, sino potenciarlas mediante la adopción de tecnologías como el *edge computing*, que permite realizar procesamiento de datos local antes de enviarlos a la nube, reduciendo la latencia y el tráfico innecesario sin comprometer el control de los procesos críticos. Una de las virtudes más significativas del IIoT frente a las limitaciones de los sistemas SCADA convencionales es su capacidad para establecer conectividad segura, abierta y escalable mediante protocolos como *MQTT, AMQP, REST, OPC UA*, entre otros. Estos estándares facilitan la integración de dispositivos de diferente fabricantes, promoviendo la transparencia y el analisis de datos en tiempo real.

2.3. Conectividad y seguridad

2.3.1. Comunicaciones remotas seguras

La comunicación remota segura se ha convertido en un componente esencial para el acceso y la supervisión de sistemas distribuidos dentro del paradigma del IIoT. Este tipo de comunicación permite el intercambio de información entre dispositivos, controladores y servidores remotos a través de redes públicas, lo que convierte la seguridad de los datos transmitidos en un aspecto crítico. Para garantizar la confidencialidad, integridad y autenticación de las conexiones, se emplean protocolos de seguridad como las VPN y la Seguridad de la capa de transporte (TLS, por sus siglas en inglés).

De acuerdo con [Nyakomitta, *et al.*, 2020], una VPN establece un canal cifrado ,o túnel, sobre una red pública, generalmente internet, con el propósito de permitir el acceso remoto seguro a una red privada. Este túnel protege los datos frente a interceptaciones o manipulaciones mediante la implementación de algoritmos de cifrado y mecanismos de autenticación mutua entre el cliente y el servidor. En entornos industriales, las VPN se utilizan ampliamente para acceder de forma remota a controladores, sistemas SCADA y dispositivos IIoT, sin comprometer la integridad de la información transmitida. Su uso posibilita que los sistemas de supervisión remotos gestionen equipos, realicen mantenimiento y ejecuten acciones de control sin la necesidad de presencia física.

El establecimiento de una conexión VPN se basa en la creación de un túnel lógico seguro entre dos extremos de comunicación. Este proceso se sustenta en el protocolo *IPsec (Internet Protocol Security)*, el cual garantiza la autenticación de las partes involucradas, la confidencialidad de los datos mediante cifrado y la integridad a través de funciones criptográficas. [Sawalmeh, *et al.*, 2021].

Por otra parte, el protocolo TLS proporciona una capa adicional de seguridad en las comunicaciones industriales al proteger los datos a nivel de transporte. Este protocolo permite establecer canales cifrados mediante autenticación mutua y el uso de claves dinámicas entre los extremos de comunicación. Entre sus principales ventajas destacan la interoperabilidad y compatibilidad con aplicaciones basadas en *HTTP, MQTT* o *Modbus TCP/IP*, lo que facilita su integración en infraestructuras industriales.

Cabe mencionar que este protocolo es empleado por soluciones de VPN basadas en TLS, como *OpenVPN*, para fortalecer la seguridad del canal de comunicación [Badra y Hajjeh, 2006].

La combinación de ambas tecnologías resulta fundamental para garantizar la seguridad en la supervisión remota de procesos industriales. Mientras la VPN establece el túnel cifrado y asegura la conexión punto a punto, el TLS protege la sesión de aplicación y garantiza el cifrado extremo a extremo de los datos transmitidos.Lo anterior permite mantener la disponibilidad, integridad y confidencialidad de la información.

2.3.2. Amenazas comunes en entornos IIoT

Detro de las arquitecturas IIoT a medida que se integran mas sensores, controladores, redes inalámbricas y plataformas en la nube, también se amplía la posibilidad de sufir ciberataques y explotar los puntos potenciales para actividades maliciosas. La seguridad de los sistemas IIoT no solo se limita a proteger la confidencialidad de los datos, sino también a garantizar su integridad, disponibilidad y autenticación.

Para [Cartuche-Calva, 2020] uno de los factores que contribuyen a estas vulnerabilidades es la fragmentación tecnológica de los ecosistemas IIoT, donde se encuentran múltiples dispositivos con capacidades diferentes de seguridad y estándares de comunicación. Esta situación genera brechas que pueden ser explotadas mediante ataques como el secuestro de protocolos, suplantación de dispositivos, intercepción de información, modificación maliciosa de datos o ataques de denegación de servicio distribuido, entre otros.

Tambien menciona que muchas de estas amenazas pueden clasificarse de acuerdo con una taxonomía de activos, considerando tanto los componentes físicos (como dispositivos IIoT y redes de comunicación) como los lógicos (infraestructura, plataformas y servicios). Esta categorización permite analizar el nivel de riesgo e impacto que tiene cada amenaza en las distintas capas, desde el dominio de sensores hasta la capa de aplicación. Así, amenazas como el *malware*, *exploit chains*, ataques dirigidos, *man-in-the-middle* o pérdida de servicio, pueden comprometer seriamente la operación del sistema si no se implementan mecanismos de protección adecuados.

Por otro lado, desde una perspectiva normativa, [Juárez, 2019] señala que los sistemas IIoT enfrentan retos adicionales derivados de la falta de interoperabilidad, la escasez de laboratorios de evaluación acreditados y la insuficiente aplicación de estándares internacionales de ciberseguridad. Además, muchos de los protocolos más utilizados en la industria, como *Modbus* o *DNP3*, fueron desarrollados en una época en la que la ciberseguridad no era una prioridad, lo que los convierte en objetivos vulnerables si no son reforzados con capas adicionales de protección.

El incremento en la sofisticación de los cibertataques, como los casos de *malware* específicamente diseñados para entornos industriales, muestra una evolución preocupante hacia amenazas persistentes dirigidas a sabotear infraestructuras. Este tipo de ataques no solo buscan comprometer los datos, sino que pueden generar consecuencias físicas sobre los procesos industriales, poniendo en riesgo la seguridad de los operadores y la continuidad operativa de las planta [Juárez, 2019].

Ante este panorama, es necesario que los entornos IIoT adopten un enfoque de seguridad integral, que contemple no solo la protección a nivel perimetral, sino también la implementación de arquitecturas seguras desde el diseño, el uso de estándares de cifrado robustos, mecanismos de autenticación fuertes, y la actualización constante de *firmware* y políticas de acceso. Asimismo, se recomienda que se realicen metodologías de análisis de amenazas y vulnerabilidades, así como el uso de herramientas de prueba de penetración y monitoreo de eventos, como parte de una estrategia de gestión de ciberseguridad

proactiva. Es aquí donde entran una de las normas diseñadas para salvaguardar la ciberseguridad de los sistemas industriales, la familia de normas *IEC 62443*.

2.3.3. Normativa de ciberseguridad aplicable *IEC 62443*

La familia de normas *IEC 62443* constituye el marco normativo más completo y reconocido a nivel internacional para garantizar la ciberseguridad en IACS. Desarrollada por la *International Electrotechnical Commission (IEC)* en conjunto con la *International Society of Automation (ISA)*, esta serie de normas ofrece un enfoque basado en el riesgo, para proteger sistemas industriales frente a amenazas cibernéticas durante todo su ciclo de vida. En la Figura 2.2 se muestra el desgloce de las partes que comoponen esta familia de normas [ISA, 2024].

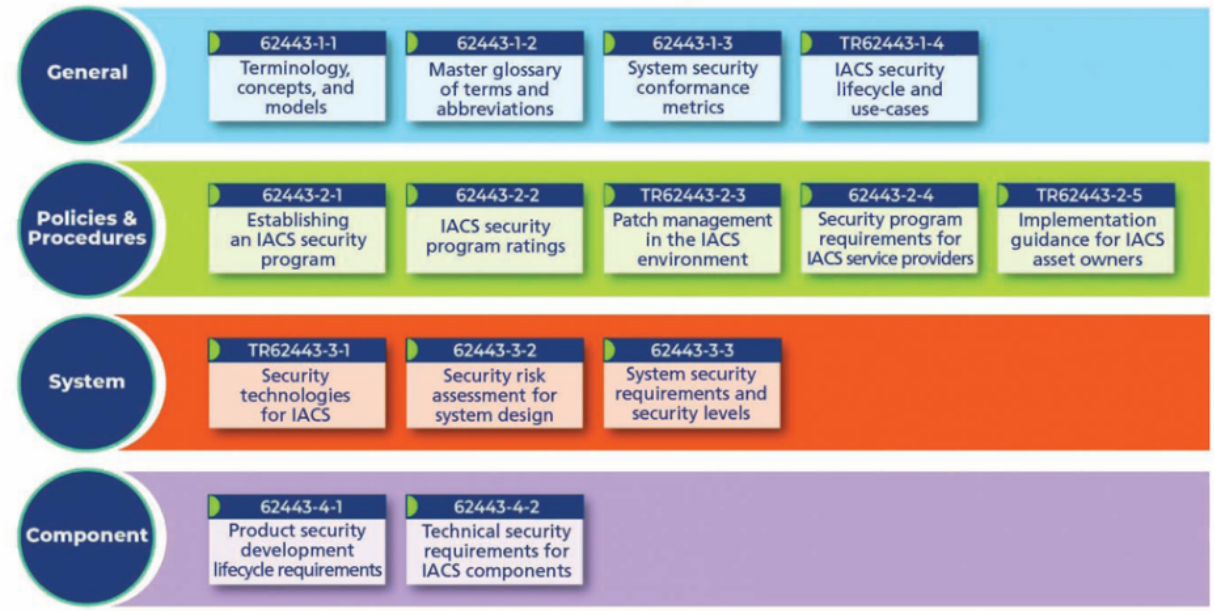

Figura 2.2 Familia de normas *IEC 62443*.[2]

Los IACS presentan requisitos específicos como alta disponibilidad, tiempos de respuesta cortos, largos ciclos de vida y una fuerte dependencia de la operación continua. Por ello, las medidas de seguridad deben adaptarse a sus particularidades técnicas y operativas, es por ello que las normativas de la *IEC 62443* resultan clave.

Según [ISA, 2024] se requieren siete requisitos fundacionales que guían las medidas técnicas a implementar, estas son:

- Control de identificación y autenticación: Se refiere a la necesidad de verificar que todos los usuarios y dispositivos que intentan interactuar con el sistema puedan ser identificados de forma única y autenticados correctamente. Esto incluye la implementación de credenciales, autenticación multifactor o validación de dispositivos mediante certificados digitales, de modo que se impida el acceso no autorizado a los componentes críticos del sistema.

- Control de uso: Establece que, una vez autenticadas los usuarios, su actividad dentro del sistema debe estar restringida conforme a sus permisos. Este principio, conocido como “mínimo privilegio”,

[2]Tomada de [ISA, 2024].

garantiza que cada usuario o dispositivo solo pueda ejecutar las acciones necesarias para su función específica. De esta manera, se evita que un operador o componente mal configurado acceda o modifique funciones ajenas a su perfil.

- Integridad del sistema: Tiene como objetivo proteger la consistencia y correcto funcionamiento del sistema frente a alteraciones no autorizadas o accidentales. Esto se logra mediante mecanismos como firmas digitales, verificación de integridad de archivos, y monitoreo de cambios en configuraciones, *firmware* o *software*, asegurando que los componentes operen conforme al diseño original.
- Confidencialidad de los datos: Busca evitar la exposición de información sensible a personas o sistemas no autorizados. Para ello, se recurre a técnicas de cifrado de datos, además de controles de acceso a registros, credenciales, parámetros de configuración y cualquier información crítica que circule por la red.
- Flujo de datos restringido: Establece la necesidad de controlar y limitar las rutas de comunicación entre dispositivos o zonas del sistema, de forma que solo los canales estrictamente necesarios estén habilitados. Esto se traduce en una segmentación de la red mediante zonas, además de la implementación de *firewalls* industriales y para permitir únicamente comunicaciones autorizadas.
- Respuesta oportuna a eventos: Está enfocado en garantizar que el sistema cuente con capacidades adecuadas para detectar, registrar y responder a incidentes de seguridad. Esto implica la generación de alertas en caso de eventos anómalos, el registro de intentos de acceso fallidos o cambios en parámetros críticos, así como la habilitación de respuestas automáticas ante ciertos tipos de amenazas.
- Disponibilidad de recursos: Busca asegurar que los recursos necesarios para el funcionamiento continuo del sistema estén siempre disponibles, incluso frente a ataques como denegaciones de servicio o sobrecargas. Este requisito incluye prácticas como el monitoreo del uso de recursos, la redundancia de componentes y la tolerancia a fallos, lo cual es esencial en sistemas donde la disponibilidad es un requerimiento clave.

2.4. Analítica y contextualización de datos

Ahora bien, el verdadero valor de los datos industriales no radica únicamente en su recopilación, sino en la capacidad de interpretarlos y convertirlos en información accionable. A través del análisis de tendencias, la detección de patrones y la identificación de comportamientos no evidentes a simple vista, es posible obtener una comprensión más profunda del estado operativo de los procesos. Con este propósito, surgen las métricas e indicadores que permiten contextualizar los datos y traducirlos en elementos útiles para la toma de decisiones informadas. Estos indicadores, conocidos como KPI, constituyen una herramienta fundamental para evaluar el desempeño de los sistemas y orientar estrategias de mejora continua dentro de la industria.

2.4.1. Indicadores de desempeño

Desde un enfoque teórico, los KPI son métricas cuantificables diseñadas para evaluar el grado de cumplimiento de objetivos estratégicos, operacionales o de mejora continua en entornos productivos.

Su implementación en sistemas automatizados permite vincular datos de operación con modelos de desempeño, proporcionando así una base para la toma de decisiones, la planificación de recursos y la optimización de procesos [Tumbajoy, *et al.*, 2022].

La utilidad de los KPI reside en su capacidad para transformar datos técnicos provenientes de sensores, controladores o plataformas de supervisión, en información comprensible y accionable. Esto requiere de una correcta definición conceptual y funcional de los indicadores, así como una estructura lógica que permita contestar el qué se mide, cómo se mide, con qué frecuencia y qué acción se deriva de su comportamiento. Según [Gusnadi y Hermawan, 2019], un KPI no puede considerarse válido si no está alineado con los objetivos del sistema, es decir, si no refleja con precisión el rendimiento de una variable clave del proceso o del negocio.

En los IACS, los indicadores más utilizados suelen estar ligados a la productividad, la eficiencia del equipo, la calidad del producto, el tiempo de inactividad, el consumo energético y la tasa de errores, entre otros.

Uno de los indicadores más representativos en entornos de manufactura es el OEE, el cual resume tres parametros críticos del rendimiento de un sistema: la disponibilidad (proporción de tiempo efectivo frente al tiempo planificado), el rendimiento y la calidad (proporción de productos conformes frente al total fabricado). El OEE opera como un modelo de eficiencia, al integrar múltiples factores operativos en un solo indicador, que permite comparar distintos procesos, líneas de producción o condiciones de operación [Tumbajoy, *et al.*, 2022].

Además, [Gusnadi y Hermawan, 2019] señala que la generación de KPI debe considerar no solo la instrumentación y adquisición de datos, sino también su representación visual e interpretación por parte de los usuarios. En ese sentido, los *dashboards* juegan un papel esencial como interfaz de traducción entre el dato técnico y la decisión operativa.

2.4.2. Dashboards

Los *dashboards* son herramientas visuales que permiten centralizar, agrupar y presentar de forma gráfica información relevante sobre el desempeño de una organización, facilitando así la toma de decisiones basadas en datos. Su implementación responde a la necesidad de interpretar grandes volúmenes de datos generados en tiempo real por los IACS, sensores y plataformas IIoT.

Su diseño está orientado a ofrecer una visualización clara, comprensible e inmediata de los KPI, permitiendo a los usuarios identificar rápidamente desviaciones, tendencias o comportamientos anómalos en los procesos monitoreados [Gusnadi y Hermawan, 2019].

Para que un *dashboard* cumpla adecuadamente su función, debe presentar datos actualizados de manera continua, integrar diferentes fuentes de información y ser fácilmente interpretable para usuarios sin conocimientos técnicos avanzados. Esto implica no solo un diseño visual atractivo, sino una estructura lógica que facilite la navegación, el análisis y la acción informada. Según [Córdova Viera, *et al.*, 2021], un *dashboard* bien estructurado debe aprovechar la percepción visual para condensar información compleja en un espacio reducido, organizando los datos en paneles, gráficos o mapas que se correspondan con los objetivos del sistema supervisado.

El uso de los *dashboards* permite mejorar significativamente la capacidad de monitoreo continuo, evaluar la evolución de los procesos y obtener una visión de los indicadores críticos. Esta visualización en tiempo real facilita el seguimiento del rendimiento operativo, la identificación de cuellos de botella, la priorización de acciones correctivas y la alineación entre los niveles operativos y estratégicos [Gusnadi y Hermawan, 2019].

Además, los *dashboards* actuales incorporan funcionalidades avanzadas como filtrado dinámico de datos, generación automática de reportes, configuración de umbrales, alertas visuales y notificaciones automatizadas.

La correcta implementación de *dashboards* implica también la atención a aspectos de seguridad, tales como la gestión de accesos por roles, la protección de datos mediante protocolos seguros y la creación de respaldos periódicos. En entornos industriales conectados, estas precauciones son especialmente relevantes debido a la exposición potencial a amenazas cibernéticas como se menciono anteriormente.

Capítulo 3

Descripción General del Sistema Propuesto

En este capítulo se hace uso de la teoría recabada en el Capítulo 2 para desarrollar y obtener el sistema que permitirá la implementación del sistema de supervisón remota mediante tecnologías IIoT en procesos industriales.

3.1. Estructura general del sistema IIoT

La arquitectura de supervisión y acceso remoto fue diseñada considerando criterios de escalabilidad y ciberseguridad, anticipando la posible incorporación de nuevos dispositivos o procesos industriales en el futuro.

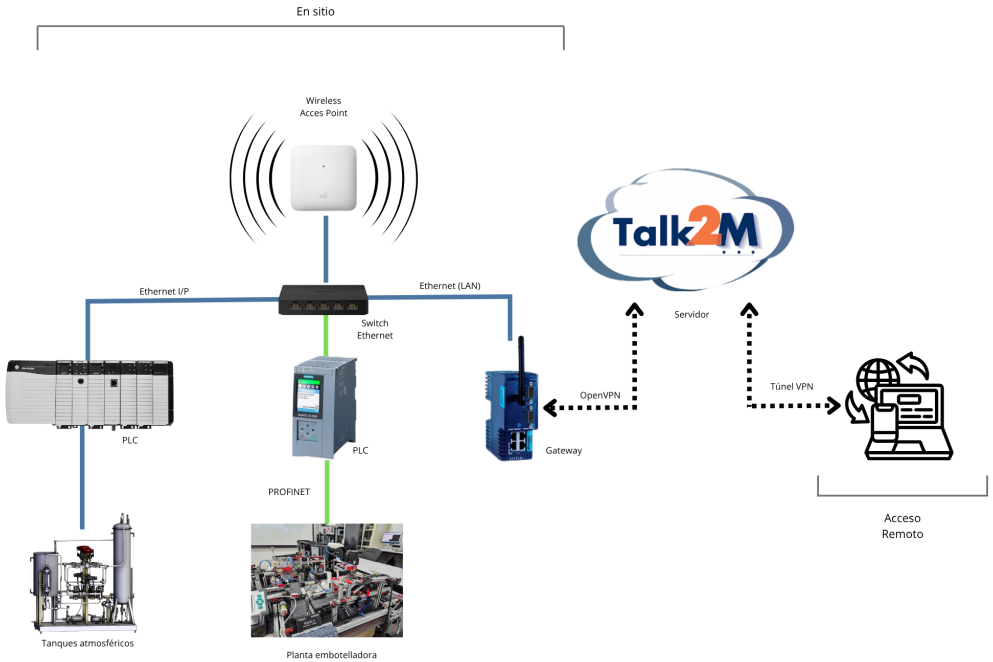

Figura 3.1 Arquitectura propuesta.

El sistema propuesto incorpora una arquitectura de control distribuido basada en dos PLC de diferentes fabricantes, cada uno con su protocolo de comunicación específico. Por un lado, se implementó un *ControlLogix L81E* de *Rockwell Automation*, que utiliza el protocolo *EtherNet/IP* para su comunicación industrial. Por otro, se incluyó un *S7-1500* de *Siemens*, el cual opera bajo el estándar *PROFINET*. Esta configuración dual permite aprovechar las ventajas particulares de cada fabricante para manejar los procesos. Como elemento integrador de la comunicación, el sistema emplea el *gateway Flexy 205* de la empresa *HMS Networks*. Este dispositivo actúa como nodo central para la adquisición de datos, el monitoreo en tiempo real y el acceso remoto seguro.

Para garantizar la seguridad en las comunicaciones remotas, el *Flexy 205* se configuró para establecer túneles VPN cifrados mediante el protocolo *OpenVPN*, conectándose de forma segura al servidor *Talk2M*. Esta implementación permite el acceso remoto autorizado desde cualquier ubicación, manteniendo los estándares de protección de datos industriales. La solución también ofrece escalabilidad para futuras ampliaciones del sistema, asegurando su adaptabilidad a necesidades emergentes. La arquitectura descrita se muestra en la Figura 3.1.

3.1.1. Procesos industriales involucrados

Para el desarrollo del sistema, se implementarán dos casos de estudio, un procesos de tanques atmosféricos interconectados y una proceso de embotellado.

- Sistema de tanques atmosféricos:

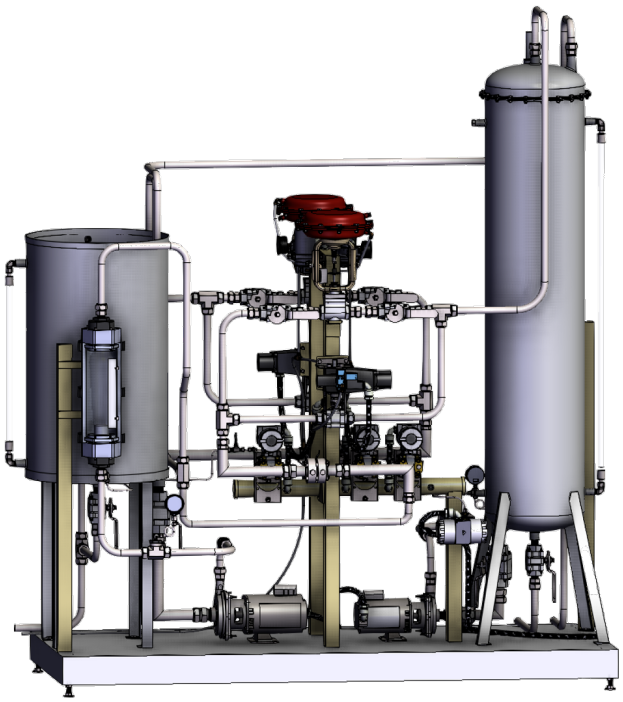

Figura 3.2 Tanques atmosféricos interconectados.

Este proceso consiste en un conjunto de tanques, cuyo objetivo principal es mantener un nivel de llenado mediante un controlador PID. Este proceso incorpora actuadores como electroválvulas, válvulas de control, bombas centrífugas y sensores de nivel, para operar de manera automática. La imagen del proceso se muestra en la Figura 3.2.

Para lograr el funcionamiento de este proceso, se desarrolló la rutina de control dentro del PLC *ControlLogix L81E*, siguiendo el estándar *IEC 61131-3*. La programación implementada hace uso dos válvulas de control neumáticas tipo diafragma, encargadas de regular el flujo a través de las tuberías del sistema. Dicho flujo es supervisado mediante indicadores de presión diferencial, los cuales también permiten conocer el nivel de líquido dentro de los tanques atmosféricos. Además, se integraron dos variadores de frecuencia responsables de controlar las bombas que impulsan el fluido en el sistema. El sistema de control incorpora el protocolo de comunicación *ControlNet* para establecer conexión con módulos de periferia descentralizada, los cuales accionan actuadores, como las electroválvulas utilizadas para introducir perturbaciones en las variables controladas y así evaluar el desempeño de la estrategia de control implementada. El digrama del sistema de control de los tanques atmosféricos se muestra en la Figura 3.3.

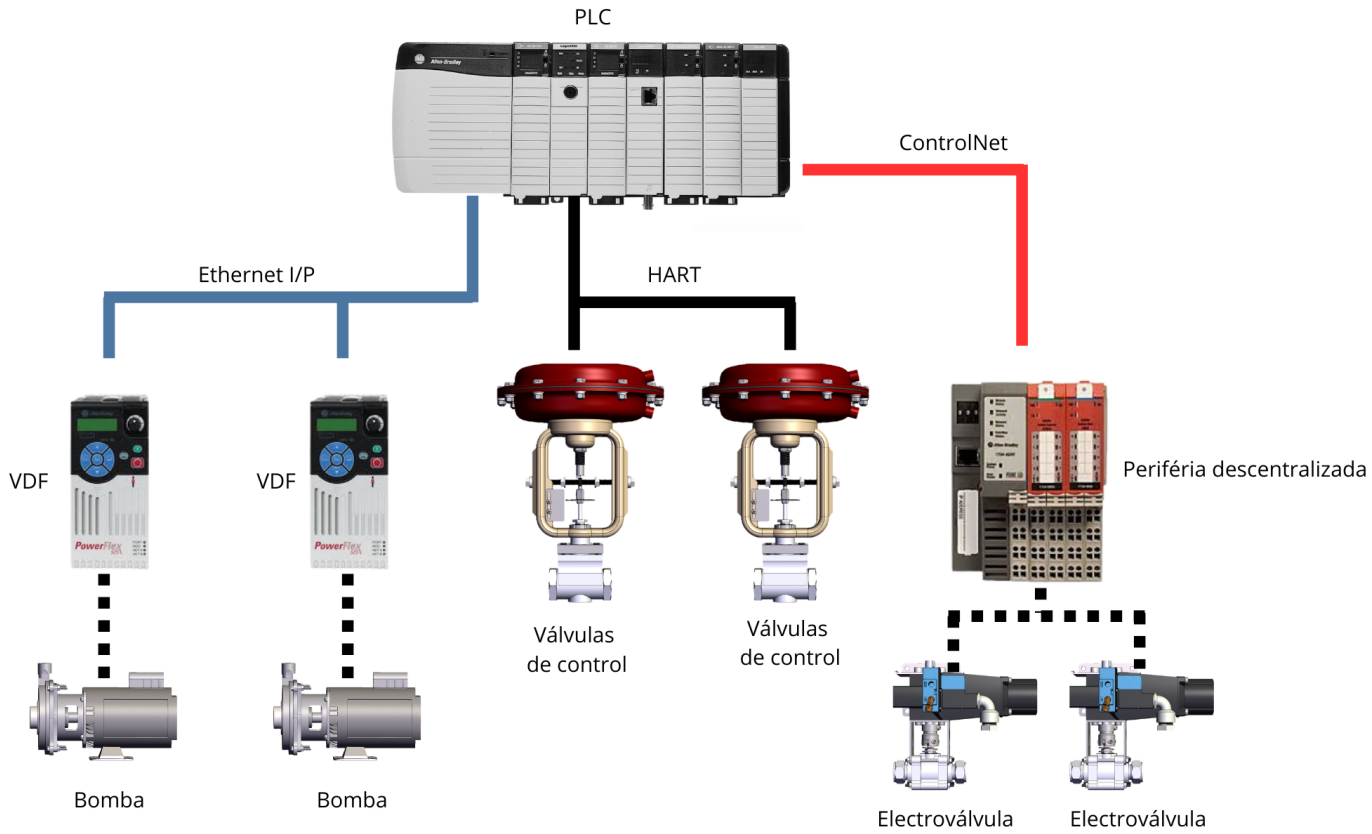

Figura 3.3 Sistema de control de tanques atmosféricos.

- Planta embotelladora: El módulo de reciclaje constituye la última etapa dentro del sistema automatizado de embotellado, encargado de recuperar y reintegrar las botellas al ciclo de producción. Su funcionamiento inicia cuando una caja con cuatro botellas llenas llega a la base de recepción. El brazo robótico toma la caja y la coloca sobre la banda transportadora superior, que la conduce hacia la zona de vaciado, donde un pistón neumático simula el proceso

de descarga. Posteriormente, el empaque llega a la estación de reciclaje, donde el robot retira las botellas y las deposita en una banda lateral que las devuelve al primer módulo, mientras la caja vacía regresa a su posición inicial, completando así el ciclo.En la Figura 3.4 se muestra una fotografía del proceso descrito.

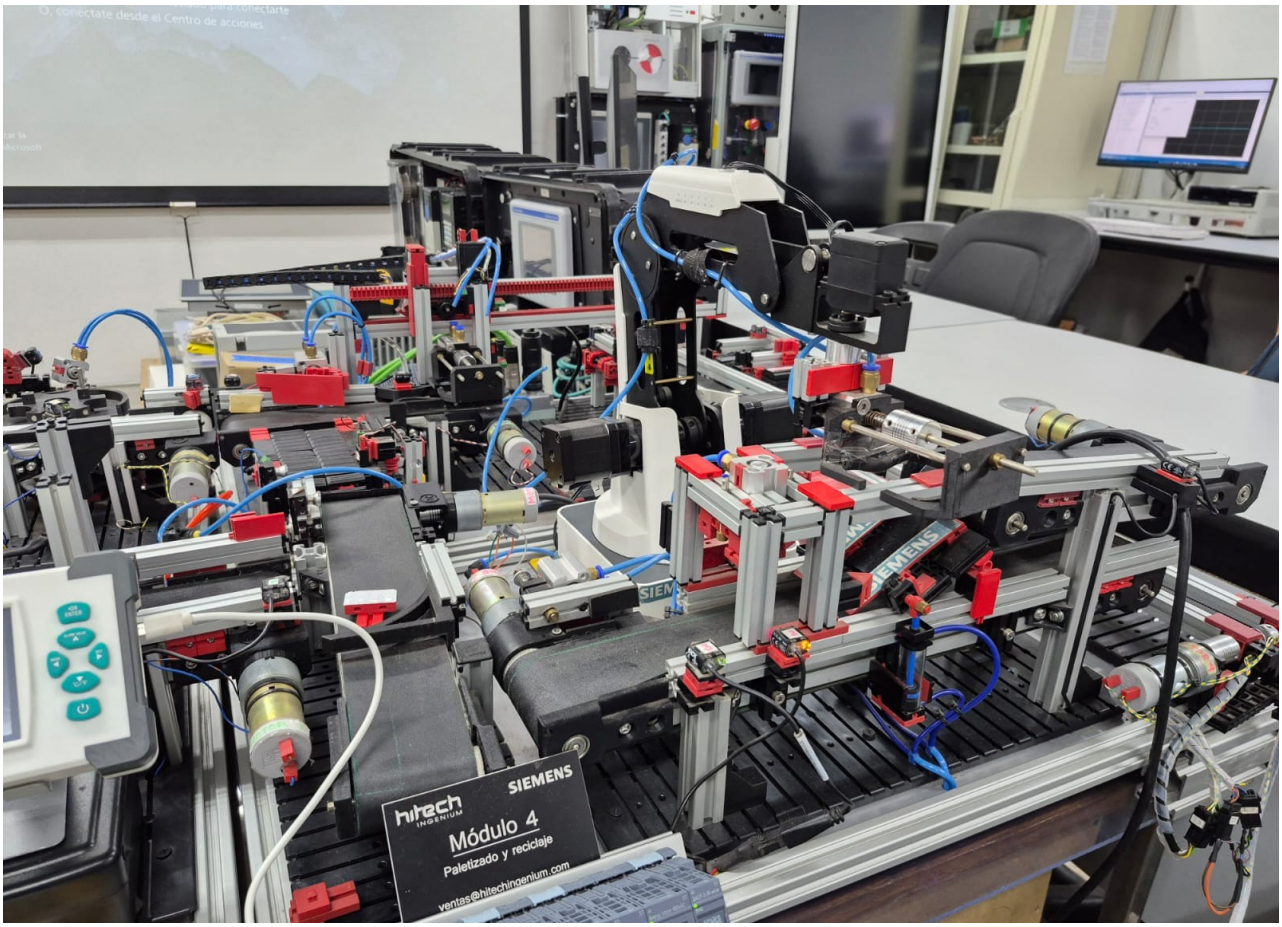

Figura 3.4 Planta embotelladora

El control del proceso se implementó en un PLC *S7-1500*, bajo el estándar *IEC 61131-3*, utilizando el protocolo *PROFINET* para la comunicación con la periferia descentralizada. Esta gestiona los sensores, electroválvulas, pistones neumáticos y controladores de motor *DC*, además de un *gateway* que permite la comunicación con el brazo robótico mediante interfaces *I2C* y *RS-232*. La arquitectura del sistema de control del módulo de reciclaje se muestra en la Figura 3.5, donde se ilustran los componentes principales y su interconexión.

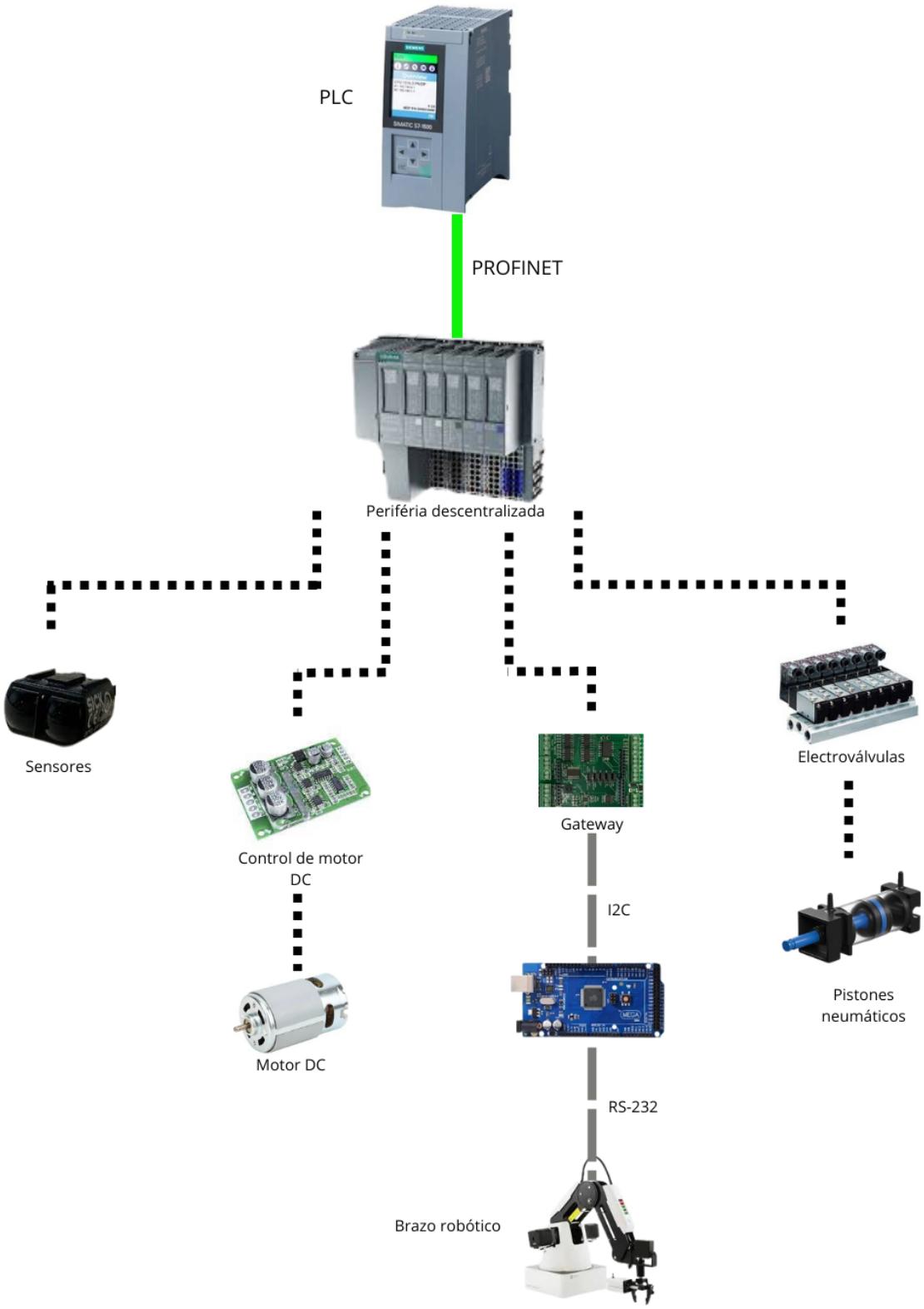

Figura 3.5 Sistema de control de planta embotelladora.

3.2. Integración de equipos y arquitectura de red

3.2.1. Integración del ControlLogix L81E y S7-1500

Esta integración tiene como objetivo centralizar la información de los procesos, independientemente de la plataforma de control empleada, en un entorno único de supervisión gestionado por el módulo *Flexy 205*.

En el caso del *ControlLogix L81E*, la comunicación se establece mediante el protocolo *EtherNet/IP*, a través del cual se transmiten variables críticas relacionadas con la disponibilidad, calidad y rendimiento de los tanques atmosféricos. Los Tags se corresponden directamente con la programación del PLC, lo que facilita la trazabilidad de los datos y su vinculación con el control.

Por otro lado, el *S7-1500* se integra mediante el protocolo *PROFINET*, utilizando direcciones de memoria específicas que permiten la extracción de datos de la planta embotelladora. Entre las variables monitoreadas se incluyen el rendimiento del proceso, el número de paros totales, así como medidas asociadas a la calidad y disponibilidad. El uso de direcciones explícitas de memoria en este caso asegura una asignación clara de las variables en el entorno de supervisión.

Ambos controladores convergen en el módulo *Flexy 205*, que actúa como pasarela de datos y nodo de seguridad. Una vez normalizada la información, esta se visualiza en *dashboards* desarrollados en el *software ViewON*, donde se unifican los indicadores de ambos procesos en una sola plataforma. De esta forma, se logra una integración que permite a los operadores monitorear el estado global de la planta sin importar la procedencia de los datos ni las diferencias entre fabricantes.

3.3. Configuración del módulo de comunicación IIoT

3.3.1. Configuración del modúlo *Flexy 205*

Para llevar a cabo una configuración segura del módulo IIoT, se emplea el software *eCatcher*, desarrollado por *HMS Networks* como parte del servidor *Talk2M*. Este programa permite establecer una conexión segura entre una cuenta de usuario autorizada y el dispositivo *gateway Flexy 205*, mediante túneles VPN cifrados. Durante el proceso de vinculación, es fundamental autenticar la identidad del usuario y registrar correctamente el equipo para evitar accesos no autorizados.

Adicionalmente, dentro de *eCatcher* se procede a la modificación de los parámetros predeterminados de fábrica, como el nombre del equipo y su dirección IP local, con el fin de adaptarlos al entorno de red específico y mejorar la trazabilidad dentro del sistema. En este caso, el dispositivo fue renombrado como "*Lab. Automatización*" y configurado con la dirección IP estática 192.168.1.182. La vista general de *eCathcer* se muestra en la Figura 3.6.

Una vez asignada la dirección IP al dispositivo, es posible acceder a su interfaz web local a través de un navegador, lo cual permite completar la configuración inicial del *gateway*. En esta etapa, se definen parámetros generales como la zona horaria, el idioma de la interfaz y la asignación de roles a los puertos de red disponibles, según el esquema de red definido para la planta en la que se configure.

Un aspecto fundamental durante esta fase es establecer la conexión del módulo *Flexy 205* a internet mediante la red *Wi-Fi* local, lo cual habilita sus funciones de comunicación remota a través del servicio del servidor de *Talk2M*. La Figura 3.7 muestra la vista general de la configuración del dispositivo una vez finalizada esta etapa.

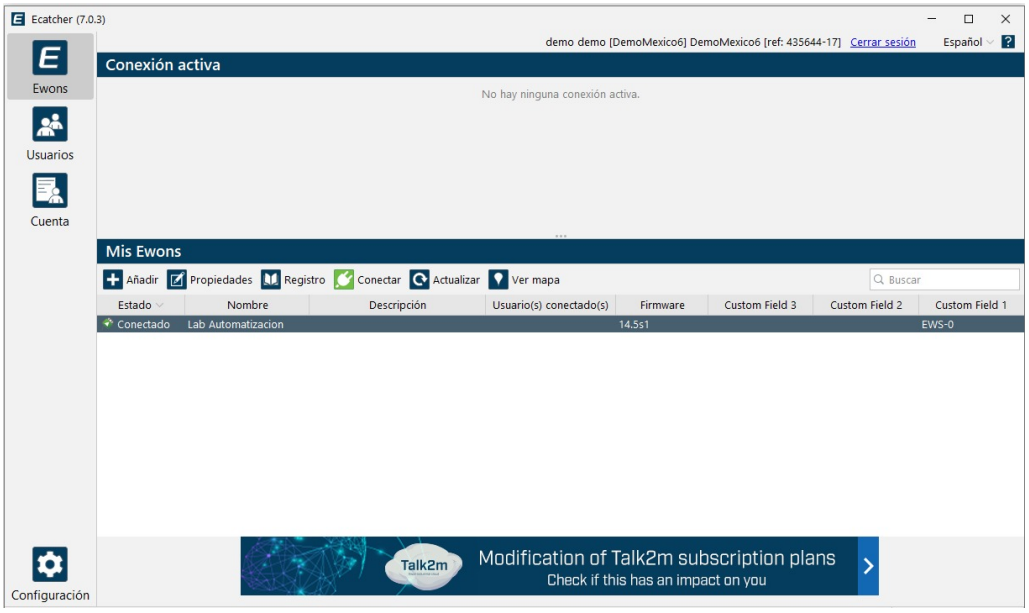

Figura 3.6 Herramienta *eChatcher*.

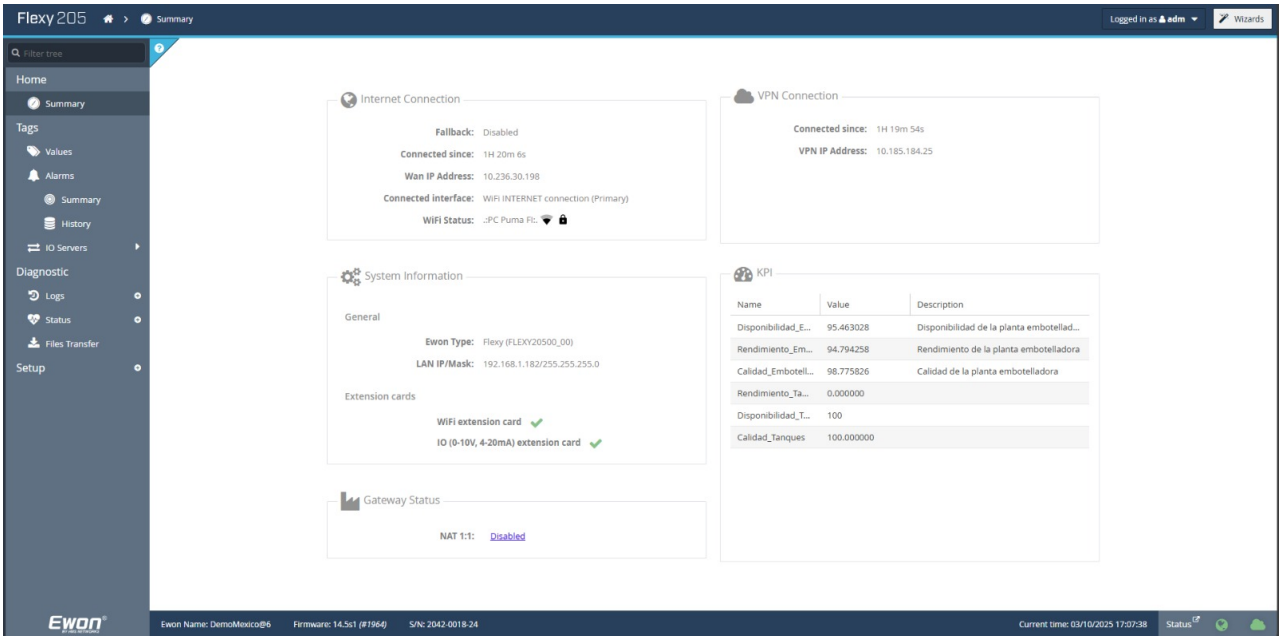

Figura 3.7 Vista general del *Flexy 205*.

3.3.2. Configuración de la adquisición de tags desde los PLC

Para establecer la vinculación entre los PLC y el módulo IIoT *Flexy 205*, es indispensable que ambos dispositivos se encuentren dentro del mismo segmento de red local, lo que permite una comunicación directa entre ellos. Posteriormente, en la aplicación *eCatcher*, se debe registrar la dirección IP del PLC junto con una etiqueta identificadora que facilite su gestión remota.

En este caso de estudio, se realizó la integración del PLC *Siemens S7-1500*, asignándole la dirección IP 192.168.1.95. Esta configuración, que permite al *gateway* reconocer y comunicarse con el controlador, como se muestra en la Figura 3.8.

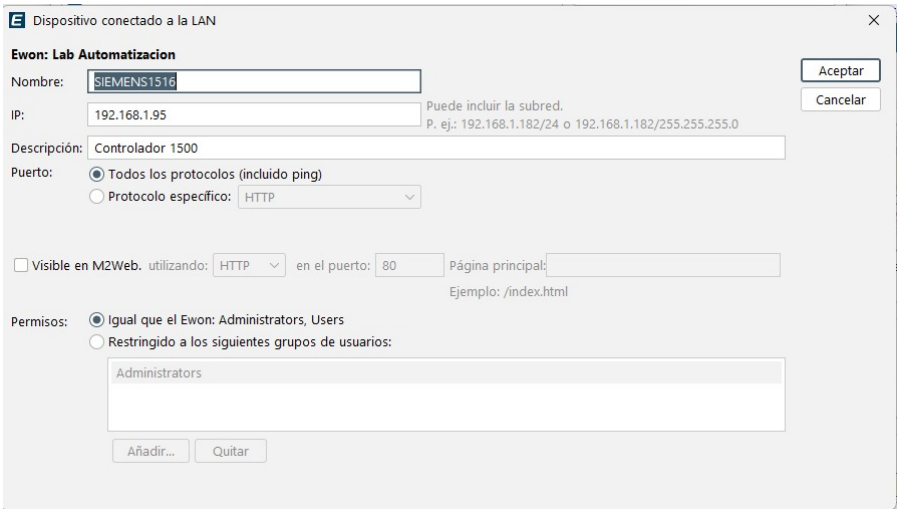

Figura 3.8 Alta PLC con el módulo IIoT.

Una vez realizada la vinculación con el primer PLC, estos pasos deben repetirse para establecer la comunicación con el segundo controlador, en este caso, el *ControlLogix L81E*, el cual se encuentra configurado con la dirección IP: 192.168.1.24. Es fundamental asegurarse de que este equipo también esté dentro del mismo segmento de red que el módulo IIoT, a fin de garantizar la correcta detección y transmisión de datos entre dispositivos.

De la misma fomrma que la para el PLC anterior, en la plataforma *eCatcher*, se registra esta dirección IP, asignándole una etiqueta dentro de la red virtual privada creada por el servidor *Talk2M*.

La vista general de los PLC vinculados al *gateway Flexy 205*, ya configurados dentro del entorno del sistema IIoT, se presenta en la Figura 3.9. Esta imagen resume la conectividad establecida entre el módulo y los diferentes controladores industriales, lo cual constituye la base para la supervisión unificada de los procesos físicos implementados.

Con la configuración previamente establecida, es posible habilitar la conexión remota entre el usuario y los PLC vinculados al módulo *gateway*. No obstante, para realizar el monitoreo específico de Tags, es necesario dar de alta los servidores de comunicación correspondientes dentro de la interfaz web local del *Flexy 205*, específicamente en el apartado denominado "*IO Servers*".

La configuración de estos servidores depende de la familia del PLC con la que se pretende establecer la comunicación. En el caso del controlador *S7-1500*, se debe habilitar un servidor dentro de la pestaña*S73/400*. Para este procedimiento, es indispensable especificar en el campo "*Global Device Address*" el protocolo de comunicación correspondiente, que en este caso es *ISOTCP*, seguido de la

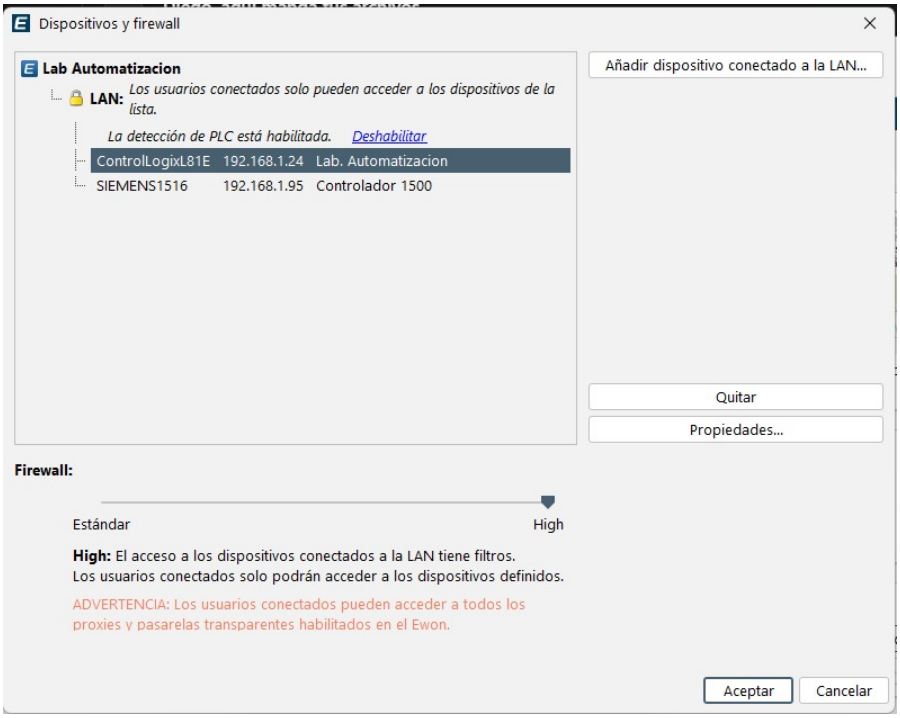

Figura 3.9 Vinculación de dipositivos con el módulo IIoT.

dirección IP del equipo. Además, se deben establecer parámetros técnicos adicionales como el modelo exacto del PLC, la ubicación del *rack* y la *slot* en la que se encuentra la *CPU* dentro del sistema.

Un parámetro clave en esta configuración es la casilla "*Poll Rate*", en la cual se define la frecuencia con la que el *Flexy 205* consultará los Tags del PLC para actualizar sus valores en tiempo real. Esta tasa de muestreo debe ser definida de acuerdo con los requerimientos del sistema y la relevancia de las variables a supervisar.

Esta configuración es esencial para que, posteriormente, se pueda realizar la correcta dirección y lectura de los Tags deseados mediante herramientas de monitoreo remoto. En la Figura 3.10 se presenta la configuración establecida para el servidor responsable de adquirir las variables del modelo de la planta embotelladora. Por otro lado, en la Figura 3.11 se muestran las características del servidor configurado para obtener los datos provenientes del proceso de tanques atmosféricos.

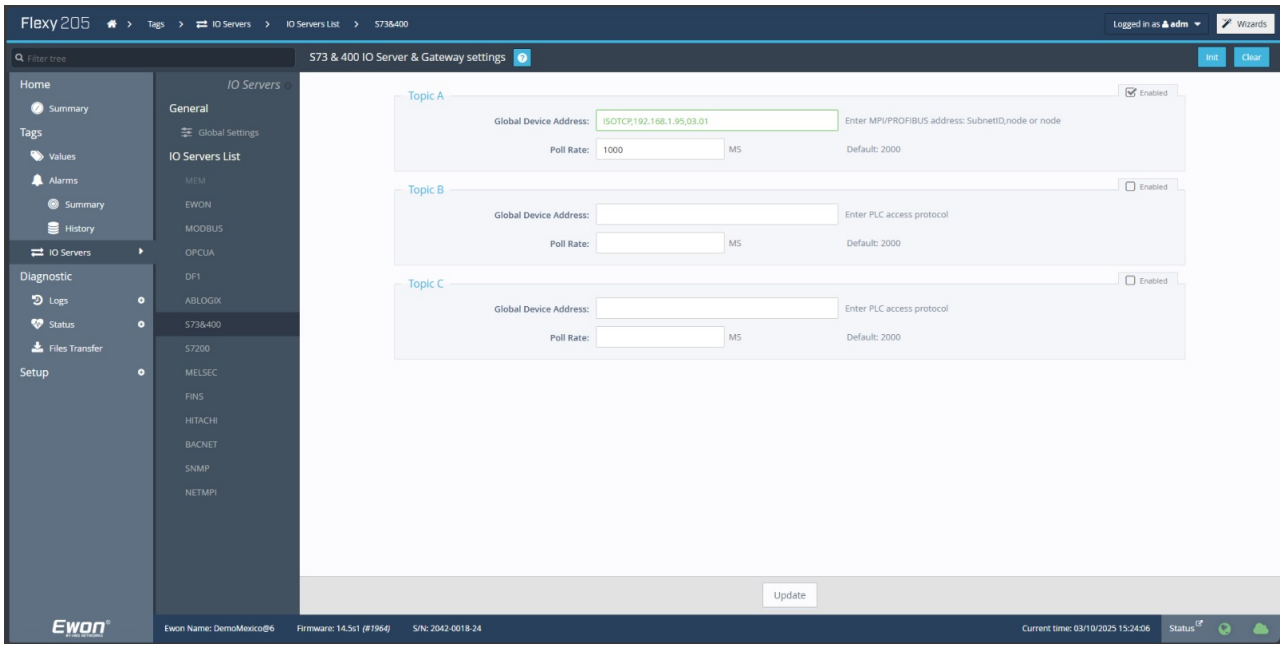

Figura 3.10 Configuración del servidor para el PLC *S7-1500*.

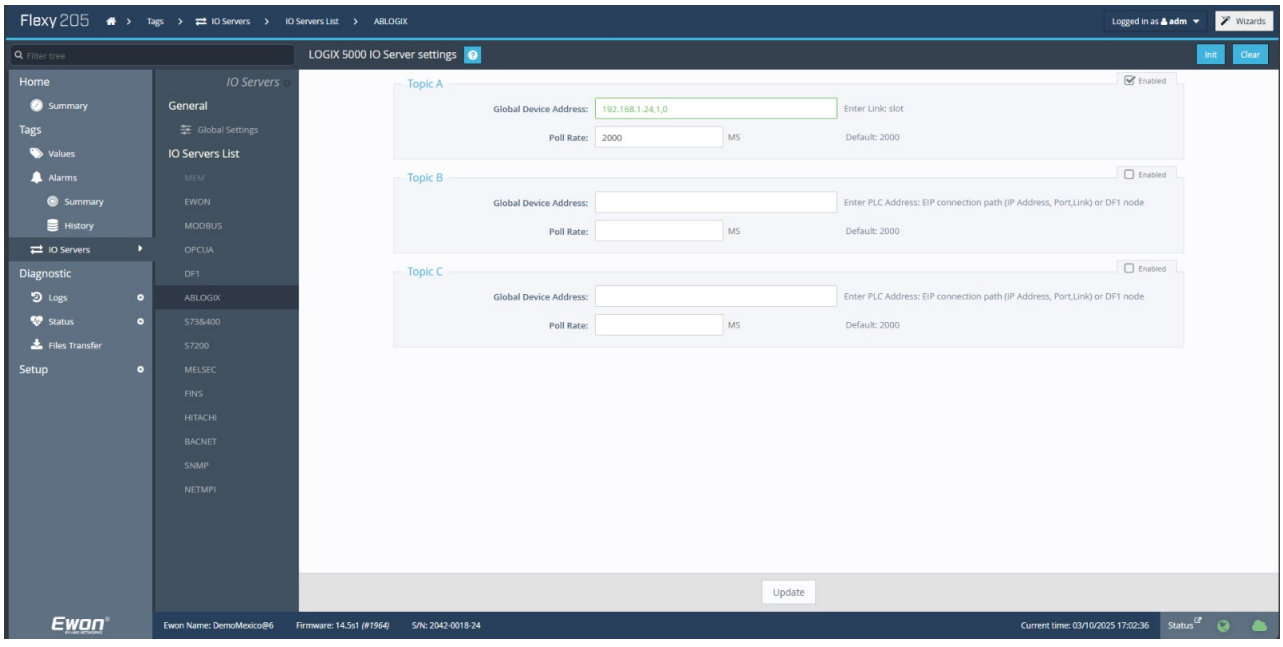

Figura 3.11 Configuración del servidor para el PLC *ControlLogix L81E*.

Una vez habilitados los servidores desde los cuales se obtendrán los Tags a supervisar, es necesario dirigirse a la sección "*Values*" dentro de la interfaz web del módulo*Flexy 205*, donde se lleva a cabo la configuración individual de cada Tags. En esta sección se asignan atributos importantes como el nombre, la descripción del Tags y el grupo al que pertenece, lo cual permite mantener una estructura organizada especialmente útil en sistemas con múltiples variables.

Además del nombre y la descripción, se debe indicar el servidor desde el cual se obtendrán los valores de los Tags. Gracias a la configuración previa en la sección "*IO Servers*", basta con seleccionar de una lista desplegable el servidor correspondiente, cuyas características ya han sido definidas.

El aspecto más relevante de esta sección es la asignación correcta de la dirección de memoria que corresponde al valor que se desea monitorear. Esta dirección debe coincidir con la ubicación exacta dentro del espacio de memoria del PLC. Es importante recalcar que cada familia de controladores industriales maneja esquemas distintos de direccionamiento, los cuales dependen tanto del tipo de dato, como del segmento de memoria donde esté almacenado.

La configuración de esta etapa asegura que los valores monitoreados sean representaciones fieles del estado real de los procesos industriales. La vista general de la configuración de los Tags para el caso del PLC *S7-1500* se muestra en la Figura 3.12.

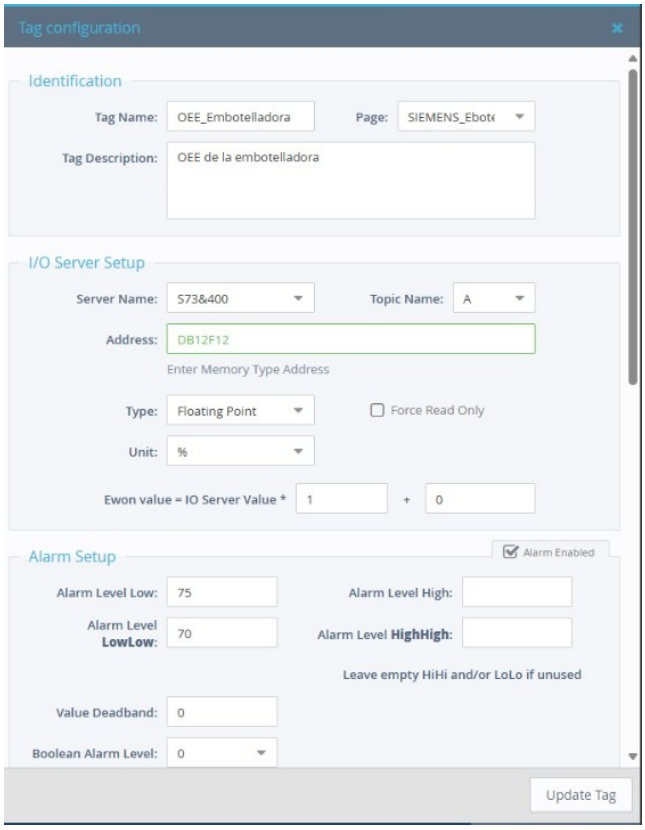

Figura 3.12 Configuración de Tags para el PLC *S7-1500*.

Para este caso de estudio se seleccionaron variables representativas del proceso para su monitoreo, tales como los Tags asociados al rendimiento, la disponibilidad de la planta, la calidad del proceso y los paros totales. Estos valores son fundamentales para el cálculo del OEE de la planta embotelladora, ya que proporcionan una visión integral sobre el estado operativo general del sistema.

Con el fin de mantener una mejor organización y claridad en el análisis, los Tags correspondientes a cada sistema fueron agrupados en pestañas específicas dentro de la interfaz del *Flexy 205*, denominadas "SIEMENS Embotelladora" y "ControlLogix Tanques". En la Figura 3.13 se muestra la vista general de estas variables, donde es posible observar, además del valor actual de los Tags, el estado o status de cada variable, el servidor al que está vinculados y la dirección de memoria correspondiente en el caso de los controladores *Siemens*.

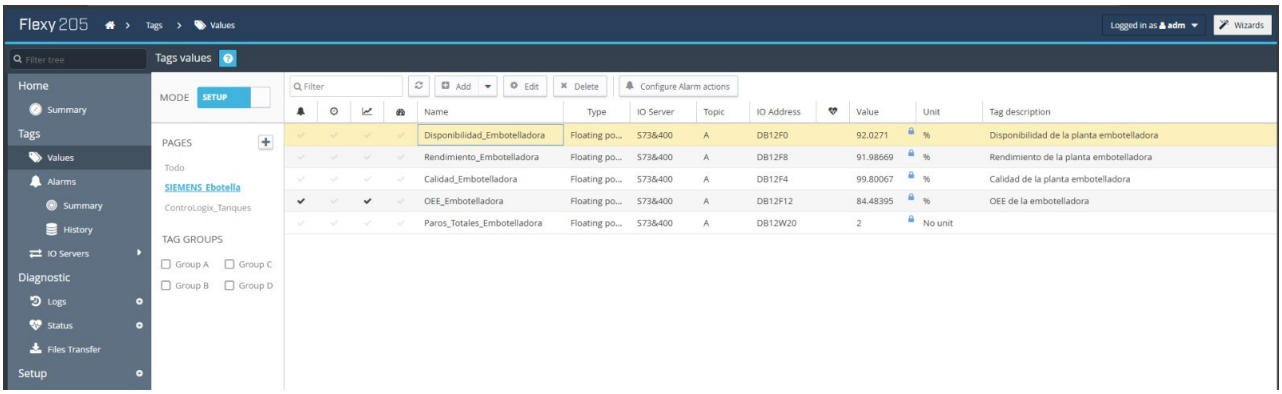

Figura 3.13 Tags monitoreados para el PLC *S7-1500*.

En el caso de los Tags provenientes del proceso de tanques atmosféricos, la ubicación de memoria se asigna directamente utilizando el nombre exacto con el que la variable fue declarada dentro del programa del PLC *ControlLogix L81E*. Este método de direccionamiento facilita la vinculación cuando se utilizan entornos de programación estructurados que permiten nombrar explícitamente cada variable del proceso.

Al igual que en el proceso de la planta embotelladora, se seleccionaron para su monitoreo los Tags más representativos del comportamiento del sistema, específicamente aquellos relacionados con la disponibilidad, calidad y rendimiento del proceso. Estos indicadores son esenciales para el análisis del desempeño de los tanques atmosféricos.

En la Figura 3.14 se presentan los Tags monitoreados correspondientes al proceso de tanques atmosféricos, donde es posible observar tanto los nombres de las variables como su estado actual y el servidor desde el cual se obtienen.

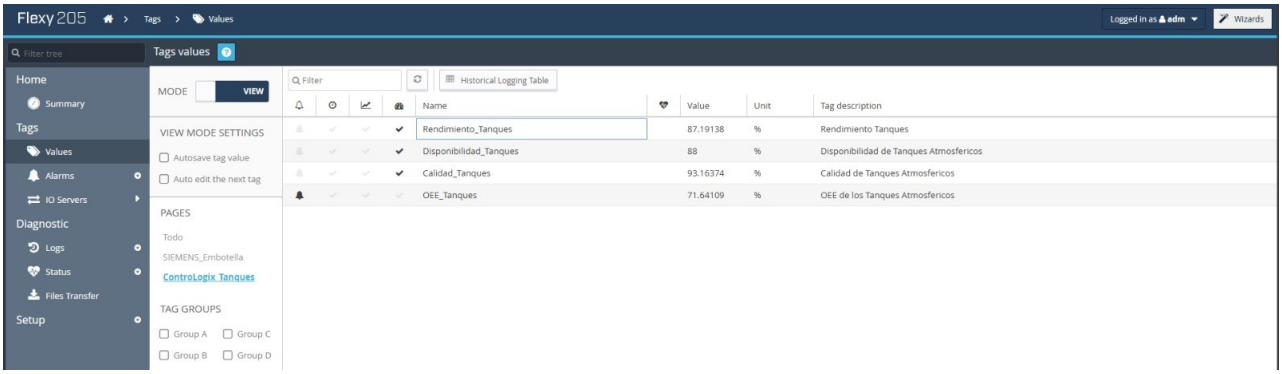

Figura 3.14 Tags monitoreados para el PLC *ControlLogix L81E*.

3.3.3. Alertas y notificaciones

El sistema de alertas y notificaciones es una parte esencial dentro de cualquier arquitectura de supervisión, ya que permite detectar eventos anómalos o condiciones críticas en tiempo real, facilitando una respuesta inmediata que prevenga daños, detenciones no planificadas o pérdida de calidad en el proceso. En el módulo IIoT *Flexy 205*, estas funcionalidades se implementan a través de la configuración de alarmas asociadas a los Tags, permitiendo no solo la visualización de eventos, sino también el envío automático de notificaciones a los usuarios autorizados.

A través de la interfaz local del equipo, dentro de la sección "*Tags*", es posible establecer condiciones de activación para cada variable mediante el ajuste de umbrales mínimos y máximos. Cuando una variable monitoreada excede los límites definidos, se dispara una alarma, la cual queda registrada dentro del sistema y puede ser configurada para enviar notificaciones automáticas por correo electrónico, utilizando el servicio "*Talk2M Mail Relay*".

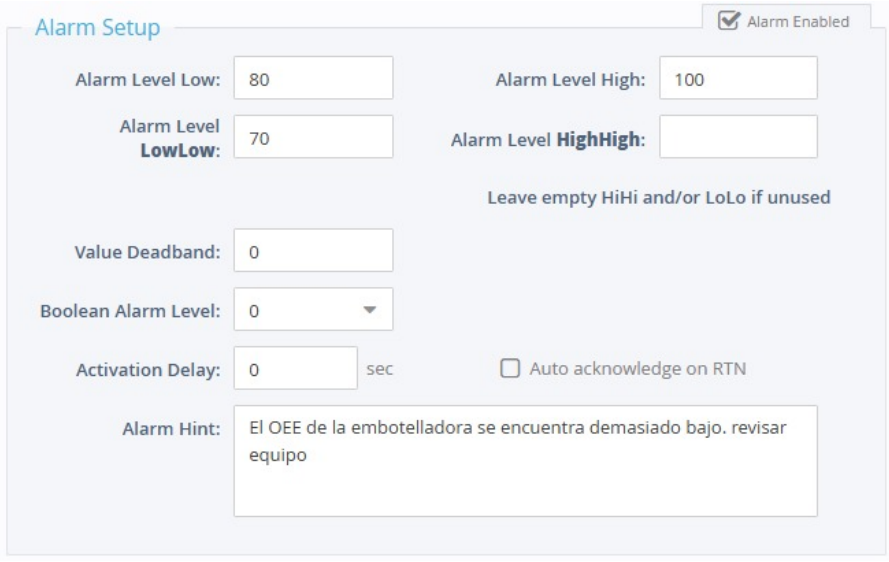

Figura 3.15 Configuración de alarma.

La Figura 3.15 muestra un ejemplo de esta configuración, donde se observa la activación de alarmas en función de valores específicos de proceso. Posteriormente, la Figura 3.16 se muestra un ejemplo real de notificación por correo electrónico generada automáticamente ante la detección de una condición

anómala de bajo nivel, incluyendo información como el nombre del Tags afectado y la hora exacta del evento.

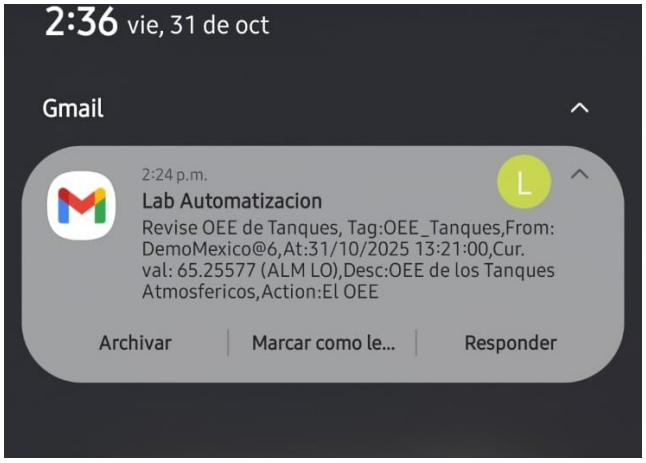

Figura 3.16 Notificación de alarma vía correo electrónico.

Adicionalmente, el sistema permite gestionar las alarmas mediante herramientas visuales integradas. La Figura 3.17 se muestra el panel de "*Summary*", que muestra de manera resumida todas las alarmas activas en el sistema, indicando su estado (activa, reconocida, o solucionada), prioridad y descripción. Esta vista es fundamental para el operador, ya que permite conocer el estado del sistema industrial.

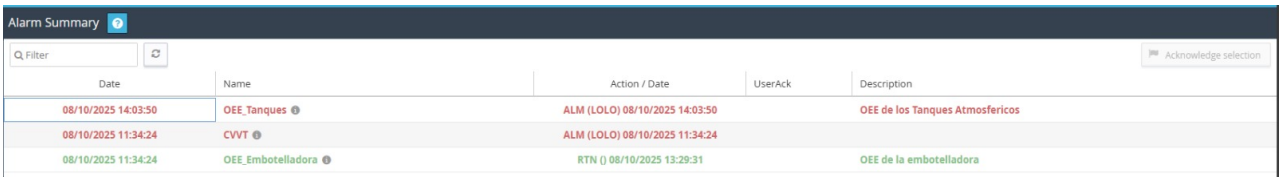

Figura 3.17 Resumen de alarmas.

Por otra parte, la Figura 3.18 muestra el historial completo de alarmas generadas en el sistema. Este registro cronológico contiene información detallada sobre eventos pasados, incluyendo fecha, hora y variable implicada. Esta herramienta es clave para la trazabilidad de eventos, permitiendo analizar fallos recurrentes, identificar causas raíz y puede ayudar a mejorar la estrategia de mantenimiento preventivo o correctivo.

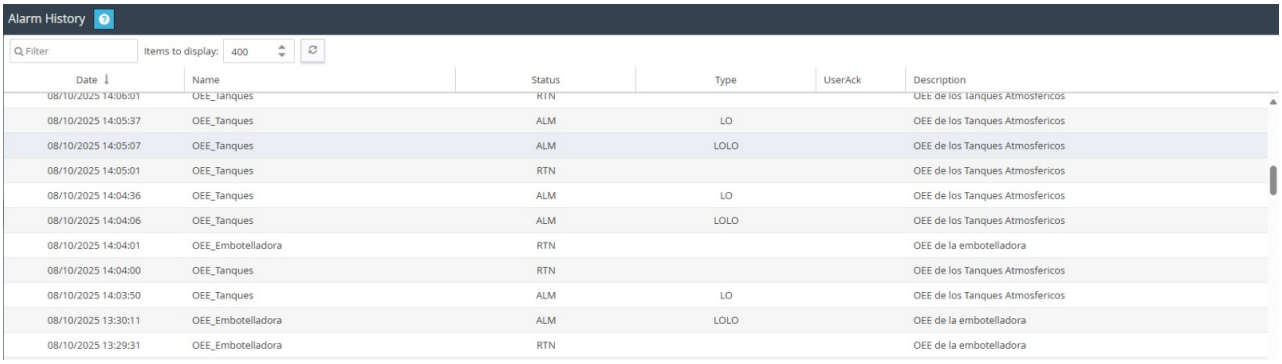

Figura 3.18 Historial de alarmas.

Cabe destacar que todas las alarmas pueden ser clasificadas por nivel de criticidad (baja, media o alta), y pueden requerir reconocimiento manual por parte del operador, reforzando la responsabilidad y la vigilancia constante del sistema.

3.3.4. Diseño del *dashboard* de supervisión

Como parte de la solución de supervisión remota implementada, se desarrolló una interfaz gráfica utilizando el *software ViewON*, el cual permite crear visualizaciones interactivas que se ejecutan directamente dentro del *Flexy 205*. Esta interfaz no solo proporciona una visualización clara de los procesos industriales, sino que también posibilita el acceso remoto seguro a través de la red VPN del servidor *Talk2M*, sin requerir *software* adicional en el equipo del usuario.

La primera pantalla del sistema corresponde a una vista resumida de los procesos supervisados, diseñada con el objetivo de ofrecer una panorámica rápida y clara del estado de cada sistema. En esta vista se integran indicadores clave como la calidad, el rendimiento y el OEE de cada uno de los procesos conectados. Estos parámetros permiten evaluar, en tiempo real, la eficiencia global del sistema industrial, facilitando así la toma de decisiones basada en datos.

Para complementar la supervisión en tiempo real, se incluyeron gráficas dinámicas de tendencia, las cuales muestran la tendencia de cada uno de los indicadores a lo largo del tiempo. Esta gráfica facilita el análisis de comportamiento histórico, permitiendo identificar patrones, detectar caídas en el desempeño o evaluar la efectividad de acciones correctivas implementadas. Las gráficas fueron configuradas para actualizarse automáticamente según el *poll rate* definido en la sección de adquisición de datos del *Flexy 205*, garantizando así la coherencia entre la visualización y las condiciones reales del proceso. En la Figura 3.19 se muestra la vista resumida del ambos procesos, donde se pueden simular los datos para realizar las pruebas de funcionamiento de los elementos gráficos implementados.

View pages as: Viewer on Laptop

Tag	Value	Function	Minimum	Maximum	Period (milliseconds)
Rendimiento_Embotelladora *eWON Tag*	12	Triangle	0	100	100
OEE_Tanques *eWON Tag*	54	Triangle	0	100	100
Calidad_Tanques *eWON Tag*	10	Triangle	0	100	100
Disponibilidad_Tanques *eWON Tag*	20	Triangle	0	100	100
Rendimiento_Tanques *eWON Tag*	36	Triangle	0	100	100
Disponibilidad_Embotelladora *eWON Tag*	28	Triangle	0	100	100
Calidad_Embotelladora *eWON Tag*	63	Triangle	0	100	100
OEE_Embotelladora *eWON Tag*	38	Triangle	0	100	100

Figura 3.19 Pantalla de vista resumida.

Además de su valor visual, esta pantalla representa un punto centralizado de supervisión, desde el cual el usuario puede acceder a vistas más detalladas de cada proceso individual. Toda la estructura

gráfica fue diseñada bajo principios de usabilidad y ergonomía, priorizando la claridad, simplicidad y accesibilidad de la información para distintos perfiles de usuario, ya sea operador o administrador.

Además de la vista general, el sistema de supervisión desarrollado incluye pantallas individuales para cada uno de los procesos industriales integrados. Estas pantallas permiten al usuario acceder a una visualización más específica y detallada de las variables clave que caracterizan el comportamiento de cada proceso, complementando el monitoreo global.

- Pantalla del proceso de tanques atmosféricos

  En esta interfaz se presenta la información correspondiente al sistema de almacenamiento, operado por el controlador *ControlLogix L81E*. La pantalla muestra en tiempo real tres indicadores fundamentales del desempeño del proceso: disponibilidad, rendimiento y calidad. Estos valores permiten evaluar el correcto funcionamiento del sistema de bombeo y válvulas.

  Para facilitar la interpretación de la información, la interfaz gráfica incluye una representación esquemática del proceso físico, en la cual se ilustran los componentes clave del sistema, como tanques, tuberías, válvulas y bombas. Esta representación ayuda al usuario a identificar visualmente el flujo del proceso y a correlacionarlo con las variables que se están monitoreando. En la Figura 3.20 se muestra la pantalla diseñada para la supervision del proceso de tanques atmosféricos, nuevamente simulando los datos para corroborar la funcionalidad de los elementos visuales.

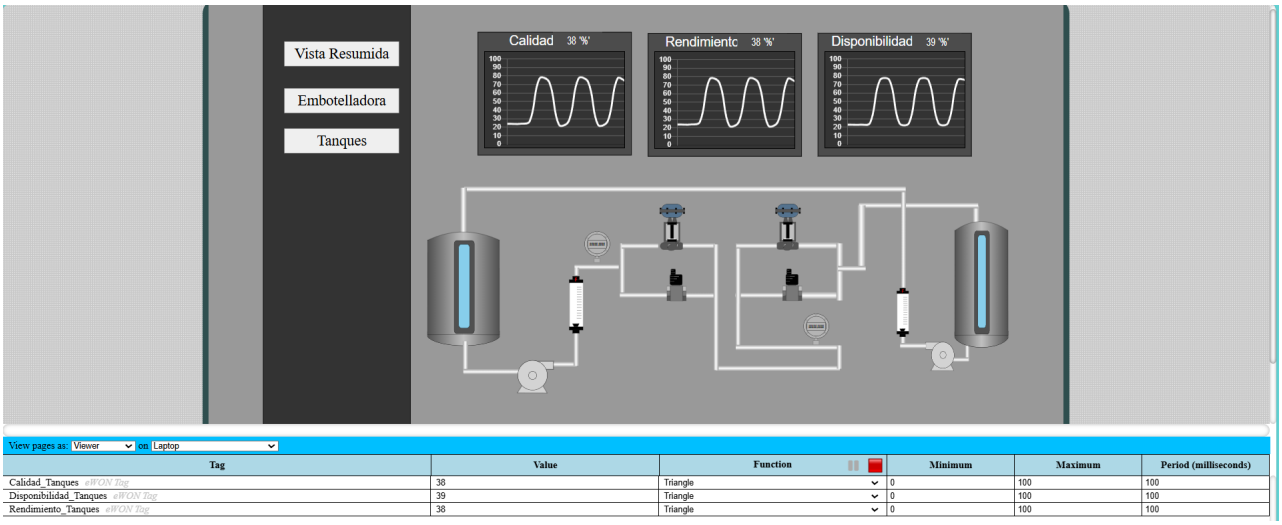

Figura 3.20 Pantalla de supervisión de tanques atmosféricos.

- Pantalla del proceso de embotellado

  De forma similar, la pantalla destinada al proceso de embotellado industrial, supervisado mediante el controlador *S7-1500* proporciona acceso a variables clave como rendimiento, calidad, disponibilidad y la cantidad de paros totales acumulados. Este último permite al usuario identificar posibles fallas recurrentes dentro de la rutina de funcionamiento del sistema.

  La pantalla diseñada se muestra en la Figura 3.21, la interfaz presenta también una imagen representativa del proceso de embotellado, con elementos gráficos que ayudan a comprender visualmente la secuencia del sistema y su relación con las variables de eficiencia monitoreadas.

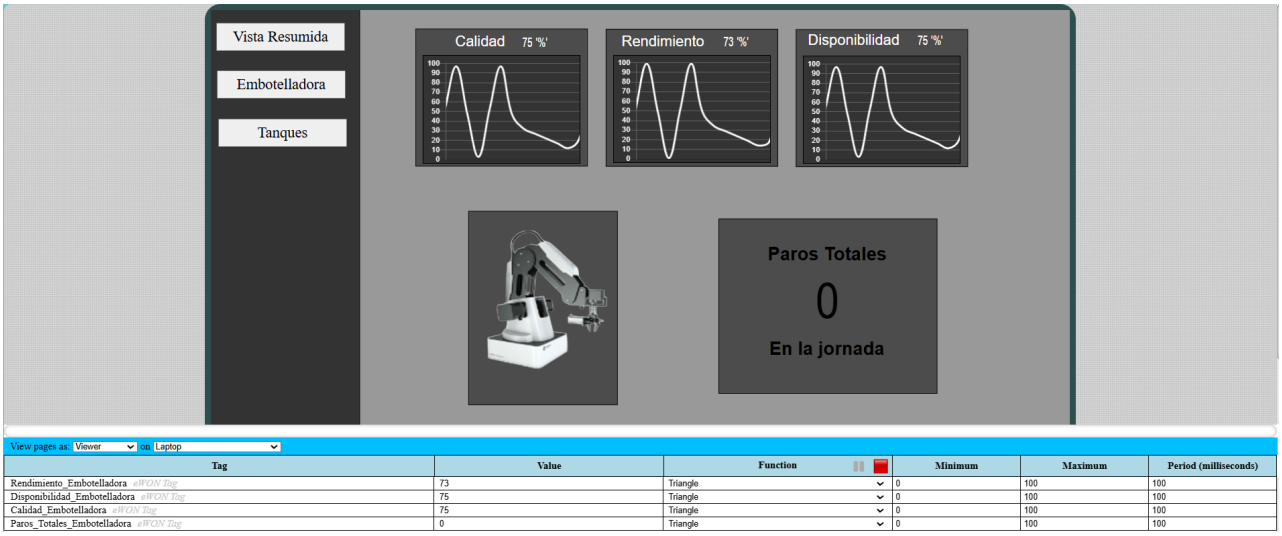

Figura 3.21 Pantalla de supervisión de planta embotelladora.

Ambas vistas detalladas mantienen la coherencia visual y funcional con la interfaz general del sistema, y están diseñadas para integrarse dentro del entorno operativo del *Flexy 205*, asegurando que los datos mostrados estén siempre sincronizados con las condiciones actuales de planta. La navegación entre pantallas se realiza a través de botones interactivos diseñados en *ViewON*, lo que permite una supervisión fluida y jerárquica, con distintos niveles de profundidad según el interés del operador.

3.4. Autenticación y control de accesos

La autenticación y el control de acceso constituyen elementos esenciales para garantizar la seguridad en la supervisión y operación remota de sistemas industriales, ya que permiten identificar de forma confiable a los usuarios, asignar privilegios según sus funciones y restringir el acceso únicamente a personal autorizado.

En el módulo *Flexy 205*, la autenticación se implementa mediante cuentas únicas por usuario, las cuales combinan un nombre de usuario y una contraseña para el acceso tanto a la interfaz web local como a la conexión remota a través del servicio *Talk2M*. Para este caso de estudio, se implemento el uso de contraseñas con una extenisón mínima de ocho caracteres, incluyendo letras mayúsculas, minúsculas, dígitos y caracteres especiales, siguiendo las recomendaciones de la norma *IEC 62443*.

El control de acceso se configuró bajo el principio de privilegios, asignando a cada cuenta los permisos necesarios para la función que desempeña, ya sea como usuario “Administrador” u “Operador”, lo que permite restringir funciones como la modificación de parámetros de red, la gestión de servidores, la edición de Tags o la configuración de alarmas. El sistema de gestión de usuarios del *Flexy 205* permite crear, modificar o eliminar cuentas, así como asignar permisos específicos, las acciones habilitadas para cada usuario se muestran en la Figura 3.22. Esta segmentación no solo evita la manipulación indebida de parámetros, sino que también fortalece la trazabilidad de las operaciones, ya que cada acción queda registrada y asociada a la identidad del usuario que la ejecutó.

Adicionalmente, se habilitó el registro de eventos “*event logs*”, lo que permite monitorear intentos fallidos de inicio de sesión, cambios en la configuración y conexiones establecidas, proporcionando así una herramienta eficaz para la detección temprana de incidentes de seguridad.

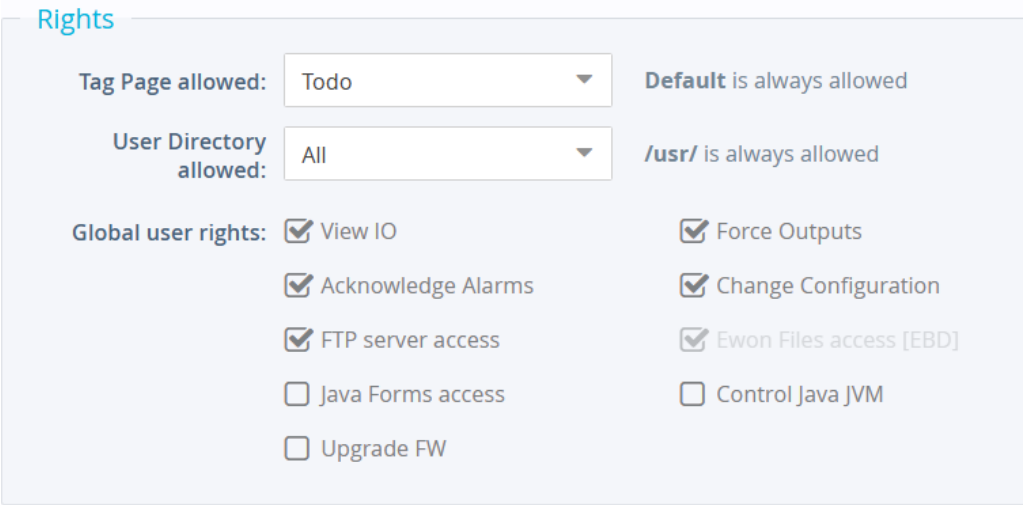

Figura 3.22 Control de derechos de usuarios dentro del *Flexy 205*.

La Figura 3.23 muestra la interfaz de configuración de usuarios del *Flexy 205*, en la que se aprecian las cuentas creadas, sus identificadores únicos y sus respectivos niveles de privilegio. Esta estructura previene accesos indebidos, también facilita el monitoreo y la respuesta ante incidentes, contribuyendo a la ciberseguridad de la infraestructura.

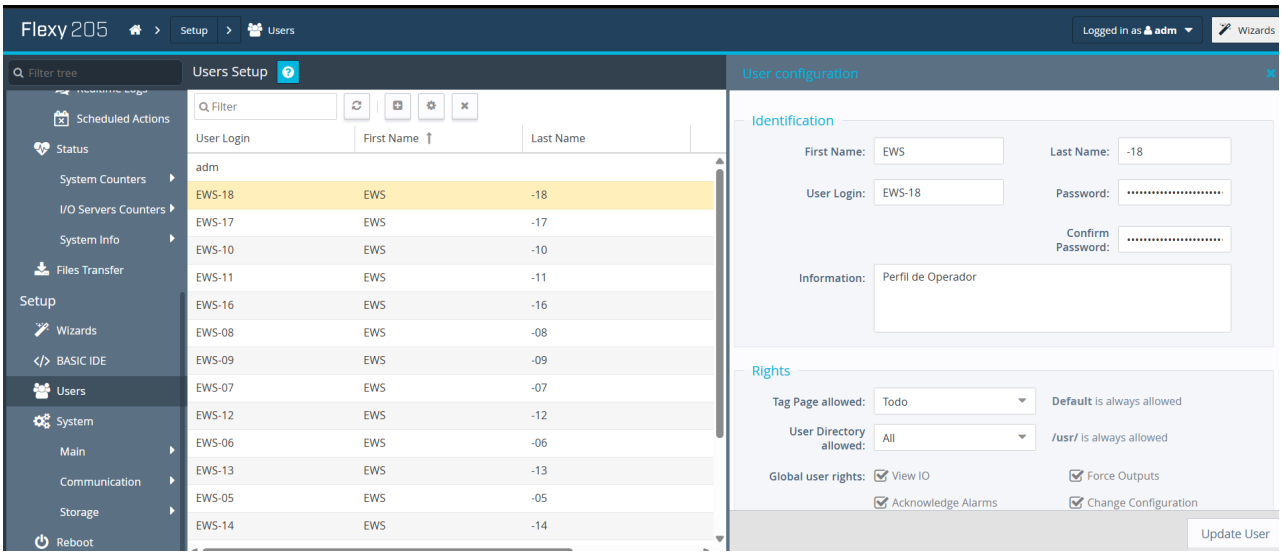

Figura 3.23 Control de usuarios dentro del *Flexy 205*.

Ahora, en el apartado correspondiente a la interfaz gráfica, se implementó una segmentación de la información que permite mostrar u ocultar determinados elementos del proceso según el nivel de privilegios asignado a cada usuario. Esta funcionalidad contribuye a reforzar el control y la seguridad operativa dentro del sistema, garantizando que cada perfil acceda únicamente a los datos y funciones que le corresponden. De esta forma, se limita la exposición de información y se facilita la trazabilidad de las acciones realizadas por los diferentes tipos de usuario. En la Figura 3.24 se presenta la asignacion de roles de usuarios dentro de la interfaz gráfica.

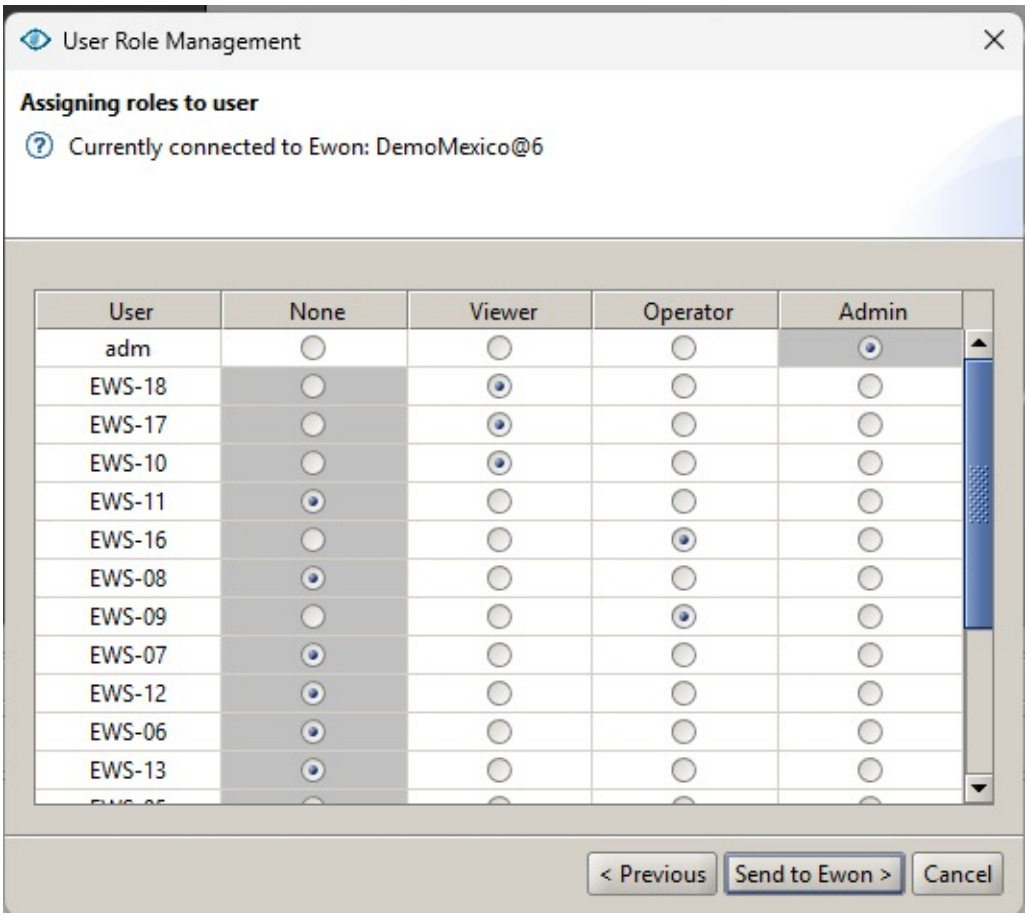

Figura 3.24 Control de usuarios dentro de la interfaz gráfica.

Capítulo 4

Evaluación y validación

4.1. Pruebas de conectividad y comunicación

Como parte de la evaluación de los resultados obtenidos, es fundamental verificar y corroborar la comunicación entre los diferentes elementos de control involucrados.

En el caso del proceso de embotellamiento, se empleó una herramienta del software *TIA Portal* que permite crear un bloque de datos para agrupar los Tags que serán visualizados posteriormente en la pantalla de supervisión. En la Figura 4.1 se muestran los Tags generados por el controlador *S7-1500*, correspondientes a las variables monitoreadas en este proceso.

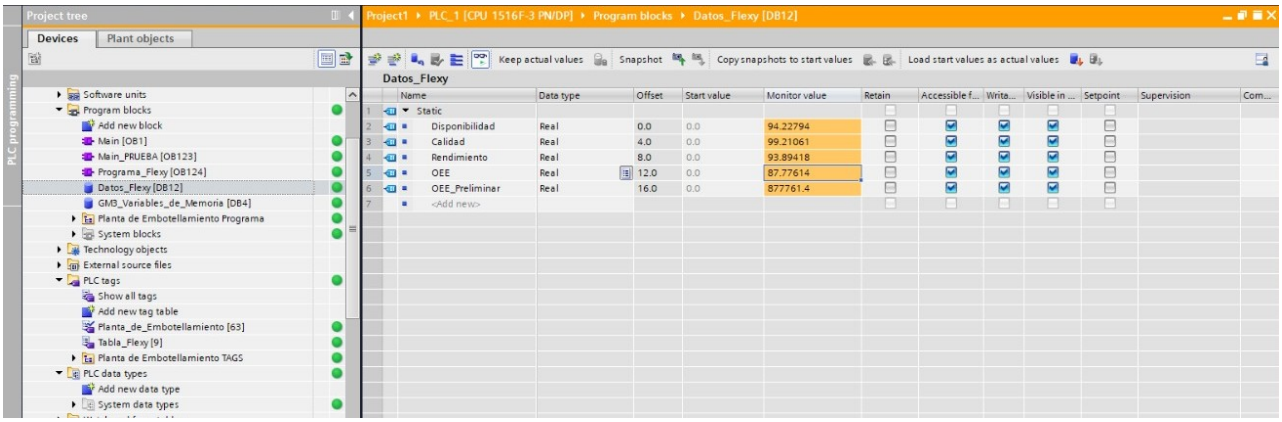

Figura 4.1 Datos generados por el controlador *S7-1500*.

Dentro de la interfaz web local del módulo *Flexy 205*, es posible verificar el estado de comunicación entre los PLC y el módulo IIoT a través del apartado con ícono de corazón dentro de la sección denominada "*Values*". En este panel, el sistema muestra una advertencia en forma de signo de exclamación rojo cuando la comunicación se interrumpe o está deshabilitada, mientras que el ícono permanece vacío cuando el intercambio de datos se realiza correctamente. Para confirmar la constancia de la comunicación entre ambos equipos, se generó una gráfica de tendencia en tiempo real correspondiente a una de las variables monitoreadas como se muestra en la Figura 4.2, observa la estabilidad de la señal transmitida, lo que demuestra una transmisión continua y sin interrupciones entre el controlador y el módulo.

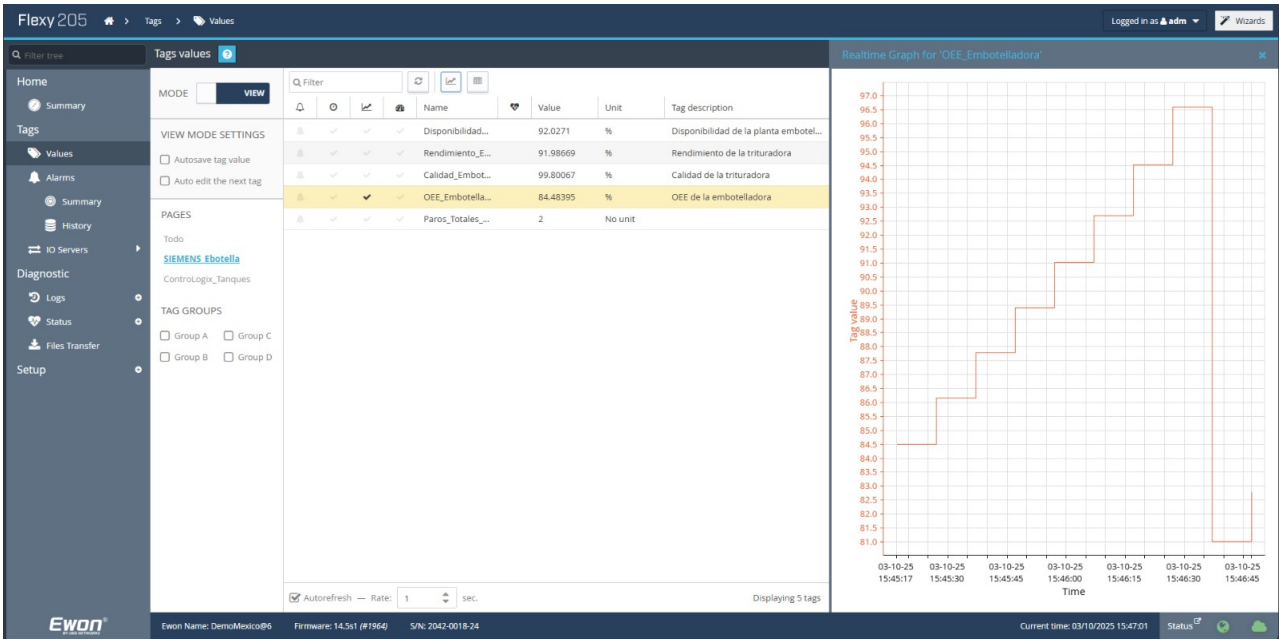

Figura 4.2 Monitoreo en tiempo real del OEE generado por el controlador *S7-1500*.

De la misma forma, en el proceso de tanques atmosféricos se llevó a cabo la comprobación de la comunicación entre el controlador y el módulo. En la Figura 4.3 se muestran los Tags del controlador *ControlLogix L81E* que fueron configurados para su monitoreo dentro del sistema de supervisión, mientras que en la Figura 4.4 se presenta la tendencia de uno de los valores obtenidos, confirmando así el intercambio correcto de información.

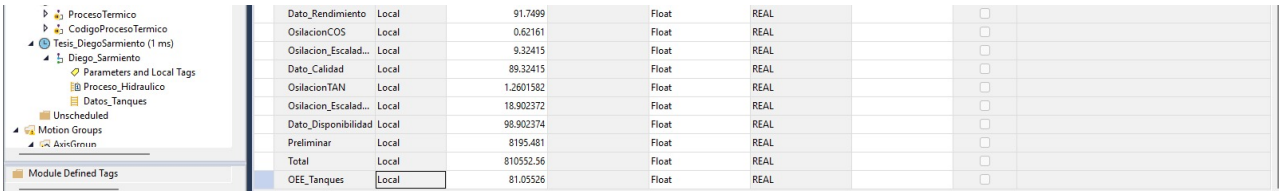

Figura 4.3 Tags configurados para monitoreo en el controlador *ControlLogix L81E*.

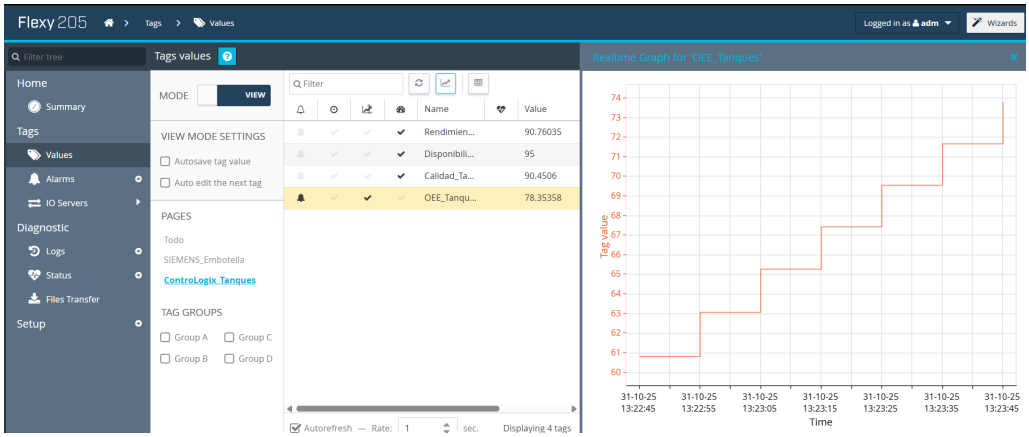

Figura 4.4 Monitoreo en tiempo real del OEE generado por el controlador *ControlLogix L81E*.

Con estas verificaciones se valida la comunicación efectiva y estable entre el módulo IIoT y los sistemas de control. Esto confirma la correcta integración entre las plataformas de automatización y el módulo *gateway*, garantizando la confiabilidad en la adquisición de datos y su visualización en tiempo real.

4.2. Supervisión remota y visualización en *dashboard*

Para validar el acceso remoto a los procesos de embotellamiento y de tanques, se realizó una prueba de conexión desde un equipo externo a la red local de los controladores, denominado "PC Puma FI". Este equipo se conectó a una red pública de internet ajena al entorno de los procesos industriales, con el fin de comprobar la funcionalidad del enlace remoto seguro. En la Figura 4.5 se muestra el proceso de activación de la conexión remota mediante el software *eCatcher*. Tras iniciar sesión en la cuenta correspondiente, se habilita la opción para establecer la conexión con el módulo llamado "*Lab. Automatización*". Al seleccionar esta opción, el sistema inicia la creación de un túnel seguro a través de una red pública, estableciendo así la comunicación con el módulo mediante una VPN.

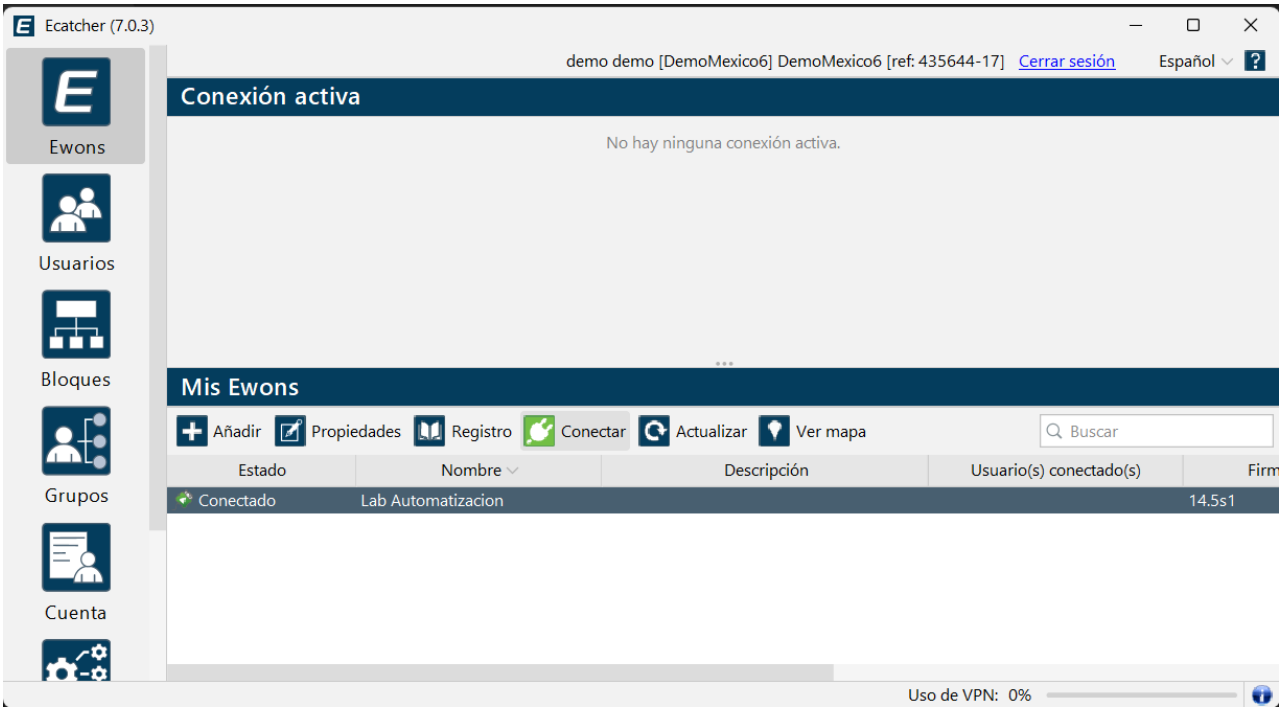

Figura 4.5 Activación de la conexión remota mediante túnel VPN.

En primera instancia, se intentó acceder directamente al PLC *ControlLogix L81E* a través de su dirección IP local (192.168.1.24) para ingresar a su interfaz web. Tal como se muestra en la Figura 4.6, el intento de conexión no fue exitoso, debido a que el controlador se encuentra fuera del dominio de la red local de la computadora, lo que confirma la imposibilidad de establecer comunicación.

Posteriormente, se procedió a establecer una conexión remota mediante el servidor *Talk2M*, utilizando el software *eCatcher*. Este servicio crea un túnel VPN sobre la red pública, asignando a la compuadora una dirección IP virtual (10.185.184.25) dentro de la red privada del sistema industrial. Una vez establecida la conexión, fue posible acceder a la interfaz web del PLC *ControlLogix L81E* con

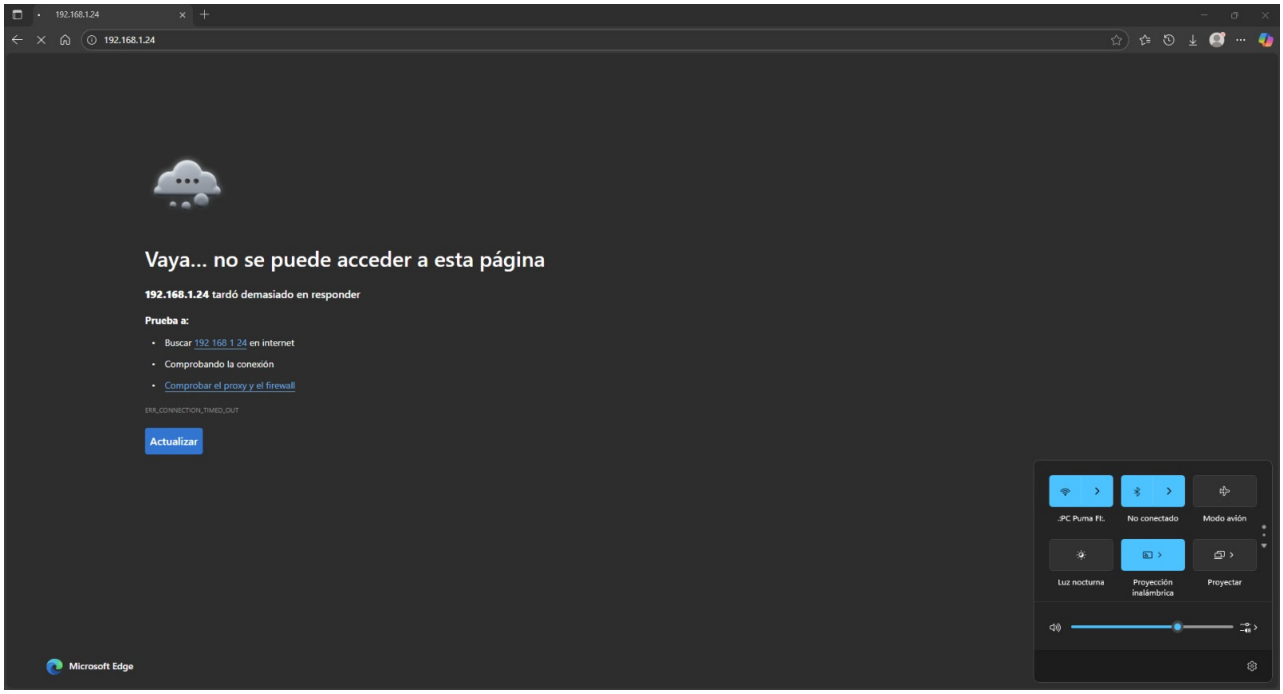

Figura 4.6 Intento de acceso local al controlador fuera de la red.

exito, como se observa en la Figura 4.7, demostrando que la comunicación cifrada permite el acceso remoto seguro a los dispositivos del sistema.

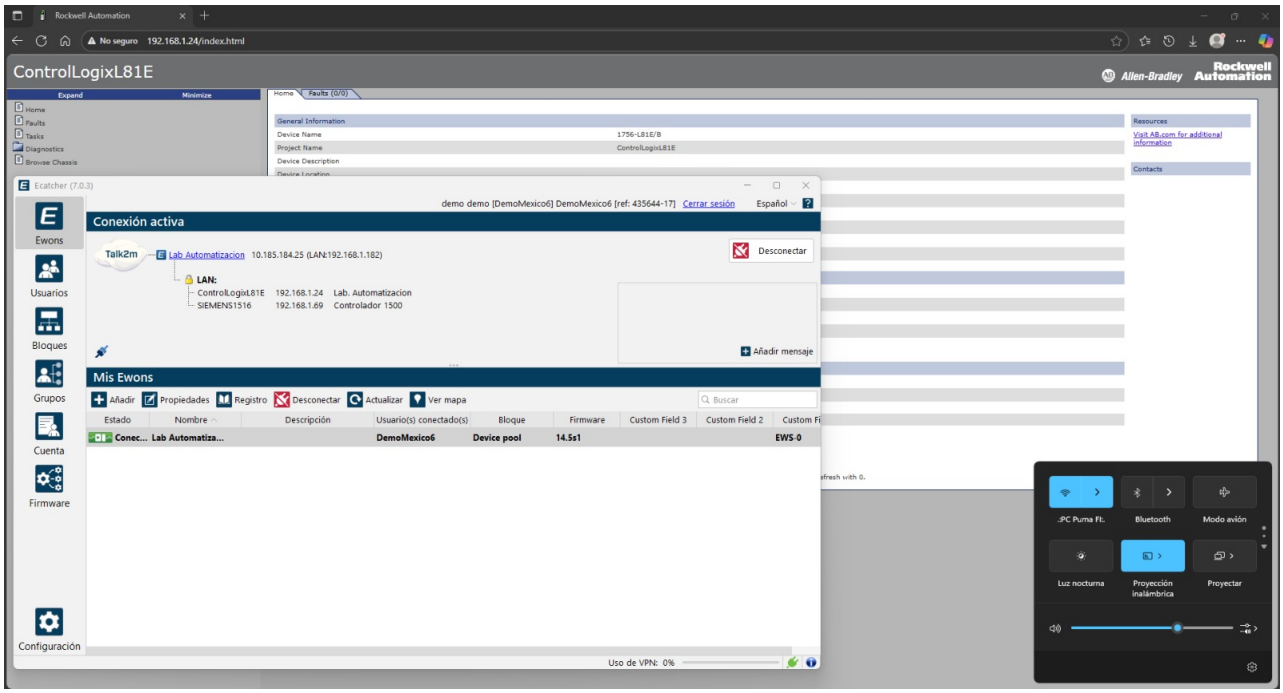

Figura 4.7 Acceso remoto exitoso al controlador mediante conexión VPN.

Adicionalmente, se verificó la comunicación mediante pruebas en la consola de comandos del sistema operativo. Primero, se desconectó el servicio *eCatcher* y se ejecutó la instrucción "*ping* 192.168.1.24",

comprobando que la red de destino era inaccesible. Posteriormente, al restablecer la conexión VPN y repetir el comando, se obtuvo respuesta exitosa desde el PLC, confirmando la conectividad remota a través del túnel seguro. En la Figura 4.8 se muestran los resultados obtenidos de ambas pruebas.

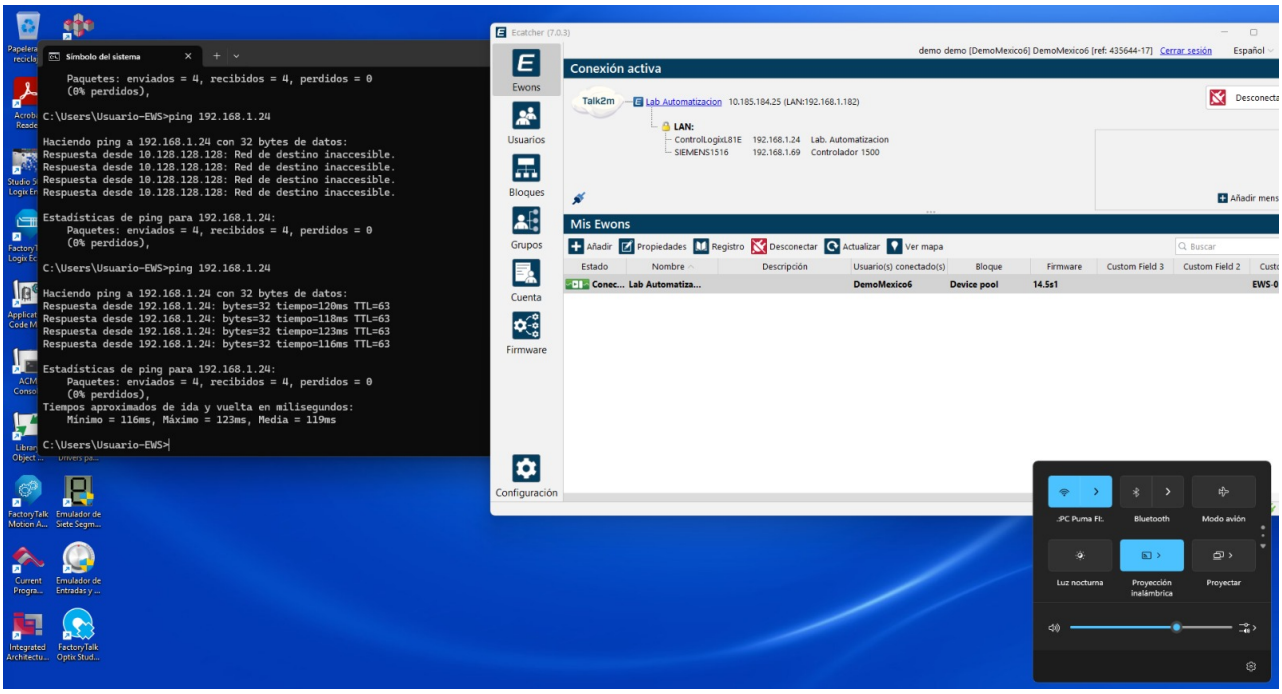

Figura 4.8 Validación de comunicación mediante prueba de conexión "*ping*" con el PLC *ControlLogix L81E*.

Los pasos descritos anteriormente se repiten para establecer la conexión remota con el controlador *S7-1500*, lo que permite acceder al proceso de embotellamiento desde una computadora externa. En la Figura 4.9 se presentan los resultados de la validación de comunicación realizada mediante la consola del sistema, utilizando el comando "*ping*" dirigido a la dirección IP del controlador (192.168.1.95). Esta prueba confirma que el enlace remoto se establece correctamente a través de la red privada virtual, garantizando la comunicación bidireccional entre el PLC y el equipo cliente.

Como parte de la etapa de evaluación y validación de la visualizacion en *dashboard*, se llevó a cabo la comprobación de la correcta visualización de las variables operativas a través del *dashboard* implementado. Este entorno gráfico permite observar en tiempo real los KPI asociados a los procesos industriales monitoreados.

La validación consistió en verificar la actualización dinámica de los valores y la sincronización de las gráficas de tendencia con los datos provenientes de los PLC. En la Figura 4.10 se presenta la vista general del *dashboard*, la cual integra en una misma interfaz los principales indicadores de ambos procesos, junto con gráficas de comportamiento histórico que permiten analizar la estabilidad y variabilidad de los parámetros supervisados.

En la Figura 4.11 se aprecia la interfaz correspondiente al proceso de embotellado, donde se visualizan las variables de calidad, rendimiento y disponibilidad, junto con el conteo de paros totales ocurridos durante la jornada. La disposición gráfica permite identificar fácilmente desviaciones y evaluar el desempeño general del sistema de manera intuitiva.

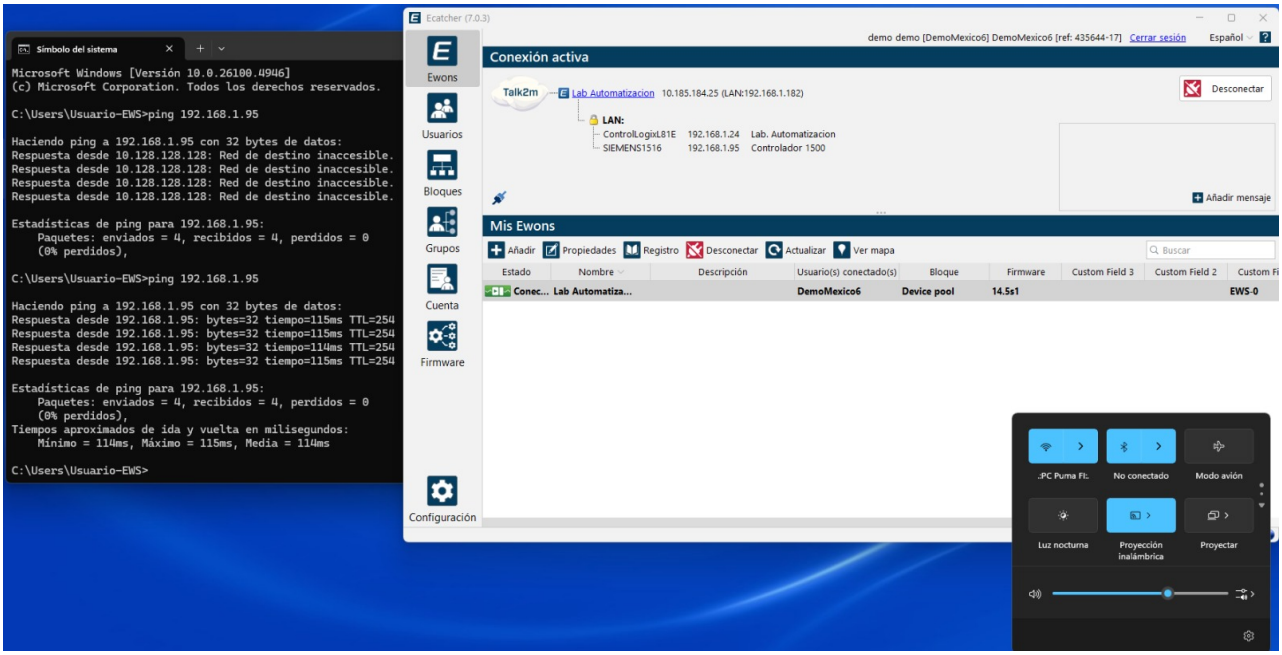

Figura 4.9 Validación de comunicación mediante prueba de conexión "*ping*" con el PLC *S7-1500*.

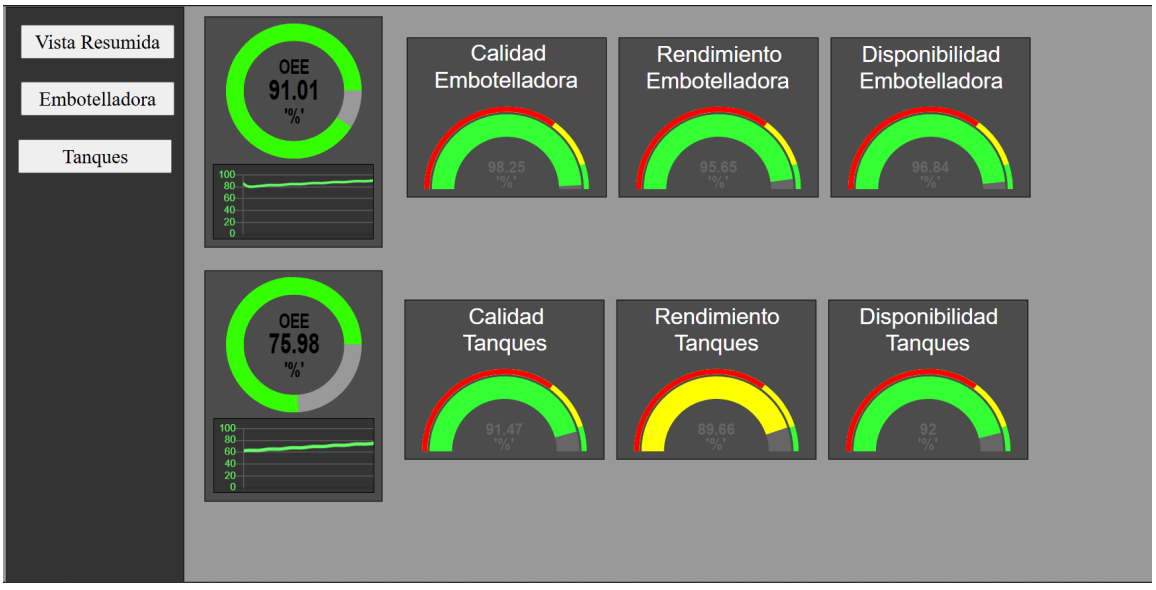

Figura 4.10 Vista resumida del *dashboard* con indicadores de OEE y KPI operativos.

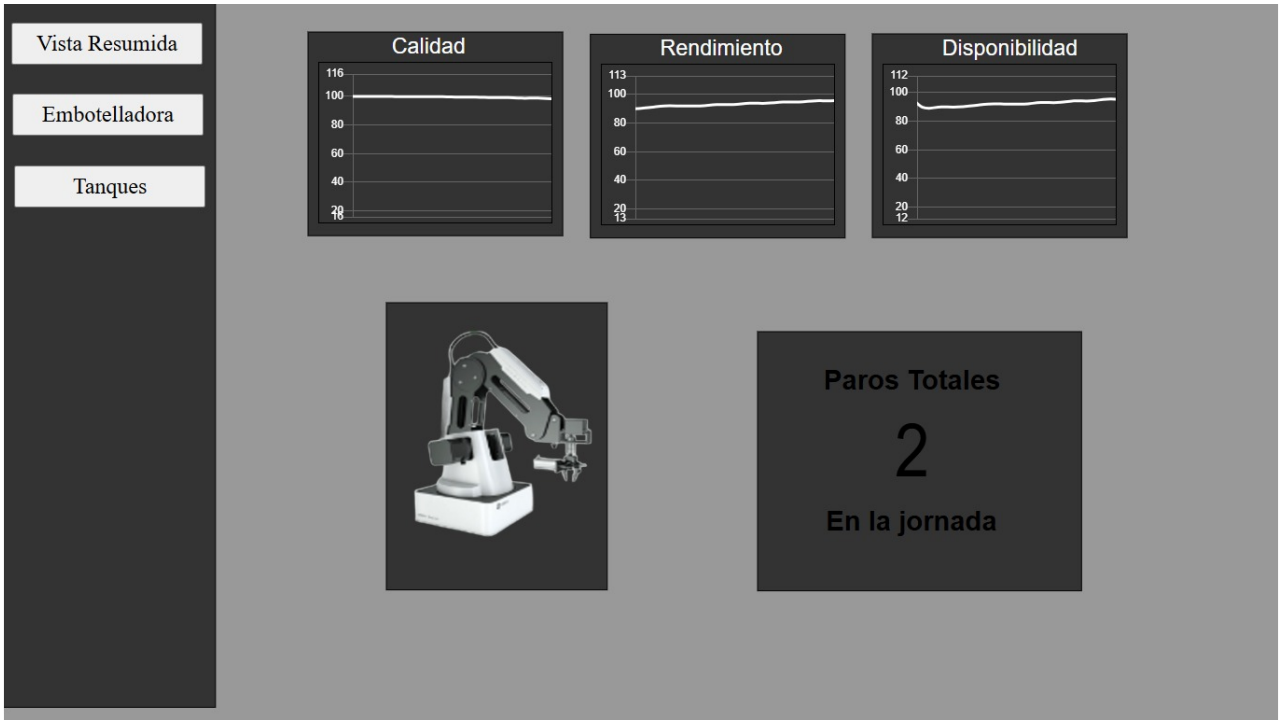

Figura 4.11 Visualización del proceso de embotellado en el *dashboard*.

Por su parte, la Figura 4.12 muestra la interfaz de supervisión del proceso de tanques atmosféricos, en la cual se representa esquemáticamente el flujo del sistema junto con los indicadores de desempeño de calidad, rendimiento y disponibilidad.

Finalmente, se comprobó el acceso remoto seguro a la interfaz de supervisión mediante el uso del módulo IIoT configurado, asegurando la integridad de la comunicación y la correcta actualización de los datos desde ubicaciones externas como se muestra en la Figura 4.13 es posible acceder a los datos de los procesos aun estando fuera de la red local mediante internet y el túnel VPN creado con el servidor de *Talk2M*. Con ello, se valída el funcionamiento integral del sistema de monitoreo, la coherencia entre los valores registrados por los controladores y su visualización en el *dashboard* de manera remota.

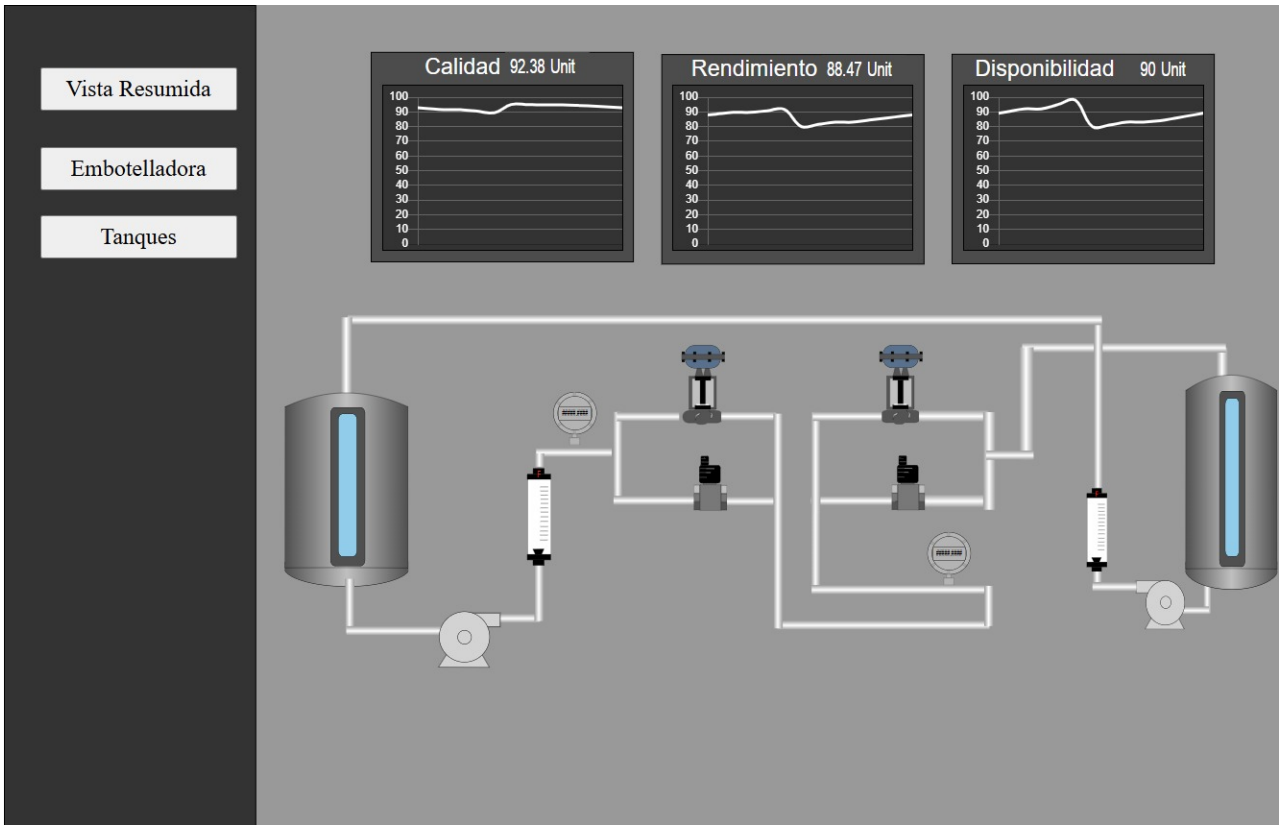

Figura 4.12 Interfaz de supervisión del proceso de tanques atmosféricos.

Figura 4.13 Interfaz de supervisión principal mediante una conexión remota.

4.3. Pruebas de medidas de ciberseguridad implementadas

Se realizó la evaluación del sistema en los aspectos relacionados con la autenticación de usuarios, el control de accesos, la segmentación de permisos y la protección del flujo de datos. Asimismo, se revisó la correcta generación de "*Logs*" de eventos como parte del proceso de trazabilidad y detección de intentos de acceso no autorizados.

Durante las pruebas se verificó la correcta aplicación de los mecanismos de autenticación y control de acceso dentro del módulo IIoT. A través de la interfaz de administración de usuarios, se comprobó que cada cuenta dispone de credenciales únicas y niveles de privilegio diferenciados, asignados conforme a las funciones y responsabilidades del usuario.

Los resultados demostraron que el sistema únicamente permite el ingreso mediante credenciales válidas, restringiendo las acciones disponibles según el perfil del usuario autenticado. De esta forma, se garantiza que las operaciones críticas queden reservadas al personal con los permisos adecuados, cumpliendo con el principio de mínimo privilegio. En la Figura 4.14 se presentan las credenciales utilizadas para acceder con privilegios de administrador, mientras que en la Figura 4.15 se muestra la pantalla de supervision mostrada para dicho perfil dentro del sistema que trae consigo informacion segmentada acerca de los eventos y alarmas que se presentan en los procesos.

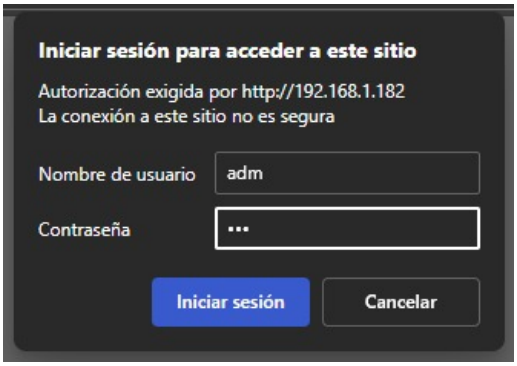

Figura 4.14 Acceso a *dashboard* de supervisión como usuario "Administrador".

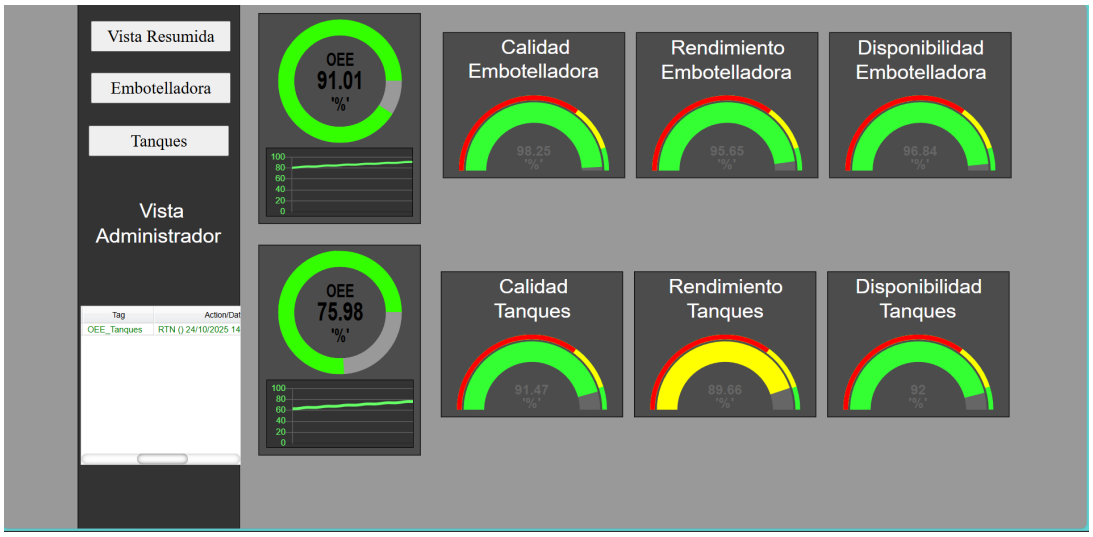

Figura 4.15 Vista de supervision en usuario "Administrador".

De la misma forma en la Figura 4.16 se muestran las credenciales para ingresar al *dashboard* de supervisión con los privilegios de "Operador" como se muestra en la Figura 4.10.

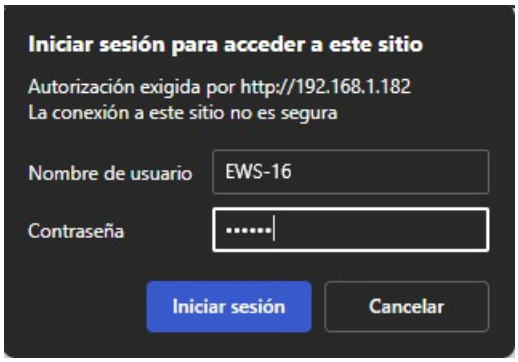

Figura 4.16 Acceso a *dashboard* de supervisión como usuario "Operador".

Adicionalmente, se validó que el sistema registre de forma automática los intentos de inicio de sesión fallidos, los accesos exitosos y las modificaciones realizadas en la configuración dentro del apartado "*Event Logs*". Esta funcionalidad permite garantizar la trazabilidad completa de las acciones efectuadas por los usuarios, contribuyendo a la detección temprana de incidentes y posibles intentos de acceso no autorizados. En la Figura 4.17 se muestra un extracto de los registros generados durante las pruebas de autenticación, donde es posible observar los intentos de conexión con credenciales incorrectas, evidenciando la capacidad del sistema para identificar y registrar eventos que pudieran comprometer la seguridad del entorno de supervisión.

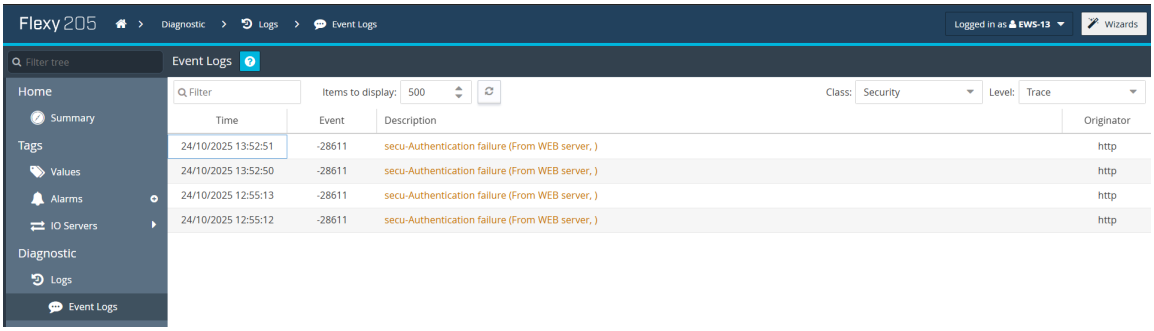

Figura 4.17 Registro de eventos de seguridad del sistema IIoT.

4.4. Discusión

Tras la implementación y evaluación del sistema propuesto, se logró comprobar el funcionamiento correcto de la arquitectura de supervisión remota mediante tecnologías IIoT. Los resultados obtenidos evidencian una comunicación estable entre los distintos controladores industriales y el módulo de supervisión, permitiendo la visualización de los datos operativos en tiempo real dentro del *dashboard*. Los KPI, como la calidad, el rendimiento y la disponibilidad, presentaron una actualización continua y coherente con las variables de proceso, lo cual valida la correcta adquisición y transmisión de datos a través del sistema.

La integración de los procesos industriales en una sola plataforma permitió observar que el módulo IIoT puede funcionar como un enlace confiable entre equipos de diferentes fabricantes, garantizando la interoperabilidad sin afectar el desempeño de los mismos. El monitoreo remoto, complementado con la visualización gráfica de los valores en tendencia, confirmó la capacidad del sistema para operar en condiciones de conexión estable y un intercambio de información constante entre los controladores y el servidor de supervisión.

En la ciberseguridad, las pruebas realizadas sobre los mecanismos de autenticación, control de acceso y cifrado de datos demostraron la efectividad de las medidas aplicadas. La autenticación por usuario y la asignación de privilegios diferenciados garantizaron que solo personal autorizado tuviera acceso a las funciones críticas del sistema. Además, la conexión mediante túneles VPN y el uso de protocolos seguros reforzaron la confidencialidad y la integridad de los datos durante la transmisión.

Es importante mencionar que, aunque el sistema cumplió con los objetivos de seguridad y funcionalidad planteados, se identifican oportunidades de mejora relacionadas con la gestión centralizada de usuarios y la automatización del registro de eventos de seguridad. Estas mejoras podrían fortalecer la trazabilidad alineándose aún más con los puntos clave establecidos por la norma *IEC 62443*.

El desarrollo de este trabajo evidencia la utilidad de los sistemas IIoT para la transformación digital de los entornos industriales. La integración de supervisión, control y ciberseguridad dentro de una misma arquitectura proporciona una base sólida para la evolución hacia plantas inteligentes, interconectadas. De esta forma, se valida que el sistema diseñado cumple con los objetivos técnicos y de seguridad establecidos, además de servir como punto de partida para futuras mejoras.

Capítulo 5

Conclusiones

5.1. Conclusiones

El sistema de supervisión y acceso remoto implementado, basado en tecnologías IIoT, demostró ser una solución eficaz para la integración y monitoreo de procesos industriales heterogéneos dentro de una misma arquitectura cibersegura. La comunicación establecida entre los distintos PLC y el módulo de supervisión permitió la visualización confiable de variables críticas en tiempo real, validando la interoperabilidad entre plataformas bajo estándares industriales comunes.

En este trabajo se integraron conceptos fundamentales de la transformación digital y la ciberseguridad industrial, orientados a la protección de la infraestructura conectada. Se implementaron mecanismos acorde con los requisitos de identificación y autenticación, garantizando que el acceso a los dispositivos y a la interfaz de supervisión solo fuera posible mediante credenciales válidas y perfiles definidos. Asimismo, se aplicaron controles de uso basados en privilegios diferenciados, permitiendo que cada usuario interactuara únicamente con las funciones asignadas a su rol. La confidencailidad de la información operativa y el cifrado de las comunicaciones se reforzó mediante el uso de túneles VPN reduciendo la probabilidad de exposición o manipulación no autorizada de datos sensibles. Adicionalmente, se evaluó el registro y gestión de eventos relevantes, lo que permitió confirmar la capacidad del sistema para detectar accesos fallidos, generar alertas y mantener la trazabilidad requerida para una respuesta oportuna ante incidentes. Estas implementaciones se alinean con los principios establecidos en la norma *IEC 62443*, consolidando una arquitectura resiliente ante posibles ciberamenazas.

La configuración del entorno de supervisión permitió obtener KPI como disponibilidad, calidad, rendimiento y OEE, los cuales fueron monitoreados mediante un *dashboard* dinámico con actualización en tiempo real. Esta visualización integral contribuyó a una mejor comprensión del estado operativo de los procesos, favoreciendo la toma de decisiones y el mantenimiento predictivo.

El trabajo muestra el potencial de las soluciones IIoT en la digitalización industrial, al permitir la union entre los dominios de las tecnologías de operación y las de información.

Finalmente, el desarrollo de este sistema representa un paso significativo hacia la adopción de infraestructuras industriales conectadas, seguras y escalables. La metodología utilizada sienta las bases para futuras aplicaciones en entornos industriales que requieran supervisión remota, interoperabilidad entre equipos y protección integral frente a riesgos cibernéticos.

Referencias

[Badra y Hajjeh, 2006] Badra, M. & Hajjeh, I. (2006). Enabling VPN and Secure Remote Access Using TLS Protocol. (pp. 308–314)., https://doi.org/10.1109/WIMOB.2006.1696366. (Citado en página 9.)

[Bagyaveereswaran, *et al.*, 2023] Bagyaveereswaran, V., Pang, W. L., Pragatheshwaran, N., Epcipha, R., Anitha, R., & Pandian, B. J. (2023). A Modular Industrial IoT Scheme to Monitor and Control Distribution in a Substation Model. *2023 Innovations in Power and Advanced Computing Technologies (i-PACT)*, (pp. 1–6)., https://doi.org/10.1109/i-PACT58649.2023.10434692. i-PACT 2023 Conference https://doi.org/10.1109/i-PACT58649.2023.10434692. (Citado en página 1.)

[Boyes, *et al.*, 2018] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12, https://doi.org/https://doi.org/10.1016/j.compind.2018.04.015 https://www.sciencedirect.com/science/article/pii/S0166361517307285. (Citado en páginas 5 y 8.)

[Campoverde, *et al.*, 2015] Campoverde, A. M., Hernández R., D. L., & Mazón O., B. E. (2015). Cloud computing con herramientas open-source para Internet de las cosas. *Maskana*, *6*(Supl.), 173–182 https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/712. (Citado en página 6.)

[Cartuche-Calva, 2020] Cartuche-Calva, J. J., H.-R. D. L. M.-R. R. F. . R.-G. C. D. (2020). Seguridad IoT: Principales amenazas en una taxonomía de activos. *Revista cuatrimestral de divulgacióon científica, Universidad alas peruanas*, *7*(3), 51–59, https://doi.org/http://dx.doi.org/10.21503/hamu.v7i3.2192 http://dx.doi.org/10.21503/hamu.v7i3.2192. (Citado en páginas 5, 6 y 9.)

[Córdova Viera, *et al.*, 2021] Córdova Viera, Y., Martínez Borrego, J., & Córdova Viera, E. (2021). Propuesta de metodología para el diseño de dashboard. *Revista Cubana de Transformación Digital*, *2*(3), https://doi.org/10.5281/zenodo.5545998 https://doi.org/10.5281/zenodo.5545998. (Citado en página 12.)

[Gusnadi y Hermawan, 2019] Gusnadi, Y. & Hermawan, A. (2019). Designing Employee Performance Monitoring Dashboard Using Key Performance Indicator (KPI). *bit-Tech*, *2*, 81–88, https://doi.org/https://doi.org/10.32877/bt.v2i2.107 https://jurnal.kdi.or.id/index.php/bt/article/view/107. (Citado en página 12.)

[ISA, 2024] ISA (2024). Security of Industrial Automation and Control Systems: An Overview of ISA/IEC 62443 Standards. Accessed: 2025-09-01 https://isagca.org/isa-iec-62443-standards. (Citado en página 10.)

[Jadhav, *et al.*, 2018] Jadhav, S., Patil, S. V., Thanuja, T., Shivu, M., & Shankar, G. (2018). Monitoring of Industrial Water Usage by using Internet of Things. *2018 International Conference on Information, Communication, Engineering and Technology (ICICET)*, (pp. 1–4)., https://doi.org/10.1109/ICICET.2018.8533822. ICICET 2018 Conference https://doi.org/10.1109/ICICET.2018.8533822. (Citado en página 1.)

[Juárez, 2019] Juárez, F. A. B. (2019). Cybersecurity in an Industrial Internet of Things Environment (IIoT) Challenges for Standards Systems and Evaluation Models. *2019 8th International Conference On Software Process Improvement (CIMPS)*, (pp. 1–6)., https://doi.org/10.1109/CIMPS49236.2019.9082437. (Citado en páginas 1 y 9.)

[Manral, 2020] Manral, K. (2020). SCADA vs IoT: el papel de los sistemas SCADA en la industria manufacturera 4.0 https://blogespanol.se.com/industria/2020/06/03/scada-vs-iot-el-papel-de-los-sistemas-scada-en-la-industria-manufacturera-4-0/. (Citado en página 8.)

[Moscol y Sánchez, 2021] Moscol, D. J. C. & Sánchez, V. H. M. (2021). Implementación de un sistema de monitoreo del consumo de vapor en Nestlé Ecuador mediante tecnología basada en Industria 4.0. (Citado en página 1.)

[Nyakomitta, *et al.*, 2020] Nyakomitta, P., Silvance, O., & Abeka, S. (2020). Security Investigation on Remote Access Methods of Virtual Private Network. *Global Journal of Computer Science and Technology*, *20*, 10, https://doi.org/10.1016/S1353. (Citado en página 8.)

[Rockwell Automation, 2015] Rockwell Automation (2015). Flexible Solutions for Your Supervisory Control and Data Acquisition (SCADA) Needs. https://www.rockwellautomation.com/es-mx/search.html?keyword=SCADA&tab=documents https://www.rockwellautomation.com/es-mx/search.html?keyword=SCADA&tab=documents. (Citado en páginas 6 y 7.)

[Sawalmeh, *et al.*, 2021] Sawalmeh, H., Malayshi, M., Ahmad, S., & Awad, A. (2021). VPN Remote Access OSPF-based VPN Security Vulnerabilities and Counter Measurements. (pp. 236–241)., https://doi.org/10.1109/3ICT53449.2021.9581512. (Citado en página 8.)

[Tumbajoy, *et al.*, 2022] Tumbajoy, L. M., Muñoz-Añasco, M., & Thiede, S. (2022). Enabling Industry 4.0 impact assessment with manufacturing system simulation: an OEE based methodology. *Procedia CIRP*, *107*, 681–686, https://doi.org/https://doi.org/10.1016/j.procir.2022.05.045. Leading manufacturing systems transformation – Proceedings of the 55th CIRP Conference on Manufacturing Systems 2022 https://www.sciencedirect.com/science/article/pii/S2212827122003298. (Citado en página 12.)