Prototipado de una Plataforma SCADA Portátil para el Análisis de Vulnerabilidades en Redes OT

Prototyping a Portable SCADA Platform for Vulnerability Analysis in OT Networks

Gonzalo Hernan Heinen, **Valentina Lorelei Heinen**
CAETI – Universidad Abierta Interamericana – Facultad de Tecnología Informática, Av. Montes de Oca 745, Ciudad de Buenos Aires, Argentina.

DOI *https://doi.org/10.59471/raia2025221*
Enviado: junio 2025. **Aceptado**: octubre 2025. **Publicado:** diciembre 2025
Como citar: Heinen, G. H., & Heinen, V. L. (2025). Prototipado de una Plataforma SCADA Portátil para el Análisis de Vulnerabilidades en Redes OT. Revista Abierta De Informática Aplicada, 9(1). *https://doi.org/10.59471/raia2025221*

Resumen

La tecnología operacional (OT según sus siglas en inglés) es hardware y software que supervisa directamente dispositivos y procesos físicos en entornos industriales. Los sistemas OT buscan mantener la continuidad, seguridad y fiabilidad de las operaciones. Son responsables de la automatización de los procesos industriales. Así, por su robustez, se utilizan en las Infraestructuras críticas de las naciones.

Nuevos requerimientos de gestión eficiente de la producción sugieren la integración de las redes de producción con las redes corporativas o IT (siglas en inglés de Tecnologías de la Información). Con filosofías totalmente diferentes, la integración entre ambas tecnologías abre brechas de seguridad,

La ciberseguridad en las redes OT constituye un desafío creciente debido a la prioridad de mantener procesos físicos en funcionamiento continuo frente a la aplicación limitada de mecanismos de protección. En este contexto, los sistemas SCADA cumplen un rol central al concentrar la supervisión y el control de operaciones industriales, mientras que los controladores lógicos programables (PLC según sus siglas en inglés) representan la capa de interacción directa con la infraestructura física.

Para facilitar el estudio de estas tecnologías y sus vulnerabilidades, un sistema SCADA portátil permite recrear escenarios de red donde es posible realizar análisis de ciberdefensa desplegable y recopilar datos sobre ataques dirigidos a PLC en un entorno controlado. Este enfoque posibilita la experimentación práctica sin comprometer infraestructuras críticas y contribuye a fortalecer la seguridad en entornos industriales estratégicos.

PALABRAS CLAVES: Infraestructuras críticas, Ciberseguridad, Redes OT, Ransomware, Sistema SCADA Portátil.

Abstract

Operational technology (OT according to their acronym) is hardware and software that directly monitors physical devices and processes in industrial environments. OT systems seek to maintain the continuity, security, and reliability of operations. They are responsible for the automation of industrial processes. However, due to their robustness, they are used in critical national infrastructure.

New requirements for efficient production management suggest the integration of production networks with corporate or IT (Information Technology) networks. With completely different philosophies, the integration between the two technologies opens security gaps.

Cybersecurity in OT networks is a growing challenge due to the priority of maintaining physical processes in continuous operation versus the limited application of protection mechanisms. In this context, SCADA systems play a central role by concentrating the monitoring and control of industrial operations, while programmable logic controllers (PLCs according to their acronym) represent the layer of direct interaction with the physical infrastructure. To facilitate the study of these technologies and their vulnerabilities, a portable SCADA system allows for the recreation of network scenarios, enabling deployable cyber defense analysis and the collection of data on attacks targeting PLCs in a controlled environment. This approach enables practical experimentation without compromising critical infrastructure and contributes to strengthening security in strategic industrial environments.

KEYWORDS: Critical Infrastructure, Cybersecurity, OT Networks, Ransomware, Portable SCADA System.

INTRODUCCIÓN

La expansión de la digitalización convirtió a la ciberseguridad en un eje central para resguardar tanto la información como la continuidad de los servicios. No se trata únicamente de prevenir ataques, sino también de contar con mecanismos capaces de detectarlos y responder de manera temprana.

En ese marco, las redes cumplen funciones distintas según su orientación. Las redes IT concentran la protección de datos y la disponibilidad de servicios digitales, mientras que las redes OT se enfocan en la operación ininterrumpida de procesos físicos. Esta diferencia de prioridades ha hecho que OT, apoyada en sistemas de control pre-existentes y protocolos poco flexibles, quede expuesta a mayores riesgos.

Los sistemas SCADA se ubican en el núcleo de estas redes, ya que permiten observar y coordinar procesos industriales desde un punto central. Su capacidad de supervisar múltiples equipos al mismo tiempo los vuelve imprescindibles, pero también convierte cualquier incidente en un evento de gran impacto.

Finalmente, en el nivel más próximo a la infraestructura, los PLC representan la capa física de interacción con sensores y actuadores. Su rol en la ejecución directa de las órdenes los hace críticos para la continuidad operativa y, al mismo tiempo, objetivos sensibles dentro de un escenario de ciberseguridad.

Es por ello que el objetivo del presente trabajo es contextualizar la importancia de los sistemas SCADA dentro de las redes OT, como componentes fundamentales para la supervisión y control de procesos industriales, y presentar el diseño y prototipado de un sistema SCADA portable que permita el análisis de vulnerabilidades de red como herramienta de ciberdefensa desplegable, así como la recopilación de datos de ataques a PLC en un entorno controlado.

MARCO TEÓRICO

La Ciberseguridad y las Redes

La ciberseguridad, en la época de la digitalización global, se ha vuelto un elemento esencial a considerar para el desarrollo seguro de las sociedades contemporáneas.

Este término implica un grupo de políticas, prácticas y herramientas que se han creado con el objetivo de proteger dispositivos, datos, sistemas informáticos o redes contra ciberataques. Sin embargo, la ciberseguridad no solo se encarga de la prevención de amenazas, sino también de la detección temprana y neutralización de las mismas [1].

Los pilares básicos de la ciberseguridad se basan en la llamada tríada CIA (Confidentiality, Integrity and Availability). La confidencialidad garantiza que únicamente usuarios autorizados accedan a la información; la integridad asegura que los datos no sufran modificaciones sin consentimiento; y la disponibilidad protege que los sistemas estén operativos siempre que se los necesite. Para reducir las vulnerabilidades y mantener la confianza en contextos digitales, es esencial el balance entre estos principios [2].

En este contexto, se comprende el ciberataque como la combinación de diferentes formas de delitos informáticos, como por ejemplo ciberguerra, cibercrimen o ciberdelincuencia. La finalidad de estos es robar, exponer, modificar o destruir información a través del acceso no autorizado a sistemas [3].

Diversos tipos de software dañinos, conocidos bajo el término general de malware, representan una amenaza significativa para la seguridad digital. Entre los más comunes se encuentran los virus, troyanos o spyware, que buscan destruir o manipular datos sin notificar al usuario.

En contraparte se destaca el ransomware, un tipo de malware que bloquea el acceso a sistemas o cifra archivos importantes del usuario, exigiendo un “rescate” económico para restablecerlos. No solo la disponibilidad y la integridad de los datos se ven comprometidas con este tipo de ataque, sino que puede llegar a tener un impacto sobre el funcionamiento de infraestructuras completas. A diferencia de otras variantes de malware mencionadas previamente, el ransomware opera de forma explícita con una extorsión directa y visible. Su propagación puede darse a través de correos electrónicos fraudulentos, descargas maliciosas o vulnerabilidades de red, lo que resalta la necesidad de mecanismos de detección y respuesta temprana [4].

A medida que las tecnologías digitales avanzan, también lo hacen las amenazas que buscan vulnerarlas. Los ciberataques han progresado hasta volverse operaciones complejas que se llevan a cabo con objetivos políticos, estratégicos o económicos. A su vez, el desarrollo de nuevas tecnologías, como el Internet de las cosas (IoT), la inteligencia artificial o los sistemas ciberfísicos, ha incrementado la superficie de ataque y creado nuevos frentes previamente considerados “seguros”. Esto subraya la necesidad de modificar las estrategias de ciberseguridad para lograr una protección integral [5].

Sin embargo, este proceso no se da de manera uniforme en todos los ámbitos tecnológicos. Mientras que las redes de Tecnología de la Información (IT), orientadas a la gestión de datos y servicios digitales, cuentan con mecanismos de defensa consolidados —como antivirus, firewalls o sistemas de detección de intrusos—, en otros entornos persisten limitaciones importantes. En particular, las redes de Tecnología Operacional (OT), encargadas de controlar procesos físicos, presentan brechas de seguridad que las hacen especialmente atractivas para los atacantes [13]. En estas redes, no es de importancia la tríada CIA. Se entiende así, que la ciberseguridad esté ausente entre sus prioridades.

Redes OT y su Diferencia con las Redes IT

Las redes OT se encargan de supervisar y manejar procesos físicos en el mundo industrial y digital. Esto incluye áreas de infraestructuras críticas, como el transporte, la fabricación, la energía y otros servicios básicos.

Aunque las redes tienen el mismo objetivo de sostener la actividad empresarial, sus prioridades, estructuras y riesgos son diferentes. En IT, se busca mantener un buen equilibrio entre la privacidad, la seguridad y el acceso a los datos. Se pone mucho esfuerzo en proteger la información y asegurar que los servicios digitales sigan funcionando. Por otro lado, en OT es más importante mantener la operación física sin interrupciones, aunque eso signifique usar sistemas más antiguos o protocolos de ciberseguridad menos robustos [6].

La unión gradual de las redes, llamada convergencia IT/OT, puede ofrecer grandes ventajas si se hace de forma controlada y segura. Esta unión ayuda a reunir y analizar datos de operaciones en tiempo real. Esto permite planificar mejor los recursos, optimizar la producción y reducir los costos de mantenimiento.

La digitalización y la necesidad de recopilar datos han hecho que las redes se acerquen más, lo que ha aumentado considerablemente el riesgo de ciberataques. Componentes que antes estaban separados ahora se están conectando a redes de empresas y, en algunos casos, se están poniendo en línea. Esto rompe la protección de aislamiento que tenían y ofrece oportunidades para atacantes [7].

Uno de los mayores desafíos para proteger las redes OT es que dependen de sistemas antiguos o heredados (legacy), muchos de los cuales fueron creados sin pensar en la ciberseguridad. Estos equipos a menudo no tienen apoyo, no reciben actualizaciones de seguridad y usan software desactualizado, lo que los hace muy vulnerables a las amenazas actuales. Además, las herramientas de monitoreo tradicionales generalmente no son compatibles con los protocolos industriales que son de propiedad privada. Esto dificulta contar con visibilidad sobre posibles incidentes o actividades sospechosas [8].

Estos problemas se vuelven más serios porque las soluciones en entornos OT suelen implicar grandes inversiones y tiempos de inactividad prolongados, lo cual desincentiva a las empresas a actualizar o reforzar la seguridad hasta que enfrentan un incidente grave. En otras palabras, la ciberseguridad en OT muchas veces se aborda de manera reactiva y no preventiva, lo que amplifica las consecuencias cuando un ataque finalmente ocurre [9].

La criptografía, parte esencial del ecosistema actual de la ciberseguridad, está mayormente ausente de las redes OT: los mensajes viajan en claro, lo que puede explotarse mediante ataques Hombre-en-el-Medio para lograr fácilmente el robo de secretos industriales o inyección de Malware, entre otros [10].

Este panorama destaca la necesidad urgente de desarrollar estrategias de ciberseguridad que se adapten a la realidad de las redes OT. Dentro de este contexto, los sistemas SCADA resultan esenciales para la supervisión y el control de procesos industriales, pero al mismo tiempo constituyen uno de los puntos más vulnerables y críticos dentro de estas infraestructuras.

SCADA y PLC

Los sistemas de Supervisión, Control y Adquisición de Datos (SCADA) son plataformas que permiten observar y coordinar en tiempo real procesos industriales distribuidos. Gracias a ellos es posible conectar sensores, actuadores y Controladores Lógicos Programables (PLC) que trabajan en distintos puntos de una planta o red, y centralizar toda esa información en un único sistema de gestión. Esta capacidad los convierte en una herramienta fundamental

en contextos donde resulta indispensable mantener la continuidad de operaciones a gran escala [11].

Su relevancia radica en que concentran funciones críticas que antes estaban dispersas. Desde un solo punto se pueden ajustar parámetros de producción, detectar anomalías en equipos o incluso activar protocolos de emergencia. Esa centralización, si bien facilita la operación, también implica que cualquier incidente en el SCADA pueda repercutir de manera inmediata sobre múltiples procesos al mismo tiempo. A diferencia de otros componentes de la red OT, que suelen afectar solo a un área reducida, un fallo o manipulación en estos sistemas puede tener un impacto mayor [12].

Por este motivo, se consideran un objetivo de alto valor en ciberseguridad. Una intrusión no solo compromete la disponibilidad de la información, sino que puede traducirse en interrupciones físicas de servicios esenciales.

DESARROLLO TÉCNICO

El Sistema Portátil

El escenario expuesto evidencia la necesidad de contar con un entorno controlado y flexible que permita analizar vulnerabilidades de red y evaluar el comportamiento de los PLC sin depender de infraestructuras críticas reales. Esto invita al desarrollo de un sistema SCADA portátil que posibilite desplegar escenarios de prueba en distintos ámbitos académicos o de investigación, facilitando la auditoría, la recopilación de datos y la formación práctica en ciberseguridad industrial de manera segura y reproducible.

Hardware de la Valija

Para el diseño del sistema SCADA portátil se seleccionó una valija amplia de plástico rígido, capaz de ofrecer resistencia mecánica y, al mismo tiempo, un peso reducido que facilite el transporte. En su interior se instalaron dos plataformas de madera: una en la base y otra en la tapa. Sobre estas se fijaron rieles DIN que permiten el montaje ordenado de los distintos componentes eléctricos, concentrando especialmente en la base los elementos que conforman la zona caliente.

La zona caliente se encuentra dedicada a la gestión de la alimentación eléctrica del sistema. La entrada de energía se realiza a través de un conector hembra estándar de cable de computadora (IEC C14, utilizado habitualmente en fuentes de PC). Desde este punto, la corriente se distribuye mediante dos conductores —marrón y celeste— hacia una llave térmica y posteriormente a un disyuntor diferencial, que proporcionan protección ante sobrecargas y fugas de corriente.

Una vez superadas estas etapas de protección, la instalación incluye un testigo luminoso que indica la presencia de tensión, brindando una señal visual inmediata al operador.

A continuación, se dispone de una doble toma hembra que facilita la conexión de equipos auxiliares y una fuente de alimentación Schneider Electric[1] modelo ABLS1A24031, diseñada para aplicaciones industriales. Esta fuente ofrece una entrada de 100–240 VCA (con rango extendido de 140–340 VCA) y una salida de 24 VDC con una corriente máxima de 3.13 A. Cuenta con terminales de entrada L (+) y N (–), y de salida +1, +2, –3 y –4, lo que permite una distribución estable y segura de energía para los dispositivos electrónicos internos del sistema.

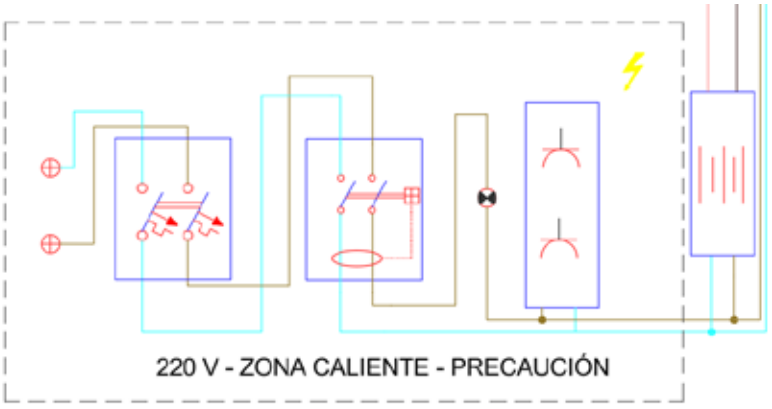

Figura 1. *Diagrama de zona caliente 220V*

Figura 2. *Prototipo de zona caliente*

La Figura 1 muestra el diagrama eléctrico de la zona caliente del sistema. En la Figura 2 se presenta su implementación física dentro del prototipo del sistema SCADA portátil.

En la base de la valija se ubica un panel de control equipado con fusibles de protección y una llave de arranque que habilita la alimentación general del sistema. Una vez activado,

[1] *Sitio Oficial de Schneider Electric Argentina: https://www.se.com/ar/es/*

un indicador luminoso señala al usuario la presencia de tensión, confirmando que el sistema se encuentra operativo.

El panel también incluye una bornera con salidas luminosas que representan las cargas controladas por el PLC, permitiendo una referencia visual del estado de las señales digitales. Además, se dispone de un puerto RJ45 Ethernet, que facilita la conexión a la red interna de la valija, y un módulo USB de 5V, destinado a la alimentación de periféricos.

En el esquema eléctrico se observa la presencia de una toma doble auxiliar, utilizada para la conexión de equipos adicionales. Esta segunda toma se encuentra instalada en la tapa del equipo, pero por fines prácticos se realizó el diagrama eléctrico completo. En la misma base se encuentran instalados la Raspberry Pi[2], ubicada en la parte inferior de la caja, y el espacio reservado al PLC, que recibe alimentación directa a través de conductores positivo y negativo (rojo y negro). Esta disposición asegura tanto la funcionalidad del sistema como la facilidad de acceso a los elementos principales durante el uso o la auditoría.

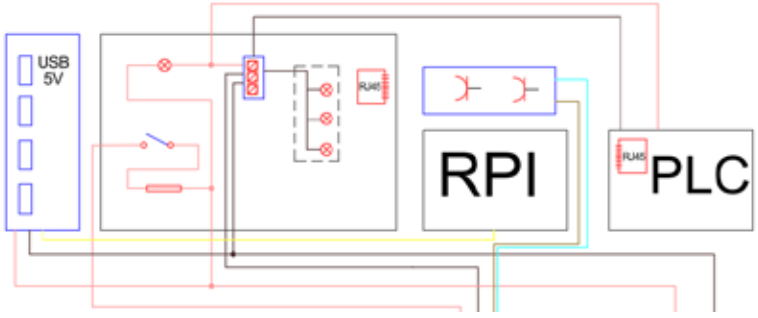

Figura 3. *Diagrama de zona de mando y control*

Figura 4. *Prototipo de mando y control*

La Figura 3 muestra el diagrama eléctrico de la zona de mando y control. En la Figura 4 se presenta su implementación física dentro del prototipo del sistema SCADA portátil. La tercera sección de la base incorpora un módulo destinado a facilitar la interacción del PLC con dispositivos externos. Este panel cuenta con una palanca de activación y un indicador

[2] *Sitio oficial de Raspberry Pi: Link: https://www.raspberrypi.com/*

luminoso (LED) que confirma al usuario que la etapa se encuentra habilitada, además de un fusible de protección para resguardar el circuito frente a sobrecorrientes.

En cuanto a su disposición, se incluyen bornes de 24V positivo y negativo, que constituyen la referencia de tensión utilizada por el PLC para accionar cargas o recibir señales. Junto a ellos se encuentran las conexiones de INPUT y OUTPUT, que permiten vincular sensores, actuadores u otros elementos de prueba, simulando condiciones de operación reales. De este modo, el módulo se convierte en un puente entre la lógica programada en el PLC y la respuesta física de los dispositivos, permitiendo experimentar con señales de control en un entorno seguro y controlado.

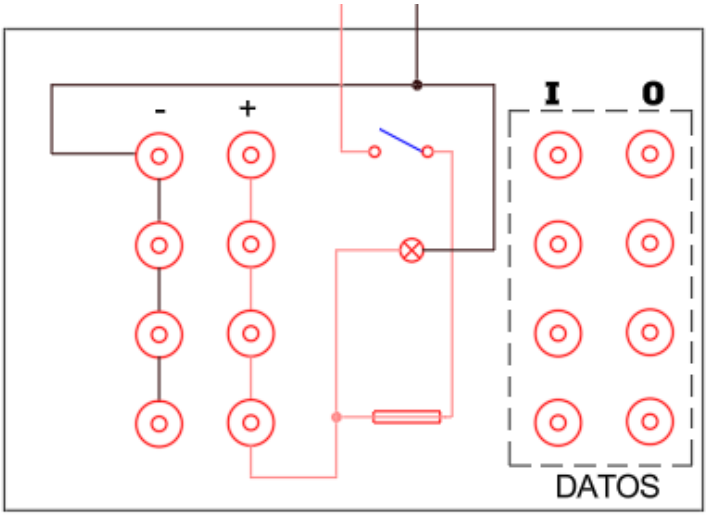

Figura 5. *Diagrama de zona de interacción*

Figura 6. *Prototipo de zona de interacción*

La Figura 5 muestra el diagrama eléctrico de la zona de interacción. En la Figura 6 se presenta su implementación física dentro del prototipo del sistema SCADA portátil.

En la tapa del sistema SCADA portátil se encuentran los elementos de visualización y comunicaciones. Se instaló una pantalla táctil LCD de 7" (1024x600, HDMI), que actúa como interfaz de visualización directa para la Raspberry Pi cuando se utiliza como estación SCADA de ingeniería. Junto a ella se dispone un switch HDMI USB 4K (Amitosai), encargado de seleccionar entre la salida de video de la Raspberry Pi y la de la PC tipo NUC, dirigiéndola hacia la pantalla o hacia un monitor externo según la necesidad.

Para la gestión de red se incorporó un switch TP-Link Omada[3] de 5 puertos (4 PoE, 65 W, Gigabit, metálico), que interconecta la Raspberry Pi, el NUC y el PLC dentro de la red local de la valija. El NUC Intel i5-11300H, con 8 GB de RAM y un disco sólido de 240 GB, cumple el rol de estación de programación de PLC, soportando software de distintas marcas (ejemplo: Siemens, Modicon, Delta).

En el diagrama eléctrico se utilizaron uniones simplificadas por fines prácticos; sin embargo, la representación corresponde a que tanto el NUC como la Raspberry Pi se encuentran conectados de manera independiente al switch TP-Link y al conmutador HDMI. Esta disposición asegura flexibilidad en las pruebas de red y en la visualización de las interfaces de control.

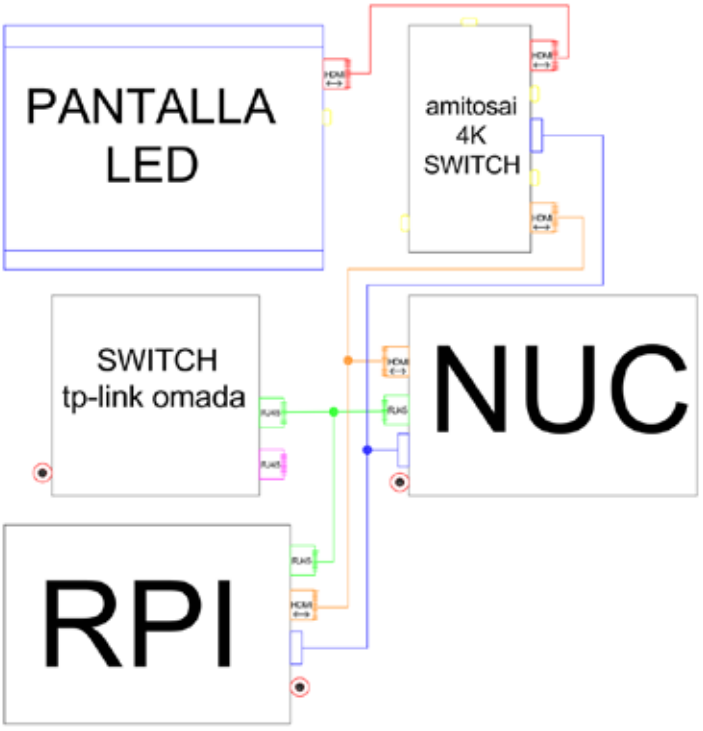

Figura 7. *Diagrama de la zona de hardware*

[3] *Sitio oficial de TP-Link Omada: https://www.tp-link.com/mx/omada/blog2/*

Figura 8. *Prototipo de zona de interacción*

La Figura 7 muestra el diagrama eléctrico de la zona de hardware. En la Figura 8 se presenta su implementación física dentro del prototipo del sistema SCADA portátil.

Software y Aplicaciones

La valija configura una celda OT completa: un PLC conectado a un SCADA Server que corre en la terminal basada en Raspberry Pi y una estación ingeniería basada en una PC tipo NUC, todos interconectados en la red local del switch.

Las terminales SCADA, tanto Server como Ingeniería tienen instalado Windows 11[4] como sistema operativo de base, utilizando en la Raspberry Pi una versión adaptada para ARM.

El panel de E/S proporciona los puntos para inyectar señales y accionar cargas a 24 V, mientras que la zona caliente concentra alimentación y protecciones. En los esquemas se emplean uniones por practicidad, pero el NUC y la Raspberry se conectan de forma independiente tanto al switch de red como al conmutador HDMI.

En la capa de software, el PLC ejecuta la lógica de control y conmuta entradas/salidas de 24 V; expone variables de proceso por Ethernet para que el SCADA las consuma. Para programación se contemplan stacks habituales del mercado: Siemens (TIA Portal, con integración de ingeniería de PLC y HMI/SCADA WinCC), Schneider Electric M221 (EcoStruxure Machine Expert Basic), Schneider Electric M262 (EcoStruxure Control Expert) y Delta[5] (WPLSoft, ISPSoft y COMMGR). Todos estos entornos se instalaron en la PC NUC.

4 *Sitio Oficial de Microsoft: https://www.microsoft.com/es-es/*

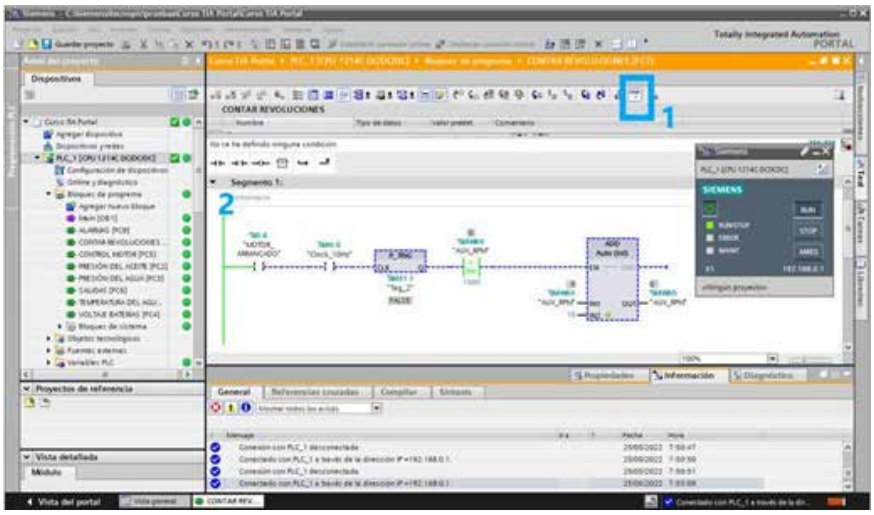

Figura 9. *Entorno de programación TIA Portal en ejecución*

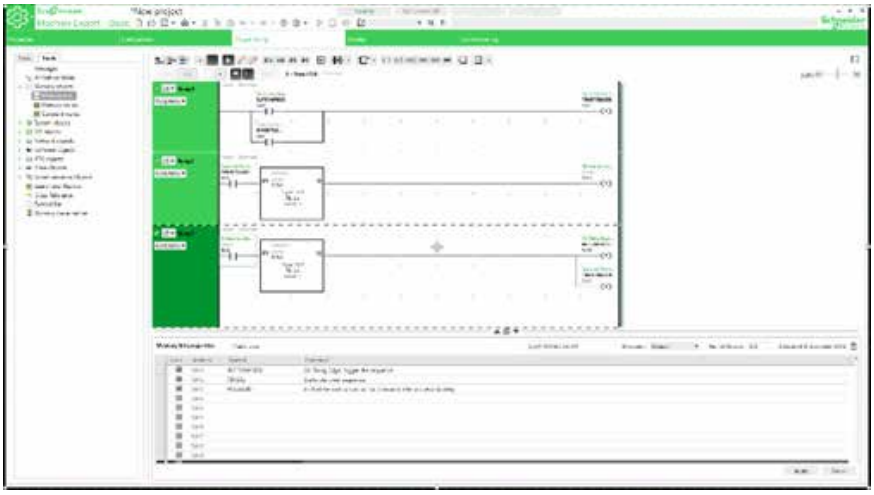

Figura 10. *Entorno de programación EcoStruxure Machine Expert – Basic en ejecución*

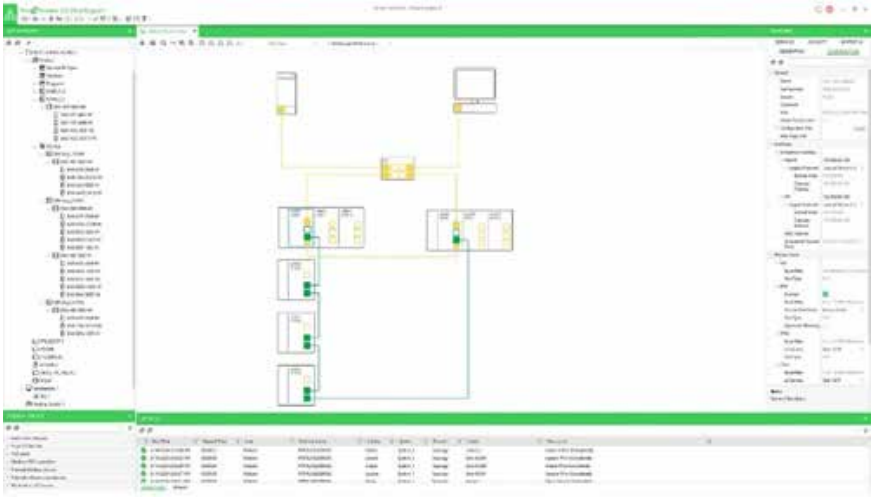

Figura 11. *Entorno de programación EcoStruxure Control Expert en ejecución*

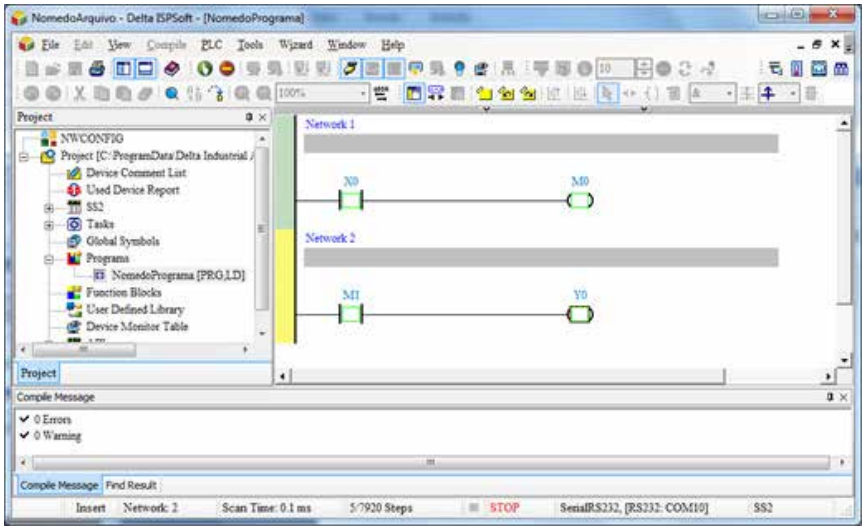

Figura 12. *Entorno de programación Delta ISPSoft en ejecución*

El SCADA servidor en la Raspberry Pi hospeda el runtime HMI/SCADA. Se instaló allí la plataforma Rapid SCADA; desde allí se visualiza, registra y opera el proceso.

La PC NUC funciona como estación de ingeniería/operador: muestra el “plano en caliente” (compuertas, luces, alarmas) y sirve como consola liviana para diagnóstico, ya sea contra el runtime (Raspberry Pi) o contra paneles expuestos por el propio SCADA.

La Red de Comunicaciones

La comunicación de datos puede realizarse mediante drivers del fabricante y también mediante estándares de interoperabilidad. Entre estos, OPC UA (IEC 62541) permite intercambiar variables entre PLC, SCADA y clientes de manera independiente de plataforma; para compatibilidad amplia, también puede emplearse Modbus/TCP en escenarios donde resulte conveniente (este esquema tiene implementado Modbus TCP). La elección concreta de protocolo y nivel de seguridad depende de la configuración del proyecto y del software instalado.

Funcionamiento Típico

El funcionamiento típico comienza con la energización: la zona caliente habilita térmica y disyuntor, y el testigo confirma presencia de tensión. Luego, PLC, NUC y Raspberry se asocian al switch; el conmutador HDMI permite seleccionar qué equipo se visualiza. Desde la NUC se descarga o ajusta el programa del PLC (según el stack elegido) y se levanta el runtime SCADA con sus tags, pantallas, alarmas e históricos. La Raspberry muestra el estado en tiempo real y el módulo de 24 V + I/O permite conectar sensores y accionar actuadores, reproduciendo condiciones de operación en un entorno mínimo controlado.

Una vez que el sistema se encuentra en operación, se conectan los dispositivos elegidos para cada caso de uso de interés. Así, las interacciones con el dispositivo conectado se capturan y se almacenan para su posterior análisis.

Casos de Uso: Escenarios de Prueba

Sobre esta base, la valija habilita actividades de ciberdefensa desplegable y auditoría de red sin afectar infraestructuras reales. Es posible capturar tráfico, etiquetar pruebas y correlacionar eventos / alarmas / históricos para construir conjuntos de datos orientados a análisis.

Los desarrollos en Forensia Informática sobre SCADA son muy escasos. Un objetivo de este proyecto es brindar un marco de pruebas para investigaciones en esta disciplina (reconstrucción de líneas de tiempo con logs, descargas y pcaps).

Se dispone de terminales portables que permiten realizar pruebas de intrusión controladas sobre PLCs. Al instalarse sobre riel DIN, es posible intercambiar los PLCs y probar el efecto de estos ataques sobre diferentes marcas y modelos de PLC.

Se busca también que este escenario pueda usarse para instalar y experimentar con herramientas criptográficas.

CONCLUSIONES

La valija SCADA presentada articula, en un único soporte transportable, los elementos esenciales de una celda OT: PLC, servidor SCADA en Raspberry Pi, estación de ingeniería/operador en NUC, red local y panel de E/S a 24 V con protecciones dedicadas. Esta integración habilita un entorno controlado y reproducible para programar, visualizar y auditar procesos, ejecutar pruebas de red y obtener trazas de operación sin comprometer infraestructuras reales.

El enfoque propuesto aporta valor práctico en varios frentes, presentados en los casos de uso, aunque no se limita a ellos, y puede expandirse a otros: pudiéndose montar escenarios de evaluación, ejercicios de respuesta para distintos ámbitos, recopilar datos sobre comportamientos del sistema y del tráfico asociado, facilitando el análisis posterior; así como para formación e investigación aplicada.

TRABAJOS FUTUROS

Como futuras líneas de trabajo, se prevé que la valija sirva como un banco de pruebas multiproveedor y multiprotocolo, donde se podrían incorporar distintas familias de PLC y pilas de comunicación para contrastar comportamientos de ingeniería y operación. Asimismo, se podrían empaquetar “escenas” reproducibles —topologías, tags, alarmas, históricos y reglas

de red— como proyectos versionados, de modo que un mismo caso se levantaría en minutos y permitiría comparar métricas entre equipos y sesiones.

En paralelo, la plataforma podría profundizar la instrumentación de datos mediante telemetría unificada y etiquetado de estados del PLC, cambios de programa, alarmas, tendencias y capturas de red. Sobre esa base, se definiría un tablero de indicadores —latencias de ciclo, jitter de E/S, tiempos de conmutación, carga de CPU/memoria, utilización de enlaces, tiempos de deploy y de recuperación— que permitiría análisis objetivos y comparables entre configuraciones.

Para la observabilidad y la forensia, se prevé un canal de registro centralizado que recogería eventos de red, SCADA/HMI y PLC, los normalizaría y permitiría consultas históricas y playbacks de incidentes. Ese pipeline podría complementarse con procedimientos de cadena de custodia —sellado temporal e integridad de artefactos—, facilitando la reconstrucción de líneas de tiempo con evidencia cruzada entre capas.

En materia de seguridad de comunicaciones, se evaluarían configuraciones criptográficas disponibles en los protocolos soportados y su impacto en el desempeño y la disponibilidad, junto con políticas de gestión y rotación de credenciales. A ello se sumaría una segmentación orientada a OT (zonas y conductos, VLANs, listas de control) y la incorporación de sensores de tráfico para inventario, línea base de comportamiento y alertas ante desviaciones. La orquestación de servicios auxiliares en contenedores o máquinas virtuales permitiría aislar roles, acotar interferencias entre pruebas y habilitar rollbacks limpios.

Con vistas a la validación operativa, se construiría una biblioteca de emulación de acciones de adversario y de fallas del proceso (errores de operador, inconsistencias de sensores, rebotes, inversiones lógicas), cada una con criterios de activación, observables esperados y métricas de detección/recuperación. El acople a una planta simulada o digital twin permitiría cerrar el lazo de control y ensayar perturbaciones, saturaciones, arranques / paradas y fail-safes sin riesgo físico, además de planificar campañas de estrés con condiciones adversas controladas (pérdida intermitente de red, degradación de ancho de banda, latencias inducidas o ráfagas de eventos).

Finalmente, el proyecto podría derivar módulos didácticos con rúbricas de evaluación y check-lists de seguridad, incluso en modalidad multiusuario con ejercicios tipo red/blue team. En lo físico, se contemplarían mejoras de portabilidad y resiliencia —alimentación ininterrumpida, guiado y etiquetado de cableado, organización de conectores, serigrafía y ergonomía— junto con guías operativas y pautas éticas que asegurarían un uso seguro, repetible y medible en contextos académicos y de laboratorio. En conjunto, estas líneas permitirían consolidar la valija como una plataforma versátil para estudiar, con control y trazabilidad, el comportamiento de sistemas OT/SCADA bajo diversas configuraciones operativas y de seguridad.

REFERENCIAS

[1] Craigen, D., Diakun-Thibault, N. y Purse, R., "Defining Cybersecurity". Technology Innovation Management Review, Octubre 2014. *https://timreview.ca/article/835*. Recuperado online en junio de 2025.

[2] Chai, K. Y., y Zolkipli, M. F., "Review on confidentiality, integrity and availability in information security". Journal of ICT in Education, 8(2), 34-42. 13-07-2021. *https://ejournal.upsi.edu.my/index.php/JICTIE/article/view/5203*. Recuperado online en junio de 2025.

[3] Centeno, F. J. U., "Ciberataques, la mayor amenaza actual". Pre-bie3, 2015, no 1, p. 42, enero 2015. *https://dialnet.unirioja.es/descarga/articulo/7684551.pdf*. Recuperado online en junio de 2025.

[4] Gamboa Suarez, J. L., "Importancia de la seguridad informática y ciberseguridad en el mundo actual". (Trabajo de Grado), Universidad Piloto de Colombia, agosto 2020. *https://repository.unipiloto.edu.co/handle/20.500.12277/8668*. Recuperado online en junio de 2025.

[5] Salman, H. A. y Alsajri, A., "The evolution of cybersecurity threats and strategies for effective protection. A review". (Artículo en revista científica), SHIFRA vol. 2023, p. 73-85, agosto 2023. *https://peninsula-press.ae/Journals/index.php/SHIFRA/article/view/36* Recuperado online en junio de 2025.

[6] Candelario, E. H., y González, J. M. E., "Ciberseguridad en Sistemas de Control Industrial". (Trabajo de Grado), Universidad de Sevilla, junio 2024. *https://idus.us.es/items/4acbe8c1-a2eb-464e-b788-c641700b6fd2*. Recuperado online en agosto 2025.

[7] Cortés-Llanganate, L., y Quevedo-Sacoto, A., "Soluciones de monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. Revisión de literatura". (Artículo en revista científica), 593 Digital Publisher CEIT, 9(6), 5-17, noviembre 2024. *https://dspace.ucacue.edu.ec/handle/ucacue/18741*. Recuperado online en agosto 2025.

[8] García Núñez, N., "Análisis, explotación y refuerzo de vulnerabilidades en entornos de convergencia IT/OT." (Trabajo de grado), Universidad de Valladolid. Escuela de Ingeniería Informática de Valladolid, 2024. *https://uvadoc.uva.es/handle/10324/71360*. Recuperado online en agosto 2025.

[9] Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., y Benjamin, J. "Vulnerabilities and attacks against industrial control systems and critical infrastructures." (Preprint académico), arXiv:2109.03945 [cs.CR], 2021. *https://arxiv.org/abs/2109.03945*. Recuperado en agosto 2025.

[10] Tramontina, J. F. C., Neil, C., Kamlofsky, J., & Hecht, P. (2023). Criptografía aplicada en entornos industriales: un mapeo sistemático de la literatura. JAIIO, Jornadas Argentinas de Informática, 9(8), 58-73.

[11] Yadav, G., y Paul, K., "Architecture and Security of SCADA Systems: A Review." (Preprint académico), arXiv:2001.02925 [cs.CR], 2020. *https://arxiv.org/abs/2001.02925*. Recuperado online en agosto 2025.

[12] Smurthwaite, M., & Bhattacharya, M., "Convergence of IT and SCADA: Associated Security Threats and Vulnerabilities." (Preprint académico), arXiv:2005.04047 [cs.CR], 2020. *https://arxiv.org/abs/2005.04047*. Recuperado online en agosto 2025.

[13] Simon Daniel Duque Anton, & Daniel Fraunholz. “The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World”. (Preprint académico), arXiv:2111.13862 [cs.CR]. *https://arxiv.org/abs/2111.13862*. Recuperado online en agosto 2025.