XX Simposio CEA de Control Inteligente
25-27 de junio de 2025, Huelva

Banco de pruebas para evaluación de técnicas IA en la detección de anomalías en sistemas ciberfísicos industriales

Martín-Fraile, J.V.[a, *], Sierra-García, J.E.[a], Basurto, N.[b]

[a] *Departamento de Digitalización, Ingeniería de Sistemas y Automática, Universidad de Burgos, C/ Hospital de Rey, sn, 09001 Burgos, España.*
[b] *Departamento de Digitalización, Ciencia de la Computación e Inteligencia Artificial, Universidad de Burgos, C/ Hospital de Rey, sn, 09001 Burgos, España.*

To cite this article: Martín-Fraile, J.V., Sierra-García, J.E., Basurto, N., 2025. Testbed for the Evaluation of AI Techniques in Anomaly Detection for Industrial Cyber-Physical Systems. XX Simposio CEA de Control Inteligente, Huelva (Spain), 2025.

Resumen

Los Sistemas Ciberfísicos (CPS) industriales, impulsados por la Industria 4.0, han mejorado la monitorización y el control en tiempo real de procesos productivos, así como la automatización en fábricas inteligentes, lo que ha incrementado la demanda de datos. Esta situación ha acelerado la convergencia entre tecnologías de la información (IT) y operativas (OT), aumentando la exposición de sistemas de control, especialmente los basados en Controladores Lógicos Programables (PLCs), a ciberataques. En este contexto este artículo presenta un Banco de Pruebas para la Detección de Anomalías y Protección de Sistemas Ciberfísicos Industriales (DAyPSCI), una plataforma híbrida, abierta y flexible, orientada a la investigación y formación en ciberseguridad aplicada a Sistemas de Control Industrial (ICS). DAyPSCI permite generar conjuntos de datos (datasets) con información de proceso y del estado del sistema, siguiendo la metodología GEMMA. Además, posibilita la ejecución de ataques controlados sobre dispositivos industriales reales, facilitando el estudio de vulnerabilidades y la validación de mecanismos de detección y protección.

Palabras clave: Sistema ciberfísico, Control industrial, Controlador lógico programable (PLC), Interfaz hombre-máquina (HMI), Detección de anomalía, Ciberseguridad.

Testbed for the Evaluation of AI Techniques in Anomaly Detection for Industrial Cyber-Physical Systems

Abstract

Industrial Cyber-Physical Systems (CPS), driven by the implementation of Industry 4.0, have enhanced real-time monitoring and control of production processes, as well as automation in smart factories, leading to increased data demand. This situation has accelerated the convergence of Information Technology (IT) and Operational Technology (OT), increasing the exposure of control systems—especially those based on Programmable Logic Controllers (PLCs)—to cyberattacks. This article presents the Testbed for Anomaly Detection and Protection of Industrial Cyber-Physical Systems (DAyPSCI), a hybrid, open, and flexible platform designed for research and training in cybersecurity applied to Industrial Control Systems (ICS). DAyPSCI enables the generation of datasets containing both process data and system state information, following the GEMMA methodology (Guide for the Study of Operating Modes of an Automated System). Additionally, it allows the execution of controlled cyberattacks on real industrial devices, facilitating the study of vulnerabilities and the validation of detection and protection mechanisms.

Keywords: Cyber-physical system, Industrial control, Programmable logic controller (PLC), Human-machine interface (HMI), Anomaly detection, Cybersecurity.

1. Introducción

Los sistemas Ciberfísicos (CPS, por sus siglas en inglés) integran procesos computacionales y físicos para automatizar tareas complejas del mundo real (Serpanos, 2018; Hosseinzadeh *et al.*, 2024). Estos sistemas aprovechan los avances tecnológicos en sensores, redes de comunicación y computación embebida especialmente mediante el uso de Controladores Lógicos Programables (PLC). Combinan

*Autor para correspondencia: jvmartin@ubu.es

componentes de software y hardware para interactuar con el entorno físico de forma automática y eficiente.

Entre sus funcionalidades destacan la monitorización y control en tiempo real de procesos físicos, como la gestión energética en redes inteligentes o la optimización y automatización de la producción en fábricas inteligentes.

Sin embargo, esta creciente evolución tecnológica no está exenta de riesgos. En el año 2024, el número de ciberataques a sistemas ciberfísicos creció de forma significativa en comparación con el año anterior (Fortinet, 2024; Faelli, 2025). Este aumento evidencia su creciente vulnerabilidad y exposición, y refuerza la necesidad urgente de implementar medidas de ciberseguridad más robustas para proteger los Sistemas de Control Industrial (ICS) y reducir el impacto de las amenazas cibernéticas (Han *et al.*, 2021; Nankya, Chataut, & Akl, 2023).

Según el informe del Equipo de Respuesta a Emergencias Informáticas del Centro Criptológico Nacional CCN-CERT (2024), así como estudios como los de Pospisil et al. (2021), Domínguez *et al.* (2022) y Benka *et al.* (2025), la creciente integración de tecnologías de la información (IT) y las tecnologías operativas (OT) con sistemas como SCADA (Supervisory Control and Data Acquisition), HMI (Human Machine Interface), PLC (Programmable Logic Controllers) y DCS (Distributed Control Systems) ha incrementado significativamente la exposición de los sistemas de control industrial (ICS, Industrial Control Systems) a amenazas cibernéticas.

La implementación de la industria 4.0 ha acelerado esta convergencia IT/OT permitiendo a las empresas mejorar su eficiencia operativa, tomar decisiones basadas en datos en tiempo real y reducir costes mediante la automatización avanzada y el mantenimiento predictivo. Esta integración proporciona una visión holística de los procesos productivos y del negocio, lo que se traduce en una mayor capacidad de adaptación, competitividad y optimización de recursos.

En este artículo se presenta el Banco de Pruebas para la Detección de Anomalías y Protección de Sistemas Ciberfísicos Industriales (DAyPSCI), una plataforma diseñada con fines de investigación y formación en ciberseguridad aplicada a Sistemas de Control Industrial (ICS). El objetivo de DAyPSCI es doble: por un lado, facilitar el desarrollo y validación de nuevos mecanismos de detección y protección frente a amenazas cibernéticas; y por otro, proporcionar un entorno experimental accesible para la docencia en ciberseguridad industrial.

La estructura del resto del artículo es la siguiente. La sección 2 introduce la arquitectura de los CPS industriales. El banco de pruebas se presenta en la sección 3. La sección 4 ejemplifica un caso de uso del banco. La sección 5 explica cómo se pueden generar un dataset con el banco de pruebas. Se presentan resultados en la sección 6. El artículo finaliza con las conclusiones y trabajos futuros.

2. Arquitectura de los CPS industriales

La arquitectura de un CPS clásico generalmente consta de tres capas principales:

- **Capa física:** Incluye todos los sensores y actuadores que interaccionan con el mundo físico. Los sensores captan información de las variables relevantes del proceso y los actuadores ejecutan acciones físicas basadas en órdenes de la capa computacional.
- **Capa de red**: Está formada por la infraestructura que permite la comunicación entre la capa física y la capa de computacional.
- **Capa de computacional**: Procesa los datos recibidos de los sensores, realiza cálculos y toma decisiones para controlar los actuadores. Esta capa puede incluir sistemas de control en tiempo real, análisis de datos y algoritmos de inteligencia artificial (Oks *et al.*, 2022).

La Figura 1, muestra una imagen de dicha arquitectura. En aplicaciones industriales, como los CPS basados en PLCs, la capa computacional se implementa mediante el propio PLC, que actúa como el componente principal encargado del procesamiento de datos y la ejecución de tareas de control.

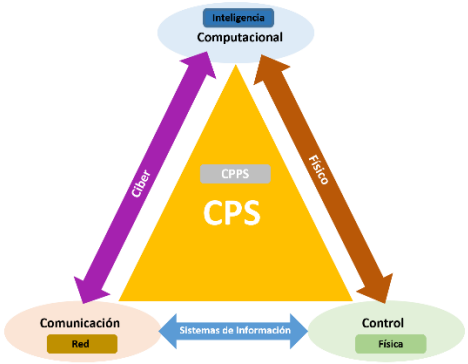

Figura 1: Arquitectura de un CPS Industrial

A nivel de implementación, diversos autores han adoptado la Arquitectura de Referencia Empresarial de Purdue (PERA), como es el caso de Alrumaih, Alenazi, AlSowaygh, Humayed y Alablani (2023), así como Hosseinzadeh *et al.* (2024). Esta arquitectura también ha sido incorporada por empresas líderes en soluciones de ciberseguridad, como Fortinet.

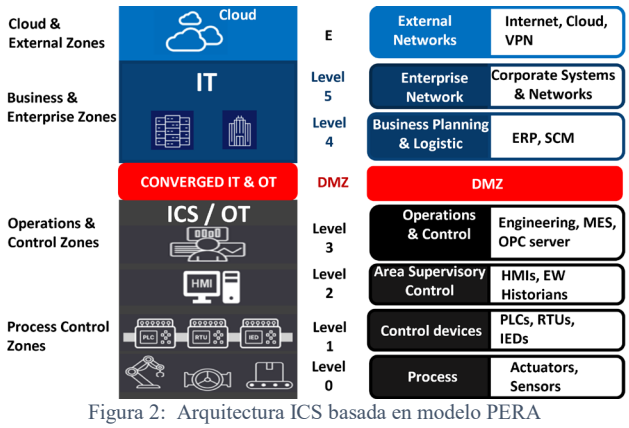

Figura 2: Arquitectura ICS basada en modelo PERA

La arquitectura PERA es un marco para organizar los ICS en zonas o niveles definidos (Alrumaih *et al.*, 2023), creando una estructura jerarquizada separando equipos IT/OT y facilitando la implementación de los requisitos de seguridad establecidos por la norma ISA/IEC 62443-2-1:2024 (International Society of Automation [ISA] & Comisión Electrotécnica Internacional [IEC], 2024). En la Figura 2, se pueden apreciar las zonas, con sus distintos niveles, separadas por la región convergencia entre tecnologías también designada como zona desmilitarizada (DMZ, por sus siglas en inglés), cuya misión es la de permitir a la organización conectarse de manera segura a redes con diferentes requerimientos de seguridad y de este modo proteger la zona empresarial y la de control.

3. Banco de Pruebas para evaluación de técnicas IA en la detección de anomalías en CPS industriales

En general los bancos de prueba de CPS industriales se clasifican, según los componentes que integran en los siguientes tipos (Hosseinzadeh *et al*. 2024):

- **Virtuales**: Son soluciones basadas exclusivamente en software lo que les dota de gran flexibilidad y escalabilidad.
- **Físicos**: Incluyen componentes reales, como sensores, actuadores, dispositivos de red, controladores, etc., es decir son un reflejo del ICS real.
- **Híbridos**: Combinan componentes virtuales y físicos. Son adecuados para probar sistemas integrados industriales sin un elevado coste del equipo de pruebas.

El banco de pruebas presentado en este artículo se enmarca dentro de la categoría híbrida porque combina componentes físicos y virtuales.

3.1. Arquitectura

El banco de pruebas presenta una arquitectura abierta y flexible basada en el modelo PERA, lo que permite recrear condiciones propias de un entorno industrial real. Esto es posible gracias a que la mayoría de sus componentes son equivalentes a los presentes en sistemas automatizados reales, con la excepción del proceso industrial físico (sensores, actuadores, piezas, etc.), el cual se implementa mediante un gemelo digital.

Un gemelo digital es una representación virtual de objetos, procesos o sistemas que existen y operan en tiempo real (Javid, Haleem, & Suman, 2023). Para simular condiciones de comunicación industrial más realistas, este gemelo digital emplea un PLC como interfaz Profinet con el sistema, el cual está conectado a un switch industrial. De esta forma, el PLC de nivel 1 puede enviar órdenes y recibir señales de entrada del proceso a través del PLC de nivel 0, como si estuviera controlando un proceso físico mediante Profinet I/O. Además, el sistema incorpora una interfaz HMI que permite al operador interactuar con el proceso virtual. Esta versión inicial contempla únicamente los niveles correspondientes a la zona de control del proceso, como se muestra en la Figura 3. No obstante, su arquitectura modular y escalable permite la incorporación de nuevos componentes, lo que facilita la expansión hacia otras zonas y niveles del modelo PERA.

Figura 3: Arquitectura de red del Banco

Con el objetivo de utilizar el banco de pruebas para la evaluación de técnicas de inteligencia artificial (AI) en la detección de anomalías y la protección de sistemas ciberfísicos, y así contribuir a mejorar su resiliencia, se ha incorporado una base de datos gestionada mediante Microsoft SQL Server 2022. Esta base de datos permite la generación y almacenamiento de conjuntos de datos (datasets) para su posterior análisis. Aunque por defecto se encuentra alojada en la estación de ingeniería, su ubicación no constituye un requisito obligatorio, ya que puede ser desplegada en otros entornos compatibles.

Asimismo, el banco permite la conexión de un PC de monitorización para la captura de tramas y paquetes de comunicación mediante herramientas como Wireshark u otras similares. También se contempla la posibilidad de conectar un equipo con Kali Linux, lo que facilita la ejecución y evaluación de diversas técnicas de ataque, con fines de prueba y validación de mecanismos de defensa.

3.2. Componentes

La Tabla 1 muestra los componentes que conforman la versión inicial del Banco de pruebas:

Tabla 1: Componentes del Banco de pruebas.

Nº	Dispositivo	Modelo	Descripción
1	PS	6EP1333-4BA00	Fuente de alimentación
2	PLC	6ES7512-1CK01-0AB0	PLC
3	PC		Gemelo digital
4	PLC	215-1BG40-0XB0	Interfaz profinet I/O
5	Switch	208-0BA00-2AC2	Switch industrial
6	HMI	6AV2128-3GB06-0AX1	Panel HMI
7	PC		Estación de ingeniería

4. Contextualización de un caso de uso

En esta sección se presenta un caso de uso del banco de pruebas con el fin de mostrar su aplicabilidad. Para ello, se ha elegido un proceso industrial muy sencillo, como es un sistema de marcaje de piezas. El objetivo de este sistema es el de alimentar con piezas el marcador, realizar la operación de marcaje, y posteriormente expulsar las piezas procesadas por el sistema.

4.1. Gemelo digital de un sistema de marcaje de piezas

Con el fin de disponer de información de sensores, piezas, pre-accionadores y actuadores, es decir datos de proceso comparables a los de un proceso real, junto con su correspondiente visualización animada se ha empleado la aplicación *PCSimu* (PCSimu, 2023). Esta herramienta permite el diseño y visualización 2D y ha sido utilizada para generar el gemelo digital del sistema de marcaje.

Como se muestra en la Figura 4, el sistema está compuesto por tres actuadores (A, B y C), cada uno con sus respectivos sensores magnéticos de posición (a0, a1, b0, b1, c0 y c1), un generador de piezas, y dos sensores de presencia (B1 y B2), ubicados en las zonas de alimentación y marcaje, respectivamente. Los actuadores están configurados como cilindros de doble efecto, controlados mediante electroválvulas 5/2 de tipo biestable.

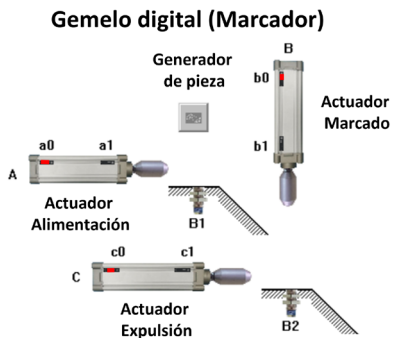

Figura 4: Gemelo digital.

La aplicación *PCSimu* también permite ajustar las velocidades de avance y retroceso de los actuadores, lo que contribuye a una simulación más realista del comportamiento dinámico del proceso. Además, como se muestra en la Figura 3, el gemelo digital se conecta al PLC 2, que actúa como interfaz Profinet I/O (PNIO), mediante su conexión al puerto 1 del switch industrial. Esta configuración permite el intercambio de información entre el gemelo digital y el PLC 1 a través de comunicación Profinet I/O, reproduciendo así una arquitectura de periferia descentralizada típica de entornos industriales modernos.

4.2 Interfaz HMI

Para interactuar con el sistema ICS, se ha implementado una interfaz como la mostrada en la Figura 5. A través de esta interfaz, el operador puede ajustar parámetros como el **tiempo de actuación** de la matriz sobre la pieza, el **número de golpes** del marcador por pieza y la **cantidad de piezas** a marcar en cada lote. Además, el selector **MAN/AUT** permite elegir entre el modo manual y el modo automático de funcionamiento de la instalación. En modo manual, los pulsadores **AV_x** y **RE_x** (donde $x = A, B \ o \ C$), con contacto **NO** (Normally Open), permiten al operador emitir órdenes de avance y retroceso a los actuadores, si fuera necesario.

La interfaz también incorpora otros pulsadores como **marcha**, **paro**, **rearme**, **reset** y **ack**, cuya función es emitir las siguientes órdenes: inicio del modo automático, parada al final del ciclo, rearme de la instalación, reseteo del lote de piezas y confirmación de eventos solicitados, respectivamente.

Asimismo, se incluye un **pulsador de parada de emergencia** con contacto **NC** (Normally Closed, por sus siglas en inglés). En cuanto a la señalización, el sistema cuenta con una **baliza luminosa** compuesta por cuatro pilotos de colores: **rojo**, **verde**, **azul** y **amarillo**, que proporcionan información visual sobre el estado de las salidas digitales.

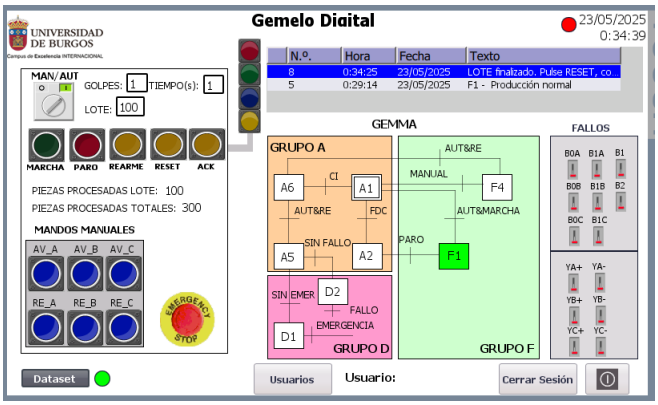

Figura 5: Interfaz Hombre Máquina.

Como ya se ha comentado anteriormente el equipo está diseñado también con fines educativos y por ello incorpora la metodología **GEMMA** (Guía de Estudio de los Modos de Marchas y Paradas, de un sistema automatizado). El **grupo A** incorpora procedimientos de parada. **A1**: parada en el estado inicial, **A2**: parada pedida a fin de ciclo, **A5**: preparación para la puesta en marcha tras fallo y **A6**: puesta del sistema en el estado inicial. El **grupo F**, proceso en funcionamiento incorpora **F1**: producción normal y **F4**: marchas de verificación sin orden o modo manual. Finalmente, el **grupo D** proceso en defecto contempla **D1**: para de emergencia y **D2**: diagnóstico y/o tratamiento de los defectos.

La gestión de la parada de emergencia y el rearme se debe considerar la parte principal de un programa de autómata (Piedrafita, 2004). Por ello, para facilitar al operador la operación de rearme está dotado entre otros con dicho pulsador y de un sistema de avisos que lo guía e informa del estado de la instalación con objeto de facilitar al operador la operación del rearme de la instalación.

Otro de los objetivos es la detección de anomalías en el sistema y en ese sentido está dotado con los interruptores **B0x**, **B1x**, **Yx+** e **Yx-** ($x = A, B \ y \ C$) que permiten simular fallos en los sensores (B) y en los preaccionadores, es decir en las electroválvulas (Y) que gobiernan a los actuadores. Esto permite contemplar fallos o anomalías como ocurre en los sistemas reales y añadir esta información en la generación del dataset.

4.3. Proyecto TIA Portal

Para llevar a cabo la configuración, programación y puesta en marcha del banco de pruebas, se generó un proyecto utilizando la herramienta TIA Portal (Totally Integrated Automation Portal) en su versión 18, desarrollada por el fabricante Siemens (TIA Portal, 2022). La Figura 6 muestra la configuración de red realizada dentro de dicho proyecto.

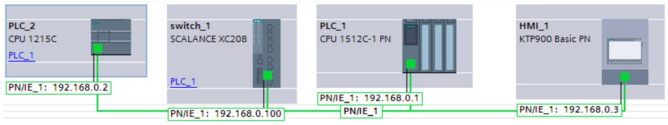

Figura 6: Configuración de red en TIA Porta V18.

Una vez realizada la configuración del hardware del proyecto el siguiente paso fue abordar la programación del PLC 1, cuya función principal es controlar el proceso de marcado. Esta programación se llevó a cabo utilizando programación estructurada, empleando los siguientes lenguajes definidos por la norma IEC-61131-3: diagrama de contactos KOP, diagrama de funciones secuenciales S7-Graph y lenguaje de control estructurado SCL.

5. Creación de un conjunto de datos

Como se mencionó anteriormente el banco de pruebas está equipado con una base de datos que registra todos los eventos programados que ocurren en el sistema, lo que le permite la generación de conjuntos de datos (datasets) para su posterior análisis. Las variables recogidas se describen en la Tabla 2 indicando el tipo de datos y una breve descripción con el significado de la información que registra.

Tabla 2: Campos del dataset.

Variable	Tipo	Descripción
Timestamp	Time	Hora del evento.
Duración	Int	Unidades en milisegundos.
Sensores	Boolean	B0_x0, B1_x1, x=a, b y c, B1 y B2
Actuadores	Boolean	YA+, YA-, YB+, YB-, YC+, YC-.
Anomalías	Int	0-Sin anomalía, 1-Sensores, 2-Actuadores, 3-Múltiple.
GEMMA	Int	Modos: 0-A1, 1-F1, 2-A2, 3-D1, 4-F4, 5-A5, 6-A6, 7-D2.
Ataques	Int	0-Sin ataque, 1- DoS, 2-MITM.

5.1 Captura de datos de proceso

Para validar la información contenida en el conjunto de datos, relativa a las comunicaciones con la periferia descentralizada, se incluye en la Figura 7 una captura de Wireshark que muestra los datos de proceso correspondientes a las entradas, transmitidos mediante el protocolo Profinet IO. En dicha captura, el valor hexadecimal 0x55 indica que los actuadores se encuentran en su posición inicial y que el sistema dispone de una pieza en el alimentador (véase Tabla 2).

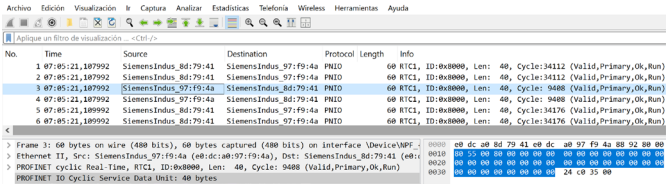

Figura 7: Datos de proceso de entradas.

5.2 Etiquetado del dataset

Con el objetivo de disponer de datos adecuados para su evaluación mediante técnicas de AI orientadas a la detección de anomalías y la protección de sistemas ciberfísicos, se han generado dos conjuntos de datos conforme a la información recogida en la Tabla 2: uno correspondiente a un proceso sin anomalías y otro con anomalías introducidas de forma controlada.

- **Sin anomalías**: Este conjunto recoge la información del banco de pruebas configurado con un lote de 100 piezas, aplicando un golpe por pieza y un tiempo de apriete de un segundo por unidad (véase Figura 5).
- **Con anomalías**: En este caso, la configuración del banco es idéntica a la anterior. No obstante, se han introducido de forma controlada 12 fallos en las electroválvulas que gobiernan los actuadores.

6. Resultados

A partir del conjunto de datos generado sin anomalías, se realizó un análisis exploratorio utilizando la Transformada Rápida de Fourier (FFT) con el objetivo de clasificar los datos en intervalos correspondientes a eventos de origen real o ciclos de proceso. Esta técnica permite identificar patrones periódicos subyacentes en los datos, derivados de la naturaleza cíclica de los procesos de producción automatizados (Sai, *et al.*, 2023).

Aplicando esta metodología, se realizó la reconstrucción temporal de las señales de ambos conjuntos de datos y a continuación se muestrearon a intervalos uniformes de 10 ms. Las señales resultantes de los datos recogidos con anomalías se presentan en la Figura 8 y en ella claramente se observan las 12 anomalías.

A continuación, se aplicó la Transformada Rápida de Fourier (FFT) a las señales binarias de sensores y actuadores, del conjunto de datos sin anomalía identificándose la frecuencia dominante, en el espectro de frecuencias que se representa en la siguiente Figura 9.

Para el conjunto de datos generado con anomalías, también se realizó la FFT de las mismas señales y su espectro se muestra en la Figura 10.

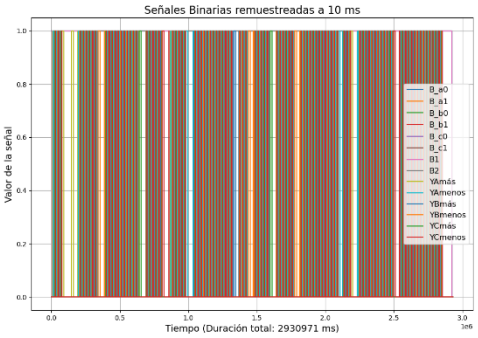

Figura 8: Señales de datos de proceso con anomalías.

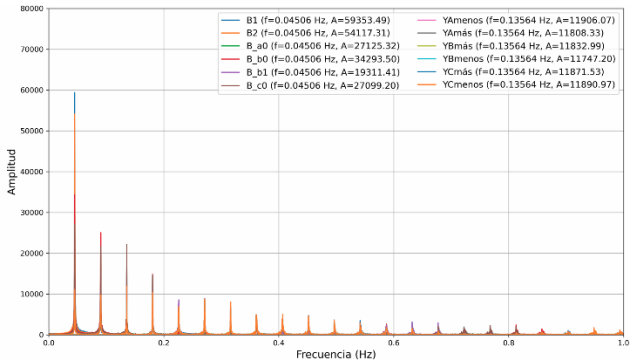

Figura 9: FFT de datos de proceso sin anomalías

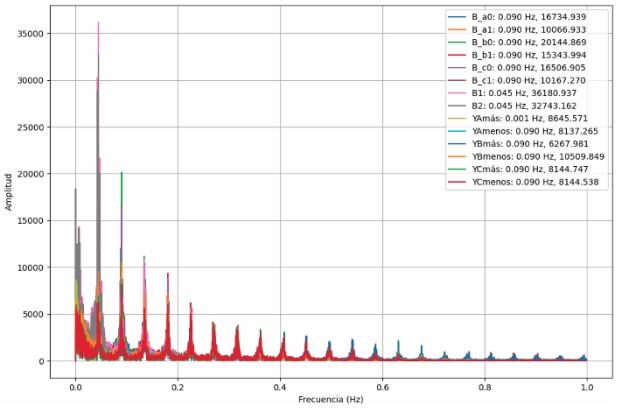

Figura 10: FFT de datos de proceso con anomalías

5.1 Análisis de resultados

El tiempo total empleado en el marcado del lote programado del conjunto de dados sin anomalía fue de **2.223.568 milisegundos**, es decir, aproximadamente **37,06 minutos**.

De forma complementaria, en la Figura 9 se identifica un pico dominante en la frecuencia de **0,04506 Hz**. A partir de esta frecuencia, es posible calcular el tiempo de ciclo de producción utilizando la siguiente expresión:

$$t_{Ciclo} = \frac{1}{f_{pico}} \qquad (1)$$

Aplicando la ecuación (1), se obtiene un tiempo de ciclo aproximado de **22,2 segundos**. Al dividir el tiempo total de marcado del lote por este valor, se obtiene el número de ciclos, lo que permite validar el tamaño del lote ajustado: 100 piezas.

En cuanto al conjunto de datos con anomalías, se observa prácticamente la misma frecuencia dominante **0.045 Hz**, indicando igual tiempo de ciclo de producción dominante, si bien aparecen nuevas frecuencias debido a los fallos registrados y también se puede ver en la Figura 8 como el tiempo total de marcado del lote fue de unos **48,85 minutos**, lo que hace que el tiempo de ciclo medio de las piezas con fallo sea superior al del lote sin anomalías, aproximadamente **29,3 segundo**s en como era de esperar debido a los fallos inducidos en las electroválvulas.

7. Conclusiones

Este artículo presenta un banco de pruebas para la Detección de Anomalías y Protección de Sistemas Ciberfísicos Industriales (DAyPSCI), el cual integra componentes industriales de última generación y adopta una arquitectura híbrida, abierta y flexible.

Se ha mostrado un caso de uso basado en el gobierno de un gemelo digital de un proceso de marcado, utilizando la metodología GEMMA, y se ha validado su utilidad para la generación de conjuntos de datos destinados a análisis posteriores. En dichos conjuntos se ha incorporado información sobre el estado del proceso, conforme a esta metodología de diseño.

Asimismo, se aplicó un análisis exploratorio de datos y la metodología propuesta por Sai, Gram y Bauernhansl (2023) a un conjunto de datos sin anomalías, logrando identificar el tiempo de ciclo de producción y el número de piezas procesadas con resultados satisfactorios.

También se realizaron capturas de datos de proceso mediante comunicación Profinet I/O, obteniendo resultados positivos. Esta información permitirá, en trabajos futuros, disponer de datos de red industrial para aplicar técnicas de inteligencia artificial orientadas a la detección y protección frente a ciberataques en sistemas ciberfísicos industriales.

Agradecimientos

Esta actividad se lleva a cabo en ejecución del Proyecto Estratégico "Inteligencia Artificial para la Securización de Dispositivos IoT" (C032.23), fruto de un convenio de colaboración suscrito entre el Instituto Nacional de Ciberseguridad (INCIBE) y la Universidad de Burgos. Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiadas por la Unión Europea (Next Generation), el proyecto del Gobierno de España que traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo, para la reconstrucción económica sólida, inclusiva y resiliente tras la crisis de la COVID19, y para responder a los retos de la próxima década.

Referencias

Alrumaih, T. N. I., Alenazi, M. J. F., AlSowaygh, N. A., Humayed, A., & Alablani, I., 2023. Cyber resilience in industrial networks: A state of the art, challenges, and future directions. Journal of King Saud University - Computer and Information Sciences, 35(9), 101781. https://doi.org/10.1016/j.jksuci.2023.101781.

Benka, D., Horvath, D., Spendla, L., Gaspar, G., & Stremy, M., 2025. Machine learning-based detection of anomalies, intrusions, and threats in industrial control systems. IEEE Access, 13, 12502–12514. https://doi.org/10.1109/ACCESS.2025.3530902.

CCN-CERT. 2024. CCN-CERT IA-04/24: Ciberamenazas y tendencias. Edición 2024. Centro Criptológico Nacional. https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html.

Domínguez, M., Fuertes, J. J., Prada, M. A., Alonso, S., Morán, A., & Pérez, D., 2022. Design of platforms for experimentation in industrial cybersecurity. Applied Sciences, 12(13), 6520. https://doi.org/10.3390/app12136520.

Faelli, M., 2025. Informe global de ciberataques del primer trimestre de 2025 de Check Point Software. Check Point Research. https://www.itsitio.com/seguridad/informe-global-de-ciberataques-del-primer-trimestre-de-2025-de-check-point-software/.

Fortinet, 2024. 2024 State of Operational Technology and Cybersecurity Report. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf.

Han, S., Lee, K., Cho, S., & Park, M., 2021. Anomaly detection based on temporal behavior monitoring in programmable logic controllers. Electronics, 10(10), 1218. https://doi.org/10.3390/electronics10101218.

Hosseinzadeh, S., Voutos, D., Barrie, D., Owoh, N., Ashawa, M., & Shahrabi, A., 2024. Design and development considerations of a cyber physical testbed for operational technology research and education. Sensors, 24(12), 3923. https://doi.org/10.3390/s24123923.

International Society of Automation & Comisión Electrotécnica Internacional, 2024. ISA/IEC 62443-2-1:2024 - Seguridad para sistemas de automatización y control industrial – Parte 2-1: Requisitos del programa de seguridad para propietarios de activos de IACS. https://www.isa.org/products/ansi-isa-62443-2-1-2024-security-industrial-automa.

Javid, M., Haleem, A., & Suman, R., 2023. Digital Twin applications toward Industry 4.0: A review. Cognitive Robotics, v. 3, p. 71-92.. https://doi.org/10.1016/j.cogr.2023.04.003.

Nankya, M., Chataut, R., & Akl, R., 2023. Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. Sensors, 23(21), 8840. https://doi.org/10.3390/s23218840.

Oks, S. J., Jalowski, M., Lechner, M., Mirschberger, S., Merklein, M., Vogel-Heuser, B., & Möslein, K. M., 2022. Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. Information Systems Frontiers, 26, 1731–1772. https://doi.org/10.1007/s10796-022-10252-x.

PCSimu, 2023. PCSimu: Simulador de automatización industrial (Versión 3.0) [Software]. https://cade-simu.com/pc-simu.

Piedrafita, R., 2004. Ingeniería de la automatización industrial. Ra-Ma.

Pospisil, O., Blazek, P., Kuchar, K., Fujdiak, R., & Misurec, J., 2021. Application perspective on cybersecurity testbed for industrial control systems. Sensors, 21(23), 8119. https://doi.org/10.3390/s21238119.

Sai, B. K., Gram, J., & Bauernhansl, T., 2023. Information-based preprocessing of PLC data for automatic behavior modeling. Procedia CIRP, v. 120, p. 565-571.https://doi.org/10.1016/j.procir.2023.09.038.

Serpanos, D., 2018. The Cyber-Physical Systems Revolution. IEEE Computer, 51(3), 70–73. https://doi.org/10.1109/MC.2018.1731058.

TIA Portal, 2022. TIA_Portal: STEP 7 Basic/Professional, STEP 7 Safety Basic/Advanced and WinCC Basic/Comfort/Advanced and WinCC Unified (Versión 18.0) [Software]. https://support.industry.siemens.com/cs/attachments/109807109/TIA_Portal_STEP7_Prof_Safety_WINCC_Prof_V18.iso.