Seguridad Cibernética OT Defensiva: Estrategias para entornos industriales

Protección de sistemas de control industrial mediante estándares IEC 62443 y NIST

Mariano Millañanco Fernández
Puertollano. Ciudad Real, España
Universidad de Sevilla — Máster en Microelectrónica
UTAMED — Máster en Inteligencia Artificial
github.com/tangodelta217/ACQC
mariano.millananco@gmail.com

2026

Resumen

Se presenta un enfoque de ciberseguridad defensiva para entornos de *Operational Technology* (OT) industriales, aplicable a una refinería como Repsol Puertollano. Se definen el alcance (modo asesor con operario en bucle) y el modelo de amenazas, enfatizando riesgos típicos en sistemas de control industrial: suplantación de señales, ataques de repetición y manipulación de datos. Para mitigar estas amenazas, se proponen medidas técnicas: segmentación en zonas OT/DMZ/IT, establecimiento de límites de confianza, arranque seguro con raíz de confianza de hardware, firma digital de datos de proceso y de modelos predictivos, endurecimiento de sistemas (servicios mínimos, cortafuegos, registro de eventos) y operaciones seguras (gestión de parches, rotación de credenciales, plan de respuesta a incidentes). Finalmente, se mapea la solución a buenas prácticas reconocidas (IEC 62443, NIST).

Abstract

A defensive cybersecurity approach is presented for industrial Operational Technology (OT) environments, applicable to a refinery such as Repsol Puertollano. The scope (advisory mode with human-in-loop) and threat model are defined, highlighting typical risks in industrial control systems: signal spoofing, replay attacks, and data manipulation. To counter these threats, technical measures are proposed: network segmentation into OT/DMZ/IT zones with defined trust boundaries, secure boot with hardware root-of-trust, digital signing of process data and predictive models, system hardening (minimal services, firewalls, event logging), and secure operations (patch management, credential rotation, incident response plan). Finally, the solution is mapped to recognized best practices (IEC 62443, NIST).

Keywords: OT security; ICS; IEC 62443; NIST CSF; secure boot

Resumen ejecutivo (entregables medibles)

- **Modelo de amenazas y alcance delimitado**: catálogo de escenarios de ataque relevantes (suplantación de sensores, repetición de comandos) y aclaración de que el sistema opera en modo lectura/asesor **Bhamare2020**.
- **Arquitectura segmentada OT–DMZ–IT**: diseño de red con enclaves de confianza separados, empleando cortafuegos y proxies para que todo acceso entre zonas pase por la DMZ **Mathezer2021**.
- **Integridad de dispositivos y software**: habilitación de *secure boot* y firma de firmware/modelos en el dispositivo edge, garantizando que solo código autenticado se ejecute **Schweizer2023**.
- **Protección de datos y detección de ataques**: implantación de criptografía (firmas digitales, cifrado OPC-UA) en la telemetría de proceso **Isnardon2023**.
- **Operación cibersegura continua**: plan de mantenimiento de seguridad, incluyendo parches, rotación de credenciales y plan de respuesta a incidentes **ISA2021**.

1. Introducción

En los sistemas de control industrial (Industrial Control Systems, ICS), la integración creciente con tecnologías de información ha ampliado la superficie de ataque y los riesgos cibernéticos asociados **Bhamare2020**. Tradicionalmente aislados, muchos entornos OT de refinería ahora comparten datos con redes corporativas o la nube para habilitar analítica avanzada (*Industry 4.0*), lo que expone a los controladores lógicos programables (PLCs), sistemas SCADA/DCS y sensores de planta a vectores de ataque antes exclusivos de TI. Estos sistemas suelen operar procesos físicos críticos, de modo que un incidente de ciberseguridad puede traducirse en daños materiales o riesgos para la seguridad humana. Por ello, asegurar la infraestructura OT es prioritario para empresas como Repsol.

Alcance y modo de operación: El presente trabajo se enfoca exclusivamente en ciberdefensa (medidas preventivas y de protección), sin incluir capacidades ofensivas. El sistema industrial considerado (p. ej. célula ACQC en la refinería) funcionará en modo asesor: realiza monitorización en línea

y proporciona recomendaciones al operario, pero *no* ejecuta control automático cerrado. De este modo se evitan cambios directos en la operación sin autorización humana.

Modelo de amenazas OT: Se identifican como amenazas principales aquellas que buscan comprometer la integridad y disponibilidad de los datos de proceso. En entornos ICS tradicionales abundan protocolos sin autenticación ni cifrado **NIST80082**, lo que permite a un adversario realizar ataques de suplantación (*spoofing*) de sensores/actuadores, envío de comandos falsos o inserción de datos manipulados sin ser detectado. Un vector crítico es el *ataque de repetición* (*replay*): un intruso con acceso a la red OT puede capturar tramas legítimas y volver a transmitirlas posteriormente para hacer creer al operador que el proceso está bajo condiciones normales cuando en realidad se están ejecutando acciones maliciosas. Por ejemplo, en casos documentados, atacantes reprodujeron señales de control capturadas previamente, provocando cambios no autorizados **MITRE2025**.

El objetivo de la estrategia defensiva es mitigar estas amenazas garantizando la autenticidad de los dispositivos y software en operación, la integridad y frescura de los datos de proceso, y la robustez de la red OT frente a accesos no autorizados.

2. Metodología

Para contrarrestar las amenazas identificadas, se diseña un conjunto integral de controles de ciberseguridad, abarcando desde la arquitectura de red hasta la gestión operativa.

2.1 Segmentación de red y límites de confianza OT/IT

Se implementa una arquitectura en zonas de distinta confianza, siguiendo el principio de *segregación* de redes ICS recomendado por estándares como ISA/IEC 62443-3-3 **IEC62443-3-3**. Se definen tres dominios principales: la red OT de control de planta (PLCs, DCS, sensores/actuadores), una zona desmilitarizada industrial (DMZ) intermedia, y la red corporativa IT. La DMZ OT actúa como zona tampón entre OT e IT **Mathezer2021**. Todos los flujos de información entre la planta y los sistemas corporativos deben pasar por esta DMZ, donde se ubican servidores de enlace (historiador réplica, servidores de acceso remoto seguro y pasarelas de datos). La comunicación directa desde la red corporativa hacia dispositivos OT críticos está prohibida.

En la práctica, el historiador de proceso de la refinería (que recopila datos de sensores vía OPC-UA) se replica en un servidor de la DMZ. El sistema de análisis de calidad (ACQC) en el edge se desplegaría preferiblemente en la DMZ o en una zona segregada de la OT con comunicaciones estrictamente controladas. Un cortafuegos perimetral DMZ–OT se configura con listas blancas de protocolos y direcciones permitidas **Young2025**. Este esquema de zonas y conduits establece claros *límites de confianza*: la red OT es altamente confiable (solo dispositivos validados), la DMZ tiene confianza media y la red IT se considera no confiable desde la perspectiva OT.

2.2 Integridad de dispositivos: Secure Boot y raíz de confianza

Garantizar que cada equipo en la capa OT/edge ejecuta únicamente software legítimo es fundamental para prevenir la inserción de malware o firmware malicioso. Para ello, se adopta la técnica de arranque seguro (*secure boot*) apoyada en una raíz de confianza de hardware. En los controladores (PLCs de última generación) y en el servidor de inferencia edge se habilita un mecanismo en el que, al encender el dispositivo, el procesador verifica criptográficamente la firma digital del firmware y del sistema operativo antes de cargarlos **Schweizer2023**. Solo si la firma concuerda con la clave pública del fabricante (almacenada en una memoria segura del hardware) se permite el arranque del software.

La raíz de confianza reside típicamente en un módulo seguro (TPM o microcontrolador dedicado) que contiene claves criptográficas inalterables. Cada etapa de la secuencia de arranque valida la siguiente (cadena de confianza). Si alguna comprobación falla (firma inválida), el dispositivo entra en un modo seguro o no arranca, previniendo que código potencialmente malicioso tome control. Esta capacidad es considerada obligatoria para alcanzar niveles de seguridad elevados en entornos industriales; por ejemplo, la certificación IEC 62443 nivel SL3 la exige para componentes críticos **Young2025**.

2.3 Integridad de datos: firmado y protección anti-replay

Con las comunicaciones ICS expuestas a espionaje o inyección, se implementan contramedidas criptográficas para asegurar que los datos que consumen los algoritmos de calidad y los operadores no han sido alterados en tránsito y son actuales (no reproducciones antiguas). En el protocolo OPC-UA utilizado por el historiador, se configura el nivel de seguridad *SignAndEncrypt*: cada mensaje es firmado digitalmente y cifrado, garantizando integridad y confidencialidad simultáneamente **Isnardon2023**. La firma añade un código (MAC) calculado con la clave privada del remitente de modo que el receptor verifica con la clave pública correspondiente que el mensaje realmente proviene de la fuente legítima y no ha sido modificado.

Además, para prevenir ataques de repetición, se habilitan contadores o *nonces* únicos en las tramas de comunicación. Los algoritmos criptográficos implementados evitan que dos mensajes idénticos generen el mismo texto cifrado **NIST80082**. Así, aunque un atacante capture un paquete firmado, no podrá simplemente retransmitirlo más tarde, ya que el receptor detectará que ese identificador temporal ya fue procesado.

2.4 Protección de modelos y configuraciones

Dado que el valor del sistema ACQC reside en su modelo predictivo y las configuraciones calibradas, se implementan controles de integridad específicos sobre estos artefactos. Cada modelo de aprendizaje automático entrenado será firmado digitalmente por la autoridad designada antes de desplegarlo en la plataforma edge. Esta firma asegura al entorno de ejecución que el modelo proviene de una fuente confiable y no ha sido adulterado. El motor de inferencia validará la firma del modelo al cargarlo en memoria. Si

alguien intentara sustituir el archivo del modelo por uno modificado, la firma no coincidiría y la carga sería abortada o generaría alarmas.

Lo mismo se aplica a ficheros de configuración críticos: umbrales de alarmas, parámetros de calibración, lista de variables monitoreadas, etc. Todos estos se almacenan en el sistema de archivos del edge de forma cifrada o al menos con sumas de verificación firmadas. Esta práctica de *code signing* y *config signing* está alineada con los requisitos técnicos de integridad del estándar IEC 62443-4-2 **Young2025**.

2.5 Endurecimiento de sistemas y registro de eventos

A nivel de cada sistema involucrado (servidores edge, estaciones de operador, gateways), se lleva a cabo un proceso de *hardening* o endurecimiento para reducir su exposición y aumentar la trazabilidad. Esto incluye deshabilitar todos los servicios de red innecesarios en los equipos OT/DMZ, restringiendo los puertos abiertos únicamente a los estrictamente requeridos. Se aplica una política de *lista blanca* de aplicaciones: solo se permiten ejecutar los procesos predefinidos del sistema ACQC y software de control **ISA2021**.

La recopilación de **logs** o bitácoras es otro pilar: todos los eventos relevantes de seguridad y operación se registran en un servidor de logs central (preferentemente en la DMZ). Esto incluye: intentos de autenticación, cambios de configuración, alertas de integridad, ejecución de inferencias y recomendaciones emitidas, conexiones de red establecidas, etc. Esto facilita la detección temprana de actividades anómalas al correlacionar eventos.

2.6 Operaciones seguras: parches, credenciales y respuesta a incidentes

La ciberseguridad OT no es un producto, sino un proceso continuo. En la fase operativa se implementan políticas y procedimientos para mantener la postura de seguridad a lo largo del ciclo de vida del sistema.

En primer lugar, un programa de **gestión de parches** específico para entornos ICS. Se mantiene un inventario detallado de todos los activos de software y firmware en OT/DMZ. Periódicamente, se revisan boletines de proveedores y avisos de vulnerabilidades (ICS-CERT) para identificar actualizaciones de seguridad aplicables. Dado que en OT muchas veces no es factible instalar parches de inmediato, se planifican *ventanas de mantenimiento* coordinadas con producción para aplicar los parches más críticos **ISA2021**. Si algún parche no pudiera aplicarse, se implementan controles compensatorios temporales.

La **gestión de credenciales y claves** es igualmente rigurosa. Se establecen políticas de cambio periódico de contraseñas en las cuentas de operador/ingeniería de sistemas OT, evitando credenciales por defecto o compartidas. Siempre que sea posible, se habilita autenticación multifactor para accesos remotos. Las claves privadas usadas para firmas digitales se guardan en módulos seguros y se rotan antes de su fecha de expiración **NIST80082**.

Por último, se desarrolla un **plan de respuesta a incidentes** específico para OT, en coordinación con el CSIRT corporativo. Este plan define procedimientos para diferentes escenarios: detección de malware en un HMI, indicios de intrusión de red, fallo de integridad en un PLC, etc. Por cada tipo de incidente se establecen acciones inmediatas (aislar segmento de red, cambiar credenciales, conmutar a modo manual de operación), roles y responsabilidades.

3. Resultados / Evaluación

Dado el carácter de propuesta, se definen los resultados esperados y cómo se evaluarían las medidas anteriores en un despliegue real o piloto controlado.

3.1 Resultados esperados

La implementación de este plan de ciberdefensa debe elevar significativamente la resiliencia del sistema ACQC y de la red OT de soporte. Se espera, en primer lugar, lograr **cero** alteraciones de datos no detectadas: cualquier intento de modificar o repetir una señal de proceso será identificado y registrado.

En términos de **rendimiento**, se espera que las medidas criptográficas (firmado, cifrado) introduzcan una sobrecarga mínima, no comprometiendo la operación en tiempo real. La latencia añadida en la comunicación OPC-UA con cifrado debería ser del orden de milisegundos y dentro de los márgenes tolerables.

3.2 Plan de evaluación

Para validar la eficacia de las medidas, se propone un conjunto de pruebas y métricas:

- *Prueba de replay*: retransmitir un paquete antiguo y verificar que el sistema lo detecta y rechaza. Métrica: tasa de detección = 100 %.
- *Prueba de MITM*: modificar un valor en tránsito y verificar que la firma inválida bloquea el procesamiento.
- *Prueba de secure boot*: cargar firmware no autorizado e intentar arrancar. Esperado: el dispositivo no arranca completamente.
- *Prueba de firma de modelo*: manipular el archivo del modelo y observar que se rechaza.
- *Prueba de hardening*: escanear puertos y verificar que solo los definidos responden.
- *Prueba de respuesta a incidentes*: simular malware y medir el tiempo de detección y aislamiento (< 30 min).

4. Discusión

La solución propuesta aborda las principales amenazas de ciberseguridad en OT, pero conlleva ciertas consideraciones. En primer lugar, la **complejidad** añadida: la introducción de criptografía, firmas digitales y segmentación estricta implica mayor carga de gestión y necesidad de competencias especializadas en el personal.

Otro aspecto es la **compatibilidad con equipamiento legado**. No todos los PLCs antiguos soportan secure boot o comunicaciones cifradas. En estos casos, se ha contemplado el uso de soluciones externas (gateways VPN o módulos de autenticación) **MITRE2025**, pero estas pueden introducir puntos de fallo adicionales.

La **disponibilidad operativa** es prioritaria en entornos 24/7 como una refinería. Si bien se ha diseñado para minimizar impacto en tiempo real, algunas medidas podrían ocasionar interrupciones si no se gestionan correctamente.

En cuanto a **alineamiento con estándares**, la solución muestra correspondencia con varios requisitos de IEC 62443 y con las funciones del NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) **NISTCSF2018**.

5. Conclusiones

En este documento se ha desarrollado un plan integral de ciberseguridad defensiva para entornos OT industriales, tomando como caso de referencia la implantación de un sistema de analítica de calidad en una refinería. Mediante una combinación de arquitectura en zonas seguras, tecnologías de arranque verificado, firma digital de datos y modelos, endurecimiento de infraestructuras y buenas prácticas operativas, se logra crear múltiples capas de defensa que mitigan los riesgos de suplantación, repetición y manipulación de la información de proceso.

La propuesta enfatiza la importancia de mantener la integridad y confiabilidad de los datos en sistemas donde decisiones automatizadas podrían impactar la seguridad física. Al asegurar que tanto los dispositivos de control como los algoritmos avanzados operan en un entorno confiable y monitorizado, se habilita la introducción de soluciones de Industria 4.0 (como la ACQC) sin exponer la planta a vectores de ciberataque inaceptables.

Como trabajo futuro, se sugiere profundizar en la implementación de capacidades de *detección de intrusiones específicas de OT* (por ejemplo, análisis del tráfico MODBUS/OPC-UA en busca de patrones anómalos) que complementen las medidas preventivas aquí descritas. Asimismo, conforme evolucione la normativa y políticas corporativas, el sistema debería adaptarse, incorporando requisitos de futuras actualizaciones de IEC 62443.