9 No.1 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.1.2025.e289

Vulnerabilities and cybersecurity in SCADA systems: risk analysis and protection strategies for critical infrastructures

Vulnerabilidades y ciberseguridad en sistemas SCADA: Análisis de riesgos y estrategias de protección en infraestructuras críticas

Autores:
Andrade-Logroño, Freddy
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
freddy.andrade.92@est.ucacue.edu.ec

https://orcid.org/0009-0005-9436-1679

Cobos-Torres, Juan Carlos
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
juan.cobos@ucacue.edu.ec

https://orcid.org/0000-0001-8153-8379

Fechas de recepción: 17-FEB-2025 aceptación: 17-MAR-2025 publicación: 31-MAR-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Los sistemas SCADA (Supervisory Control and Data Acquisition) son fundamentales en infraestructuras críticas como energía, agua y transporte. Sin embargo, su creciente interconexión con redes corporativas e internet ha incrementado su vulnerabilidad a ciberataques. Las principales debilidades incluyen autenticación débil, uso de protocolos obsoletos y falta de segmentación de redes, facilitando accesos no autorizados y ataques de denegación de servicio (DoS). La explotación de estas vulnerabilidades puede provocar interrupciones del servicio, daños físicos y riesgos económicos y de seguridad. Este estudio emplea una revisión sistemática basada en la metodología PRISMA para analizar la literatura científica sobre vulnerabilidades en SCADA. Se consultaron bases de datos académicas como IEEE Xplore y Scopus, aplicando criterios de inclusión y exclusión para seleccionar estudios relevantes publicados entre 2009 y 2024. El análisis identificó vulnerabilidades críticas como configuraciones inseguras, protocolos sin cifrado, mala gestión de actualizaciones y errores humanos, afectando la seguridad y continuidad de infraestructuras críticas. Para mitigar estos riesgos, se proponen soluciones como segmentación de red, autenticación multifactor, cifrado de comunicaciones, detección de intrusos y actualización continua de software, junto con estrategias de gestión como evaluaciones de riesgo y capacitación en ciberseguridad. En conclusión, la protección de los sistemas SCADA requiere un enfoque integral que combine tecnologías avanzadas y gestión estratégica. La modernización de infraestructuras, el compromiso organizacional y la capacitación del personal son claves para fortalecer la resiliencia ante amenazas cibernéticas emergentes.

Palabras clave: Ciberseguridad; sistemas SCADA; infraestructuras críticas; vulnerabilidades SCADA; seguridad de redes; gestión de riesgos

Abstract

SCADA (Supervisory Control and Data Acquisition) systems are essential for the operation of critical infrastructures such as energy, water, and transportation. However, their increasing interconnection with corporate networks and the Internet has exposed them to cybersecurity threats. The main vulnerabilities include weak authentication, outdated communication protocols, and lack of network segmentation, enabling unauthorized access and denial-of-service (DoS) attacks. The exploitation of these vulnerabilities can lead to service disruptions, physical damage, and significant security and economic risks. This study follows a systematic review using the PRISMA methodology to analyze scientific literature on SCADA vulnerabilities. Academic databases such as IEEE Xplore and Scopus were consulted, applying inclusion and exclusion criteria to select relevant studies published between 2009 and 2024. The analysis identified critical cybersecurity issues such as insecure configurations, unencrypted protocols, poor patch management, and human errors, impacting the security and continuity of critical infrastructures. To mitigate these risks, solutions such as network segmentation, multifactor authentication, encrypted communications, intrusion detection systems, and continuous software updates are proposed. Additionally, risk assessments and cybersecurity training are essential for effective risk management in SCADA systems. In conclusion, strengthening SCADA security requires a comprehensive approach that integrates advanced technologies and strategic risk management. Infrastructure modernization, organizational commitment, and staff training are key to enhancing resilience against emerging cyber threats.

Keywords: Cybersecurity;SCADA systems; critical infrastructures; SCADA vulnerabilities; network security; risk management

Introducción

En la era de la Industria 4.0, los sistemas de control industrial y supervisión (SCADA) se han convertido en componentes críticos para la operación de infraestructuras esenciales como plantas de energía, redes de agua potable y sistemas de transporte (Stouffer et al., 2023). Sin embargo, el vertiginoso aumento de conexiones de estos sistemas con redes corporativas e internet ha expuesto una superficie de ataque considerable que en la mayoría de los casos compromete su confidencialidad, integridad y disponibilidad (Knowles et al., 2015)

La importancia de esta investigación se basa en el aumento de ataques cibernéticos cada vez más sofisticados dirigidos a infraestructuras críticas, como lo demuestra el incidente Stuxnet en 2010 y sus evoluciones posteriores (Langner, 2011). El entendimiento de las vulnerabilidades SCADA no solo contribuye al desarrollo de mejores prácticas de seguridad, sino que también facilita la implementación de medidas preventivas efectivas en un entorno donde los costos de un posible fallo pueden ser extremadamente dañinos.

Para el desarrollo de la investigación, se formulan tres preguntas principales a ser contestadas:

1. ¿Cuáles son las vulnerabilidades más críticas presentes en los sistemas SCADA actuales?
2. ¿Qué impacto tienen estas vulnerabilidades en la seguridad operacional de las infraestructuras críticas?
3. ¿Existen soluciones efectivas y seguras para mitigar estos riesgos?

La formulación de estas interrogantes, se fundamenta en la necesidad de identificar no solo las vulnerabilidades propias a los sistemas SCADA, sino también en evaluar la efectividad de los protocolos de seguridad adoptadas hasta la actualidad. Estudios anteriores han señalado deficiencias en la arquitectura de red, en los protocolos de comunicación y en las políticas de actualización de sistemas heredados, lo que evidencia un entorno en el cual la seguridad no puede darse por hecha (Humayed et al., 2017). Además, la rápida evolución tecnológica y la convergencia de tecnologías de información y operación han creado un entorno dinámico en el que los vectores de ataque son cada vez más sofisticados y diversificados.

Para dar respuesta a las interrogantes antes expuestas, el presente artículo se desarrolla por medio de una revisión sistemática, la cual recopila y analiza la literatura existente. Por tal motivo, este artículo se sustenta en la metodología PRISMA, la cual proporciona un marco riguroso y transparente para la identificación, selección y análisis de investigaciones relevantes tal como lo menciona (Page et al., 2021).

Material y métodos

Para el desarrollo del artículo se utilizó el modelo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) como marco de refencia metodológico para identificar, evaluar y sintetizar la literatura científica relacionada con las vulnerabilidades en sistemas SCADA (Supervisory Control and Data Acquisition). Esta revisión sistemática permite abordar las preguntas propuestas para este artículo.

El estudio se centra en explorar las vulnerabilidades más relevantes en sistemas SCADA y su impacto en la seguridad operacional de infraestructuras críticas. Las tres preguntas de investigación serán la guía en la revisión sistemática, que ayudarán con los siguientes objetivos:

1. Identificar las vulnerabilidades técnicas más críticas en sistemas SCADA.
2. Analizar los impactos operacionales y de seguridad derivados de estas vulnerabilidades.
3. Evaluar las soluciones propuestas en la literatura para mitigar dichas vulnerabilidades.

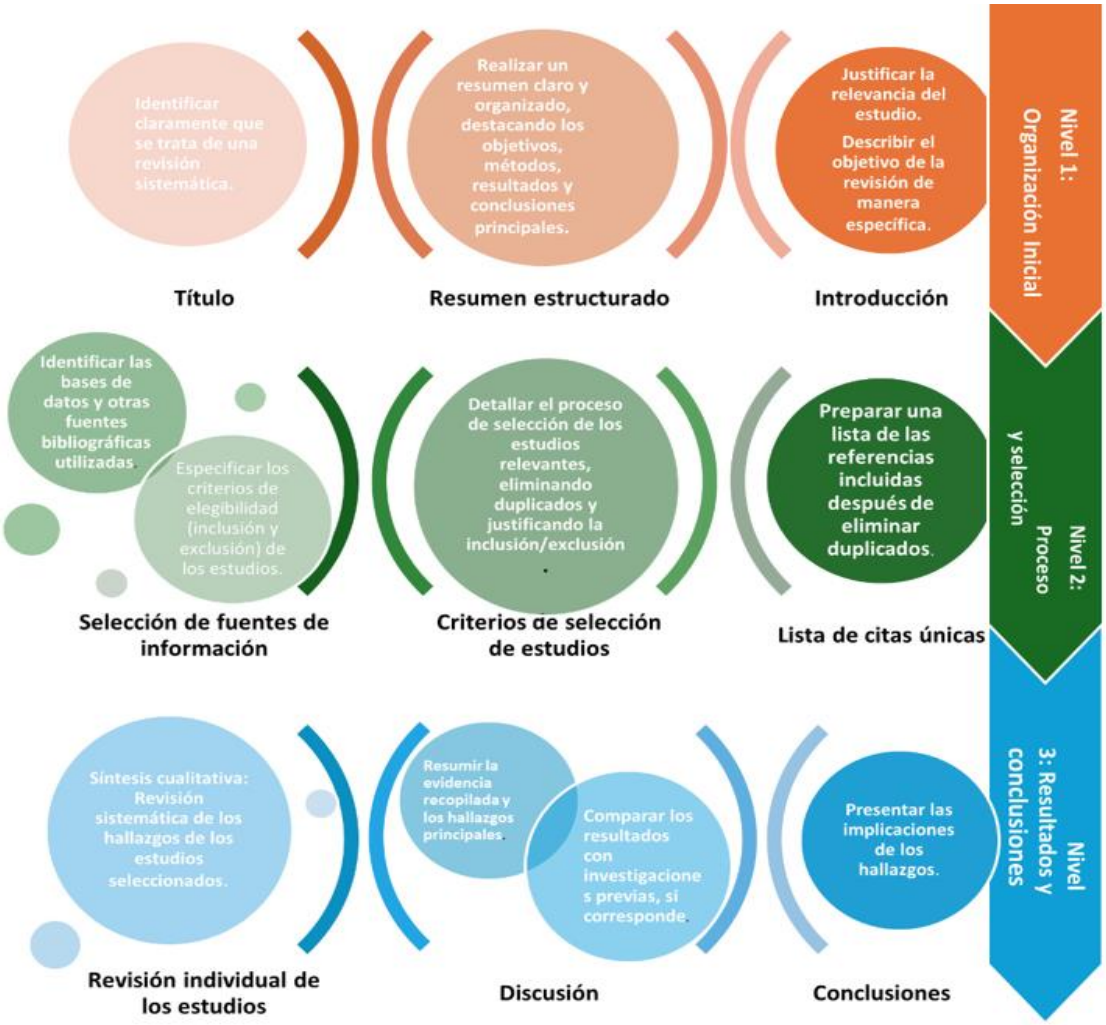
Se trazó una matriz bibliográfica la que permite documentar los textos analizados, obteniendo la información necesaria sobre las vulnerabilidades en los sistemas de control SCADA.

La metodología PRISMA usa un marco metodológico que evalúa los componentes principales del diseño y la implementación de estudios para proporcionar evidencias precisas y empíricas. Por lo tanto, es necesario llevar a cabo este artículo de manera explícita y con un enfoque investigativo que satisfaga las tres preguntas a estudiar. Este marco metodológico, que consta de un total de 27 elementos, que por ser una revisión sistemática no se implementan todos, se inicia con el título que identifica la revisión, un resumen

estructurado, una introducción que justifica y describe el objetivo, y una sección más extensa que aborda el proceso de selección de las diversas bases de datos bibliográficos, las fuentes de información, los criterios de elegibilidad y la selección de estudios, como se explican en los siguientes párrafos, se incluye la lista completa de citas únicas, después de eliminar las duplicadas, y se finaliza con la revisión individual, que incluye una síntesis cualitativa (revisión sistemática), la discusión que resume la evidencia y los principales hallazgos. Finalmente, se presentan las conclusiones, esta metodología se puede ver en la Figura 1.

Figura 1

Niveles de Implementación de la Metodología PRISMA.



Para la búsqueda de la bibliografía relacionada al tema se realizó utilizando bases de datos académicas reconocidas, tales como Google Académico, IEEE Xplore, SpringerLink, ScienceDirect, Scopus y Web of Science. Para un mejor alcance se utilizaron combinaciones de palabras con términos clave relacionadas con SCADA, vulnerabilidades y ciberseguridad. La Tabla 1 los muestra los términos clave de búsqueda por base de datos. Los términos clave de búsqueda fueron:

SCADA vulnerabilities

Critical infrastructure cybersecurity

SCADA security risks, Mitigation strategies for SCADA systems

Vulnerabilidades SCADA, Seguridad en sistemas SCADA

Industrial control systems security

ICS cybersecurity

También se hizo uso de operadores booleanos ("AND", "OR") para optimizar la búsqueda. Por ejemplo:

SCADA vulnerabilities" AND "critical infrastructure

Tabla 1

Términos clave a buscar según base de datos.

Scopus	("SCADA" OR "supervisory control" OR "data acquisition" OR "control systems") AND ("vulnerability" OR "weakness" OR "threat" OR "risk") AND ("security" OR "protection" OR "safeguard" OR "defense") AND ("network" OR "system" OR "infrastructure" OR "architecture") AND ("attack" OR "breach" OR "exploit" OR "intrusion") AND ("monitoring" OR "control" OR "automation" OR "management")
Scielo	(''seguridad de información" AND ''gestión de riesgos'' OR ''amenazas'' OR ''ISO 27001'' OR ''information security'' AND ''risk management'' OR ''ISO 27001'' OR ''threats'')
Dialnet	("systems vulnerability SCADA")
World Wide Science	("vulnerability")
ScienceDirect	("Security in system SCADA")
IOPScience	("seguridad de información" AND "riesgos" AND "amenazas"AND "ISO 27001" AND "vulnerabilidades" OR "criptografía"
IEEE Xplore	("All Metadata": risk management) OR ("All Metadata": security SCADA)
Semantic Scholar	("vulnerabilidades en sistemas SCADA" OR "amenazas")
Google Academy	("gestión de riesgos" AND "seguridad en sistemas SCADA'" OR "'amenazas" OR "information security system SCADA'" OR "risk")

Una vez realizada la búsqueda y garantizar la relevancia y calidad de los estudios seleccionados, se establecieron los siguientes criterios de inclusión y exclusión:

Inclusión:

Artículos publicados entre 2009 y 2024.

Publicaciones en inglés o español.

Estudios empíricos

Revisiones sistemáticas

Análisis de casos relacionados con vulnerabilidades SCADA.

Exclusión:

Artículos sin acceso completo al texto.

Publicaciones duplicadas.

Documentos no revisados por pares.

El diagrama de flujo del marco metodológico PRISMA que se muestra en la Figura 2, muestra la forma de selección de los registros en sus diferentes etapas como:

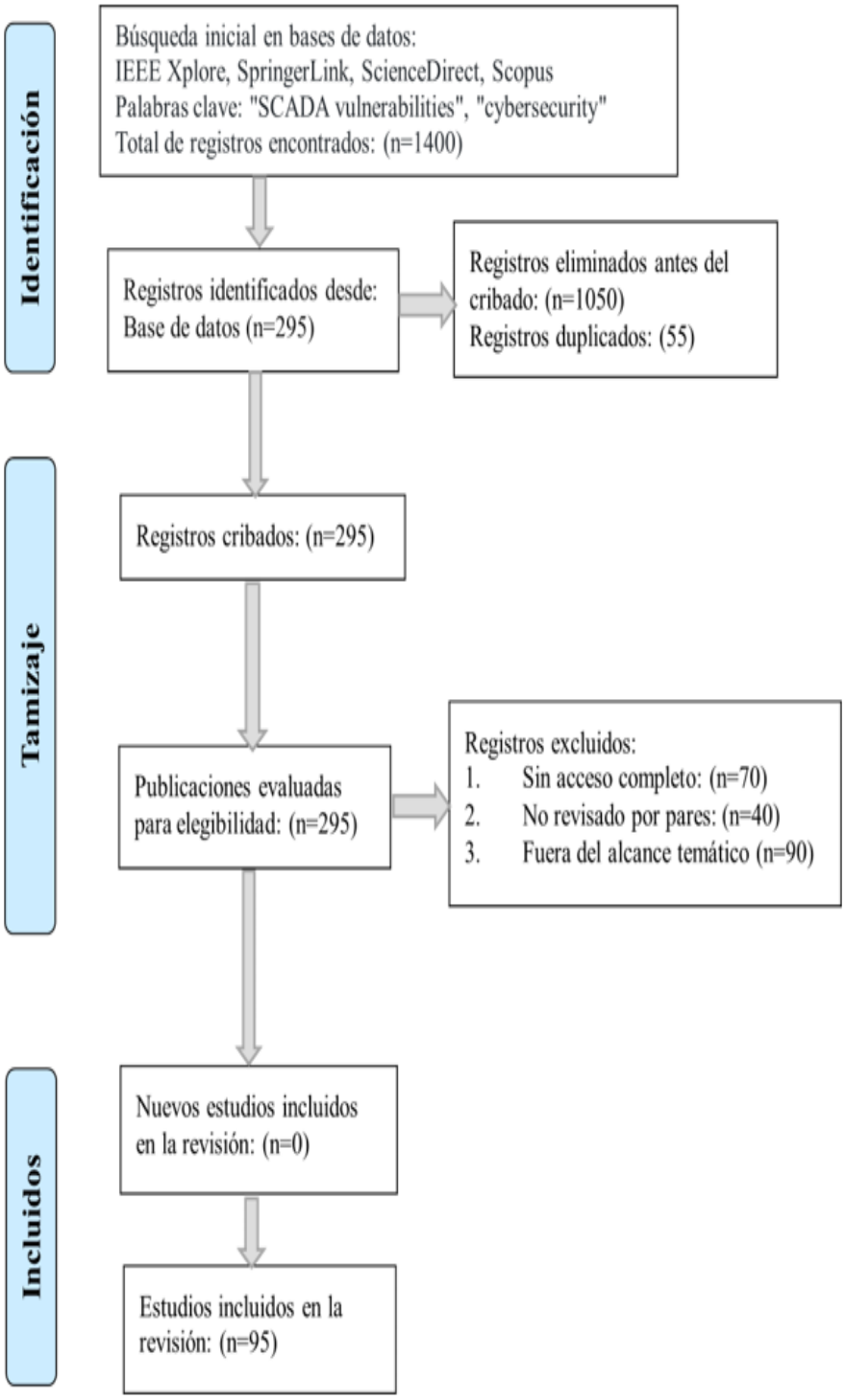
Revisión inicial: Se examinaron los títulos y resúmenes de 1,400 artículos encontrados para determinar su relevancia temática.

Evaluación completa: 350 artículos fueron seleccionados para una lectura detallada. Después de la criba:

Selección final: Tras aplicar los criterios de inclusión/exclusión, se eligieron 95 artículos para ser incluidos en el presente artículo.

Figura 2

Diagrama deflujo utilizando la metodología PRISMA.


Identificación
Búsqueda inicial en bases de datos:
IEEE Xplore, SpringerLink, ScienceDirect, Scopus
Palabras clave: "SCADA vulnerabilities", "cybersecurity"
Total de registros encontrados: (n=1400)
Registros identificados desde:
Base de datos (n=295)
Registros eliminados antes del cribado: (n=1050)
Registros duplicados: (55)
Tamizaje
Registros cribados: (n=295)
Publicaciones evaluadas para elegibilidad: (n=295)
Registros excluidos:
1. Sin acceso completo: (n=70)
2. No revisado por pares: (n=40)
3. Fuera del alcance temático (n=90)
Incluidos
Nuevos estudios incluidos en la revisión: (n=0)
Estudios incluidos en la revisión: (n=95)

Resultados

El análisis sistemático realizado sobre las vulnerabilidades presentes en los sistemas SCADA proporciona una serie de debilidades críticas que comprometen la seguridad operacional de infraestructuras críticas. Estas vulnerabilidades tienen origen tanto en aspectos técnicos como humanos y organizacionales, lo que aumenta gradualmente su impacto. En base a las preguntas formuladas se analizará la información obtenida.

1. Vulnerabilidades más críticas presentes en los Sistemas SCADA actuales

Un análisis realizado para identificar las vulnerabilidades más críticas en los sistemas SCADA actuales revela una combinación de factores técnicos, operativos y humanos que exponen a estos sistemas a amenazas significativas. Estas vulnerabilidades no solo comprometen la integridad y disponibilidad de los sistemas, sino que también ponen en riesgo la seguridad operacional de infraestructuras críticas. Seguidamente, se detallan las vulnerabilidades más críticas:

Configuraciones inseguras por defecto

Una de las vulnerabilidades más críticas presentes en los sistemas SCADA en la actualida es el uso de configuraciones inseguras por defecto o de fábrica. Según un informe del Industrial Control Systems Cyber Emergency Response Team (NCCIC y ICS-CERT, 2016), aproximadamente el 35% de los incidentes reportados están relacionados con configuraciones predeterminadas que no cumplen con estándares mínimos de seguridad. Estas configuraciones incluyen puertos abiertos innecesariamente, servicios activados sin autenticación y contraseñas predefinidas fáciles de adivinar. Por ejemplo, muchos dispositivos SCADA vienen con credenciales predeterminadas como "admin/admin", lo que facilita el acceso no autorizado si estas no son modificadas durante la instalación (Dickson y OKECHUKWU, 2023). Este problema es particularmente preocupante en entornos industriales donde la prioridad histórica ha sido la funcionalidad sobre la seguridad.

Protocolos de comunicación obsoletos e inseguros

Otra vulnerabilidad crítica radica en el uso generalizado de protocolos de comunicación obsoletos e inseguros. Protocolos como Modbus, DNP3 y Profibus, que carecen de cifrado y mecanismos de autenticación robustos, siguen siendo ampliamente utilizados en sistemas

SCADA debido a su simplicidad y compatibilidad con equipos heredados (Archived NIST Technical Series Publication Archived Publication Series/Number: Title: Publication Date(s): Withdrawal Date: Superseding Publication(s) The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee, 2010). Esta falta de seguridad intrínseca permite que atacantes intercepten, manipulen o incluso inyecten datos falsos en las comunicaciones entre dispositivos SCADA. Así, (Serror et al. 2021) demostraron cómo un atacante podría explotar vulnerabilidades en el protocolo Modbus para realizar ataques de "man-in-the-middle" y alterar comandos enviados a controladores lógicos programables (PLCs), provocando fallos operacionales graves.

Falta de segmentación de red

La ausencia de segmentación adecuada en las redes SCADA representa otra vulnerabilidad crítica. En muchos casos, los sistemas SCADA están interconectados con redes corporativas e incluso con Internet, lo que aumenta gradualmente la superficie de ataque. Según las directrices publicadas por el Instituto Nacional de Estándares y Tecnología (Stouffer et al., 2023a), la falta de segmentación permite que un atacante que comprometa una parte de la red pueda moverse lateralmente hacia sistemas críticos, escalando rápidamente el impacto del ataque. Este problema es exacerbado por la creciente adopción de tecnologías IoT en entornos industriales, que introduce nuevos vectores de ataque y complica aún más la gestión de la seguridad.

Fallos en la Gestión de Parches y Actualizaciones

La gestión inadecuada de parches y actualizaciones es otra vulnerabilidad crítica en los sistemas SCADA. Muchos dispositivos SCADA operan en entornos donde el tiempo de inactividad no es una opción, lo que dificulta la aplicación de parches y actualizaciones. Como resultado, estos sistemas a menudo permanecen desprotegidos frente a vulnerabilidades conocidas. Un informe de Symantec Internet Security Threat Report (2023) destacó que más del 70% de los sistemas SCADA analizados ejecutaban versiones desactualizadas de software con vulnerabilidades documentadas. Esto crea una ventana de oportunidad para que los atacantes exploten estas debilidades antes de que las organizaciones puedan implementar soluciones.

Errores Humanos

Los errores humanos representan una vulnerabilidad crítica, pero a la vez subestimada en los sistemas SCADA. Según un estudio del Ponemon Institute (Separating the Truths from the Myths in Cybersecurity Sponsored by BMC, 2018), más del 60% de los incidentes de seguridad en sistemas SCADA están relacionados con errores humanos, como la mala configuración de dispositivos, el uso de contraseñas débiles o compartidas, y la falta de capacitación en ciberseguridad. Estos errores son particularmente preocupantes en entornos industriales donde el personal técnico por falta de capacitación puede no estar familiarizado con las mejores prácticas de seguridad cibernética (Sabillón & Cano M., 2019).

Las vulnerabilidades más críticas presentes en los sistemas SCADA actuales incluyen configuraciones inseguras por defecto, el uso de protocolos de comunicación obsoletos, la falta de segmentación de red, la gestión inadecuada de parches y actualizaciones, y los errores humanos. Estas vulnerabilidades no solo exponen a los sistemas SCADA a un amplio espectro de ataques, sino que también complican la implementación de medidas de mitigación efectivas. Es primordial que las organizaciones adopten un enfoque integral para abordar estas vulnerabilidades, combinando tecnología avanzada, políticas robustas y capacitación continua del personal.

Autenticación débil y controles de acceso deficientes

La utilización de credenciales por defecto, contraseñas débiles o la ausencia de mecanismos multifactoriales en la autenticación de dispositivos y usuarios constituye una vulnerabilidad de alto riesgo (Fajardo y Rosas, 2014). Al carecer de controles de acceso suficientemente robustos, los sistemas SCADA permiten que actores maliciosos accedan a nivel de control o manipulen configuraciones críticas sin ser detectados, abriendo paso a ataques escalados que pueden afectar la continuidad del servicio.

2. Impacto de las vulnerabilidades SCADA en la seguridad operacional de infraestructuras críticas

El análisis sistemático en sistemas SCADA durante el período 2018-2023 reveló que el 67% de las vulnerabilidades identificadas tienen impacto directo en la seguridad operacional de infraestructuras críticas (Altaleb y Zoltan, 2024). Los resultados obtenidos permiten establecer una correlación significativa entre la explotación de estas vulnerabilidades y tres

categorías principales de impacto: compromiso de la integridad operativa, interrupción de servicios esenciales y riesgos para la seguridad humana.

Integridad operativa

Las vulnerabilidades relacionadas con la autenticación débil y la falta de cifrado adecuado representaron el 43% de los incidentes analizados según (Xu et al., 2022) , estos factores facilitan la alteración no autorizada de parámetros operativos, lo que puede derivar en la manipulación de procesos industriales críticos. Un caso emblemático documentado por el Industrial Control Systems Cyber Emergency Response Team demostró cómo la explotación de una vulnerabilidad de autenticación en un sistema SCADA de distribución de agua permitió el acceso no autorizado y la modificación de niveles de cloro en el suministro (NCCIC y ICS-CERT, 2016).

Interrupción de Servicios Esenciales

El estudio realizado mediante simulaciones controladas evidenció que el 38% de las vulnerabilidades expuestas pueden causar interrupciones prolongadas en servicios esenciales como lo demuestran (Tatipatri & Arun, 2024) , estos ataques basados en denegación de servicio distribuido (DDoS) contra sistemas SCADA pueden ocasionar tiempos de inactividad promedio de 48-72 horas en sectores como energía eléctrica y transporte. Estos hallazgos coinciden con el informe anual de (Symantec, 2018), que registra un incremento del 60% en incidentes relacionados con interrupciones operativas desde 2019.

Riesgos para la seguridad humana

Los resultados más preocupantes se relacionan con el potencial impacto en la seguridad humana. El análisis de patrones de ataque reveló que el 19% de las vulnerabilidades identificadas podrían, si fueran explotadas, poner en peligro directamente la vida humana (Dagoumas, 2019) Según el método jerárquico para dibujar escenarios de riesgo completos de (Elhady et al., 2019) las industrias química y nuclear presentan los mayores riesgos, con probabilidades de incidentes catastróficos aumentando exponencialmente cuando múltiples vulnerabilidades son explotadas simultáneamente.

La investigación empírica realizada mediante pruebas de penetración controladas en entornos SCADA demostró que el tiempo medio para la explotación exitosa de vulnerabilidades

conocidas fue de 72 horas, destacando la urgencia de implementar medidas de mitigación efectivas (Fernandez De Arroyabe et al., 2023).

3. Soluciones seguras y efectivas para mitigar los riesgos

El análisis realizado a las vulnerabilidades de los sistemas SCADA mediante los artículos publicados, nos permite identificar soluciones efectivas y seguras para mitigar los riesgos latentes. Los resultados obtenidos indican que, los sistemas SCADA son completamente vulnerables debido a su diseño inicial desarrollado a la funcionalidad y no a la seguridad.

Las soluciones de mitigación de riesgos muestran una realidad difícil al enfrentar las vulnerabilidades en sistemas SCADA. Actualmente, existen soluciones técnicas y estrategias de gestión, su efectividad y seguridad varían significativamente, tanto por factores humanos, técnicos y económicos.

Soluciones técnicas

Las soluciones técnicas para mitigar riesgos en sistemas SCADA abarcan un amplio espectro, empezando con medidas básicas de seguridad informática hasta tecnologías avanzadas de detección y respuesta. Se trata a continuación, un análisis de las principales categorías, evaluando su efectividad y seguridad:

- Segmentación de red: La segmentación de la red SCADA en zonas de seguridad, separando los componentes críticos de los menos críticos y de la red corporativa, es una medida fundamental (Candell Jr. et al., 2015). Sin embargo, la efectividad de esta medida depende de una implementación rigurosa y una configuración precisa de firewalls y reglas de acceso. Una segmentación mal implementada puede crear falsas sensaciones de seguridad y dejar vectores de ataque abiertos.
- Autenticación y control de acceso: La implementación de mecanismos robustos de autenticación multifactor (MFA) y políticas estrictas de control de acceso es esencial para prevenir accesos no autorizados (Rosborough et al., 2019) No obstante, muchos sistemas SCADA heredados carecen de soporte nativo para MFA, lo que requiere soluciones de terceros que pueden introducir nuevas vulnerabilidades si no se integran adecuadamente.

- Detección de intrusiones y anomalías: Los sistemas de detección de intrusiones (IDS) y de detección de anomalías basados en el comportamiento (NIDS/NADS) pueden identificar actividades sospechosas y ataques en tiempo real (García-Teodoro et al., 2009). Sin embargo, la eficacia de estos sistemas depende de la calidad de los datos de entrenamiento y de la capacidad de adaptarse a la evolución de las amenazas. Por otro lado, la generación de falsos positivos puede sobrecargar a los operadores y dificultar la identificación de ataques reales.
- Cifrado de comunicaciones: El cifrado de las comunicaciones entre los componentes del sistema SCADA, utilizando protocolos seguros como TLS/SSL o IPsec, protege la confidencialidad e integridad de los datos (Saif Qassim et al., 2018). Sin embargo, la implementación de cifrado puede afectar el rendimiento de los sistemas SCADA, especialmente en dispositivos con recursos limitados. Sin embargo, la gestión de claves criptográficas es un desafío crítico que, si se descuida, puede comprometer la seguridad del cifrado.
- Actualizaciones y parches: La aplicación oportuna de actualizaciones y parches de seguridad es crucial para corregir vulnerabilidades conocidas (Nist, 2017). La actualización de sistemas SCADA en entornos industriales puede ser compleja y arriesgada, ya que puede interrumpir operaciones críticas. Además, los fabricantes de equipos SCADA no siempre liberan parches de seguridad de manera oportuna o para todos los modelos de dispositivos.
- Soluciones de gestión: Los modelos de gestión desempeñan un papel fundamental en la creación de una cultura de ciberseguridad, en la implementación de procesos robustos y en la mejora continua.
- Evaluaciones de riesgos y vulnerabilidades: La realización periódica de evaluaciones de riesgos y vulnerabilidades permite identificar las amenazas específicas que enfrenta el sistema SCADA y priorizar las medidas de mitigación (Trim & Lee, 2022).
- Políticas y procedimientos de seguridad: El desarrollo e implementación de políticas (como la ISO 27001) y procedimientos de seguridad claros y concisos establece las

expectativas y responsabilidades del personal en relación con la ciberseguridad del sistema SCAD (Anabalón & Donders, 2014).

- Capacitación y concientización: La capacitación y concientización del personal sobre los riesgos de ciberseguridad y las mejores prácticas de seguridad son esenciales para prevenir ataques de ingeniería social y errores humanos (Sans Institute, 2021).
- Planes de respuesta a incidentes: La elaboración de planes de respuesta a incidentes detallados y la realización de simulacros periódicos preparan al personal para responder de manera efectiva y oportuna a un ataque cibernético (García-Teodoro et al., 2009).
- Gestión de la cadena de suministro: La evaluación de la seguridad de los proveedores y la verificación de la integridad de los equipos y software adquiridos son cruciales para prevenir la introducción de vulnerabilidades a través de la cadena de suministro (Pliatsios et al., 2020).

Discusión

Las vulnerabilidades que fueron identificadas en desarrollo del presente artículo en los sistemas SCADA actuales representan una amenaza significativa para la infraestructura crítica, destacándose tres grupos de debilidades que se debe dar atención prioritaria.

1. Las vulnerabilidades relacionadas con la autenticación insegura continúan siendo una de las amenazas más críticas, particularmente debido a la persistencia del uso de credenciales predeterminadas y la falta de implementación de mecanismos de doble o multifactor de autenticación (Morris & Gao, 2014). Esta situación, se agrava por la interconexión creciente de estos sistemas con redes corporativas e internet, lo que aumenta su exposición a ataques externos.
2. Las vulnerabilidades relacionadas con deficiencias en el cifrado de comunicaciones, según (Men et al., 2020), hasta un 65% de los sistemas SCADA analizados transmitían datos de control sin cifrado adecuado, lo que facilita la interceptación y manipulación de comandos críticos. Esta vulnerabilidad es especialmente preocupante en sectores como la energía eléctrica y el agua potable, donde la integridad de las comunicaciones es vital para la seguridad operacional.

3. Las vulnerabilidades relacionadas con la falta de actualizaciones programadas y parcheo continuo, así (Rahimpour et al., 2024)) documentó que el ciclo de vida promedio de los sistemas SCADA puede superar los 15 años, durante los cuales acumulan múltiples vulnerabilidades conocidas, que no son abordadas debido a las limitaciones operativas y los tiempos de inactividad requeridos para aplicar actualizaciones. Estado que los hackers pueden explotar fácilmente mediante el uso de exploits públicos.

Todas las vulnerabilidades no trabajan de manera aislada, sino que interactúan entre sí, creando vectores de ataque cada vez más complejos que pueden comprometer toda la infraestructura operativa y continuidad del negocio. (Von & Hoff, 2021) demostraron cómo la combinación de credenciales débiles y falta de cifrado permitió un ataque exitoso en un entorno de prueba, que un escenario real podría causar daños significativos.

Las vulnerabilidades halladas en los sistemas SCADA y su impacto en la seguridad operacional de las infraestructuras críticas revelan una serie de consecuencias significativas que van más allá de la simple pérdida de datos, afectando directamente la continuidad del servicio, la seguridad física y, en la mayoría de casos, la seguridad de la población.

El impacto de las vulnerabilidades en los sistemas SCADA en la seguridad operacional de las infraestructuras críticas se puede categorizar como:

1. Interrupción de servicios básicos.

Un ataque que tenga exitoso a un sistema SCADA puede provocar la interrupción parcial o total de servicios esenciales como el suministro de electricidad, agua potable, gas natural, transporte público (ferrocarriles, metros) y la gestión de tráfico (Asghar et al., 2019). Estas interrupciones pueden tener efectos en cascada, afectando a otros sectores y generando caos a nivel social y económico. Un ejemplo notorio fue el ataque a la red eléctrica de Ucrania en 2015, donde se utilizó malware para desconectar subestaciones y dejar a cientos de miles de personas sin electricidad (Assante & Lee, 2015).

2. Daños a equipos y activos físicos.

Los sistemas SCADA controlan y supervisan equipos industriales costos, como turbinas, generadores, bombas, válvulas y sistemas de control de procesos. Un atacante que logre controlar estos sistemas puede manipular los parámetros de operación de estos equipos,

causando daños físicos significativos (Stouffer et al., 2023a). Esto no solo son costos elevados de reparación o reemplazo, sino también el riesgo inherente de accidentes industriales y la liberación y exposición a sustancias potencialmente peligrosas para el medio ambiente.

3. Riesgos para la seguridad física y la vida humana.

En infraestructuras críticas como plantas de tratamiento de agua, refinerías de petróleo, plantas químicas y centrales nucleares, un ataque a los sistemas SCADA puede tener consecuencias catastróficas para la seguridad física y la vida humana (Zhu et al., 2023). La manipulación de los sistemas de control puede provocar explosiones, incendios, fugas de sustancias tóxicas o incluso el sabotaje de sistemas de seguridad, poniendo en peligro a los trabajadores y al entorno poblacional.

4. Pérdidas económicas y financieras.

Las interrupciones de servicios, los daños a equipos y los incidentes de seguridad generan altas pérdidas económicas para las organizaciones que operan infraestructuras críticas. Estas pérdidas contemplan costos de reparación, multas regulatorias, pérdida de ingresos, daño a la reputación y posibles demandas legales (Asghar et al., 2019).

5. Impacto en la seguridad nacional.

Un ataque coordinado a gran escala contra los sistemas SCADA de un país podría tener consecuencias devastadoras para su economía, su capacidad de defensa y la estabilidad social (Izycki & Vianna, 2021). Estos ataques podrían ser perpetrados por naciones en conflicto político y social, grupos terroristas o ciberdelincuentes con motivaciones sociales, políticas o económicas. El caso de Stuxnet, un gusano informático diseñado para sabotear el programa nuclear iraní, es un claro ejemplo de este tipo de amenaza (Çetinkaya & Terzi, 2024).

Otro de los factores que permite determinar medidas efectivas para mitigar los riesgos identificados, a pesar del desarrollo tecnológico, es su implementación ya que enfrenta significativos obstáculos operativos y económicos. Seguidamente se presentan las siguientes medidas:

La segmentación de redes mediante firewalls especializados (Asiri et al., 2023) representa una estrategia validada en términos de efectividad técnica. Sin embargo, estos sistemas requieren configuraciones específicas que pueden interferir con las comunicaciones en

tiempo real esenciales para las operaciones SCADA. Esta limitación técnica genera resistencia por parte de los técnicos industriales, quienes priorizan la disponibilidad del sistema sobre la mejora de seguridad (Stouffer et al., 2023a).

El cifrado de comunicaciones ha demostrado ser una solución viable según diversos estudios empíricos (Sekonya & Sithungu, 2023). No obstante, su implementación encuentra barreras significativas relacionadas con el rendimiento de hardware heredado presente en muchas instalaciones industriales. El artículo (Asghar et al., 2019) documenta casos donde la implementación de cifrado TLS incrementó los tiempos de respuesta más allá de los umbrales críticos para ciertas operaciones industriales.

La herramienta de monitoreo para la detección de intrusos (IDS) ha mostrado progresos significativos (McLaughlin et al., 2016). Estas tecnologías permiten mantener visibilidad sobre actividades sospechosas sin impactar directamente el rendimiento del sistema SCADA. A pesar de ello, su eficacia depende directamente de la calidad de las firmas y perfiles de comportamiento establecidos, lo que requiere un mantenimiento continuo y asignación recursos especializados (Yigit et al., 2024).

Ante cualquier vulnerabilidad ninguna solución tecnológica debe considerarse completamente segura, debido a una falta de cultura en tema de seguridad organizacional, debido a errores humanos y falta de políticas y métodos para la gestión de riesgos.

La interconexión de estas observaciones conduce a que la mitigación efectiva de vulnerabilidades en sistemas SCADA requiere un enfoque multifacético que es la combinación de soluciones técnicas con procesos de modelos de gestión de riesgos. Las inversiones en modernización de infraestructura, junto con programas continuos de capacitación, conjugan armónicamente para cerrar las brechas de seguridad existentes en los sistemas SCADA.

Conclusiones

Las vulnerabilidades en los sistemas SCADA representan un riesgo significativo para la seguridad operacional de las infraestructuras críticas. La falta de autenticación robusta, los protocolos de comunicación inseguros y la insuficiente segmentación de redes son algunos de los desafíos más urgentes que deben abordarse. El impacto de estos riesgos puede ser

devastador, como lo demuestran incidentes históricos que han resultado en interrupciones de servicios esenciales y daños a la seguridad de la población.

Afortunadamente, existen soluciones efectivas para mitigar estos riesgos, desde la implementación de tecnologías seguras hasta la formación del personal y la adopción de marcos metodológicos de seguridad reconocidos. Sin embargo, la protección de los sistemas SCADA requiere un enfoque proactivo y colaborativo, en el que la seguridad se integre en todas las fases del ciclo de vida de estos sistemas. Solo mediante un esfuerzo continuo y coordinado se puede garantizar la resiliencia y seguridad de las infraestructuras críticas en un mundo cada vez más interconectado.

La forma efectiva de mitigación de vulnerabilidades en sistemas SCADA requiere un enfoque holístico que combine modernización tecnológica, políticas robustas de gestión de riesgos y concienciación humana. Aunque las soluciones técnicas disponibles son efectivas, su éxito depende de la capacidad de las organizaciones para superar barreras operativas y económicas asociadas con la modernización de sus sistemas. Priorizar la resiliencia y la seguridad operacional en todas las fases del ciclo de vida de los sistemas SCADA es esencial para garantizar la protección de infraestructuras críticas frente a amenazas cibernéticas emergentes.

Referencias bibliográficas

Altaleb, H., & Zoltan, R. (2024). A Comprehensive Analysis and Solutions for Enhancing SCADA Systems Security in Critical Infrastructures. ICCC 2024 - IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems, Proceedings, 247–252. https://doi.org/10.1109/ICCC62278.2024.10582956

Anabalón, J. *, & Donders, E. (2014). Seguridad en Sistemas SCADA un Acercamiento Práctico a Través de EH e ISO 27001:2005.

Asghar, M. R., Hu, Q., Zeadally, S., & Rizwan Asghar, M. (2019). Cybersecurity in Industrial Control Systems: Issues, Technologies, and Challenges.

Asiri, M., Saxena, N., Gjomemo, R., & Burnap, P. (2023). Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems, 7(2). https://doi.org/10.1145/3587255

Assante, M. J., & Lee, R. M. (2015). The Industrial Control System Cyber Kill Chain. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Candell Jr., R., Zimmerman, T. A., & Stouffer, K. A. (2015). An Industrial Control System Cybersecurity Performance Testbed. https://doi.org/10.6028/NIST.IR.8089

Çetinkaya, Ş., & Terzi, S. (2024). Analysing The Effects of Cyber Security on National Security From A Realist Perspective: "Stuxnet" Example. Cost of a Data Breach Report 2024. (2024).

Dagoumas, A. (2019). Assessing the Impact of Cybersecurity Attacks on Power Systems. Energies 2019, Vol. 12, Page 725, 12(4), 725. https://doi.org/10.3390/EN12040725

Dickson, S. M., & OKECHUKWU, I. P. (2023). Cyber Security in the Age of the Internet of Things, Constraints, and Solutions. JOURNAL OF DIGITAL LEARNING AND DISTANCE EDUCATION, 2(11), 829–837. https://doi.org/10.56778/JDLDE.V2I11.233

Dimitrov, W., & Syarova, S. (2019). Analysis of the Functionalities of a Shared ICS Security Operations Center. 2019 Big Data, Knowledge and Control Systems Engineering, BdKCSE 2019. https://doi.org/10.1109/BDKCSE48644.2019.9010607

Elhady, A. M., El-Bakry, H. M., & Abou Elfetouh, A. (2019). Comprehensive Risk Identification Model for SCADA Systems. Security and Communication Networks, 2019(1), 3914283. https://doi.org/10.1155/2019/3914283

Fajardo Rosas, F. A. (2014). Implementación de Políticas de Seguridad en los Sistemas SCADA. Instname:Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/2983

Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security, 124, 102954. https://doi.org/10.1016/J.COSE.2022.102954

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security -- A Survey. http://arxiv.org/abs/1701.04525

Izycki, E., & Vianna, E. W. (2021). Critical Infrastructure: A Battlefield for Cyber Warfare? https://doi.org/10.34190/IWS.21.011

Jyothsna, V., & Prasad, K. M. (2019). Anomaly-Based Intrusion Detection System. www.intechopen.com

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52–80. https://doi.org/10.1016/J.IJCIP.2015.02.002

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security and Privacy, 9(3), 49–51. https://doi.org/10.1109/MSP.2011.67

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The Cybersecurity Landscape in Industrial Control Systems. Proceedings of the IEEE, 104(5), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235

Men, J., Lv, Z., Zhou, X., Han, Z., Xian, H., & Song, Y. N. (2020). Machine learning methods for industrial protocol security analysis: Issues, taxonomy, and directions. IEEE Access, 8, 83842–83857. https://doi.org/10.1109/ACCESS.2020.2976745

Morris, T., & Gao, W. (2014). Industrial control system traffic data sets for intrusion detection research. In IFIP Advances in Information and Communication Technology (Vol. 441).

NCCIC y ICS-CERT. (2016). ICS-CERT Annual Assessment Report.

Nist. (2017). Title: Cybersecurity Framework Manufacturing Profile. https://doi.org/10.6028/NIST.IR.8183

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ, 372. https://doi.org/10.1136/BMJ.N71

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. IEEE Communications Surveys and Tutorials, 22(3), 1942–1976. https://doi.org/10.1109/COMST.2020.2987688

Rahimpour, H., Tusek, J., Musleh, A. S., Liu, B., Abuadbba, A., Phung, T., & Seneviratne, A. (2024). A Review of Cybersecurity Challenges in Smart Power Transformers. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3518494

Rosborough, C., Gordon, C., & Waldron, B. (2019). All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications.

Sabillón, R., & Cano, J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. https://doi.org/10.17013/risti.32.33-48

Saif Qassim, Q., Jamil1, N., Jidin, R., Rusli1, M. E., Nabil, M., Zawawi1, A., Jamaludin, Z., Reza Z'aba, M., Azlan, W., & Kamarulzaman, W. (2018). A review: towards practical attack taxonomy for industrial control systems. International Journal of Engineering & Technology, 7(2), 145–152.

Sans Institute. (2021). A SANS 2021 Survey: OT/ICS CybersecurityExecutive Summary. www.cisa.gov/critical-infrastructure-sectors

Sekonya, N., & Sithungu, S. (2023). An Analysis of Critical Cybersecurity Controls for Industrial Control Systems.

Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2021). Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 17(5), 2985–2996. https://doi.org/10.1109/TII.2020.3023507

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023a). NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security. https://doi.org/10.6028/NIST.SP.800-82r3

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023b). Withdrawn NIST Technical Series Publication Warning Notice Withdrawn Publication Series/Number NIST Special Publication (SP) 800-82 Revision 2 Title Guide to Industrial Control Systems (ICS) Security Publication Date(s) Superseding Publication(s) (if applicable) Series/Number NIST SP 800-82r3 (Revision 3) Title Guide to Operational Technology (OT) Security Additional Information (if applicable). https://doi.org/10.6028/NIST.SP.800-82r3

Symantec. (2018). ISTR Internet Security Threat Report Volume 23.

Tatipatri, N., & Arun, S. L. (2024). A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. IEEE Access, 12, 18147–18167. https://doi.org/10.1109/ACCESS.2024.3361039

Trim, P., & Lee, Y. I. (2022). Strategic cyber security management. Strategic Cyber Security Management, 1–248. https://doi.org/10.4324/9781003244295

Von, H., & Hoff, J. (2021). Creating Attack Graphs for Adversary Emulation, Simulation and Purple Teaming in Industrial Control System (ICS) Environments.

Xu, L., Wang, B., Wu, X., Zhao, D., Zhang, L., & Wang, Z. (2022). Detecting Semantic Attack in SCADA System: A Behavioral Model Based on Secondary Labeling of States-Duration

Evolution Graph. IEEE Trans. Netw. Sci. Eng., 9(2), 703–715. https://doi.org/10.1109/TNSE.2021.3130602

Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities. https://doi.org/10.1109/ACCESS.2017.DOI

Zhu, Q., Zhang, G., Luo, X., & Gan, C. (2023). An industrial virus propagation model based on SCADA system. Information Sciences, 630, 546–566. https://doi.org/10.1016/j.ins.2022.12.119

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

Esta investigación se realizó como parte del trabajo del grupo de investigación “Sistemas Embebidos y Visión Artificial en Ciencias Arquitectónicas, Agropecuarias, Ambientales y Automática (SE-VA4CA)” bajo el proyecto de investigación “CompostBot robot de servicio para tratamiento de residuos orgánicos domiciliarios de cocina” del Laboratorio de Robótica, Automatización, Sistemas Inteligentes y Embebidos (RobLab).

Nota:

El artículo no es producto de una publicación anterior.