Desafíos de la Ciberseguridad OT en la Era NIS2: Amenazas, IA y Brechas de Implementación

Farid Bagheri-Gisour Marandyn, Néstor Rodríguez Pérez, Álvaro Jesús López López,
Juan Atanasio Carrasco Mateos, Agustín Valencia Gil-Ortega, Javier Jarauta Sánchez,
Rafael Palacios, José Antonio Rodríguez Mondéjar, Gregorio López López
Instituto de Investigación Tecnológica (IIT)
Universidad Pontificia Comillas, ICAI
Madrid, España
Email: fbagherigisour@comillas.edu

Tipo de contribución: Investigación original (4 páginas).

***Resumen*—La Directiva NIS2 y su ecosistema asociado (CRA, AI Act) imponen requisitos de detección, respuesta y gestión de vulnerabilidades que el dominio OT aún no ha madurado. Esta revisión estructurada de la literatura reciente identifica un cuello de botella común: la brecha entre validación sintética y entornos reales bloquea simultáneamente la adopción operativa de IA y el cumplimiento práctico de NIS2. Las precisiones superiores al 99 % reportadas en datasets públicos no se traducen en despliegue, y solo el 13 % de las vulnerabilidades del catálogo KEVC relevantes para OT ofrecen alternativas al parcheo aplicables a sistemas que no admiten interrupción. Se argumenta que los laboratorios OT que integran hardware industrial real, honeypots y gemelos digitales constituyen la infraestructura imprescindible para cerrar estas brechas.**

***Index Terms*—Ciberseguridad OT, ICS, SCADA, NIS2, inteligencia artificial, honeypots, testbeds, IEC 62443, gemelo digital.**

I. Introducción

La Directiva NIS2 [1], en vigor desde enero de 2023 con plazo de transposición en octubre de 2024, ha marcado un punto de inflexión para la ciberseguridad de las infraestructuras críticas europeas. Los operadores de sectores esenciales están obligados a implementar gestión de riesgos, notificación de incidentes en 24/72 horas y seguridad de la cadena de suministro, con sanciones de hasta el 2 % de la facturación global. Este marco se complementa con el Cyber Resilience Act (CRA) [2], que exige seguridad por diseño a los fabricantes de productos digitales incluidos PLCs y sensores IoT, y con el AI Act [3], que puede encuadrar como alto riesgo los sistemas de IA desplegados en infraestructuras críticas según su contexto de uso. La convergencia configura un ecosistema normativo sin precedentes que el dominio OT, históricamente aislado, no está preparado para cumplir.

La urgencia regulatoria responde a un panorama de amenazas en rápida evolución y a una asimetría estructural propia del dominio. Los entornos OT acumulan dispositivos con ciclos de vida de hasta dos décadas, protocolos como Modbus, DNP3 u OPC Classic sin cifrado ni autenticación nativa, y procesos físicos que no admiten interrupción para aplicar parches; la convergencia IT/OT ha expuesto a estos sistemas a las vulnerabilidades del dominio IT sin disponer de los mismos mecanismos de defensa ni de ventanas de mantenimiento equivalentes [4]. Los informes de industria documentan un incremento del 84 % en ataques con protocolos OT [5], vulnerabilidades nuevas en OPC UA [6] y la explotación de memoria en PLCs [7], con MaDIoT alcanzando su tercera generación [8].

Frente a surveys recientes centrados en amenazas [4] o en IA/ML [9], este artículo presenta una revisión estructurada que articula cuatro ejes (amenazas, defensas, IA/ML y estándares), complementados con tendencias emergentes y brechas identificadas, para responder: *¿cómo se distribuye el esfuerzo investigador en ciberseguridad OT bajo NIS2 y dónde están las brechas que bloquean el cumplimiento operativo?* La tesis defendida es que el cuello de botella común a la adopción de IA, la gestión de vulnerabilidades y la validación de defensas es la falta de infraestructura realista de experimentación, y que los laboratorios OT que integran hardware industrial real, gemelos digitales y honeypots, como el CiberLab de ICAI [10], constituyen la respuesta operativa a esta brecha.

II. Metodología

Se ha seguido un proceso estructurado inspirado en PRISMA. Las fuentes consultadas incluyen IEEE Xplore, ACM DL, ScienceDirect, USENIX, Springer y arXiv (2023–2025), complementadas con informes de industria (ENISA, Forescout, Honeywell, Dragos), regulaciones europeas (NIS2, CRA, AI Act, Network Code) y guías técnicas (NIST SP 800-82, IEC 62443, MITRE ATT&CK for ICS). Los criterios de inclusión exigen relevancia explícita para entornos OT/ICS, publicación en venues reconocidos y aportación técnica verificable; se excluyen trabajos exclusivamente IT y preprints sin resultados reproducibles. El corpus resultante se clasifica en seis categorías no excluyentes: contexto OT/ICS, panorama de amenazas, estrategias de defensa, IA/ML aplicada, estándares y gobernanza, y tendencias emergentes.

III. Estado del arte

III-A. Panorama de amenazas y vectores de ataque

APT y panorama industrial. El panorama de amenazas en OT ha experimentado una transformación significativa [4], [11]: Bhole et al. [12] analizan 120 grupos APT y MITRE ATT&CK for ICS [13] formaliza sus tácticas. Los informes de industria, cuyos datos hay que interpretar con cautela, convergen en la magnitud: ENISA [14] analiza 4.875 incidentes en su panorama 2025, Forescout/Vedere Labs [5] documenta el 84 % de incremento en ataques con protocolos OT (Modbus el más explotado) y Honeywell [15] sitúa al USB como

vector del 51 % del malware industrial. **Vulnerabilidades en dispositivos.** Los ataques MaDIoT han alcanzado su tercera generación coordinando recursos energéticos distribuidos [8], [16]; la sistematización de López-Morales et al. [17] sobre PLCs identifica superficies de ataque inexploradas, demostradas empíricamente por Jo y Ahmed [7] (CVE-2024-11737) y por Diemunsch et al. [6] con 8 vulnerabilidades nuevas en OPC UA mediante análisis formal con ProVerif.

III-B. Estrategias de defensa y detección

La detección de intrusiones combina enfoques basados en estado y datos. Abbas et al. [18] introducen SAIN, invariantes conscientes del estado del PLC con solo 2 % de falsos positivos, mientras que Algul et al. [19] presentan SCADANet ante la falta de realismo de los datasets existentes. Villa et al. [20] aportan ICSQuartz, el primer fuzzer nativo para Structured Text consciente del ciclo de escaneo del PLC. En el plano post-incidente, Ike et al. [21] presentan PhyLink, una técnica forense que vincula evidencia física con vectores de infección logrando 98,7 % de precisión, mientras que Zhang et al. [22] demuestran HoneyParser sobre datos de honeypots SCADA desplegados en AWS. Un desafío transversal es la validación realista de las defensas: SCASS [23] integra PLCs ABB con virtualización, MiniCPS [24] combina SDN con emulación de procesos físicos para evaluar defensas MTD, y Crabb et al. [25] contenerizan gemelos digitales en Kubernetes. Ortiz et al. [26] muestran que el tráfico SCADA real desmiente los modelos sintéticos de comportamiento monolítico.

III-C. IA/ML aplicada a seguridad OT

La aplicación de IA/ML supera el 90 % de precisión en datasets de referencia [9]: Yalçın et al. [27] alcanzan 99,99 % con XGBoost (multiclase) en WUSTL-IIOT-2021 y Mesadieu et al. [28] obtienen 99,36 % mediante DRL (binario) sobre el mismo benchmark; las cifras no son comparables (paradigmas y granularidades distintos) y, junto con particiones favorables y la ausencia de *F1-score* ponderado o AUC-ROC, inflan la apariencia de robustez frente a entornos reales [9]. Fung et al. [29] revelan que los operadores luchan más con el diagnóstico de alarmas que con la detección, y Koay et al. [30] confirman que la adopción real permanece limitada por desafíos de datos y confianza. El aprendizaje federado [31] preserva la privacidad de los datos industriales, una capacidad especialmente relevante para operadores NIS2. En el frente autónomo, el agente CAI de Mayoral-Vilches et al. [32] resolvió 32 de 34 retos del Dragos OT CTF 2025, un 37 % más rápido que equipos humanos, anticipando el doble filo de los LLMs en OT.

III-D. Estándares y marco regulatorio

La Directiva NIS2 [1], aplicable desde octubre de 2024, cubre 18 sectores e impone notificación de incidentes en 24/72 horas, responsabilidad personal de la dirección y sanciones de hasta el 2 % de la facturación global. El Cyber Resilience Act [2] regula al *fabricante*: seguridad por diseño, gestión de vulnerabilidades durante todo el ciclo de vida y marcado CE de ciberseguridad para dispositivos IoT/OT. El AI Act [3] puede encuadrar como *alto riesgo* los IDS basados en IA/ML en infraestructuras críticas según su contexto de uso, exigiendo robustez, trazabilidad y supervisión humana. A nivel sectorial, el Network Code on Cybersecurity [33] establece la primera regulación específica de ciberseguridad OT para flujos eléctricos transfronterizos. La guía NIST SP 800-82 Rev. 3 [34] y MITRE ATT&CK for ICS [35] siguen siendo las referencias técnicas centrales. Nilsson [36] identifica convergencia entre NIS2/CRA e IEC 62443 en seguridad del ciclo de vida pero brechas en vigilancia post-mercado y divulgación coordinada de vulnerabilidades.

La Tabla I resume una selección de contribuciones técnicas representativas, ilustrando la diversidad metodológica del campo (testbed real, dataset público, verificación formal, simulación, competición).

IV. Análisis y tendencias

IV-A. Distribución temática y validación

La codificación del corpus (categorías no excluyentes, Tabla II) revela un sesgo claro: defensas y amenazas dominan frente a IA/ML aplicada y, sobre todo, estándares y gobernanza, evidenciando un desacoplamiento entre la urgencia normativa NIS2/CRA/AI Act y la atención académica. De los 47 trabajos con componente experimental, el 53 % se valida con datasets públicos o simulación y solo el 38 % sobre hardware industrial real (SCASS [23], SAIN [18], ICSQuartz [20], PhyLink [21], Jo y Ahmed [7], AutoLabel [38]); la concentración de IDS validados sobre datasets contrasta con la escasez de testbeds reales para resiliencia y prevención [23], [25], [39], en línea con la falta de realismo de los datasets SCADA existentes [19].

IV-B. Brechas de investigación

Validación realista. Ortiz et al. [26] demuestran que las redes SCADA reales exhiben comportamientos que los modelos sintéticos no capturan; los testbeds híbridos [23], gemelos digitales [25] y plataformas SDN [24] avanzan en esa dirección sin replicar aún una infraestructura en producción, mientras los honeypots industriales [22] y los gemelos digitales adaptativos [37] la complementan capturando ataques reales. Akinremi et al. [40] confirman además una brecha de competencias IT/OT que laboratorios con hardware multi-generación y arquitectura Purdue, como el CiberLab de ICAI [10], permiten cerrar como plataforma de validación y formación.

Gestión de vulnerabilidades. El 65 % de las entradas del KEVC son relevantes para OT pero solo el 13 % admiten alternativas al parcheo [41]; NIS2 [1] obliga a gestionarlas activamente pese a la imposibilidad de detener procesos críticos, una paradoja que el CRA [2] aborda parcialmente trasladando al fabricante el ciclo de vida y las actualizaciones de seguridad. La alerta de CISA sobre los dispositivos Hitachi Energy FOX61x [42] ilustra la paradoja en la práctica: la mitigación exige cambios de configuración que requieren ventanas de mantenimiento planificadas, incompatibles con las ventanas de notificación 24/72 horas que NIS2 impone.

Adopción de IA. Las precisiones superiores al 99 % [27], [28] no se traducen en adopción: la interpretabilidad insuficiente y el escepticismo de los operadores [29], [30] pesan más que el rendimiento, mientras los ataques adversarios transferibles [43], el *concept drift* [44] y la falta de interoperabilidad [45] añaden riesgos que el AI Act [3] exigirá gestionar;

Tabla I
SELECCIÓN DE CONTRIBUCIONES TÉCNICAS REPRESENTATIVAS DEL CORPUS

Referencia	**Técnica**	**Contribución principal**	**Protocolo**	**Validación**[1]
Abbas et al. [18]	Invariantes de estado	Detección de ataques sigilosos con 2 % FP	PLC (ST)	Testbed real
Villa et al. [20]	Fuzzing nativo	Primer fuzzer ST consciente del ciclo de escaneo	Structured Text	Testbed real
Diemunsch et al. [6]	Verificación formal	8 vulnerabilidades nuevas en OPC UA	OPC UA	ProVerif
Ike et al. [21]	Forense ciberfísico	Vinculación síntomas físicos-intrusión (98,7 %)	Modbus	Testbed real
Mayoral-Vilches et al. [32]	Agente IA autónomo	Top-10 en Dragos OT CTF (32/34 retos)	Modbus, DNP3	Competición real
Alcaraz et al. [37]	Gemelo digital adaptativo	Protección, engaño y testeo integrados	IIoT	Simulación

Tabla II
DISTRIBUCIÓN DEL CORPUS ACADÉMICO POR CATEGORÍA (NO EXCLUYENTES)

Categoría	**N.º trabajos**
Defensas y detección	53
Amenazas y vectores	35
IA/ML aplicada	28
Contexto OT/ICS	20
Estándares y gobernanza	8
Tendencias emergentes	3

el aprendizaje federado [31] emerge como vía para entrenar modelos sin centralizar datos de infraestructuras críticas.

IV-C. Tendencias emergentes

IA generativa y agentes autónomos. CAI [32] resolvió 32/34 retos del Dragos OT CTF un 37 % más rápido que equipos humanos, anticipando que los LLMs transformarán ofensiva y defensa: automatización de reglas, análisis de logs [38] y grafos de procedencia CTI [46]. El AI Act [3] exigirá robustez adversarial y supervisión humana en un escenario donde Meskini et al. [43] demuestran la transferibilidad de evasiones contra IDS IIoT y Lara-Gutiérrez et al. [44] abordan el *concept drift* con reentrenamientos mínimos. **Gemelos digitales, honeypots y engaño.** Alcaraz et al. [37] integran protección, *deception* y testeo en un gemelo adaptativo; Zhang et al. [22] capturan ataques reales con honeypots SCADA; Arias et al. [47] y Alcaraz y López [48] acoplan gemelos digitales con SIEM y detección de anomalías. Laboratorios OT que combinan hardware real, gemelos digitales y honeypots, como el CiberLab de ICAI [10], son la infraestructura imprescindible para validar defensas y formar profesionales IT/OT [23], [49]. **Expansión del perímetro.** La superficie de ataque se diversifica hacia 5G/Industry 5.0 [50], vehículos conectados [51], manufactura aditiva [52] y la cadena de suministro regulada por el CRA mediante SBOM [2], [53].

V. CONCLUSIONES

La revisión confirma tres conclusiones alineadas con la tesis. (1) **Amenazas y regulación divergen del estado de la práctica.** La sofisticación de los ataques (MaDIoT 3.0 [8], explotación de memoria en PLCs [7], vulnerabilidades en OPC UA [6], +84 % en protocolos OT [5]) y la convergencia NIS2/CRA/AI Act/Network Code [1]–[3], [33] no encuentran respuesta en herramientas maduras: persisten brechas en vigilancia post-mercado [36] y solo el 13 % de entradas KEVC ofrecen alternativas al parcheo [41], exigiendo migrar de parches a mitigación compensatoria. (2) **La IA/ML supera el 99 % en datasets [27] pero no se adopta** por interpretabilidad insuficiente, vulnerabilidad adversaria [43], *concept drift* [44] y diagnóstico de alarmas [29]; los criterios de evaluación deben incorporar operabilidad y latencia más allá de la precisión, y los LLMs autónomos [32] emergen como doble filo. (3) **El cuello de botella común es la validación realista**: honeypots industriales [22], testbeds híbridos [23] y gemelos digitales adaptativos [37] convergen en una infraestructura de experimentación y engaño que cierra simultáneamente la brecha de IA, la de gestión de vulnerabilidades y la formación IT/OT [49].

De estas conclusiones se derivan tres implicaciones para la práctica: los criterios de evaluación de IDS deben incorporar operabilidad, latencia y diagnóstico de alarmas más allá de la precisión [29], [54]; la gestión de vulnerabilidades debe migrar hacia mitigación compensatoria ante la imposibilidad de parcheo [41]; y la formación IT/OT mediante CTF industriales [49] y testbeds [40] es una necesidad crítica.

Como trabajo futuro se priorizan dos líneas: (i) el desarrollo de **laboratorios OT** como el CiberLab de ICAI [10] que integren hardware industrial real, gemelos digitales adaptativos y honeypots, combinando validación representativa con captura de ataques reales; y (ii) la investigación en **explicabilidad, robustez adversarial y supervisión humana** de los sistemas de IA generativa que el AI Act exigirá en infraestructuras críticas. El desajuste entre la sofisticación de las amenazas y la limitada adopción de las defensas propuestas solo puede cerrarse mediante la colaboración efectiva entre academia, operadores industriales y reguladores sobre infraestructura de validación compartida.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el proyecto eFORT (Horizon Europe, Grant Agreement No. 101075665) y por el programa predoctoral del Instituto de Investigación Tecnológica (IIT), Universidad Pontificia Comillas.

REFERENCIAS

[1] European Union, “Directive (eu) 2022/2555 – nis 2 directive,” Official Journal of the European Union, 2022.

[2] ——, "Regulation (eu) 2024/2847 – cyber resilience act," Official Journal of the European Union, 2024.

[3] ——, "Regulation (eu) 2024/1689 – artificial intelligence act," Official Journal of the European Union, 2024.

[4] S. Kapoor, S. Kumar, and H. Vardhan, "Cyber security of ot networks: A tutorial and survey," arXiv, 2025.

[5] F. R. V. Labs, "2025 threat roundup," Forescout, Tech. Rep., 2025.

[6] V. Diemunsch, L. Hirschi, and S. Kremer, "A comprehensive formal security analysis of opc ua," *USENIX Security 2025*, 2025.

[7] W. Jo and I. Ahmed, "Oops, it halted again: Exploiting plc memory for fun and profit in industrial control systems," *USENIX WOOT '25*, 2025.

[8] N. Rodríguez-Pérez, J. Matanza, L. Sigrist, J. R. Torres, and G. López, "Madiot 3.0: Assessment of attacks to distributed energy resources and demand in a power system," *IEEE Open Access Journal of Power and Energy*, vol. 12, pp. 552–563, 2025.

[9] A. Bajwa, A. A. R. Tonoy, S. Rana, and I. Ahmed, "Cybersecurity in industrial control systems: A systematic literature review on ai-based threat detection for scada and iot networks," in *1st Global Research and Innovation Conference 2025*, 2025.

[10] F. B.-G. Marandyn, N. R. Pérez, and G. L. López, "Design and implementation of an OT cybersecurity laboratory with multi-generation PLC architecture and Purdue model segmentation," in *6th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP), ESORICS 2025*, ser. Lecture Notes in Computer Science. Springer, 2025.

[11] D. Inc., "8th annual year in review 2025 ot/ics cybersecurity report," *Informe de Industria*, 2025.

[12] M. Bhole, T. Sauter, and W. Kastner, "Enhancing industrial cybersecurity: Insights from analyzing threat groups and strategies in operational technology environments," *IEEE Open Journal of the Industrial Electronics Society*, vol. 6, pp. 145–157, 2025.

[13] M. ATT&CK, "Mitre att&ck for ics: T0831 - manipulation of control," *MITRE Knowledge Base*, 2025.

[14] ENISA, "Enisa threat landscape 2025," European Union Agency for Cybersecurity, Tech. Rep., 2025.

[15] Honeywell, "Cyber threat report 2025: Insights and actions to manage cyber-physical threat convergence," Honeywell, Tech. Rep., 2025.

[16] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," *USENIX Security 2018*, 2018.

[17] E. López-Morales, U. Planta, C. Rubio-Medrano, A. Abbasi, and A. A. Cardenas, "Sok: Security of programmable logic controllers," *USENIX Security 2024*, 2024.

[18] S. G. Abbas, M. O. Ozmen, A. Alsaheel, A. Khan, Z. B. Celik, and D. Xu, "Sain: Improving ics attack detection sensitivity via state-aware invariants," *USENIX Security 2024*, 2024.

[19] E. Algul, F. Dogan, A. A. Ahmad, and O. Polat, "Scadanet: A novel dataset for scada cybersecurity and intrusion detection," *Computer Networks*, vol. 278, p. 112087, 2026.

[20] C. Villa, C. Doumanidis, H. Lamri, P. H. N. Rajput, and M. Maniatakos, "Icsquartz: Scan cycle-aware and vendor-agnostic fuzzing for industrial control systems," in *NDSS Symposium 2025*, 2025.

[21] M. Ike, K. Sadoski, R. Valme, B. Sahin, S. Zonouz, and W. Lee, "Your control host intrusion left some physical breadcrumbs: Physical evidence-guided post-mortem triage of scada attacks," *ACM ASIA CCS '25*, 2025.

[22] W. Zhang, N. Dong, T. Choi, G. Bai, and R. K. L. Ko, "Intelligent data refinement and analysis of real-world cyber attacks on scada systems," *ACM E-Energy '25*, 2025.

[23] N. d'Ambrosio, G. Capodagli, G. Perrone, and S. P. Romano, "Scass: Breaking into scada systems security," *Computers & Security*, vol. 151, p. 104315, 2025.

[24] X. Etxezarreta, I. Garitano, M. Iturbe, and U. Zurutuza, "On the use of minicps for conducting rigorous security experiments in software-defined industrial control systems," *Wireless Networks*, vol. 30, no. 9, pp. 7377–7390, 2024.

[25] K. A. C. II, H. Coleman, and D. Hamilton, "Development of a digital twin software for scada focused anomaly and intrusion detection systems research," *ACM SIGSIM-PADS '25*, 2025.

[26] N. Ortiz, A. A. Cardenas, and A. Wool, "Scada world: An exploration of the diversity in power grid networks," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 8, no. 1, pp. 1–26, 2024.

[27] N. Yalçın, S. Çakır, and S. Ünaldı, "Attack detection using artificial intelligence methods for scada security," *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 39 550–39 559, 2024.

[28] F. Mesadieu, D. Torre, and A. Chennamaneni, "Leveraging deep reinforcement learning technique for intrusion detection in scada infrastructure," *IEEE Access*, vol. 12, pp. 63 381–63 399, 2024.

[29] C. Fung, E. Zeng, and L. Bauer, "Adopting ai to protect industrial control systems: Assessing challenges and opportunities from the operators' perspective," *SOUPS 2025*, 2025.

[30] A. M. Y. Koay, R. K. L. Ko, H. Hettema, and K. Radke, "Machine learning in industrial control system (ics) security: current landscape, opportunities and challenges," *Journal of Intelligent Information Systems*, vol. 60, no. 2, pp. 377–405, 2023.

[31] X. S. de Camara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous iot networks," *Computers & Security*, vol. 131, p. 103299, 2023.

[32] V. Mayoral-Vilches *et al.*, "Cybersecurity ai in ot: Insights from an ai top-10 ranker in the dragos ot ctf 2025," arXiv, 2025.

[33] European Union, "Delegated regulation (eu) 2024/1366 – network code on cybersecurity for electricity," Official Journal of the European Union, 2024.

[34] K. Stouffer *et al.*, "Guide to operational technology (ot) security," NIST Special Publication, Tech. Rep., 2023.

[35] B. Al-Sada, A. Sadighian, and G. Oligeri, "Mitre att&ck: State of the art and way forward," *ACM Computing Surveys*, vol. 57, no. 1, pp. 1–42, 2024.

[36] M. Nilsson, "Aligning eu cybersecurity regulations with ics security standards: A systematic literature review," Tesis de Maestría (University of Skövde), Tech. Rep., 2025.

[37] C. Alcaraz, H. Guzman, and J. Lopez, "Adaptive digital twin: Protection, deception, and testing," *Future Generation Computer Systems*, vol. 179, p. 108357, 2026, in press.

[38] Y. Peng *et al.*, "Autolabel: Automated fine-grained log labeling for cyber attack dataset generation," *USENIX Security 2025*, 2025.

[39] A. Raj, S. Das, H. Vardhan, H. Neema, A. Chhokra, and D. Balasubramanian, "Autonomous cybersecurity testbed for operational technology networks," *ACM DESTION '25*, 2025.

[40] T. P. Akinremi, J. K. Appiah, A. R. Asadi, O. Ibitoye, and S. Popoola, "Driving factors behind adopting virtual testbeds for ics cybersecurity education," *ACM SIGCITE 2025*, 2025.

[41] P. Huff, N. Gandu, and P. Novák, "I can't patch my ot systems! a look at cisa's kevc workarounds & mitigations for ot," arXiv, 2025.

[42] C. . H. Energy, "Ics advisory: Hitachi energy fox61x," CISA ICS Advisory, Tech. Rep., 2026.

[43] I. H. Meskini, C. Alcaraz, R. R. Castro, and J. Lopez, "Analysis of transferable adversarial evasion attack detection in iot and industrial ads," *IEEE Open Journal of the Computer Society*, vol. 7, pp. 142–153, 2025.

[44] A. Lara-Gutierrez, C. Fernandez-Gago, and J. A. Onieva, "A framework for drift detection and adaptation in ai-driven anomaly and threat detection systems," *International Journal of Information Security*, vol. 24, no. 5, p. 199, 2025.

[45] M.-A. Jibotean and O.-P. Stan, "Cybersecurity challenges and strategies in critical infrastructure systems: A comprehensive survey," *2025 ICSTCC*, 2025.

[46] A. Yusof, S. Li, A. S. Kawatra, D. Li, E.-C. Chang, and Z. Liang, "From observations to insights: Constructing effective cyberattack provenance with provcon," *WOSOC 2025*, 2025.

[47] A. Arias, C. Arellano, A. Urbieta, and U. Zurutuza, "Leveraging digital twins and siem integration for incident response in ot environments," *JNIC 2024*, 2024.

[48] C. Alcaraz and J. Lopez, "Digital twin-assisted anomaly detection for industrial scenarios," *International Journal of Critical Infrastructure Protection*, vol. 47, p. 100721, 2024.

[49] S. Abaimov, J. Gardiner, E. Samanis, J. Williams, M. Samanis, F. Shahbi, and A. Rashid, "Capture the industrial flag: Lessons from hosting an ics cybersecurity exercise," *ACM CPSS '24*, 2024.

[50] C. Alcaraz and J. Lopez, "Protecting digital twin networks for 6g-enabled industry 5.0 ecosystems," *IEEE Network Magazine*, vol. 38, no. 3, pp. 302–308, 2023.

[51] J. I. N. Vidal, "Distributed honeypots as a proactive cyber threat detection mechanism in connected vehicles," Reporte Técnico Independiente, Tech. Rep., 2025.

[52] M. H. Rais, M. Ahsan, and I. Ahmed, "Sok: 3d printer firmware attacks on fused filament fabrication," *USENIX WOOT 2024*, 2024.

[53] R. Roman, C. Alcaraz, J. Lopez, and K. Sakurai, "Current perspectives on securing critical infrastructures' supply chains," *IEEE Security & Privacy*, vol. 21, no. 1, pp. 46–56, 2023.

[54] C. Fung, E. Zeng, and L. Bauer, "Attributions for ml-based ics anomaly detection: From theory to practice," in *NDSS Symposium 2024*, 2024.