Volume 2 · Issue 1 · 2025 · pp. 43–48

Resilience Engineering for Operational Technology: The 2023-2025 Critical-Infrastructure Attack Record and the IEC 62443 Path

Cristina Alcaraz
ORCID: 0000-0003-0545-3191
Department of Computer Science, University of Málaga, Málaga, Spain

Yanxia Sun
ORCID: 0000-0002-3455-9625
Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg, South Africa

Correspondence: Cristina Alcaraz · contact details held in the journal record

Publication history. Assigned by the publisher to Cybersecurity Advances, Volume 2, Issue 1 (2025). This publisher-authorized digital edition was released on 29 October 2026 from the supplied final 2025 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2025 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is independently verified.

Background: Operational technology (OT) — the control systems behind water, energy, and manufacturing — became a headline cyber target in 2023-2025, not through novel exploits but through failures of basic hygiene: the November 2023 compromise of a western Pennsylvania water authority's Unitronics PLC by Iran-affiliated "Cyber Av3ngers" (default credentials, Internet-exposed device), the CISA advisory that followed (AA23-335A, updated December 2024), and the EPA's May 2024 enforcement alert reporting that over 70% of inspected drinking-water systems did not fully comply with Safe Drinking Water Act risk-assessment requirements. **Objective:** We analyze the 2023-2025 OT attack record and construct the resilience-engineering program it implies — one that accepts unpatchable legacy devices as a permanent condition and engineers around them. **Methods:** Incident-record analysis from government advisories and enforcement documents; architectural analysis using the Purdue hierarchy and IEC 62443's zones-and-conduits model; and a risk-versus-control coverage assessment. **Results:** The record shows a consistent mechanism: IT-side compromise traveling into flat OT networks to reach exposed, under-credentialed control devices — with real-world impact bounded not by cyber defense but by *manual fallback* (operators running treatment processes by hand). IEC 62443's zones-and-conduits segmentation, credential hygiene at the OT boundary, and rehearsed manual fallbacks are the highest-leverage controls; exotic threat intelligence ranks last. **Conclusions:** OT resilience is not IT security transplanted; it is engineered degradation tolerance. The 2023-2025 record tells utilities and industrial operators exactly what to build first.

Keywords: operational technology; ICS security; IEC 62443; critical infrastructure; water security; Purdue model; resilience engineering; digital trust

Contribution statement. This paper makes four contributions: (1) a source-verified 2023-2025 incident-and-response record for the water sector as the OT canary; (2) an architectural analysis of the IT-to-OT attack path using the Purdue hierarchy; (3) a risk-versus-control coverage assessment aligned with IEC 62443's zones-and-conduits model; and (4) a resilience-engineering priority order for resource-constrained utilities — where manual fallback capability is treated as a first-class control.

1. Introduction

Operational technology is where cybersecurity's abstractions meet physics. A compromised email server is an incident; a compromised water-treatment control system is a public-health event. The 2023-2025 record made this concrete for the water sector — the OT canary for every industrial operator — through a sequence that was remarkable for how *unremarkable* its causes were.

On November 24, 2023, the Municipal Water Authority of Aliquippa (Pennsylvania) had one of its water-pressure control devices manipulated by "Cyber Av3ngers," an Iranian Revolutionary Guard Corps-affiliated group; the compromised device was a Unitronics Vision-series PLC, Internet-exposed and protected by factory-default credentials [1][2]. CISA's advisory AA23-335A

(December 2023, updated December 2024) documented the same campaign exploiting Unitronics PLCs across multiple sectors and prescribed the elementary mitigations that would have prevented it: remove OT devices from the public Internet, change default credentials, and segment control networks [2]. In May 2024, the EPA's enforcement alert reported that over 70% of inspected community water systems did not fully comply with Safe Drinking Water Act Section 1433 risk-assessment requirements, and tied basic cyber hygiene — default passwords, asset inventory, incident-response plans, backups — to inspection and enforcement [3]. In December 2024, legislation was introduced to double federal grant funding for water-authority cybersecurity — a congressional acknowledgment that the sector's resource constraints are the binding constraint [4].

The pattern across the record is consistent and humbling: the incidents did not require zero-days, custom malware, or supply-chain craft. They required an Internet connection, a default password, and a flat network. And the *reason* impacts stayed bounded — water kept flowing — was largely analog: operators with the training and the authority to run processes manually. That last observation is this paper's organizing claim: **OT resilience is engineered degradation tolerance**, and the discipline that formalizes it is the IEC 62443 series applied honestly to resource-constrained environments [5].

1.1 Research questions

RQ1: What does the verified 2023-2025 water-sector record establish about OT attack mechanisms and government response? **RQ2:** How do compromises travel from IT into OT, and which architectural properties determine the outcome? **RQ3:** Which control classes cover which OT risk classes under IEC 62443-aligned engineering? **RQ4:** What is the priority order for resource-constrained utilities?

1.2 Contributions

(1) The verified incident-and-response record (Section 2, Figure 1, Table 1) (RQ1). (2) The IT-to-OT attack-path analysis on the Purdue hierarchy (Section 3, Figure 2) (RQ2). (3) The risk-versus-control coverage assessment (Section 4, Figure 3, Table 3) (RQ3). (4) The priority order for constrained operators (Section 5) (RQ4).

2. The 2023-2025 Record (RQ1)

Figure 1 and Table 1 present the sequence. Its signature is the gap it exposes between government knowledge and sector capacity. By December 2023, CISA had documented the exact attack mechanism (default credentials on Internet-exposed Unitronics PLCs) and the exact mitigations [2]; by May 2024, the EPA could report that the large majority of inspected systems still did not meet statutory risk-assessment requirements [3]. The record's lesson is therefore not about attacker sophistication — it is about the translation latency between known mitigations and resource-constrained deployment. Every element of the Aliquippa incident was preventable with controls that cost hundreds of dollars; the sector's problem is that hundreds of dollars compete with chlorine and pumps in a municipal budget.

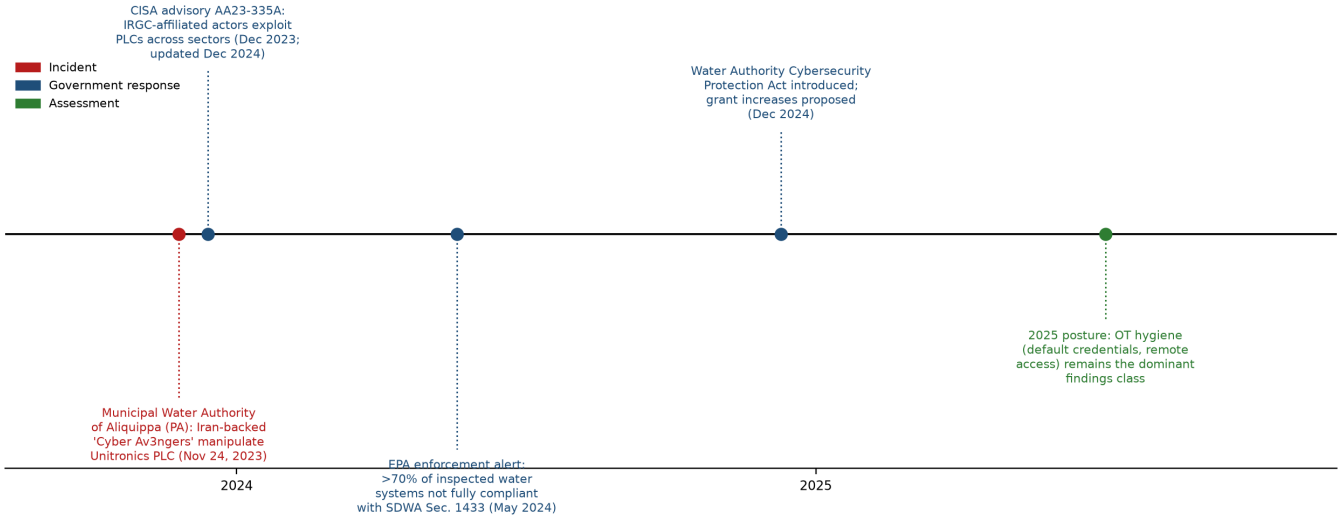

Figure 1. The water-sector OT incident-and-response record, 2023-2025 [1][2][3][4].

Event	Date	Class	Documented content	Source

Municipal Water Authority of Aliquippa (PA) compromise	Nov 24, 2023	Incident	Iran-affiliated "Cyber Av3ngers" manipulated a Unitronics Vision-series PLC (water-pressure system); Internet-exposed device, default credentials; system run manually afterward	[1][2]
CISA advisory AA23-335A	Dec 2023 (updated Dec 2024)	Government response	IRGC-affiliated actors exploiting Unitronics PLCs across water and other sectors; mitigations: remove OT from Internet, change defaults, segment	[2]
EPA enforcement alert	May 20, 2024	Government response	>70% of inspected community water systems not fully compliant with SDWA Sec. 1433; basic-hygiene checklist tied to inspections and enforcement	[3]
Water Authority Cybersecurity Protection Act introduced	Dec 2024	Government response	Proposed doubling of federal grant/technical-assistance funding for water-authority cybersecurity	[4]
2025 sector posture	2025	Assessment	Default credentials, remote-access exposure and segmentation gaps remain the dominant findings class for small utilities	[2][3]

Table 1. The water-sector OT incident and response record, 2023-2025 [1][2][3][4].

3. The IT-to-OT Attack Path (RQ2)

Figure 2 frames the mechanism on the Purdue hierarchy — the reference architecture that separates enterprise IT (levels 4-5), site operations (level 3), and the control network (levels 1-2) [9]. The 2023-2025 campaigns, and the broader OT record behind them, travel the same path: a foothold in enterprise IT (phished credentials, exposed remote access), lateral movement across networks that were flattened for operational convenience, and arrival at control devices that were never designed to be Internet-facing. IEC 62443's answer is architectural: ***zones and conduits*** *— partition the estate by criticality and trust, and force every crossing through a controlled conduit with an explicit policy [5]. Where that segmentation exists, an IT-side intrusion is an IT incident; where it does not, it is a potential process incident. NIST SP 800-82r3 harmonizes this guidance for U.S. operators [6], NIS2 imports accountability for essential-entity OT into EU law [7][8], and the European threat landscape records sustained OT targeting as a standing trend [10].*

Two properties differentiate OT security from IT security and shape every control decision. First, **availability beats confidentiality** in the impact hierarchy: the Aliquippa device was manipulated, not exfiltrated — the threat is process manipulation. Second, **patchability is not assumed**: legacy control devices may never receive vendor patches, which is why compensating controls (isolation, monitoring, manual fallback) are primary rather than supplementary. Table 2 summarizes the IT-versus-OT properties that drive the control differences.

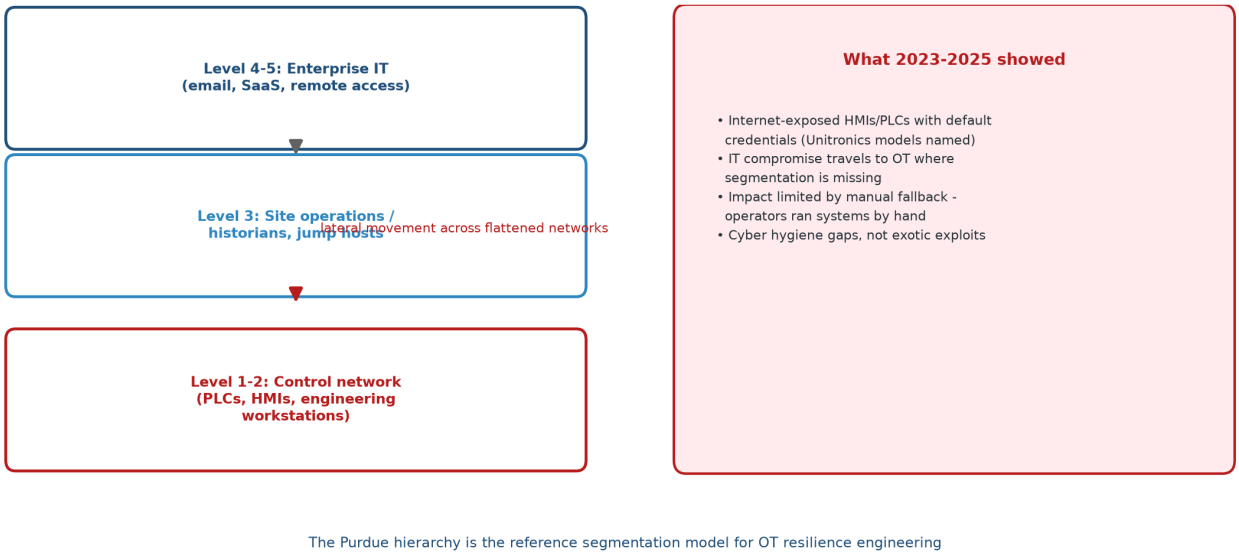

Figure 2. The IT-to-OT attack path on the Purdue hierarchy, and what the 2023-2025 record showed [1][2][9].

Property	Enterprise IT	Operational technology
Impact hierarchy	Confidentiality first	Availability and safety first

Patchability	Assumed (continuous patching)	Not assumed: legacy devices may never receive patches
Acceptable downtime	Minutes-hours (business tolerance)	Process-dependent; safety and continuity constraints
Device lifetime	3-5 year refresh	10-30 year service life
Primary architecture	Zero trust / identity-centric	IEC 62443 zones & conduits; Purdue segmentation
Fallback	Redundant systems; DR sites	Manual operation by trained operators - a first-class control
Threat objective	Data exfiltration, ransom	Process manipulation, disruption, safety impact

Table 2. IT-versus-OT security properties relevant to resilience engineering [5][6].

4. Risk and Control Coverage (RQ3)

Figure 3 and Table 3 assess six OT risk classes against six control classes. Four findings. ***Segmentation is the spine:*** *IEC 62443 zones-and-conduits score strong against the two structural risks (exposed devices, flat networks) and enable every other control.* ***Credential hygiene at the OT boundary*** *scores strong against the 2023-2025 record's actual mechanism — the incidents happened at exactly this control.* ***Manual-fallback drills*** *are the record's under-appreciated control: Aliquippa's impact stayed bounded because operators could run processes by hand; a utility that has never rehearsed manual operation does not have that capability, whatever its firewalls say.* ***Workforce and mutual aid*** *(R6) score weak against most risks but are the sector's deepest constraint — the realistic ceiling on every other control in a small utility.*

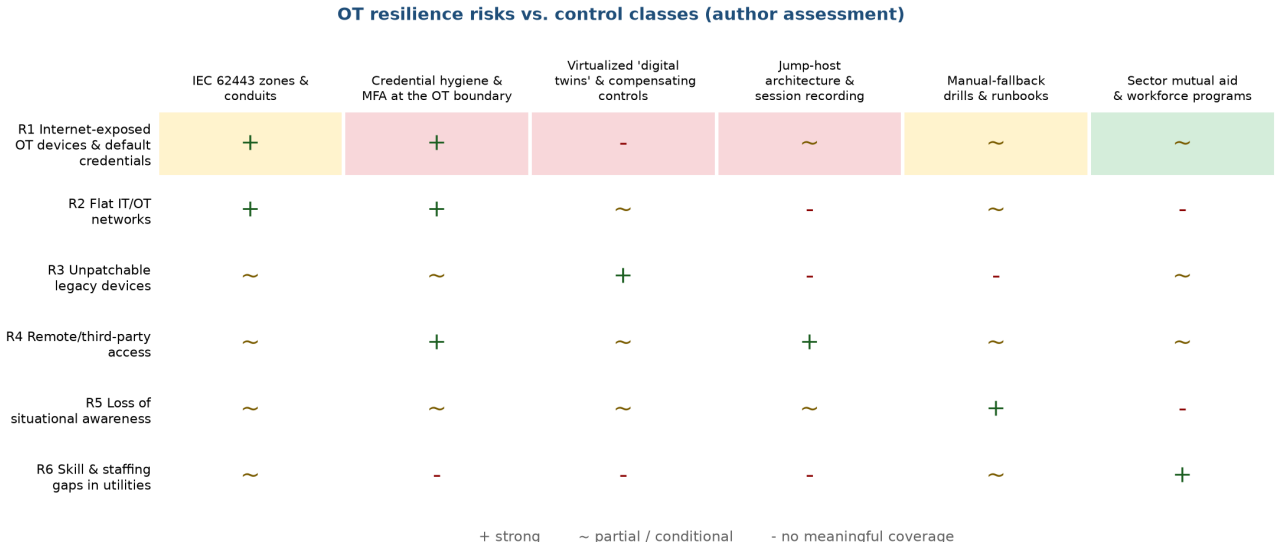

Figure 3. OT resilience risks versus control classes (author assessment; register in Table 3).

Risk class	Description	Strongest control class	Coverage note
R1 Internet-exposed OT devices & default credentials	The documented 2023 mechanism (Unitronics PLCs)	IEC 62443 zones & conduits; credential hygiene	Strong: cheap, fast, addresses the actual mechanism
R2 Flat IT/OT networks	Lateral movement from enterprise IT to control networks	IEC 62443 zones & conduits	Strong: the architectural spine
R3 Unpatchable legacy devices	Devices that will never receive vendor patches	Compensating controls: isolation, monitoring, virtual "digital twins"	Partial: engineering around permanence
R4 Remote / third-party access	Vendor and contractor paths into the control network	Jump-host architecture & session recording	Partial: necessary access must be brokered, not banned
R5 Loss of situational awareness	Operators cannot see manipulations in time	Manual-fallback drills & runbooks	Partial: detection helps but the fallback is the control
R6 Skill & staffing gaps	Small utilities cannot staff a security program	Sector mutual aid & workforce programs	Weak-to-partial: the sector's binding constraint

Table 3. OT resilience risks mapped to IEC 62443-aligned controls (author assessment) [5][6].

5. The Priority Order for Constrained Operators (RQ4)

For a small water utility or industrial site, the 2023-2025 record converts to a short list. (1) **Take OT devices off the Internet** — a CISA-level hygiene item that is cheap, fast, and addresses the documented 2023 mechanism [2]. (2) **Change every default credential** and put MFA on any remote-access path that must exist. (3) **Segment**: even a partial zones-and-conduits implementation that separates the control network from the business network converts most IT incidents into non-events. (4) **Rehearse manual operation** — the fallback that bounded Aliquippa's impact — and write the runbook. (5) **Inventory the estate** so that the EPA's Section 1433 obligation is met and the unknown devices stop being unknown [3]. Threat-intelligence feeds, AI-based anomaly detection, and zero-trust OT architectures are all valuable; none of them substitutes for the first three items, and a sector whose constraint is budget and staffing should buy resilience in the order the incidents taught.

6. Limitations and Threats to Validity

Construct validity. The six risk and six control classes are an analytical simplification of a large standards corpus (IEC 62443 spans multiple parts and roles); real deployments require the full series [5]. **Internal validity.** The record is water-sector-centered because water is where the public record is richest; manufacturing and energy OT will share mechanisms but differ in constraints. Attribution of the Aliquippa incident follows U.S. government advisories. **External validity.** Findings generalize to small/medium OT operators; large integrated operators with mature programs face different residual risks. **Temporal scope.** Frozen at 2025; the sector's regulatory trajectory (and the threat actor's adaptation to it) is out of scope.

7. Conclusion

The 2023-2025 water-sector record is the OT security conversation stripped to its essentials: adversaries exploited default credentials on Internet-exposed control devices; government documented the mechanism precisely; and the sector's capacity to act lagged the knowledge by years. The engineering answer is not exotic — it is IEC 62443 applied with realism about constrained budgets: segment the control network, kill default credentials and Internet exposure, rehearse running the plant by hand, and inventory what exists. Resilience for operational technology is ultimately the discipline of *planned degradation* — accepting that some devices cannot be patched, some networks cannot be perfected, and some incidents will happen, and engineering so that when they do, the water still flows.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRediT contribution statement. Cristina Alcaraz: conceptualization, incident-record analysis, writing – original draft. Yanxia Sun: validation, smart-grid perspective, writing – review & editing. (Corresponding author: Cristina Alcaraz.)

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated; all incident claims trace to the cited government advisories and enforcement documents [1][2][3][4].

Ethics and dual-use. The paper analyzes publicly documented incidents and contains no attack tooling or vulnerability detail beyond the published advisories.

AI assistance declaration. AI-based tools were used in a limited supporting capacity (literature search, figure preparation, and language editing); all research content, analysis, and conclusions were produced, reviewed, and verified by the authors, who take full responsibility for the work.

References

[1] WaterISAC, "Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa," Nov. 30, 2023. [Online]. Available: https://www.waterisac.org/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal

[2] Cybersecurity and Infrastructure Security Agency, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities" (AA23-335A), Dec. 1, 2023, updated Dec. 18, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[3] U.S. Environmental Protection Agency, "Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities," May 20, 2024. [Online]. Available: https://www.epa.gov/enforcement/enforcement-alert-drinking-water-systems-address-cybersecurity-vulnerabilities

[4] C. Deluzio, "Deluzio Introduces Bill to Help Local Water Authorities Strengthen Cybersecurity Efforts," Dec. 13, 2024. [Online]. Available: https://deluzio.house.gov/media/press-releases/deluzio-introduces-bill-help-local-water-authorities-strengthen-cybersecurity

[5] IEC 62443 series, Security for industrial automation and control systems. International Electrotechnical Commission, multiple parts and editions.

[6] NIST, "Guide to Operational Technology (OT) Security," NIST SP 800-82 Rev. 3, Apr. 2023. doi: 10.6028/NIST.SP.800-82r3.

[7] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333, Dec. 2022.

[8] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[9] T. J. Williams, "The Purdue enterprise reference architecture," Computers in Industry, vol. 24, no. 2-3, pp. 141-158, 1994. doi: 10.1016/0166-3615(94)90017-5.

[10] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," Oct. 2024. [Online]. Available: https://www.enisa.europa.eu