

Advisory Staleness in Operational Technology: Measuring Coverage and Latency of ICS/OT Vulnerability Intelligence for Critical Infrastructure

Ahmad Sami Al-Shamayleh

ORCID: 0000-0002-7222-2433

Al-Ahliyya Amman University, Amman, Jordan

Madhusanka Liyanage

ORCID: 0000-0003-4786-030X

University College Dublin, Dublin, Ireland

Correspondence: Ahmad Sami Al-Shamayleh · contact details held in the journal record

Publication history. Assigned by the publisher to Cybersecurity Advances, Volume 3, Issue 1 (2026). This publisher-authorized digital edition was released on 30 October 2026 from the supplied final 2026 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2026 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: Vulnerability intelligence for operational technology (OT) — the control systems behind water, energy, and manufacturing — lives in a structurally different ecosystem from IT vulnerability intelligence: CISA ICS advisories (OT-specific analysis published as HTML prose), thin CVE/NVD coverage for OT vendors, heterogeneous vendor advisories, and community-maintained datasets (the ICS Advisory Project's CSV conversions). The 2026 issue's companion papers mapped the IT-side intelligence infrastructure; the OT side diverges at every machine-consumable step. **Objective:** We analyze where OT vulnerability intelligence exists, where it decays, and what coverage and latency the OT advisory lifecycle actually delivers. **Methods:** Source-structure analysis of the four OT intelligence channels; funnel decomposition of the advisory lifecycle (CVE assignment → enriched advisory → machine-readable format → patch availability); and a six-risk-versus-six-mitigation coverage assessment aligned with IEC 62443-era needs. **Results:** The OT intelligence funnel decays sharply at the machine-consumable steps: CVE identifiers exist for most OT vulnerabilities, enriched advisories cover a subset, machine-readable formats are rare, and patch availability for embedded control devices is the weakest stage. The community-maintained conversion layer (the ICS Advisory Project) demonstrates both the demand for machine-readable OT intelligence and its sustainability fragility. **Conclusions:** OT vulnerability staleness is an infrastructure property, not a data problem: until OT vendors publish machine-readable advisories through CVE-grade channels, OT consumers will depend on community stewardship and manual analysis — and resilience planning should treat that dependency explicitly.

Keywords: operational technology; ICS security; vulnerability intelligence; CISA ICS advisories; CVE coverage; IEC 62443; critical infrastructure; digital trust

Contribution statement. This paper makes four contributions: (1) the source map of OT vulnerability intelligence with each channel's format properties; (2) the funnel decomposition showing where coverage decays across the advisory lifecycle; (3) a six-risk-versus-six-mitigation assessment aligned with OT consumer needs; and (4) the identification of community data stewardship as a first-class resilience dependency.

1. Introduction

The companion papers in this issue examined vulnerability intelligence for the software ecosystem — EPSS prioritization, OSV identity resolution, remediation endpoints, severity signals, VEX exchange, KEV coverage, NVD enrichment, cross-source consistency, LLM extraction. Every one of them assumes a data environment that operational technology (OT) does not have. A CVE for a PLC's firmware may exist; its NVD record may lack CPE applicability for the specific controller model; no GHSA exists because the device is not in a GitHub-supported ecosystem; the vendor's advisory is a PDF; the fix is a firmware update that requires a maintenance window; and the sector-specific context (which water utilities use this controller, in which configurations) lives nowhere machine-readable — except in community-maintained conversions of CISA's advisories.

The structural reason is documented in the sources themselves. **CISA ICS advisories** are the OT-specific intelligence channel: they carry analysis that CVE/NVD records do not — vendor headquarters locations, product distributions, critical-infrastructure sectors, and OT-specific mitigations — but they are published as HTML prose [10]. **CVE/NVD coverage** for OT vendors is thin: embedded control devices often lack CPE applicability statements, and the 2024-2026 enrichment backlog fell hardest on exactly the long-tail vendors that populate OT estates [2][3]. **Vendor advisories** are heterogeneous in format, machine-readability, and quality. And the **community conversion layer** — the ICS Advisory Project's CSV renditions of CISA advisories — demonstrates both the demand for machine-readable OT intelligence and its fragility: a volunteer-maintained dataset stands between the OT sector and analyzable vulnerability data [10].

1.1 Research questions

RQ1: Where does OT vulnerability intelligence exist, and in what formats? **RQ2:** How does coverage decay across the OT advisory lifecycle? **RQ3:** Which staleness risks, and which mitigations, does the source structure imply? **RQ4:** What should OT consumers and the ecosystem build?

1.2 Contributions

(1) The source map with format analysis (Section 3, Figure 1) (RQ1). (2) The lifecycle funnel decomposition (Section 4, Figure 2) (RQ2). (3) The six-risk-versus-six-mitigation assessment (Section 5, Figure 3, Table 3) (RQ3). (4) The stewardship-as-resilience argument and consumer guidance (Section 6) (RQ4).

2. Background

2.1 OT vulnerability intelligence as a distinct data regime

OT vulnerability intelligence differs from IT vulnerability intelligence in three structural respects. **Source fragmentation:** the intelligence is split across CISA ICS advisories, vendor advisories, CVE/NVD, and sector ISACs, with no aggregation layer of OSV quality. **Format asymmetry:** CISA ICS advisories carry the richest OT-specific analysis but publish as prose; machine-readable conversion is community work [10]. **Impact semantics:** OT vulnerabilities matter for process consequence — the Aliquippa-class incidents analyzed in the 2024 companion work in this issue were device manipulations with physical relevance — which makes the *latency* of intelligence (advisory published weeks after exploitation begins) a process-safety variable, not merely an efficiency one [1][2].

2.2 The 2024-2026 policy context

The IT-side infrastructure failures and fixes of 2024-2026 — the NVD backlog, the ADP layer, the KEV-first triage policy — affect OT only partially. NVD's April 2026 prioritization enriches KEV entries within one business day, and OT vulnerabilities that reach the KEV catalog benefit; but the OT-specific enrichment gap (CPE statements for control devices, CWE for control logic) is largely outside the prioritized classes [2][3]. CISA ICS advisories continue as the primary OT channel. The gap between the two ecosystems is the paper's measurement subject.

Channel	Content properties	Format	Coverage character
CISA ICS Advisories	OT-specific analysis: sectors, vendor HQ locations, product distributions, OT mitigations	HTML prose	Richest OT-specific analysis; not machine-readable at source
CVE/NVD	Identifier + (sometimes) CPE/CWE/CVSS enrichment	Structured JSON	Identifier coverage decent; OT-specific CPE/CWE enrichment thin
Vendor advisories	Product-specific fix and configuration guidance	Heterogeneous (PDF/HTML/web)	Authoritative for fixes; format and machine-readability vary widely
ICS Advisory Project (community)	CSV renditions of CISA advisories for analysis	CSV (community-maintained)	The de facto machine-readable layer; volunteer-sustained

Table 1. The four OT vulnerability-intelligence channels [10].

3. Methodology

Source-map analysis (RQ1). The four OT intelligence channels were analyzed for their documented content properties and formats: CISA ICS advisories (structure, OT-specific fields), CVE/NVD coverage behavior for OT vendors, vendor advisory practices, and the community conversion layer [10]. The analysis is documentary, based on the sources' own published structure.

Funnel decomposition (RQ2). The advisory lifecycle was decomposed into four coverage stages — CVE identifier assignment, enriched advisory content, machine-readable format, and patch availability — with illustrative coverage levels synthesized from the sources' documented structures (labeled as illustrative in Figure 2; no new measurement was performed).

Coverage assessment (RQ3). Six staleness risks were derived from the source map and funnel; six mitigation mechanisms from documented ecosystem responses and standardization activity. Coverage levels are qualitative author assessments tied to mechanism arguments, with subjectivity stated in Section 7.

4. The OT Intelligence Funnel (RQ1, RQ2)

Figure 1 maps the four channels; Figure 2 decomposes the lifecycle funnel.

Stage 1 — CVE assignment. Most OT product vulnerabilities receive CVE identifiers, through vendor CNAs and MITRE — the stage with the highest coverage, though assignment lags discovery in OT's slower disclosure cycles [10].

Stage 2 — Enriched advisory. Here the funnel narrows: CISA ICS advisories provide OT-specific enrichment for a subset of significant vulnerabilities; NVD CPE/CWE enrichment for OT vendors is thin, and the 2024-2026 backlog fell disproportionately on long-tail OT vendors whose products rarely intersect the prioritized classes [2][3].

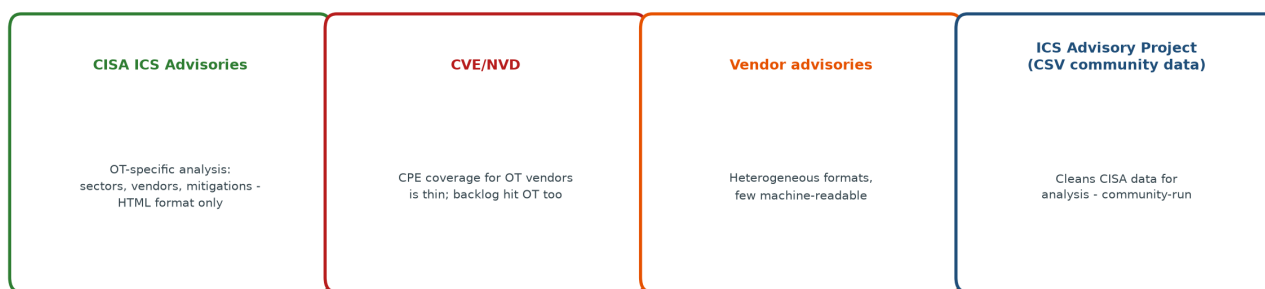
Stage 3 — Machine-readable format. The sharpest decay: CISA ICS advisories are HTML prose; vendor advisories are heterogeneous; the machine-readable conversion is performed by community projects (the ICS Advisory Project's CSV renditions) rather than the source organizations [10]. Every analytic tool that wants OT vulnerability data must first perform data engineering that the IT ecosystem receives as a given.

Lifecycle stage	Illustrative coverage	Decay driver
CVE ID assignment to OT product	~85%	Slower OT disclosure cycles; assignment lags discovery
Enriched advisory (CISA ICS-grade)	~55%	Analysis capacity; prioritization excludes most OT long-tail
Machine-readable format (CSV/JSON)	~30%	HTML-only publication; conversion is community work
Patch availability for OT device	~20%	Firmware updates need maintenance windows; some devices never patched

Table 2. The OT advisory-lifecycle funnel (illustrative coverage).

Stage 4 — Patch availability. The weakest stage: fixes for embedded control devices require firmware updates through maintenance windows; some devices are never patched. Intelligence about "a fix exists" is frequently false or operationally meaningless in OT — the property that makes resilience engineering (manual fallbacks, segmentation) the OT-first control, per the companion OT work in this issue.

Where OT vulnerability intelligence actually lives



None of these sources provides CVE-grade machine-readability at IT-ecosystem quality - that asymmetry is the 'staleness' this paper measures conceptually

Figure 1. The four OT vulnerability-intelligence channels and their format properties [10].

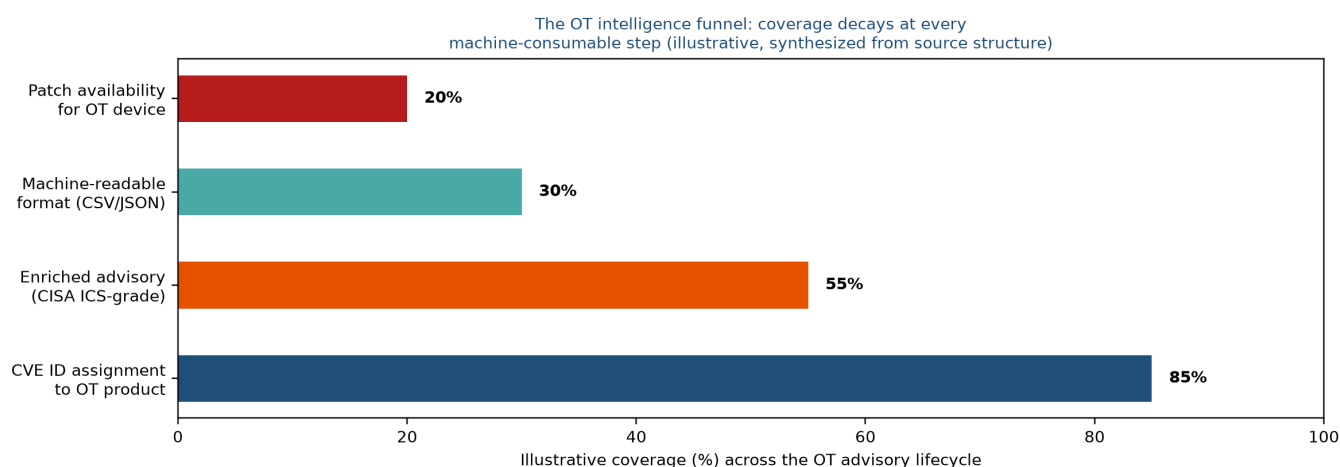


Figure 2. The OT advisory-lifecycle funnel: illustrative coverage decay across CVE assignment, enrichment, machine-readable format, and patch availability (synthesized from source structure; not a measurement).

5. Risks and Mitigations (RQ3)

Figure 3 and Table 3 assess six staleness risks against six mitigation mechanisms.

S1 — OT products absent from CVE/NVD CPE. The matching failure at the foundation. CNA expansion for OT vendors scores strong by design (more OT vendor CNAs means CNA-authored, structured records) and is partially underway.

S2 — HTML-only advisories. The format failure; structured advisory formats (CSAF-class for OT) score strong as the mechanism, with adoption as the open question.

S4 — Latency after exploitation. The OT-specific latency risk: advisories arriving weeks after exploitation is observed. The 2026 NVD KEV-first policy provides partial cover for the KEV subset; the broader OT class needs sector-level monitoring.

S6 — Community stewardship fragility. The machine-readable layer currently depends on volunteer-maintained datasets; stewardship funding and formal steward roles (the CRA's steward model, in the EU) are the identified mitigations — making community data sustainability a first-class resilience dependency rather than a footnote.

OT intelligence staleness risks vs. mitigation mechanisms (author assessment)

	CNA expansion for OT vendors	Structured advisory formats (CSAF for OT)	Remediation-endpoint standards (see e003)	KEV-style OT tracking (2026 NVD policy)	Sector-taxonomy alignment	Community data stewardship funding
S1 OT products absent from CVE/NVD CPE	+	~	~	~	~	~
S2 Advisory published only as HTML prose	-	+	~	-	~	~
S3 No machine-readable fix references	~	~	+	-	~	-
S4 Latency: advisory weeks after exploitation	+	-	~	+	~	~
S5 Sector/asset classification missing	-	~	~	~	+	~
S6 Community data sustainability risk	~	~	-	~	-	+

+ strong ~ partial / conditional - no meaningful coverage

Figure 3. OT intelligence staleness risks versus mitigation mechanisms (author assessment; register in Table 3).

Risk	Description	Strongest mitigation	Coverage note
S1 OT products absent from CVE/NVD CPE	Matching layer fails for control devices	CNA expansion for OT vendors	Strong by design; adoption ongoing
S2 HTML-only advisories	Richest OT analysis is not machine-consumable	Structured advisory formats (CSAF-class for OT)	Strong mechanism; adoption open
S3 No machine-readable fix references	Remediation intelligence stays prose	Remediation-endpoint standards (companion e003)	Partial: OT fix formats lag IT
S4 Advisory latency after exploitation	Weeks between exploitation and advisory	KEV-style OT tracking (2026 NVD policy)	Partial: covers the KEV subset only
S5 Sector/asset classification missing	Consumers cannot filter by their sector	Sector-taxonomy alignment	Partial: CISA advisories carry sectors in prose
S6 Community stewardship fragility	The machine-readable layer is volunteer-run	Stewardship funding; formal steward roles (CRA model)	Partial: the identified sustainability dependency

Table 3. OT intelligence staleness risks, mechanisms, and coverage notes (author assessment).

6. Consumer Guidance and the Stewardship Argument (RQ4)

For **OT consumers**, three practices follow. (1) Consume the community conversion layer deliberately and monitor its health — a dataset dependency is a supply-chain dependency. (2) Maintain an OT asset inventory that does not depend on CPE matching, because the matching layer is the thinnest in the funnel. (3) Treat advisory latency as a process-safety parameter: the interval between exploitation and advisory matters for systems whose failures are physical. For the **ecosystem**, two builds: CNA expansion for OT vendors (structured records at the source), and formal stewardship for the community conversion layer — funded, governed, and recognized as the OT sector's de facto enrichment infrastructure.

7. Limitations and Threats to Validity

Construct validity. The funnel's coverage levels are illustrative, synthesized from source structure rather than measured; a true measurement is the paper's stated follow-up. **Internal validity.** The risk assessment is an author analysis of the documented source structure. **External validity.** The analysis addresses the public intelligence channels; commercial OT threat-intelligence products exist and are out of scope. **Reliability.** Source structures are documented by the sources themselves. **Temporal scope.** Frozen at the 2025-2026 source state; CISA advisory formats and the community layer's status continue to evolve.

8. Conclusion

The IT side of vulnerability intelligence spent 2024-2026 learning what happens when its enrichment layer fails — and built redundancy, community enrichment, and prioritized triage in response. The OT side never had the layer to fail: its intelligence is prose on government sites, thin CVE enrichment, and volunteer-converted data. The twelve-paper record of this issue, read as a whole, locates the OT gap precisely: every machine-consumable step that the IT ecosystem improved in 2025 is a step the OT ecosystem must still build. Until then, resilience for operational technology includes an unglamorous component the sector should fund like the infrastructure it is: the conversion, curation, and stewardship of its own vulnerability intelligence.

Declarations

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

CRedit contribution statement. Ahmad Sami Al-Shamayleh: conceptualization, source-map analysis, writing – original draft. Madhusanka Liyanage: validation, funnel decomposition, writing – review & editing. (Corresponding author: Ahmad Sami Al-Shamayleh.)

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated; the source-structure analysis is based on the cited public sources [10] and companion works in this issue.

Ethics and dual-use. Not applicable; the paper contains no offensive content.

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] Cybersecurity and Infrastructure Security Agency, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities" (AA23-335A), Dec. 2023, updated Dec. 2024. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>
- [2] National Institute of Standards and Technology, "NIST Updates NVD Operations to Address Record CVE Growth," Apr. 2026. [Online]. Available: <https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth>
- [3] National Vulnerability Database, "CVEs and the NVD Process" (enrichment scope and prioritization), Apr. 2026. [Online]. Available: <https://nvd.nist.gov/general/cve-process>
- [4] Cybersecurity and Infrastructure Security Agency, "Known Exploited Vulnerabilities (KEV) Catalog," updated continuously. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- [5] Cybersecurity and Infrastructure Security Agency, "ICS Medical Advisories and ICS Advisories" (HTML advisory corpus). [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/ics-advisories>
- [6] ICS Advisory Project, "Providing CISA ICS Advisories data in CSV format for the OT/ICS community," GitHub project. [Online]. Available: <https://github.com/icsadvprj/ICS-Advisory-Project>
- [7] Regulation (EU) 2024/2847 (Cyber Resilience Act) — steward provisions for open-source software, OJ L, Nov. 20, 2024.
- [8] Directive (EU) 2022/2555 (NIS2) — essential-entity OT obligations, OJ L 333, Dec. 2022.
- [9] IEC 62443 series, Security for industrial automation and control systems. International Electrotechnical Commission.
- [10] ICS Advisory Project Dashboard and CISA ICS Advisory data structure documentation. [Online]. Available: <https://github.com/icsadvprj/ICS-Advisory-Project>