OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

OT-ISAC TLP:CLEAR *– Recipients may share* ***TLP:CLEAR*** *information without restriction, subject to standard copyright controls. This advisory is prepared for public release and is based on publicly available reporting and defensive analytical assessment.*

OT-ISAC ENERGY SECTOR THREAT ADVISORY

In the spirit of community-driven effort, OT-ISAC encourages members and partners to share information that enables the community to improve defensive awareness and situational understanding. OT-ISAC members and partners requiring direct assistance may submit requests through the OT-ISAC Member Portal. Public readers should coordinate through their internal security, incident response, or sector coordination channels as appropriate.

Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

Issue Date	24 April 2026
Prepared By	OT-ISAC Threat Intelligence, with analytical support from Protos AI
Audience	Public awareness / APAC critical infrastructure stakeholders / OT-ISAC Members
Reviewed Source(s)	CERT Polska, FBI/CISA/NSA/EPA/DOE/CNMF AA26-097A, CISA SSVC, FIRST TLP 2.0, Dragos, CISA ICS advisories, vendor/security advisories
Assessment Window	1 November 2025 - 24 April 2026

Executive Summary

Between November 2025 and April 2026, public reporting on the energy sector reflected a mixed threat picture involving direct OT disruption, OT-adjacent compromise, enterprise-to-operations disruption, and exposure of distributed energy assets. The most operationally significant public developments were the 29 December 2025 destructive attacks against Polish renewable and combined heat and power environments, the April 2026 U.S. joint advisory on Iranian-affiliated exploitation of internet-facing PLCs, and continued reporting on OT-focused threat activity, engineering workstation exposure, industrial ransomware risk, and energy-sector vulnerabilities.

For APAC energy operators, the primary takeaway is that public cyber risk signals are increasingly relevant beyond central control rooms and high-value generation assets. Remote renewable sites, RTUs, PLCs, protection relays, engineering workstations, vendor remote access, BESS/DER platforms, EVSE/OCPP backends, backup systems, virtualization infrastructure, and OT-adjacent identity systems can create operationally meaningful exposure. APAC relevance is based on shared vendor ecosystems, similar remote-site architectures, rapid electrification and renewable expansion, and portable adversary tradecraft rather than confirmed public reporting of destructive OT incidents in APAC during this period.

At-a-Glance

Attribute	Assessed Value
Risk Level	High sector-wide exposure; Medium-High near-term APAC relevance where internet-exposed OT, remote renewable sites, DER/BESS platforms, EVSE/OCPP services, or weak vendor access paths exist.
Confidence	Medium-High overall. High for global public reporting on Poland, AA26-097A, CISA SSVC, and selected CISA/vendor vulnerability advisories; Medium for APAC-specific realized impact due to limited public victim reporting.
Key Finding	Public reporting during the period shows credible operational risk from exposed OT devices, distributed energy environments, OT-adjacent engineering systems, and enterprise-to-operations dependencies. APAC relevance is strongest where similar technologies and operating models are present.
Primary Action	Validate and reduce public-facing OT exposure; harden remote access and vendor pathways; prioritize vulnerabilities based on exposure and mission impact; prepare for loss-of-view/loss-of-control and enterprise-to-operations disruption scenarios.

Key Judgments

Judgment	Confidence	Threat to OT/ICS	OT-ISAC assessment
Exposed OT assets remain the highest-priority risk class for energy operators.	High	High	Public reporting shows internet-facing PLCs and OT devices can enable direct interaction with operational systems.
Distributed renewable and grid-edge environments require stronger security governance.	High	Medium-High	The Poland incident shows remote renewable sites and grid-connection infrastructure can be operationally relevant targets.
Ransomware and enterprise compromise remain relevant even without confirmed OT compromise.	Medium-High	Medium	Business systems may support dispatch, logistics, maintenance, billing, restoration, and communications.
APAC-specific destructive OT impact was not confirmed in reviewed public sources.	Medium	Medium	Regional relevance remains credible through shared exposure patterns and technology overlap.

Threat Landscape Overview

The reporting period showed escalation in operational relevance rather than a uniform rise in publicly confirmed OT compromise. The most important public developments involved exposed field-connected systems, distributed renewable environments, industrial communications, engineering workstations, and OT-adjacent business dependencies.

The Poland case is the strongest public example of direct OT-relevant disruption in the timeframe. CERT Polska reported coordinated destructive activity on 29 December 2025 affecting wind and photovoltaic farms and a combined heat and power plant. The attacks damaged RTUs and local operator interfaces, disrupted communication between renewable sites and the distribution system operator, and used destructive methods including firmware damage, file deletion, and wiper malware. Electricity production and heat supply reportedly continued.

The April 2026 U.S. joint advisory is the strongest public example of exposed PLC risk. It reported Iranian-affiliated exploitation of internet-facing OT devices, including Rockwell Automation/Allen-Bradley PLCs, leading to disruptions through malicious interaction with project files and manipulation of HMI/SCADA display data.

Public Threat Actors and Clusters of Interest

Actor / Cluster	Activity During Timeframe or Public Reporting Period	Energy-Sector Relevance	APAC Relevance	Confidence
Static Tundra / Berserk Bear / Ghost Blizzard / Dragonfly overlap	CERT Polska assessed infrastructure overlap with these public cluster names in relation to the Poland incident. Attribution should be treated as public-source overlap, not definitive legal attribution.	Relevant due to destructive activity affecting renewable and CHP environments.	High relevance where APAC operators use similar remote-site, grid-connection, and DSO/TSO communication models.	Medium-High
Iranian-affiliated OT actors / CyberAv3ngers-aligned public reporting	April 2026 public advisory reported Iranian-affiliated exploitation of internet-facing OT devices, including PLCs.	Directly relevant where energy operators maintain exposed PLCs, HMIs, SCADA systems, or OT remote access paths.	High relevance for APAC operators with internet-facing OT or weakly governed remote access.	High
VOLTZITE / Volt Typhoon-overlapping public reporting	Dragos 2026 reporting described OT-relevant prepositioning and engineering workstation activity.	Relevant to electric, pipeline, and OT engineering environments where configuration and alarm data can support process understanding.	Moderate to high relevance due to strategic interest in regional critical infrastructure; public APAC victim specificity remains limited.	Medium-High
AZURITE	Dragos reported AZURITE activity involving engineering workstations and operational data collection, including reporting across Asia-Pacific exposure.	Operational data collection can support future disruption planning and process understanding.	High relevance as an APAC watchpoint, but organization-level victim details are limited publicly.	Medium-High
Ransomware groups and access brokers	Industrial ransomware activity continued to affect energy and industrial organizations through enterprise, virtualization, backup, and IT-layer dependencies.	Relevant where ransomware affects systems required for logistics, recovery, dispatch support, or maintenance coordination.	High relevance due to global portability of criminal tradecraft and common IT/OT dependencies.	High

Public Incidents of Note

Date	Organization / Country	Sector	Incident Type	Operational Impact	Attribution / Caveat	Why It Matters	APAC Relevance
29 Dec 2025	Renewable farms and CHP plant / Poland	Energy	Destructive cyberattack affecting IT and industrial devices	RTU and local interface damage; renewable-site communication disruption; no reported halt to electricity production or heat delivery.	Public-source cluster-overlap assessment; attribution remains caveated.	Strong example of operational risk to distributed energy and heat-generation environments.	Strong relevance through technology and remote-site operating-model overlap.
Dec 2025	PDVSA / Venezuela	Oil and gas	Cyberattack affecting centralized administrative systems	Reuters reported cargo delivery disruption and later resumption; direct OT compromise not publicly confirmed.	Attribution claim is politically contested and should be treated cautiously.	Highlights logistics and administrative-system dependency in energy operations.	Relevant to APAC oil, gas, LNG, port, and logistics-heavy operators.
Jan 2026	Endesa / Spain	Electricity retail / energy services	Customer data breach	Customer data exposure; no public evidence of OT disruption.	Unknown / not publicly confirmed.	Relevant to energy retail trust, fraud, and phishing follow-on exposure.	Moderate relevance for APAC utilities with customer-service portals and digital retail platforms.
Feb 2026	Conpet / Romania	Oil pipeline	Cyberattack / ransomware claim	Corporate IT disruption; company stated SCADA, telecommunications, and oil transport operations were unaffected.	Qilin claim reported; public attribution should remain caveated.	Shows operationally relevant business disruption without confirmed OT compromise.	Relevant to pipeline and energy logistics operators with enterprise/OT dependencies.
Apr 2026	Multiple U.S. critical infrastructure organizations	Energy and other CI sectors	Exploitation of internet-facing OT devices	Public advisory reported PLC disruptions and HMI/SCADA display manipulation, resulting in operational disruption and financial loss.	Iranian-affiliated actors per joint advisory.	Direct public evidence of exposed OT device exploitation.	High relevance where APAC organizations maintain exposed OT assets or weak remote access controls.

Vulnerabilities and Exposure Themes

Theme	Affected environment	Public context	Why It Matters
Exposed PLC / HMI / SCADA paths	Rockwell Automation / Allen-Bradley PLCs and comparable OT devices	April 2026 public advisory reported exploitation of internet-facing OT devices with operational disruption.	Exposed OT devices can provide a direct path to operational systems if reachable from untrusted networks.
RTU and industrial communications availability	RTUs, IEC-104 environments, grid-connection sites	RTU availability and communications loss can affect telemetry, supervision, and restoration coordination.	Loss of RTU communications can degrade visibility, supervision, dispatch coordination, and restoration decisions.
Protection relay exposure	Protection relays and management interfaces	Public Schneider advisory reporting highlights relay-management security relevance; impact depends on exposure and segmentation.	Relay-management exposure may support reconnaissance or unauthorized access to protection-related assets if poorly segmented.
Engineering workstation software	Relay and configuration tooling such as Enervista UR Setup	OT-adjacent risk; concern increases where engineering systems are weakly isolated.	Engineering software issues can create OT-adjacent pivot opportunities on workstations used for configuration and firmware workflows.
EVSE / OCPP backend weaknesses	Charging platforms and backend communications	Relevant to energy and transport electrification, availability, and trust in load/charging workflows.	Backend weaknesses can affect charging availability, data integrity, and electrification-dependent operations.

SSVC-Informed Prioritization

The priority labels below use SSVC terminology as OT-ISAC analytical guidance for public awareness. They are not official CISA SSVC determinations. Operators should adjust priority based on local exposure, segmentation, asset criticality, compensating controls, and operational dependency.

Exposure / Theme	SSVC-informed priority	Rationale
Internet-exposed PLC / HMI / SCADA paths	Act	Public reporting shows exposed OT assets remain actively targeted and may create operational disruption risk.
RTU and protection relay vulnerabilities	Attend / Act where mission-critical	Priority depends on exposure, segmentation, and whether the asset supports critical visibility, control, or protection functions.
Engineering workstation software issues	Track* / Attend	Higher concern where engineering systems are weakly isolated or used for sensitive configuration or firmware workflows.
EVSE / OCPP backend weaknesses	Attend	Relevant to charging availability, fleet operations, and energy/transport electrification dependencies.
DER / BESS / renewable-site exposure	Attend / Act where exposed	Distributed energy assets may depend on remote monitoring, third-party access, and centralized operational visibility.

TTPs and Intrusion Trends

TTP / Trend	MITRE Mapping Where Supported	Energy-Sector Relevance	Defensive Value
Internet-facing OT discovery and exploitation	Enterprise: Exploit Public-Facing Application; ICS: Internet Accessible Device, where applicable	Relevant to exposed PLCs, HMIs, RTUs, gateways, and remote management interfaces.	Maintain an accurate public-exposure inventory and remove direct internet access to OT devices.
Credential abuse and weak remote access governance	Enterprise: Valid Accounts; ICS: Valid Accounts, where applicable	Relevant to vendor support, remote sites, and shared or weakly controlled accounts.	Use MFA, named accounts, session controls, and periodic access review.
Manipulation of operator-facing views	ICS: Manipulation of View, where supported by advisory reporting	Reported in public PLC exploitation advisory and relevant to operator trust in HMI/SCADA displays.	Monitor for unauthorized configuration or display changes and validate operator view against field state.
Engineering workstation targeting and operational data collection	Enterprise: Collection; ICS: Engineering Workstation Compromise, where applicable	Relevant where attackers collect configuration files, alarm data, network diagrams, or process knowledge.	Harden engineering workstations and limit uncontrolled file transfer, internet access, and removable media use.
Destructive activity against distributed energy assets	ICS impact mapping may include Loss of View, Loss of Control, or Denial of Control depending on event details	Poland reporting demonstrates destructive effects against RTUs and local interfaces at renewable grid-connection points.	Rehearse loss-of-view, loss-of-control, and communication-loss scenarios for remote sites.
Ransomware with operational spillover	Enterprise: Data Encrypted for Impact; Exfiltration, where applicable	Business-system disruption can affect logistics, recovery, customer service, and operational coordination.	Validate backups, recovery plans, and business-system dependencies required for safe operations.

APAC Context and Sector Implications

APAC energy members should treat the global public developments in this report as relevant because the underlying exposure patterns are common across the region. Many APAC operators are expanding renewable generation, EV charging, BESS, DER orchestration, remote monitoring, and vendor-managed support for geographically distributed assets. These operating models create exposure classes similar to those observed in global reporting: remote-site connectivity, RTUs and relays at grid-connection points, third-party access, cloud or centralized management dependencies, and limited local visibility during communication loss.

The April 2026 PLC exploitation advisory is also relevant to APAC even though the advisory focused on U.S. critical infrastructure. Scanning for exposed OT services, interacting with PLC project files, and manipulating operator-facing views are portable behaviors once devices are reachable. APAC organizations should therefore use the advisory as a public reminder to validate whether any OT devices, engineering workstations, serial gateways, RTUs, or management interfaces are internet-accessible or weakly governed.

Ransomware cases should be interpreted as enterprise-to-operations warnings rather than automatic evidence of OT compromise. For APAC oil, gas, pipeline, LNG, utility, and energy retail organizations, the operational question is whether corporate IT, identity, logistics, billing, cargo, scheduling, maintenance, or restoration systems are required to sustain safe and reliable operations during a cyber incident.

No publicly confirmed destructive OT incident in APAC was identified in the reviewed open-source material for the reporting window. This reduces confidence in realized regional impact but does not reduce the need to address exposure, tradecraft portability, and operational dependency risks.

Analytical Assessment

OT-ISAC assesses that the energy sector faced a mixed threat environment during the reporting period: direct OT risk for exposed PLCs, RTUs, HMIs, and renewable-site assets; OT-adjacent risk through engineering workstations, relay software, remote support, and EVSE/OCPP platforms; and enterprise spillover risk through ransomware, data theft, logistics disruption, and recovery dependencies.

The most important near-term concern for APAC energy stakeholders is the convergence of grid-edge expansion, persistent remote access, and uneven OT visibility. Distributed renewable sites, BESS/DER platforms, EVSE backends, and remote substations may not receive the same security attention as central generation or transmission environments, yet they can materially affect operational visibility, dispatch coordination, customer impact, and restoration activity.

From an SSVC-informed perspective, public vulnerability prioritization should focus on the intersection of exploitation evidence, exposure, and mission relevance. Internet-facing OT devices, RTUs, protection relays, engineering workstations, DER/BESS platforms, EVSE/OCPP services, and remote renewable-site connectivity should be prioritized where compromise could affect operational view, remote control, restoration, or safety-relevant decision-making.

***Confidence level of threat to OT/ICS environment**: Medium-High globally; Medium for APAC-specific realized impact. Confidence is high that exposed OT and OT-adjacent systems are being targeted globally. Confidence is lower on public APAC victimization because detailed regional incident reporting remains limited.*

Recommended Actions for Energy-Sector Stakeholders

#	Recommendation	Public-Safe Rationale	Suggested Owner
1	Validate internet-facing OT exposure.	Confirm that PLCs, HMIs, RTUs, engineering workstations, gateways, and OT management interfaces are not directly reachable from the public internet.	OT/ICS operations, network security
2	Prioritize vulnerabilities by exposure and mission role.	Use SSVC-informed thinking to elevate vulnerabilities affecting operational visibility, remote control, protection, restoration, or critical business processes.	OT security, risk, asset owners
3	Harden remote access and vendor pathways.	Use MFA, named accounts, least privilege, session control, allowlisting, and regular vendor access review.	Third-party risk, OT operations
4	Review distributed energy and grid-edge assets.	Inventory renewable sites, DER/BESS platforms, EVSE/OCPP services, RTUs, relays, cellular routers, serial gateways, and centralized management platforms.	Energy operations, engineering
5	Segment and monitor engineering workstations.	Reduce routine internet access, uncontrolled removable media, unmanaged software execution, and broad enterprise connectivity for engineering systems.	OT security, engineering
6	Validate backup and restoration readiness.	Confirm backup integrity, recovery sequencing, offline copies, and recovery time expectations for systems supporting safe operations.	IT/OT recovery, operations
7	Prepare for loss-of-view and loss-of-control scenarios.	Exercise scenarios involving remote-site communication loss, HMI trust degradation, relay or RTU unavailability, and manual fallback.	Operations, incident response
8	Monitor for OT-relevant anomalies.	Monitor for abnormal OT protocol activity, unauthorized configuration changes, unexpected remote access, unusual engineering tool usage, and unexplained telemetry gaps.	SOC, OT monitoring
9	Map enterprise dependencies that support operations.	Identify identity, logistics, customer, dispatch support, billing, cargo, scheduling, and maintenance systems required for operational continuity.	Risk, business continuity
10	Keep APAC relevance evidence-based.	Treat global incidents as operational learning opportunities, but distinguish confirmed local compromise from technology overlap and tradecraft portability.	CTI, leadership

Detection and Hunting Opportunities

- Exposure monitoring: maintain an updated inventory of internet-reachable OT assets, remote access gateways, engineering services, and cloud-managed operational platforms.
- Remote access monitoring: review unusual access times, new geographies, dormant accounts, vendor sessions, and privilege escalation on systems that support OT operations.
- OT integrity monitoring: watch for unauthorized project changes, unexplained HMI display differences, communication loss, device resets, and abnormal engineering-tool activity.
- Recovery monitoring: validate whether backups, virtualization infrastructure, and identity systems can support restoration during ransomware or destructive activity.

What to Watch Next

- Follow-on public reporting on distributed energy, BESS, DER, and EVSE/OCPP targeting as energy transition infrastructure expands.
- Whether exploitation emphasis shifts from visible internet-facing PLCs toward engineering workstations, firmware workflows, relay configuration software, or vendor remote-support pathways.
- Ransomware incidents that are described as IT-only but affect logistics, customer service, restoration, billing, cargo movement, or maintenance coordination.
- Public advisories from major OT vendors affecting energy-relevant RTUs, protection relays, HMIs, gateways, engineering tools, EVSE platforms, and industrial data systems.
- Evidence of APAC-specific exploitation attempts or incidents involving exposed OT services, renewable sites, EVSE platforms, or energy-sector remote access providers.

Analyst Note

Confirmed public reporting supports a credible global pattern of exposed-OT risk, destructive activity affecting Polish renewable and heat-generation environments, and U.S. reporting on exploitation of internet-facing PLCs. Public evidence reviewed for this TLP:CLEAR version does not confirm APAC destructive OT compromise in the assessment window. OT-ISAC therefore assesses APAC risk primarily through exposure similarity, technology overlap, remote-site operating models, and the portability of attacker tradecraft.

The TLP:CLEAR version intentionally removes member-sensitive detail and keeps SSVC at a public-safe prioritization level. Asset owners should tailor prioritization to their own exposure, compensating controls, safety dependencies, and restoration requirements.

Limitations

- This version uses public reporting only and omits member-specific observations, internal collection details, and tactical IOCs.
- Attribution for some activity remains caveated, especially where public reporting relies on infrastructure overlap or third-party clustering.
- Public incident reports often do not disclose enough detail to distinguish corporate IT, OT-adjacent systems, and direct control-system impact with high confidence.
- APAC implications are primarily based on technology overlap, similar operating models, and tradecraft portability; public reporting did not identify a confirmed destructive APAC OT incident in the reviewed period.
- SSVC-informed priorities in this document are analytical guidance and should be adapted to each operator’s asset criticality, exposure, safety case, and maintenance constraints.

Source Reviewed

[1] Energy Sector Incident Report - 29 December 2025 | CERT Polska | 30 Jan 2026 | https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[2] AA26-097A: Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure | FBI / CISA / NSA / EPA / DOE / CNMF | 7 Apr 2026 | https://media.defense.gov/2026/Apr/07/2003907538/-1/-1/0/AA26-097A-IRANIAN-AFFILIATED-CYBER-ACTORS-EXPLOIT-PROGRAMMABLE-LOGIC-CONTROLLERS-ACROSS-US-CRITICAL-INFRASTRUCTURE_508C.PDF

[3] Stakeholder-Specific Vulnerability Categorization (SSVC) | CISA | Accessed Apr 2026 | https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

[4] 2026 OT/ICS Cybersecurity Report / Year in Review public reporting | Dragos | Feb 2026 | https://www.dragos.com/resources/press-release/dragos-2026-year-in-review-new-ot-threats-ransomware

[5] ICSA-26-013-02: Rockwell Automation FactoryTalk DataMosaix Private Cloud / CVE-2025-12807 | CISA / Vulners mirror | 13 Jan 2026 | https://vulners.com/ics/ICSA-26-013-02

[6] Iranian-Affiliated APT Targeting Rockwell / Allen-Bradley PLCs: Internet Exposure Findings | Censys | Apr 2026 | https://censys.com/blog/iranian-affiliated-apt-targeting-rockwell-allen-bradley-plcs/

[7] CVE-2026-27772: EV Energy ev.energy Missing Authentication for Critical Function | CVE / CISA-derived vulnerability record | 27 Feb 2026 | https://db.gcve.eu/vuln/CVE-2026-27772

[8] Romanian oil pipeline operator Conpet discloses cyberattack | Oilfield Technology | 6 Feb 2026 | https://www.oilfieldtechnology.com/digital-oilfield/06022026/romanian-oil-pipeline-operator-conpet-discloses-cyberattack/

[9] Venezuela's PDVSA resuming oil cargo deliveries after cyberattack, sources say | Reuters | 17 Dec 2025 | https://www.reuters.com/business/energy/venezuelas-pdvsa-resuming-oil-cargo-deliveries-after-cyberattack-sources-say-2025-12-17/

[10] Endesa customer data leak public advisory | Government of Catalonia | Jan 2026 | https://web.gencat.cat/en/ciutadania/actualitat/noticies/2026/01/que-fer-si-ets-un-dels-afectats-per-la-filtracio-d-endesa-

[11] CVE-2026-1773: Hitachi Energy RTU500 IEC 60870-5-104 denial-of-service vulnerability | NVD | Feb 2026 | https://nvd.nist.gov/vuln/detail/CVE-2026-1773

[12] Control Systems - Schneider Electric Security Advisory AV26-350 | Canadian Centre for Cyber Security | 14 Apr 2026 | https://www.cyber.gc.ca/en/alerts-advisories/control-systems-schneider-electric-security-advisory-av26-350

[13] Traffic Light Protocol (TLP) Version 2.0 | FIRST | Current standard | https://www.first.org/tlp/

[14] GE Vernova Enervista UR Setup security advisory public reporting | CISA CSAF-derived / ISSSource | Feb 2026 | https://www.isssource.com/ge-vernova-patch-for-enervista-ur-setup/

End of Advisory

Disclaimer

This TLP:CLEAR report is provided for general public awareness and defensive planning. It is based on publicly available information and OT-ISAC analytical assessment at the time of writing. It does not confirm compromise of any organization unless explicitly stated in cited public sources. Organizations should validate applicability against their own asset inventory, architecture, safety case, regulatory obligations, and operational constraints before taking action.