DENEXUS™

SEPTEMBER 2026 | NEWSLETTER

OT CYBER RISK INTELLIGENCE NEWSLETTER

• Quantify • Reduce • Transfer

Thought leadership on controls validation and testing, the practical operating model for OT risk management, and the DeRISK platform for quantifying and reducing cyber risk.

denexus.io

CONTENTS

Thought Leadership

Reduce and Validate: Controls That Move the Loss Curve

01

In OT, the question isn't what scores worst. It's what measurably reduces loss when tested.

Reduce and Validate: Controls That Move the Loss Curve

A control you have not tested is a claim, not a defense; risk reduction begins the moment you validate it and can prove you did.

OT remediation operates within limits that IT teams rarely face. These include uptime windows, safety rules, small teams, and vendor-controlled maintenance schedules. Within those limits, the key question is not "what scores worst?" but "what will reduce loss at this facility?" CVSS was designed for IT, where loss often centers on data and systems. OT has different priorities. Safety, process continuity, reliability, and performance matter more than a vulnerability score. A headline CVE does not reduce risk by itself. The facility-specific control change that follows from it can.

Attested Controls

- Configuration review only
- Self-reported status
- No date stamp
- Assumed effectiveness

Tested Controls

- Traffic test validation
- Access-path verification
- Restore drill with timestamp
- Proven effectiveness

The value of any risk input comes down to action. Does it change what you do at a specific facility? Does it change the likelihood of a scenario you already care about? Does it identify a control gap you can close during this operating cycle? If not, the input may be interesting, but it is not useful. Strong programs connect analysis to action. They translate OT-specific threats and techniques into facility-level control changes, then rank those changes by expected risk reduction within real operating limits. That approach builds credibility with boards and markets.

Validation is part of the most important controls. DeNexus asked senior OT practitioners which controls do the most work. Their top six were practical. They included defensible architecture; secure perimeter and external access; and secured, immutable backups. They also included OT-specific logging and incident response; hardened shared infrastructure supporting OT; and IT/OT dependency resilience. The backup control requires restoration testing. It must be done at least once a year. The IT-OT dependency control requires tests of OT isolation (like CI Fortify [13]). It also requires tests of manual operations. So two of the six require testing by definition. A backup you have never restored is an assumption. The same is true of an isolation plan you have never exercised.

Top 6 Controls

Defensible Architecture	Secure Perimeter	Secured Backups*
Hardened Infrastructure	IT/OT Resilience*	Logging & IR/DR

14 control areas identified; top 6 shown. **Two require validation by definition (*)**

That makes validation specific. A compensating control without a valid test result is still an assertion. Add a documented test (date, method, result) and a set schedule for retesting, and the control becomes risk reduction you can defend. Confirm segmentation with real traffic tests, not only a configuration review. Validate access paths against the live environment. Prove restoration through a drill with a recorded recovery time, not an assumed window. Tested controls are governance assets. Attested controls without evidence are paperwork. The gap between what was documented and what was tested is also where claims disputes can arise.

> **"A compensating control without a validated test result is an assertion. With documented results and a refresh cadence, it is risk reduction with an audit trail."**
>
> DeNexus — OT Cyber Risk Intelligence, September 2026

This creates a simple loop: analyze, act, measure, and update. Measuring a control shows whether it reduced risk as expected. Remediation can then move beyond generic patching toward a specific loss outcome. Organizations that build this discipline before the next renewal cycle can bring tested evidence to the discussion. Those that rely on attestation alone cannot offer the same proof.

See the top 6 controls for industrial environments

Based on DeNexus research with 8+ OT experts, 15+ years experience

View Report

Next Month: Benchmarks and Executive Reporting

Comparability across facilities, sectors, and regions. How to build defensible metrics that CFOs and boards can understand and act upon.

Industry News

OT Cyber Attacks, Regulation & Security Guidance

Water-sector PLC attacks, UK power resilience, policy developments, and OT security guidance

OT CYBER ATTACKS & INCIDENTS

U.S. water-sector PLC attacks show real OT aggregation risk, be careful as new facts arrive daily

Minnesota IT Services said a coordinated cyberattack targeted operational technology at more than 30 community water systems on July 26–27, triggering a statewide response with state, federal, local, Tribal, and private-sector partners [1]. The Minnesota Department of Health was not aware of any active requests for residents to modify drinking-water usage, and ISSSource's coverage made the same practical point: manual fallback and local response appear to have limited the immediate public-health impact, even though the risk was real [1], [2]. FBI and EPA then warned that water and wastewater utilities in at least seven states had reported incidents since July 27 involving internet-facing Rockwell Automation / Allen-Bradley MicroLogix 1100 and 1400 PLCs, with attackers changing IP addresses and passwords, causing loss of monitoring and control, and in some cases degrading operations through pressure loss or flooding [3]. Forescout's follow-up analysis found 4,407 internet-facing Rockwell/Allen-Bradley controllers exposing EtherNet/IP on port 44818, including 22 hosts in cities targeted in the campaign, but also stressed there was no confirmation that a CVE was exploited in the campaign [4].

30+	4,407	7+	22+
Water Systems Targeted	Exposed Controllers	States Affected	Hosts in Targeted Cities

Reported UK power-plant shutdown highlights the small-operator gap in energy cyber resilience.

Media reports said an Iran-linked cyberattack shut down an unnamed small UK power generator for about four days in July, while the UK government confirmed only that the incident affected a small-scale energy generator and that there was no risk to the wider energy system [5], [6].

The plant has not been publicly identified, the UK government has not formally attributed the incident, and no official NCSC technical advisory was located in the public sources reviewed [6], [7]. The significance is therefore not grid-scale disruption, but distributed-energy exposure: smaller generators can be locally important, increasingly connected, and less resourced than major transmission or generation assets, while still facing state-linked or state-aligned threats [7].

For operators and insurers, this is another reminder that aggregation risk can sit in many small sites, not only in large, heavily regulated plants.

REGULATION & POLICY DEVELOPMENTS

Project Watershed 250 pairs public policy with practical water-sector cyber support.

Texas Governor Greg Abbott and White House National Cyber Director Sean Cairncross launched Project Watershed 250 on August 31, describing it as a joint effort to connect Texas water and wastewater utilities with cyber-defense resources at no cost [8]. The Texas Governor's Office said the program pairs federal and private-sector capabilities with state and local expertise, with a particular focus on closing the resource gap for rural providers.

Reporting from Nextgov and CyberScoop described it as a six-month pilot using private-sector cybersecurity and AI tools to identify and fix weaknesses, with companies including Microsoft, Dragos, Forescout, Palo Alto Networks, Google Cloud, AWS, Fortinet, Cloudflare, Zscaler, Parsons, Abnormal AI, and Reflection AI named among participants [9], [10]. The value for this newsletter is the timing: after a wave of PLC-focused water incidents, at least one region is moving from advisories toward resourced remediation for small utilities.

The U.S. bulk-power emergency order gives DOE a broader supply-chain and OT-risk intervention tool.

The White House executive order of August 26 declared a national emergency around foreign-produced bulk-power system electric equipment, citing risks from foreign actors creating or exploiting vulnerabilities in equipment that supports national defence, emergency services, critical infrastructure, and the economy [11].

The order covers transactions involving foreign-produced bulk-power system equipment, associated critical components, software, firmware, digital services, maintenance services, and remote-access capability where DOE determines there is undue or unacceptable risk. Importantly, the order is not framed as immediate wholesale replacement:

DOE is directed to issue implementing rules within 120 days, identify risky equipment, and consider reliability, safety, replacement availability, continuity of essential service, and phased compliance before directing isolation, disconnection, replacement, or removal [11], [12].

For OT risk owners, the practical implication is likely to be inventory, provenance review, monitoring, mitigation planning, and selective replacement for high-risk grid equipment rather than a simple buy/ban checklist.

OT SECURITY GUIDANCE

CI Fortify turns OT isolation into a tested resilience capability, not a paper control.

The CI Fortify guidance, led by Australia's ASD with international partners, explains how critical-infrastructure organizations can isolate vital OT and enabling systems from other networks during cyber incidents or periods of increased threat [13]. The guidance tells operators to identify the minimum systems required to deliver the critical service, map interconnections, identify isolation points, and develop and test plans to isolate OT and enabling systems during incidents. It also makes clear that isolation must be operationally planned: cutting connections can trigger manual processes, interrupt system-to-system communication, and affect upstream dependencies, peer utilities, vendors, and dispatch or scheduling partners. For risk engineers and insurers, CI Fortify provides a useful test of recoverability: can the operator keep delivering the critical service while disconnected, and has that been rehearsed before the incident?

CERT Polska's private-APN analysis shows that "not public internet" does not always mean isolated.

CERT Polska's August follow-up report on the December 2025 Polish energy-sector attacks disclosed a second, smaller CHP plant incident supplying heat to around 50,000 residents [14]. The attack shut down a steam turbine and the water-treatment system used to produce process water, interrupting cogeneration, but operators limited the event to a short-term outage and heat supplies to consumers were not disrupted. CERT Polska said, to the best of its knowledge, this was the first observed real-world cyberattack in which attackers gained access to an OT network through a private APN, made possible by a configuration that allowed arbitrary devices inside the private APN network to communicate with one another. The lesson is directly relevant to distributed energy, water, substations, renewables, and remote industrial sites: private cellular connectivity, APNs, routers, and field gateways need the same architecture review, segmentation discipline, logging, and recovery planning as any other path into OT.

WORKS CITED

[1] Minnesota IT Services. "MNIT Activates Statewide Cybersecurity Response to Support Affected Communities and Protect Critical Infrastructure." State of Minnesota, 28 July 2026, https://mn.gov/mnit/media/blog/?id=38-761869

[2] Hale, Gregory. "Water Security Worked, but 'Risk Is Real.'" ISSSource, 29 July 2026, https://www.isssource.com/water-security-worked-but-risk-is-real/

[3] Federal Bureau of Investigation and Environmental Protection Agency. "Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions." FBI, 30 July 2026, https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-internet--facing-programmable-logic-controllers-causing-operational-disruptions

[4] Molige, Sai, and Forescout Research – Vedere Labs. "OT Security Analysis: Exposed Devices Attacked in US Water Systems." Forescout, 5 Aug. 2026, https://www.forescout.com/blog/ot-security-analysis-exposed-devices-attacked-in-us-water-systems/

[5] Quinn, Ben. "Iran-Linked Hackers Blamed for Cyber-Attack That Shut Down UK Power Plant." The Guardian, 23 Aug. 2026, https://www.theguardian.com/world/2026/aug/23/iran-linked-hackers-blamed-cyber-attack-british-power-plant

[6] "Iran-Linked Hackers Shut Down a UK Power Plant for Four Days." The Next Web, 24 Aug. 2026, https://thenextweb.com/news/uk-power-plant-cyber-attack-iran-linked-hackers

[7] Ambrose, Jillian. "UK's Small Power Plants Face Higher Cyber Risk into 2030s despite Iran-Linked Hack." The Guardian, 27 Aug. 2026, https://www.theguardian.com/business/2026/aug/27/uk-small-power-plants-risk-cyber-attacks-iran-hack

[8] Office of the Texas Governor. "Governor Abbott, National Cyber Director Launch Project Watershed 250 to Defend Texas Water Supply." Office of the Texas Governor, 31 Aug. 2026, https://gov.texas.gov/news/post/governor-abbott-national-cyber-director-launch-project-watershed-250-to-defend-texas-water-supply

[9] DiMolfetta, David. "White House Launches Water Cybersecurity Pilot in Texas." Nextgov/FCW, 31 Aug. 2026, https://www.nextgov.com/cybersecurity/2026/08/white-house-launches-water-cybersecurity-pilot-texas/415725

[10] Starks, Tim. "'Watershed 250' Test Program in Texas Looks to Private Sector for Water Cybersecurity Help." CyberScoop, 31 Aug. 2026, https://cyberscoop.com/watershed-250-texas-water-cybersecurity-pilot

[11] The White House. "Declaring a National Emergency to Secure the United States Bulk-Power System." The White House, Executive Order 14420, 26 Aug. 2026, https://www.whitehouse.gov/presidential-actions/2026/08/declaring-a-national-emergency-to-secure-the-united-states-bulk-power-system/

[12] The White House. "Fact Sheet: President Donald J. Trump Declares a National Emergency to Secure America's Bulk-Power System." The White House, 26 Aug. 2026, https://www.whitehouse.gov/fact-sheets/2026/08/fact-sheet-president-donald-j-trump-declares-a-national-emergency-to-secure-americas-bulk-power-system

[13] Australian Signals Directorate's Australian Cyber Security Centre. "CI Fortify – Advice for Isolating Vital Systems." Cyber.gov.au, 28 July 2026, https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/ci-fortify/ci-fortify-advice-for-isolating-vital-systems

[14] CERT Polska. "Follow-Up Report of the December 2025 Energy Sector Incident." CERT Polska, 8 Aug. 2026, https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025

DeNexus Events

03

Events, Webinars & Research Reports

Upcoming events, live webinars, and new research reports on OT cyber risk quantification and management.

Upcoming Events

Fortinet OT Day | Cybersecurity for OT and Critical Infrastructure

José María Seara,
Founder & CEO, DeNexus

Date: Wednesday, September 23, 2026

Time: 11:00 AM – 12:00 PM EDT

Register today →

Donovan Tindill has been accepted to speak on the S4x27 Main Stage

Date: Feb 2027

Stay tuned for details when the agenda is released from S4 organizers next month.

Industrial Control Systems (ICS) Cybersecurity Conference

Donovan Tindill, CISSP, GICSP
Sr Director of OT Cybersecurity at DeNexus

From Dwell Time to Dollars: Quantifying the Financial Value of Faster OT Incident Recovery
Tuesday, October 6, 2026 | 2:20 PM - 2:50 PM

The Cyber-Physical Balance Sheet: Managing OT Cyber Risk, Insurance, and Resilience
Thursday, October 8, 2026 | 12:00 PM - 12:30 PM

Register today →

Upcoming Webinars

DeRISK CRQ & QVM — Building a Multi-Year OT Cyber Risk Management Program

A working session on standing up a multi-year OT cyber risk program — from baseline exposure to board-level reporting.

Kevin Hamman (DeNexus) & Scott Hooper (Clearway) | September 16, 2026 | 11am EST [45mins]

Register today →

DeRISK UWA — Underwriting OT Cyber Risk, End to End

Augment your underwriting team with OT cyber specialist capability — without hiring one.

Kevin Hamman (DeNexus), George Mawdsley (DeNexus), Jack Chamberlain (Chaucer)

September 23, 2026 | 11am EST [45mins]

Register today →

The DeNexus Learning Hub is live.

One place for the foundational material on OT cyber risk in financial terms: the OT Cyber Risk Knowledge Center, practitioner-level articles and guides across quantification, controls, and risk transfer, direct answers to the questions boards and CISOs ask most often, and reference tools for operationalizing a risk program. Whether you're building the business case internally or briefing a risk committee, it's designed to be the starting point.

Explore The Learning Hub →

Research Reports — Live & In the Works

Available for download

The Impact of the Iran War on Industrial Cyber Risk — Download PDF →

Manufacturing Sector Cyber Incidents — H1 2026 — Download PDF →

The US AI Data Center Industrial Complex — Download PDF →

A Framework for Infrastructure Lenders — Download PDF →

Not yet published

Edge Models & Industrial Cyber Risk — In progress

The DeRISK Platform — Quantify and Reduce

DeRISK Platform Overview

One simulation core for two critical functions: Quantify and Reduce

The DeRISK Platform covers two of the three moves in the model — **Quantify** and **Reduce** — through CRQ and QVM, built on one simulation core. One quantifies risk in dollars; together they tell you which work removes the most of it.

DeRISK CRQ
Cyber Risk Quantification

DeRISK QVM
Quantified Vulnerability Management

DeRISK UWA Agentic
Agentic Underwriting

DeRISK CRQ — Quantify

Cyber Risk Quantification translates OT exposure into Expected Annual Loss and Value at Risk, then simulates which controls and projects reduce that loss the most per dollar spent — at the facility and across the portfolio. It gives CISOs, CFOs, and boards a defensible financial view of risk instead of a red-amber-green dashboard, and reframes the cyber conversation as a capital allocation conversation.

- Translates OT exposure into financial loss
- Simulates control effectiveness
- Portfolio-level analysis

DeRISK QVM — Reduce

Quantified Vulnerability Management ranks every CVE by expected loss reduction, not by CVSS score. CVEs are matched to your asset inventory and network context, cross-referenced against active NVD and CISA advisories, mapped to MITRE ATT&CK for Enterprise and ICS through a patent-pending AI pipeline, and run through a simulation-twin of your network that computes the financial loss each vulnerability contributes. The result surfaces the 1–2% of vulnerabilities that drive roughly 90% of real risk — and lets you simulate remediation before committing an outage window.

- Ranks by expected loss reduction
- Cross-references NVD advisories
- Simulates remediation before outage

Ready to see the DeRISK Platform in action?

Schedule a demo with our team to see how DeRISK can transform your OT cybersecurity strategy.

Book a Demo →

DeRISK UWA Agentic — Transfer

AI-native underwriting platform for the cyber insurance market

DeRISK UWA Agentic completes the Quantify – Reduce – Transfer model. Our AI-native underwriting platform for the cyber insurance market — underwriters, MGAs, and Lloyd's syndicates writing industrial and OT risk — launched in May, entering early-adopter deployment with Chaucer Group as the named reference.

Underwriting OT exposure has always been hard — limited evidence, inconsistent submissions, and not enough specialist capacity to assess every risk in depth. DeRISK UWA Agentic closes that gap. Its agentic workflow moves from submission ingestion to actuarial output in minutes — expected loss, maximum foreseeable loss, full loss exceedance curves, premium indication, and a structured insurance program — with every finding traceable to its source document, pipeline step, and model version.

Agentic Workflow

Moves from submission ingestion to actuarial output in minutes: expected loss, maximum foreseeable loss, full loss exceedance curves, premium indication, and a structured insurance program.

Traceability

Every finding traceable to its source document, pipeline step, and model version. Evidence that cannot be traced cannot be audited.

Augment your underwriting team — without hiring.

Learn More →