Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/scoping-ot-security-testing-around-operational-risk/

OPERATIONAL TECHNOLOGY

Scoping SCADA and OT Security Testing Around Physical Safety and Zero Operational Downtime

A control network assessment built for plants and vessels measures real exposure on terms the plant engineers set. Scope the work with the engineers who own the process so every step has a safety boundary. Call (800) 868-8189 at any hour.

Published September 3, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Why OT Testing Follows Different Rules Than IT Testing

In power generation, water and wastewater utilities, chemical manufacturing, energy pipelines and maritime vessel operations, operational reliability and physical human safety always take precedence over traditional IT testing practices. That is why OT testing reserves automated vulnerability scanners for the IT zones and reads thirty year old programmable logic controllers, remote terminal units and real time Modbus network segments passively, protecting the fragile network stacks and human machine interfaces that keep the plant running. Plant managers and chief engineers rightly guard their live control loops, and a method built around that authority is what lets operational technology environments be tested with confidence.

A Safety First Methodology Built With Plant Engineers in Full Control

Global Digital Forensics bridges the gap between corporate cybersecurity governance and plant floor engineering authority. We scope every SCADA, ICS and maritime OT assessment around strict physical safety boundaries. In higher Purdue Model zones, such as corporate IT networks, enterprise jump hosts, firewall DMZs and vendor remote access gateways, our engineers perform controlled, manual attack path validation to see if an intruder can cross into the industrial zone. Once inside the lower industrial control levels, we switch strictly to passive network telemetry analysis via switch SPAN ports, offline configuration audits and maintenance window staging inspections, delivering security visibility through methods planned around live operations.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Rules of Engagement the Plant Signs Before Testing Begins

Every OT assessment we run starts with a written rules of engagement document that the plant manager, the control engineer and the corporate security lead sign together, and it is more detailed than the equivalent for an IT test. It classifies each asset by operational criticality and names the ones that stay with passive observation, beginning with safety instrumented systems, turbine and generator controls, chemical dosing and anything whose failure has a physical consequence. It defines the maintenance windows in which any active work may occur, the exact techniques permitted in each Purdue level, the stop conditions that halt the test and the person on the plant floor who holds the authority to call that halt on their own judgment. It also records the rollback plan for every configuration we may touch.

The document protects the client in two ways. During the engagement it keeps every engineer on our team inside what the plant has approved in writing. Afterwards it is the record that shows an insurer, a regulator or a board that the organization tested its control systems with due care for safety and reliability. Operators scoping this kind of work for the first time can draft the first version with our OT audit workbook builder (evestigate.com/tools/ot-workbook-builder/), and the OT assessment planning library holds the sector specific preparation manuals for water, power and manufacturing that feed into the rules of engagement.

Scoping also settles what success looks like before the engagement begins, because a focused OT assessment answers its chosen questions well. For a first assessment the goal is usually an accurate picture of the boundary and the asset population, with controlled testing focused on the paths an enterprise intrusion would take. For a mature program the goal may be validation of specific controls after a segmentation project or evidence for a particular mandate's submission. The rules of engagement record the goal alongside the boundaries, so that when the plant engineer asks why a technique is or is not being used the answer is already written down, and so that the final report can be judged against what it set out to establish rather than against everything an OT assessment could conceivably cover.

The Guidance That Sets the Bar

NIST SP 800-82 Revision 3, the guide to operational technology security, is explicit that OT environments differ from IT in their availability and safety requirements and that assessment methods must account for devices that cannot tolerate scanning or unexpected traffic. It describes architecture, risk management and the application of controls to OT, and it is the reference most auditors reach for when they ask how a test was designed. The ISA/IEC 62443 series supplies the zone and conduit model and the security level targets that let us express findings as a gap between the protection a zone has and the protection its risk requires, which is language plant engineering and corporate security both understand.

Sector mandates add their own requirements. Bulk electric system operators work under the NERC CIP standards, where CIP-010 requires periodic vulnerability assessments and distinguishes active from paper assessments, and where any active testing must respect the electronic security perimeter definitions in CIP-005. Community water systems serving populations above the statutory thresholds must complete risk and resilience assessments and emergency response plans under AWIA Section 2013, and a security assessment of the control network is the technical evidence that assessment rests on. Maritime operators face Coast

© 2026 Global Digital Forensics, Inc. All rights reserved.

Guard cybersecurity requirements for vessels and facilities. We map each engagement to the mandate that governs it so the report serves the compliance file as well as the engineering team, and our power and energy, water and wastewater and maritime assessment pages describe the sector detail.

What Passive Evidence Shows and What Active Testing Adds

Passive capture at switch SPAN ports and optical taps shows what is actually talking on the control network: which devices speak Modbus, DNP3, EtherNet/IP or S7, which engineering workstations push project files to controllers, which historians pull from where, and which vendor connections appear at odd hours. Identity responses in some protocols reveal firmware versions without a single packet sent by us. Offline review of firewall exports, switch configurations and PLC project files shows how the network is supposed to behave. These sources are passive, and they establish the baseline against which anything unusual stands out, which is why our method begins there in every lower level zone.

Whether a boundary actually holds is answered by a controlled test. A firewall rule that appears correct in an export may be shadowed by an earlier rule, and a VLAN that looks isolated on paper may be reachable through a dual homed host that speaks only when prompted. A controlled test from the IT side toward the DMZ and, within approved windows, from the DMZ toward the control zone is how the examiner checks whether an intruder could cross. We perform that traversal testing with the plant engineer present and with hosts the plant has designated, away from live controllers, and where the plant maintains a test bed or spare hardware we exercise controller specific techniques there. The report distinguishes what was observed passively, what was tested actively and what is drawn by inference, so the reader knows the weight each finding carries.

The report presents findings by zone and by weight of evidence, and it is written for the control engineer first. Each finding names the asset or conduit, the observation or test that produced it, the standard it bears on, the operational consequence if an attacker used it and a remediation that respects the plant's constraints, which often means a compensating control for a controller whose update waits for its next scheduled replacement. Corporate security receives the same findings mapped to the governing mandate, and the compliance function receives the rules of engagement, the coverage map and the evidence as the record that the assessment was performed with due care. When an incident later raises the question of what the operator knew about its exposure and when, that record is the answer.

Practices That Keep Testing and Production Apart

The practices are well established. Level 1 devices, whose network stacks were designed for a handful of predictable peers, are read passively rather than scanned. Credential testing runs against designated hosts, keeping live HMI operator screens available through every shift. Active work is scheduled away from startup and product changeovers, when engineers need their full attention on the process. Vendor remote access stays in scope whoever owns it, because it is the most common entry path. A control engineer is present for any active technique, as the person who can recognize an anomaly in the process before the alarm does. The rules of engagement write each of these down, which is why that document carries real weight.

Preparation before the first call makes the scoping conversation productive. The plant manager identifies the production calendar and the maintenance windows. The control engineer gathers the network drawings, the asset list as it currently exists, the PLC and HMI vendor and model inventory and the list of remote access

© 2026 Global Digital Forensics, Inc. All rights reserved.

connections with their owners. The network team exports firewall and switch configurations. Corporate security identifies which mandates apply and which prior assessments exist. With those materials, our senior OT engineer can propose a scope in the first conversation that matches the plant's tolerance, and the companion guides on segmentation validation and passive asset discovery describe the two engagements most plants begin with. The OT, ICS and SCADA assessment page describes the full service.

Prepare Your Facility With Our Interactive OT Tools and Checklists

Explore our free interactive OT audit workbook builder (evestigate.com/tools/ot-workbook-builder/), read the OT assessment planning library, or call Global Digital Forensics at (800) 868-8189 to speak with a senior OT security engineer. The initial consultation is free.

Technique Permitted at Each Purdue Level

The guide describes scoping an OT assessment around physical safety, with active techniques confined to higher zones and passive methods below. This table states, level by level, the technique the rules of engagement permit, the evidence it yields and the stop condition that halts it. Read it alongside the signed rules of engagement, because the plant engineer who holds stop authority relies on the same boundaries. Safety instrumented systems and live controllers stay with passive observation throughout.

Techniques permitted by Purdue Model zone, the evidence each yields and its stop condition.

Zone	Permitted technique	Evidence yielded	Stop condition
Enterprise IT, Level 4 and 5	Controlled manual attack path testing	Whether an intruder can reach the DMZ	Production impact or engineer call
DMZ and jump hosts, Level 3.5	Traversal testing toward the control zone	Whether the boundary actually holds	Any effect on a live service
Supervisory, Level 2 and 3	Passive capture and offline config review	Historians, workstations and vendor sessions observed	Passive methods only in this zone
Control, Level 1	Passive telemetry at SPAN ports only	Which devices speak Modbus, DNP3 or S7	The tester listens only
Process and safety, Level 0	Observation and documentation only	Device presence and firmware from identity responses	Reserved for observation and documentation
Vendor remote access path	Controlled test from the vendor entry point	How far the path reaches	Plant engineer present throughout
Spare or test bed hardware	Controller specific techniques exercised safely	Device behavior on equipment separate from production	Confined to the designated equipment

© 2026 Global Digital Forensics, Inc. All rights reserved.

Try the Tool Before You Call

Before the scoping call, open the OT audit workbook builder (evestigate.com/tools/ot-workbook-builder/) with your plant engineer, choose the sector and the systems in play, and customize the planning set so it reflects your Purdue zones, your maintenance windows and the equipment reserved for passive observation. Download the workbook set and read each overview's scope notes with it, because the set documents what you plan to test and what you have set aside, which is what an auditor or insurer will ask for later. Everything runs in your browser. Bring the workbook to the call and the examiner will build the rules of engagement around it rather than around a generic template.

How to Begin and What Happens on the First Call

Before the call, our OT Security Readiness: Inventory, Boundaries and Rules Before Testing sets out the items to secure in the order they expire. Have ready the number and type of sites, the sector and the mandates you believe apply, the current network drawings and asset list in whatever state they exist, the production calendar with upcoming maintenance windows and the list of vendor remote access connections. Our senior OT engineer asks which systems have physical safety consequences, where the IT and OT boundary sits today, what prior assessments exist, what the plant's tolerance for any active testing is and who on the floor will hold stop authority. You then receive a written scope that separates passive, offline and controlled active work by zone, a timing plan built around your windows and a proposal for the assessment and the report your engineers and compliance function will use. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST SP 800-82 Revision 3.

Authorities cited in this guide: NIST SP 800-82 Revision 3, Guide to Operational Technology Security. Establishes that OT assessment methods must account for availability and safety constraints and supplies the architecture and control guidance referenced here, in the final Revision 3 text. ISA/IEC 62443 series of standards. Supplies the zone, conduit and security level model used to express findings, as described on the ISA standards page for the series. NERC CIP standards. Provides the electronic security perimeter and vulnerability assessment requirements that govern testing for bulk electric system operators, in the currently effective standards listed by NERC. EPA, AWIA Section 2013. Describes the risk and resilience assessment and emergency response plan requirements for community water systems, as published on the current EPA water resilience page.

© 2026 Global Digital Forensics, Inc. All rights reserved.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Operational Technology

Can you test our control network without any risk of downtime?

Passive capture, offline configuration review and walkdowns send no test traffic to the process and form the bulk of the work in the control zones. Active testing is confined to the higher zones and the DMZ, within approved windows, against hosts the plant designates and with a control engineer present and holding stop authority. Active techniques stay on designated hosts, away from live controllers and safety systems. The rules of engagement record every one of those boundaries before the engagement starts, and the report notes which findings came from passive observation and which from controlled testing.

How long does an OT security assessment take?

The drivers are the number of sites and zones, the availability of maintenance windows for any active work, how many conduits must be captured passively and for how long to see all operating modes, the completeness of the existing documentation and the depth of compliance mapping required. Passive capture often needs to span a full production cycle to be representative. Multi site programs are usually sequenced so that findings from the first plant refine the scope for the rest.

What does an OT assessment cost and what drives it?

The initial consultation is free. The proposal reflects the number of plants, vessels or substations, the number of network conduits to instrument, whether active boundary testing is in scope, the sector mandates the report must address and the deliverables the engineering team, corporate security and the compliance function each need. Operators who use our planning library and workbook builder to prepare arrive with most of the scoping information in hand, which shortens the engagement.

Do we need to take the plant down for the assessment?

The plant keeps running. Passive work proceeds during normal operation, and active work is scheduled into existing maintenance windows. Where a plant has a test bed or spare controllers, controller specific testing is performed there. If a finding is serious enough that the plant decides to make a change, that change follows the plant's own change control schedule.

Who from our side needs to be involved?

The plant manager or operations lead for the production calendar and risk tolerance, the control or automation engineer for the process knowledge and the asset and drawing inventory, the network or IT lead for configuration exports and SPAN access, the corporate security lead for mandate mapping and reporting, and the vendors or integrators who hold remote access, at least to describe their connections. The control engineer is present for any active work as a fixed part of our method.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Web Addresses for the Sources Cited

1. NIST SP 800-82 Revision 3: https://csrc.nist.gov/pubs/sp/800/82/r3/final
2. ISA/IEC 62443 series: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
3. NERC CIP standards: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
4. AWIA Section 2013: https://www.epa.gov/waterresilience/awia-section-2013

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.