PRACTITIONER RESOURCE

The OT, ICS and SCADA Security Assessment Protocol

Set the operating boundaries, evidence sources, approval steps and safety controls for an OT, ICS or SCADA security review.

Edition 2026-11-03 · Updated November 3, 2026 · miami-computer-forensics.com/guides/ot-assessment-protocol/

Plan to minimize disruption, with explicit operational authority

An OT security assessment is built around the physical process it supports. A device may control treatment, power, movement, pressure, temperature or another condition, and understanding it takes the process engineers as well as the network diagram. Availability and safety constraints affect which evidence can be collected, which questions can be tested and who authorizes the work. Each technique is chosen for the operating control network rather than carried over from the office network.

The plan aims for zero disruption and builds every step around that goal. Passive observation, interviews and configuration review are planned with the same care, because connecting equipment or changing traffic affects operations. The protocol below starts with existing records and moves to active techniques through a separate decision. It is intended for asset owners, operators, engineers, security leaders and authorized assessors working together. [1]

Establish the process boundary before the network boundary

Identify the facility, process, operating states and business functions within scope. Name the operations owner, responsible engineer, safety representative, security lead and assessor. Record who can approve access and who has immediate authority to stop the work. Identify contracted or vendor responsibilities and confirm that the organization has the authority to permit the proposed activity.

Document the conditions that matter to safe operation: critical cycles, maintenance periods, environmental constraints, staffing and dependencies on remote systems. List the systems that stay out of scope. Those conditions come from the people who run the process, not from a list of IP ranges. The first deliverable should explain the operating boundary and the reasons for exclusions in terms the plant and security teams can both verify.

Gather existing evidence before introducing new traffic

Request current network drawings, asset lists, device roles, approved remote access descriptions, relevant change records and available vendor documentation. Compare those sources with the knowledge of people who operate and maintain the process. Record the document dates and known omissions. Use each drawing for orientation and confirm it against the plant and the people who run it.

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

Use existing monitoring and configuration records where they can address the question. Ask how they were collected, which portions of the environment they cover and what their retention limits are. Where a monitoring source is silent, record its coverage so the team knows which questions it speaks to. Keep discrepancies in an open items register so the team can choose a safe way to resolve them.

Prepare an assessment safety and communications plan

Write the planned activity, expected effect, authorized operator, location, timing and prerequisites. Establish the method for communicating with the control room or process owner while work is underway. Define observable stop conditions, such as unexpected communications behavior, alarms, loss of visibility or a process condition that operations considers unacceptable.

Record what the assessor will do after a stop instruction and how operations will confirm that work can resume. Operations makes that decision together with the security team. Include recovery contacts and the records needed to understand a change. Write each rollback for the specific action and the recovery method actually available.

Design passive observation with engineering review

If traffic observation is appropriate, have the authorized network and operations owners approve the collection point and connection method. Confirm how any existing mirror, tap or collection interface is configured and who may change it. Installing or reconfiguring a collection path is itself an operational action, so passive analysis goes through the same review and approval as any other change to the network.

Define the collection period, expected process states, permitted data and secure handling arrangement. Record capture loss, time basis and the visibility each collection point provides. A quiet window may omit startup, failover, maintenance or infrequent vendor activity. Describe what was observed during the actual period rather than presenting a short sample as a complete map of the facility's communications.

Reconcile assets and communication paths from corroborated sources

Build an asset record from corroborated sources. Identify device function, owner, location or zone, relevant version information and the source supporting each entry. Mark identifications that rest on a network signature, and confirm each device's model and role with the responsible engineer. Ask the responsible engineer to resolve meaningful discrepancies before planning a test against a supposed target.

For significant communication paths, identify the business purpose and the people who can approve it. Include engineering workstations, historians, remote services, identity dependencies and connections to enterprise systems. Distinguish observed communication from an allowed path in a configuration, and both from a path the team has successfully tested. Those differences affect the conclusions the assessment can support.

Review access and remote support as operating processes

Map how employees, contractors and vendors reach the environment. Identify approval, authentication, privilege assignment, monitoring and termination responsibilities. Ask operations to explain the maintenance tasks that rely on each route. A proposed access restriction accounts for the work needed to keep the facility safe and available, including the consequence of disconnecting a service.

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

Examine the supporting record: who requested access, who approved it, which identity was used, what privilege was granted and when access was removed. Shared or emergency credentials require an accountable handling process. Record MFA coverage and where it applies. The report identifies each specific control gap or open dependency, and any proposed production change goes through review.

Evaluate configuration and vulnerability information in context

Review relevant settings and supplier advisories using the available device and version information. Verify applicability with the engineering or vendor owner before treating an advisory as a confirmed vulnerability in the facility. An unverified product identification can lead to an incorrect remediation recommendation or an unsafe attempt to reproduce a condition.

When a weakness appears applicable, describe the affected function, known conditions, possible operational consequence and available mitigations. Distinguish evidence reviewed from behavior directly observed. A patch recommendation accounts for support, compatibility, maintenance planning and recovery. Where a patch waits for a maintenance window, operations and security evaluate authorized compensating measures and record the remaining risk.

Require a separate gate for active validation

Any technique that sends assessment traffic, attempts authentication, changes a configuration or tests a control's behavior requires an explicit scope decision. Define the exact target, method, rate, window, operator, stop conditions and recovery prerequisites. Obtain the approvals required by the asset owner and relevant third parties. Approval to review documentation and approval to scan are separate decisions. [2] [3]

Consider a lab, replica, spare device or maintenance environment when it can address the question safely and meaningfully. Document the differences from production. Where the operational constraints favor records and review over active validation, the report states that basis, which keeps the plant safe and the finding accurate.

Preserve an evidence trail that operators can understand

Record the source, operator, collection time, method, handling and any observed effect for each material item. Retain approved plans and significant communications with the resulting evidence. Share sensitive plant diagrams, credentials and raw captures through an agreed secure transfer method, with access restricted according to the owner's requirements.

Keep the original material and an appropriately scoped analysis copy. Where information has been redacted for a wider audience, explain the redaction without losing the reference back to the controlled source. That handling record is what lets anyone explain the finding months later.

Report operationally meaningful findings and practical next steps

Each finding should identify the affected process or asset, supporting evidence, plausible consequence, confidence level, recommended action and responsible owner. Explain whether the issue was observed, inferred from configuration or reported by another party. Record the testing performed and how it supports confidence in the conclusion.

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

Separate quick administrative corrections from engineering changes that require design, procurement or an outage window. Assign priorities with the owner using the business and safety context rather than a tool score alone. If the team accepts or defers a risk, retain the reason, approving authority and review condition. The result is a plan operations can execute, tied to the plant's own systems.

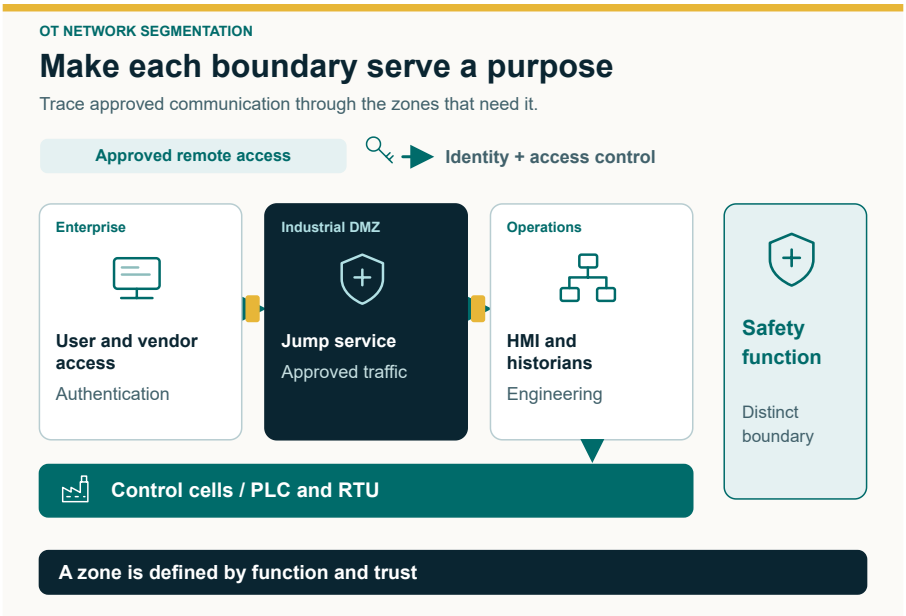
Close the assessment with follow through in place

Confirm that temporary access, collection devices and approved temporary configurations have been addressed according to the plan. Reconcile changes made during the assessment and obtain the owner's confirmation of the resulting state. Identify evidence the owner will retain, remaining open items and the people responsible for them.

Plan retesting around the actual remediation and operational constraints. Record what a successful retest demonstrates and what remains outside scope. Use the assessment to improve the accuracy of drawings, inventories, access procedures and response plans where authorized. This protocol follows NIST SP 800-82 Revision 3 (September 2023), the current final OT security guide; NIST released Revision 4 as an initial public draft on September 21, 2026. [1]

Plan the Assessment With a Senior OT Lead

Bring the process boundary, your current drawings and the people who hold stop authority to a free scoping call with a senior GDF OT security lead. On that first call we agree the operating limits, the evidence to gather first and the approval gates for any active work, and we set out the timeline and the deliverables. Call (786) 219-1210 or the 24/7 hotline at (800) 868-8189, or write to info@evestigate.com. To keep preparing, browse the OT security guide library.



OT zones and the controlled connections between them.

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

Information Gathering Q&A Checklist

Work through these questions with operations, engineering, safety and security together. Mark unknown or not applicable answers plainly, and record an owner, a confirming source and the date for each one.

Keep passwords, remote access details and raw plant diagrams off this record. Note who holds each item and how it will be shared securely once the assessment is scoped.

Which facility, process and operating states are in scope?

Name the site, the process, the operating states the assessment covers and the business functions that depend on them, with the operations owner who confirms the boundary.

Answer:

Owner, source, date and unresolved questions:

Which systems stay out of scope?

List safety systems, fragile controllers and any equipment outside the authorized boundary, with the reason for each exclusion and the person who set it.

Answer:

Owner, source, date and unresolved questions:

Which drawings, asset lists and change records exist, and how current are they?

Record each document, its date, its owner and the known omissions, and who last checked it against the plant.

Answer:

Owner, source, date and unresolved questions:

Which monitoring and configuration records are already collected?

Identify existing network monitoring, historian, firewall and configuration records, the portion of the environment each covers and how long each is retained.

Answer:

Owner, source, date and unresolved questions:

How do employees, contractors and vendors reach the control network?

Map each remote and local access route, who approves it, which identity is used, whether MFA applies and how access is removed when work ends.

Answer:

Owner, source, date and unresolved questions:

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

What are the stop conditions, and how will the team reach the control room?

Record the observable conditions that stop work, the person with stop authority, the communication method during the assessment and who confirms that work can resume.

Answer:

Owner, source, date and unresolved questions:

Which backups and recovery contacts support the systems in scope?

List the configuration and program backups for each system, where they are held, when a restore was last tested and the contact who performs recovery.

Answer:

Owner, source, date and unresolved questions:

Who receives findings, and how will sensitive plant material be shared?

Name the people authorized to receive findings and evidence, the secure transfer method and any redaction the owner requires for a wider audience.

Answer:

Owner, source, date and unresolved questions:

Who owns operations, safety, stop authority and the approved collection point?

Record process conditions and the person who can authorize resumption.

Answer:

Owner, source, date and unresolved questions:

Has any active validation been separately approved for exact targets and methods?

Record the exact targets and methods approved for active validation, the person who approved them and the date.

Answer:

Owner, source, date and unresolved questions:

Primary sources and further reading

Sources checked November 3, 2026.

1: NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security (September 2023)
https://csrc.nist.gov/pubs/sp/800/82/r3/final

2: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (September 2008)
https://csrc.nist.gov/pubs/sp/800/115/final

3: NIST rules of engagement glossary
https://csrc.nist.gov/glossary/term/Rules_of_Engagement

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

Talk to a Senior GDF Security Lead

Bring this checklist to a free scoping call. We review your answers, confirm the systems and operating limits that matter and set out the testing depth, the timeline and the deliverables.

Miami office: (786) 219-1210 · **24/7 hotline:** (800) 868-8189 · **Email:** info@evestigate.com

miami-computer-forensics.com

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