# 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 · Online at newyorkcomputerforensics.com/guides/ot-assessment-protocol/

## Plan to minimize disruption, with explicit operational authority

An OT security assessment works around the physical process it supports. A device may control treatment, power, movement, pressure, temperature or another physical condition, so the assessor reads the network diagram alongside the process narrative and the operators' account. 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 on its own terms.

Passive observation, interviews and configuration review can still create operational risk if equipment is connected incorrectly or a proposed change alters traffic. The protocol below starts with existing records and requires a separate decision before active techniques. It is intended for asset owners, operators, engineers, security leaders and authorized assessors working together. [NIST SP 800-82 Revision 3]

## 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. Include the systems the team will leave untouched. 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. Drawings orient the team, and each one is checked against the current environment.

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. Read each monitoring source against the part of the environment it covers. Keep discrepancies in an open items register so the team can choose a safe way to resolve them.

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

## 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 with the security team. Include recovery contacts and the records needed to understand a change. A rollback description is specific to the proposed action and the available recovery method.

## 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 requiring review.

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. Note which process states the window covered, such as startup, failover, maintenance or infrequent vendor activity. Describe what was observed during the actual period.

## 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 tentative identifications, and ask the responsible engineer to confirm a device's model or role before a test is planned against it.

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. Each proposed access restriction accounts for the work that keeps the facility safe and available.

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 where supported. The report names each specific control gap or open dependency and the reviewed change that addresses it.

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

## 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 must account for support, compatibility, maintenance planning and recovery. Where a patch waits for a maintenance window, operations and security evaluate authorized compensating measures.

## 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. [NIST SP 800-115] [NIST rules of engagement glossary]

Consider a lab, replica, spare device or maintenance environment when it can address the question safely and meaningfully. Document the differences from production. Where active validation sits outside the operating window, the finding states that it rests on records and review.

## 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. Agree on a secure transfer method for plant diagrams, credentials and raw captures, and set access 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. Evidence handling lets the team explain each finding later, to operators and to anyone who reviews the work.

## Report operationally meaningful findings and practical next steps

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

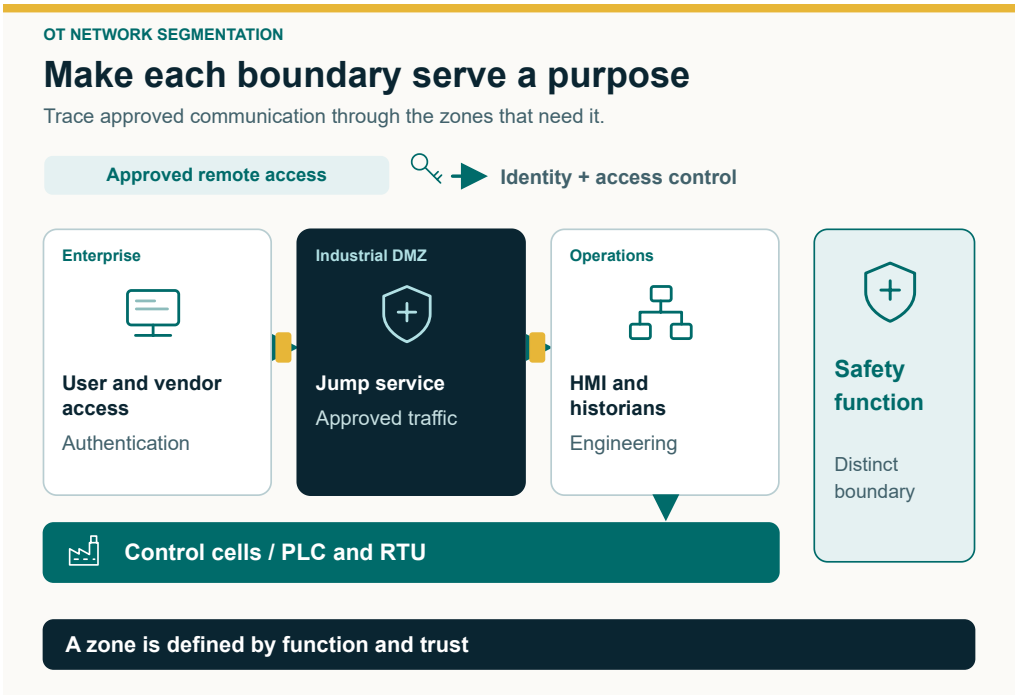
Separate quick administrative corrections from engineering changes that require design, procurement or an outage window. Assign priorities with the owner using the business and safety context rather than a tool score alone. If the team accepts or defers a risk, retain the reason, approving authority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

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

## 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, the current final publication; Revision 4 was released as an initial public draft on September 21, 2026. [NIST SP 800-82 Revision 3]




Zones and controlled connections frame where passive collection and any approved testing can occur.

## Information Gathering Q&A Checklist

Use this Q&A with the people who own the systems and the relevant legal or business decisions. Mark unknown or not applicable answers explicitly. Record an owner, a confirming source and the date.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

### 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 open questions:

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

**Which process units, sites and zones are in scope, and which are excluded?**

List each area with its owner and the reason for any exclusion.

Answer:

Owner, source, date and open questions:

**Which drawings, asset lists and network diagrams exist, and how current are they?**

Record the date and owner of each document and where it is known to be out of date. [NIST SP 800-82 Revision 3]

Answer:

Owner, source, date and open questions:

**Where can passive traffic be collected without affecting the process?**

Identify the switch, span port or network tap, its capacity and the engineer who approved its use.

Answer:

Owner, source, date and open questions:

**How do vendors and remote support reach the control network today?**

List each remote path, the account it uses, who approves a session and how sessions are recorded.

Answer:

Owner, source, date and open questions:

**Which controllers, HMIs and engineering workstations are fragile or safety critical?**

Record known sensitivities, firmware versions and any device that is sensitive to unsolicited traffic.

Answer:

Owner, source, date and open questions:

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

Name the targets, methods, window, stop conditions and the engineer who approved them. [NIST SP 800-115]

Answer:

Owner, source, date and open questions:

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

**Who receives findings, and how will corrections be scheduled into outage windows?**

Name the recipients and the change process that will carry each correction to completion.

Answer:

Owner, source, date and open questions:

## Primary sources and further reading

Sources checked November 3, 2026.


1. NIST SP 800-82 Revision 3, Guide to OT Security https://csrc.nist.gov/pubs/sp/800/82/r3/final
2. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment https://csrc.nist.gov/pubs/sp/800/115/final
3. NIST rules of engagement glossary https://csrc.nist.gov/glossary/term/Rules_of_Engagement



### Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

**Call (800) 868-8189, 24/7 · New York office (212) 561-5860**

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.