

OT Disconnect and Reconnect Planning

For small and mid-size utilities and the integrators who support their OT systems.

If disconnecting a path also cuts your access to its control, how will you reconnect it?

Use this after Practical OT Security No. 1, Vendor Access Review. Plan one connection with operations, engineering, and security. Attach diagrams and supporting evidence. Resolve dependencies before approving a change.

Site / connection ID _____ Review date _____

Plan owner _____ Change or incident record _____

1 Define the boundary and purpose

Which exact path will be disconnected, by which control, and for what reason?

What triggers the action and who approves, executes, and verifies it?

For an incident, use the site’s incident-response authority and safety procedures. For planned changes, use the approved change process.

2 Establish what depends on this path

Include control, alarms, telemetry, local operation, and shared services. Record evidence rather than assuming the process can continue locally.

Service or function	Expected effect of disconnect	Evidence or unresolved question

Which communications must remain available, and how will they be preserved?

3 Check alternate routes and management access

Could another route still reach the protected equipment? Record how it is controlled.

How will staff operate the disconnect control and verify its state while the path is down?

Record how authorized staff will manage the control through a separate path or approved local access. Check whether it depends on the same power supply, login service, or network you plan to disconnect.

Plan validation and reconnection

Connection ID _____ Plan version _____

4 Validate the expected behavior

What evidence can you review passively before testing?

For any necessary active test, record the approved window, operator, and checks for success.

What stops the test, and what approved steps will restore safe operation?

Check what happens if power fails, management access is lost, or equipment behaves unexpectedly. Agree on the required response with operations and the equipment supplier.

5 Set conditions for reconnection

What must be checked before reconnecting, and who approves and performs it?

After a suspected compromise, require incident-response approval and evidence that the relevant systems and access path are ready. A timeout or restored link alone is not a reason to reconnect.

After reconnecting, how will operations check service health and security check access limits?

6 Record the decision and remaining work

Unknown or required action	Owner	Evidence needed and due date

Decision _____ Approver / date _____

Record whether to approve the change, revise the design, or investigate further. Attach the steps for making the change and restoring service to the change or incident record.

Source and scope

NSA, Hardening Department of War Critical Operational Technology Environments with Zero Trust Principles, October 2026, version 1.0. Pages 10-11 address remote and third-party access. Pages 16-17 address safe validation.

[Read the NSA guidance](#)

TANDMM planning worksheet informed by the guidance. The disconnect and reconnect questions are our engineering interpretation. Follow your site's change and safety procedures. NSA does not endorse this worksheet or any product.

Worked example

Cedar Bend Water Utility / Fictional continuation of Practical OT Security No. 1

Cedar Bend reviews a separate maintenance connection to preserve telemetry and alarms on its shared operational uplink. The team finds a login dependency that would block new remote administrator sessions after disconnection.

1 Boundary and authority

MAINT-01 links the vendor jump host to a dedicated maintenance interface. The disconnect control cuts this path while the operational uplink remains connected. The OT manager and operations supervisor approve changes. An authorized administrator performs them, and the control-room operator checks service health.

2 Dependencies and alternate routes

Function	Required outcome	Evidence needed
Telemetry and alarms	Continue on the operational uplink	Confirm traffic paths and control-room indications.
Local control	Continue within approved operating limits	OEM review and controlled validation of communications-loss behavior.
Vendor maintenance	Unavailable when MAINT-01 is disconnected	Verify the selected boundary and restrictions on alternate routes.

The network engineer also checks whether the vendor can reach the equipment through the shared uplink or another gateway. A separate maintenance cable alone does not establish isolation.

3 The finding and required fix

The management network was separate, but its login service was not independent. Configuration review showed that the control's remote administrator login required an Active Directory server on the corporate network. The site's only configured route to that server crossed MAINT-01. There was no approved fallback. Cutting MAINT-01 would leave staff unable to start a new remote administrator session to reconnect it.

The team rejects that design. Network and security leads must provide a login method that works with MAINT-01 disconnected and document local recovery. They must check permissions, logging, power, and network dependencies.

Begin with configuration review and passive evidence. Then demonstrate a fresh administrator login and reconnection with MAINT-01 down during an approved test window. Engineering, security, and operations attend. Unexpected alarms, missing telemetry, abnormal control behavior, or lost management access stops the test and starts approved recovery.

4 Reconnection and decision

Routine reconnection requires a new approved work request specifying the user, task, destinations, and access window. Security checks access restrictions and logging. Operations checks process health. After a suspected compromise, incident response must approve reconnection. Access ends when the task or approved window ends.

Decision

Revise the management design before deployment. Acceptance requires a fresh authorized login and restoration of MAINT-01 while operational services remain available. Record test evidence, owners, and due dates in the change record.

TANDMM can help review the boundary, operational dependencies, and controls needed to implement the decision.

MissionSuccess@tandmm.ai | <https://tandmm.ai>