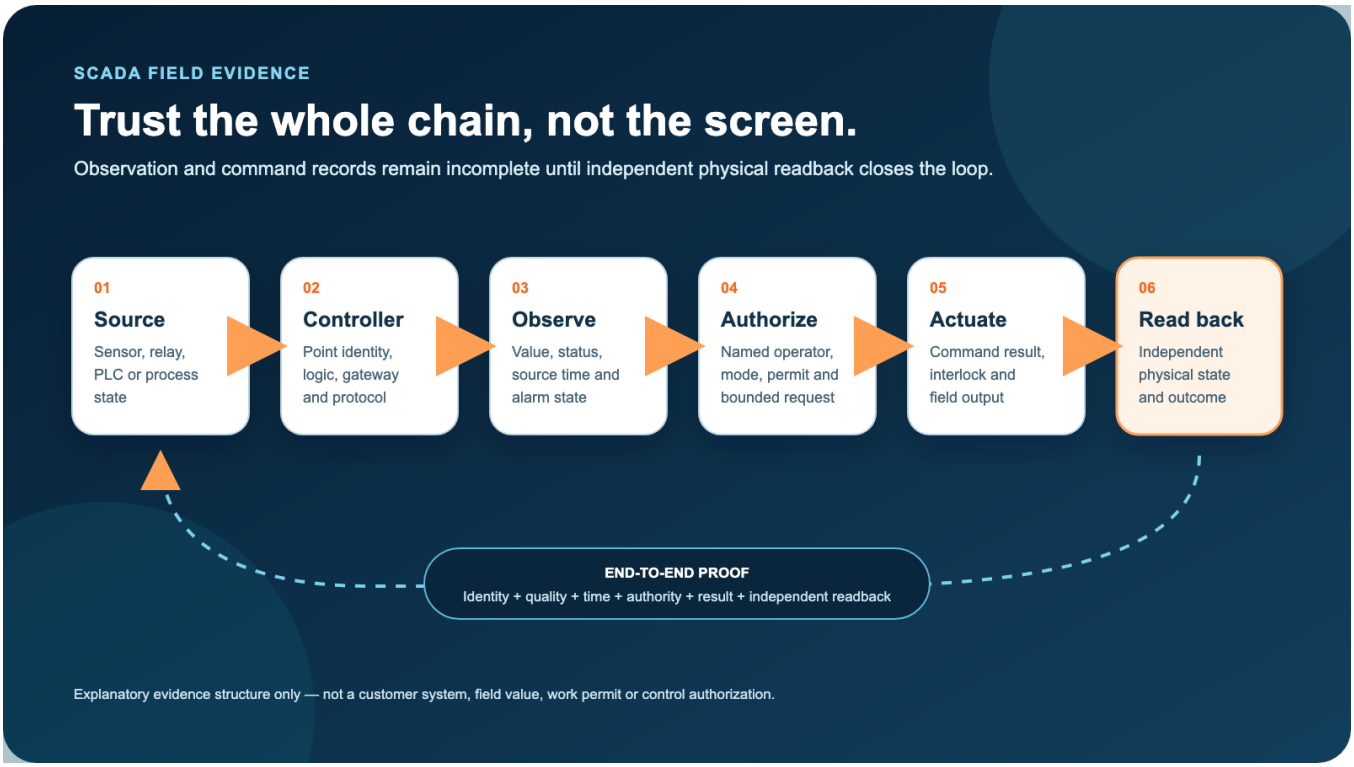
SCADA Observation, Command & Physical Readback Evidence

A correct-looking value or a successful command response does not prove the field state. Reconcile point identity, quality and time, then connect one authorized request to its actual field output and independent physical readback.

Reviewed	23 July 2026	**Audience**	Owner, OEM, integrator, operations
System	SCADA, gateway and field equipment	**Output**	Point and command validation record



Decision summary

Trust the point. Authorize the request. Prove the physical result.
Keep source identity, point contract, value, status, source/server time, alarm state, session and authority, command request/result, field output and independent readback on one event record. A missing record is a hold or a deferred decision - never a pass.

OBSERVABLE SYMPTOMS

Reopen the end-to-end evidence chain when any of these appear

- A stale, substituted or uncertain value is shown as if it were current and good.
- The source, gateway, SCADA and historian disagree on units, scaling, state or event order.
- An alarm appears, clears, acknowledges or confirms differently after reconnect or restart.
- A command is accepted but the field device, process or independent feedback does not change.
- Feedback mirrors the command bit or logic state rather than a separate physical indication.
- Communication loss or recovery creates a gap, duplicate event, stale state or unexplained transition.

STOP-WORK CONDITIONS

Hold when identity, trust, authority or independent feedback is missing

Mapping unknown	Source, address, type, unit, scale, normal state or active configuration is not reconciled.
Quality or time hidden	Status/quality, timestamp meaning or time source cannot be observed or trusted.
Authority unknown	Operator, session, mode, permit, approval or release owner is open.
Control impact unknown	Output, interlock, inhibit, bypass, safety or process consequence is unreviewed.
No independent readback	The only feedback is the command or software state.
Hazardous test unapproved	Live work, motion, process consequence or bypass lacks a qualified method and authorization.

Immediate response

Maintain or restore the safe state, preserve the as-found record and return the boundary to the named responsible authority. Do not use a web guide as permission to connect, command, bypass, energize or restart.

DATA TO COLLECT

Make each displayed state traceable to its source and physical consequence

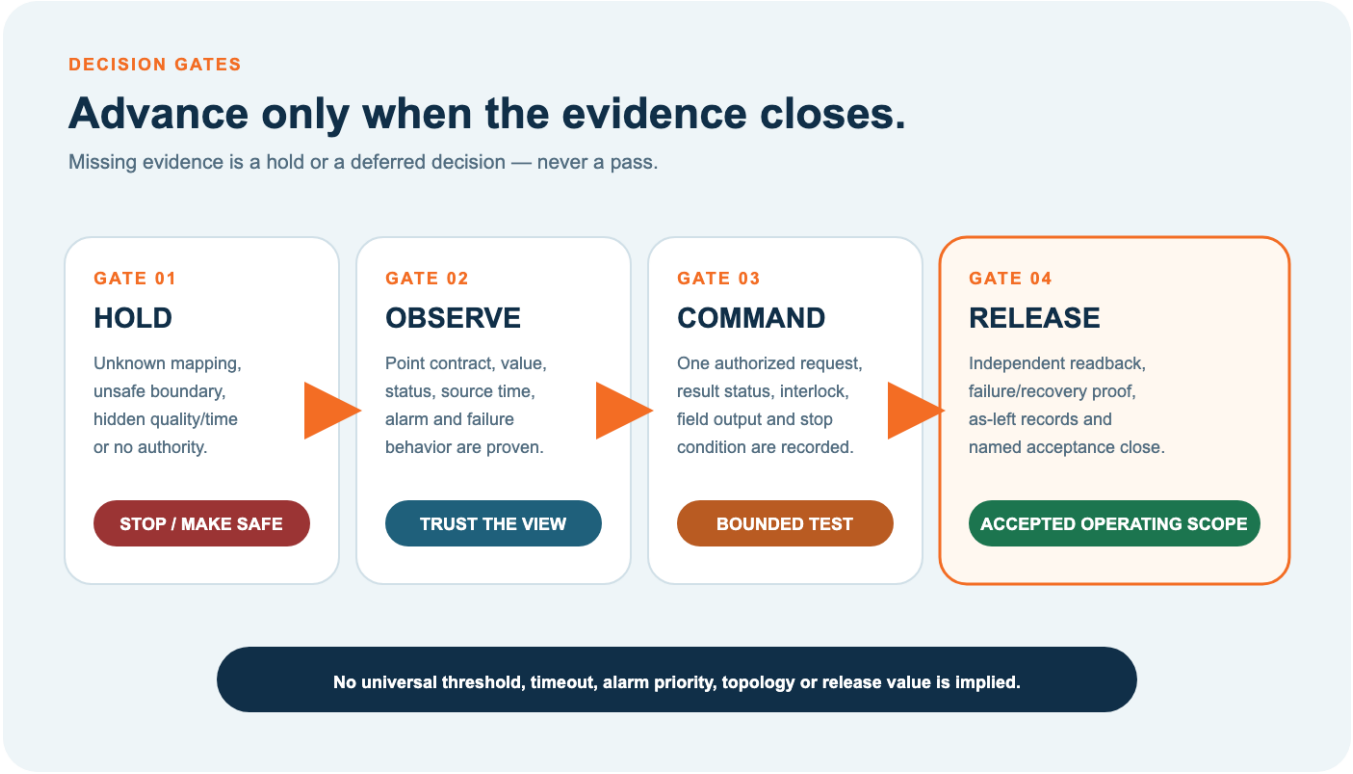
Evidence group	Minimum record	Decision supported
System identity	Site/process boundary, source device, controller/gateway, SCADA/server/client, versions and active topology	Fixes the actual system under review.
Point contract	Source/tag/address, data type, unit, scale, normal state, update/report behavior and active mapping revision	Defines what the point is expected to mean.
Observation quality	Value, status/quality, source timestamp, server timestamp, time source and clock-quality note	Separates current source evidence from a cached or uncertain display.
Alarm condition	Condition/event identity, active/inactive, acknowledged/confirmed, retained/branch state and comment where supported	Preserves alarm lifecycle rather than screen color alone.
Command authority	Named operator/session, role, local/remote mode, permit, permissive/interlock/inhibit and bounded approval	Shows who could request what, under which boundary.
Command transaction	Requested point/value, request time, service and operation result, diagnostic detail and intermediate state	Separates server acceptance from completion at the data source.
Physical proof	Field output, independent auxiliary/limit/status indication, process response and time-aligned observation	Closes the loop at equipment and process.
Failure/recovery	Link/server/client loss, queue behavior, reconnect/restart, gap/duplicate reconciliation, rollback and as-left result	Tests whether trust survives defined failure states.

OPC UA evidence note

OPC UA DataValue can carry a value, StatusCode, SourceTimestamp and ServerTimestamp. Write responses include service-level and operation-level results. These constructs are protocol-specific: confirm the exact protocol profile, product version and implementation used by the site.

DECISION GATES

Do not advance on a green screen or a single good result



Gate	Required evidence	Result
Hold	Unknown mapping, hidden quality/time, unsafe boundary, unclear authority or missing independent feedback.	Maintain or restore safe state. Do not command.
Observe	Reconciled point contract, value/status/time, alarm lifecycle and defined loss/recovery behavior.	Displayed state can be interpreted within documented limits.
Controlled command	One authorized request, expected effect, interlock/permissive, stop/rollback, result and qualified observer.	Run one bounded test without expanding the scope.
Release	Independent physical readback, process outcome, failure/recovery proof, as-left records and named acceptance.	Return only the accepted operating scope.

SIX-STEP PROCEDURE

Move from point identity to an accepted physical result

01	**Fix the system and safety boundary.** Name the source, controllers, gateways, servers, clients, process consequence, safety functions, modes and decision authorities.
02	**Preserve the active point contract.** Record source/tag/address, type, unit, scale, normal state, update/report behavior, mapping revision and as-found topology.
03	**Prove trustworthy observation.** Compare source and SCADA values with status/quality, source/server timestamps, clock basis, alarm lifecycle and communication state visible.
04	**Authorize one bounded command.** State operator/session, mode, point/value, expected effect, interlock/permissive, stop condition, rollback and approval.
05	**Trace request to physical readback.** Record service and operation result, field output, independent feedback, process response and event order. A software echo alone is not proof.
06	**Test failure and hand over the as-left state.** Verify approved loss/reconnect/restart scenarios, reconcile gaps or duplicates, restore accepted configuration and name open limitations.

EXPERT REVIEW

Questions for responsible control, operations and cybersecurity reviewers

- Does the point contract match the active source configuration and exact protocol/profile implementation?
- Can the operator distinguish value, quality/status, source time, server time and stale/substituted states?
- Are alarm active, acknowledged, confirmed, shelved/suppressed and retained states implemented and recovered as expected?
- Does the result prove only server acceptance, or also update of the underlying data source and physical equipment?
- Is feedback independent of the command path, and does it represent the intended physical or process state?
- Which failure modes, residual uncertainties and operating restrictions remain after the test?

HANDOVER PACKAGE

Leave enough evidence to reproduce each observation and command decision

System and observation	Authority, command and acceptance
- Approved topology and endpoint/version inventory - Point contract and active mapping revision - Original values, status/quality, timestamps and alarms - Time-source and clock-quality statement	- Authority, session, mode, permit and transaction - Independent field/process readback and outcome - Loss/recovery/restart test and reconciliation - As-left exports, rollback, limitations and acceptance

Release record

Name the accepted operating scope, unresolved limitation, owner, required monitoring, rollback state and next review. Do not hide uncertainty behind a generic pass/fail field.

OFFICIAL PRIMARY SOURCES

Use each source within its published protocol, product, country and site scope

1. **NIST SP 800-82 Rev. 3 - Guide to Operational Technology Security**
   https://csrc.nist.gov/pubs/sp/800/82/r3/final
   OT security guidance that explicitly considers unique performance, reliability and safety requirements.
2. **OPC UA Part 4 - DataValue**
   https://reference.opcfoundation.org/specs/OPC-10000-4/7.11
   Defines the value, StatusCode, SourceTimestamp and ServerTimestamp components used in OPC UA observation.
3. **OPC UA Part 4 - Write service**
   https://reference.opcfoundation.org/specs/OPC-10000-4/5.11.4
   Defines Write service and operation-level result handling; a result can have implementation-specific limits.
4. **OPC UA Part 9 - Acknowledgeable Condition model**
   https://reference.opcfoundation.org/Core/Part9/v105/docs/5.7
   Defines acknowledged and optional confirmed states, methods and event identity within OPC UA Alarms and Conditions.

Application limit

NIST SP 800-82 is United States government guidance. OPC UA constructs are protocol-specific and do not describe every SCADA protocol or product implementation. Confirm country, authority having jurisdiction, site permits, qualified-person requirements, cybersecurity program, actual protocol profile and product version, OEM instructions and responsible engineering/operations approval. This document does not authorize scanning, connection, command, bypass, energization or restart.