Dweve
Weaving Intelligence

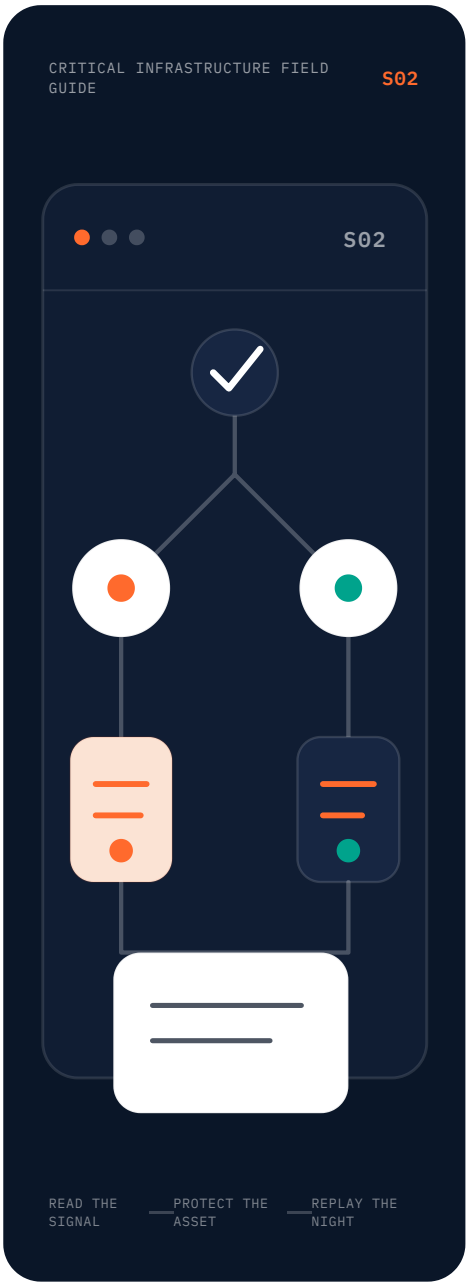
ENGLISH SOURCE EDITION · JULY 2026

CRITICAL INFRASTRUCTURE FIELD GUIDE · S02

The control-room field guide

One storm, one feeder, one operating decision, and the incident record that must survive the night.

OT BOUNDARIES · STORM RESPONSE · OPERATOR AUTHORITY · REPLAY



Not a generic resilience brochure. A storm response followed from telemetry quality to safe action, restoration, and the morning-after record.

S02

CONTENTS

The night the control room had to keep deciding

This field guide stays with feeder F-12 during a storm. The asset, telemetry, protective policy, operator, target receipt, and incident record remain connected throughout.

PRIMARY READERS	READING DEPTH	DECISION THIS SUPPORTS
control-room field guide domain, operations and assurance teams	Sector specialist	A critical-infrastructure working book for operations, OT security, control engineering, resilience, assurance, and incident command.

HOW TO USE IT

Replace the fictional values with one operator-owned event. The control boundary and authority model must come from the plant, not from this publication.

SOURCE DISCIPLINE

Dweve-specific facts are taken directly from the English website text audited 2026-07-20; web-navigation wording is humanised for print. Evaluation guidance is editorial, and scenarios and derived visuals are illustrative. Unsupported synthesis is replaced by canonical copy or omitted.

THE STORM CASE

Thirty seconds in the control room

At 02:30, three substations alarm together. The communications link to feeder F-12 drops. The anomaly display shows red, but the wall does not say why.

The operations manager has a short decision window and a long accountability tail. The immediate question is whether F-12 should be isolated under the protection procedure. The next-morning questions are broader: what telemetry was available, what quality did it carry, which policy was active, who authorised the action, and what the plant actually did?

The design constraint

A critical-infrastructure system cannot treat connectivity as a prerequisite for truth. It must distinguish a fresh measurement from a stale one, a recommendation from actuation, a lost receipt from a failed action, and a safe degraded state from a green dashboard.

OPERATOR TEST

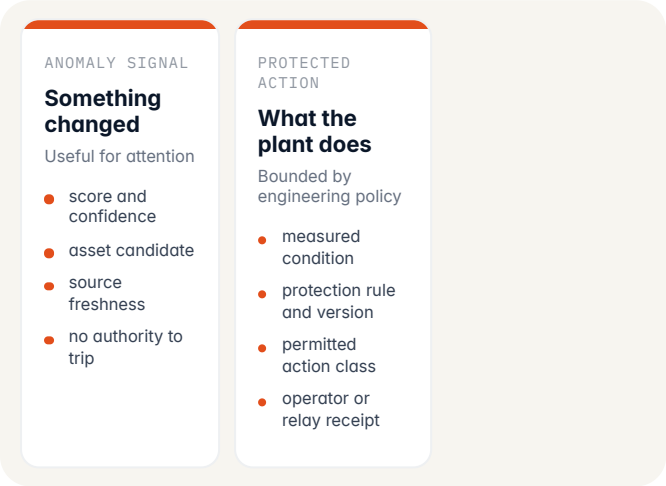
If the system cannot say what it knew when the link dropped, it cannot safely say what the operator should do next.

The useful record follows operating time, not the time an analyst later opens the dashboard.

SIGNAL VERSUS ACTION

A red score is not an operating instruction

An anomaly can focus attention. It cannot silently become an actuation command.



The detection path and the safety or protection path can cooperate without becoming the same thing.

For feeder F-12, the anomaly score is not the reason to isolate the asset. The operating decision is tied to the telemetry quality, asset class, differential-current threshold, protective relay policy 4.1, rule 3.2, and the authority permitted to trip and restore.

Separate the consequence classes

- observe and annotate
- recommend a bounded operator check
- trip or isolate under an approved protection path
- queue restoration after the asset state is reconciled
- stop and escalate when the input or target state is unknown

DO NOT FLATTEN THE MODES

A system that describes every state as an alert is not giving the operator a safe operating vocabulary.

01

THE F-12 EVENT

Follow one operational decision from signal to safe state

The event is useful because it contains the uncomfortable details: a high-value signal, a missing link, a local policy, a human confirmation, and a target that must be reconciled.

The plant state is not closed until the target and the evidence agree.

THE EVENT ENVELOPE

F-12 has an asset identity, not just a tag

A feeder label is not enough for replay. The record needs the topology, asset class, operating state, time basis, and authority boundary that made the action meaningful.

The worked event uses feeder F-12 as a compact identity. In the operator estate, the identity must resolve to the asset registry, current topology, protection settings, maintenance state, and the work or incident already open for that asset. A message that says “F-12 tripped” without those relationships is not an incident record.

Bind local context before evaluating

- asset identity and topology snapshot
- measurement units, quality flags, and source clock
- protection and engineering policy effective at event time
- communications and local-control state
- permitted action class and operator role
- target correlation for the relay, breaker, and restoration system

`event.identity` BOUND

Event

storm-02h30 · feeder F-12 · trip assessment

`asset.snapshot` PINNED

Asset

Substation, feeder, topology, class, and maintenance state

`telemetry.quality` DECLARED

Measurement

Differential current 8.4 kA with freshness and quality attached

`policy.effective` EFFECTIVE

Protection

Policy 4.1, rule 3.2, resolved against event time

`target.correlation` RECONCILED

Target

Trip, isolation, and restoration sequence receipts

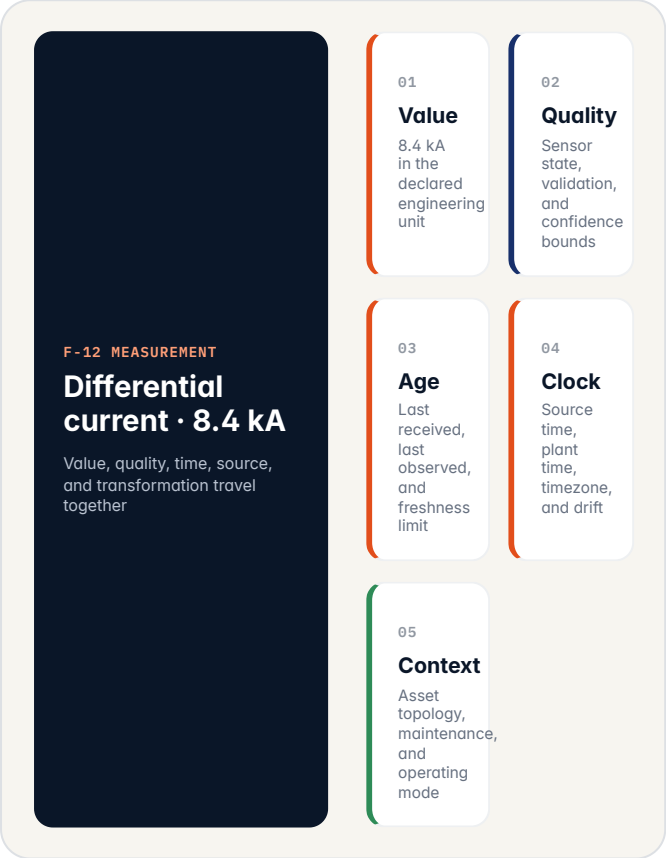
OT IDENTITY RULE

Do not let a human-readable asset tag stand in for the authoritative identity needed by the control, historian, work-order, and incident systems.

THE MEASUREMENT BOUNDARY

Telemetry has quality, age, and a clock

The last value received is not automatically the current value. A degraded system must make staleness visible before it recommends a consequence.



A stale measurement may still be valuable. It must not masquerade as a live one.

The control room needs a state for stale-but-usable, conflicting, missing, and untrusted telemetry. Each state should map to an approved consequence boundary. “Use the last snapshot” can be a valid degraded procedure only when the plant has declared its freshness, hazard, and authority limits.

Questions for the source owner

- What does the quality flag mean in this protocol?
- Which clocks can disagree, and what tolerance is acceptable?
- Who approves a last-known-good snapshot during a link outage?
- Which actions are forbidden when topology or breaker state is uncertain?

NO CONFIDENT GREEN

When the plant cannot establish the input or target state, the visible answer should be degraded, waiting, refused, or reconciling.

RULE, VERSION, AND LOCAL AUTHORITY

Protection policy is an operating instrument

Protective relay policy 4.1, rule 3.2 is not background documentation. It is part of the action that isolated F-12.

The policy object has an owner, effective date, asset class, threshold, action, reset or restoration conditions, emergency override, test corpus, and rollback process. The exact values belong to the operator and engineering authority. The field guide makes their place in the event explicit.

Illustrative protection witness

```
asset = registry://feeder/F-12@event-time\nmeasurement =
telemetry://F-12/differential-current@02:32\nquality =
declared + within local degraded bound\npolicy =
protection://relay/4.1#3.2\ncondition =
differential_current > class_threshold\naction =
trip_and_isolate\nauthority =
approved_protection_path\nreceipt = relay + operator +
incident-correlation
```

The syntax is illustrative. The plant owns the settings, procedure, and safety case.

POLICY FIELD	WHY IT MATTERS AT 02:32	OWNER
Asset class	Threshold and action are not interchangeable across equipment	Protection engineering
Effective state	The morning review must use the rule in force at the event	Policy authority
Quality bound	A stale or conflicting input may block the action	Control engineering
Action class	Trip, isolate, recommend, and restore carry different consequences	Operations
Reset condition	Restoration needs an observed safe target state	Shift lead + engineering

A rule without applicability and authority is a sentence, not an operating control.

SCADA, HISTORIAN, AND THE EVIDENCE SURFACE

The OT boundary is part of the product

The first proof should sit beside the plant systems. It should not ask the control room to replace its authoritative estate with a second dashboard.

The boundary should be legible to both an OT engineer and an incident reviewer.

The operator chooses the existing protocols, adapters, identity model, archive, and one-way or disconnected paths. Dweve's role is to hold the bounded work identity, governed context, decision state, action receipt, and evidence relationship without taking authority away from the plant.

No hidden outbound dependency

- measure actual egress from the OT-DMZ and isolated package
- record which sources, models, tools, clocks, and keys are local
- test update media, rollback, restore, and support without a live supplier connection
- keep sensitive telemetry out of broad service telemetry

OT ACCEPTANCE

A deployment statement is incomplete until the operator can show the actual paths taken during normal, degraded, and recovery operation.

MODELS, SOLVERS, AND OPERATOR CHOICE

Keep reasoning below the actuation line

An anomaly model may help an operator see a pattern. It should not silently cross the boundary into physical action.

The path may be fast. It must remain explicit.

Loom can route bounded analysis, specialist checks, and exact solver work. Nexus can give the shift, engineering, and incident roles visible tasks, escalation, and receipts. Selvedge can preserve the execution transcript. The operator and approved protection system remain the authority for the physical effect.

A safe disagreement

An anomaly check says the pattern resembles a fault. The protection rule says the measurement quality is insufficient for automatic action. The operator sees the conflict, checks the local procedure, and either follows the approved manual path or holds the asset. The conflict becomes evidence instead of disappearing inside a score.

NO AUTONOMOUS SHORTCUT

A model that can recommend a breaker action is not thereby authorised to command a breaker.

DEGRADED MODE AND TARGET STATE

The operator keeps authority when the link drops

The communications outage is not an edge case in this story. It is the point at which the architecture must prove what remains safe.

The system needs a safe state for missing information, not just a retry loop.

What must remain local

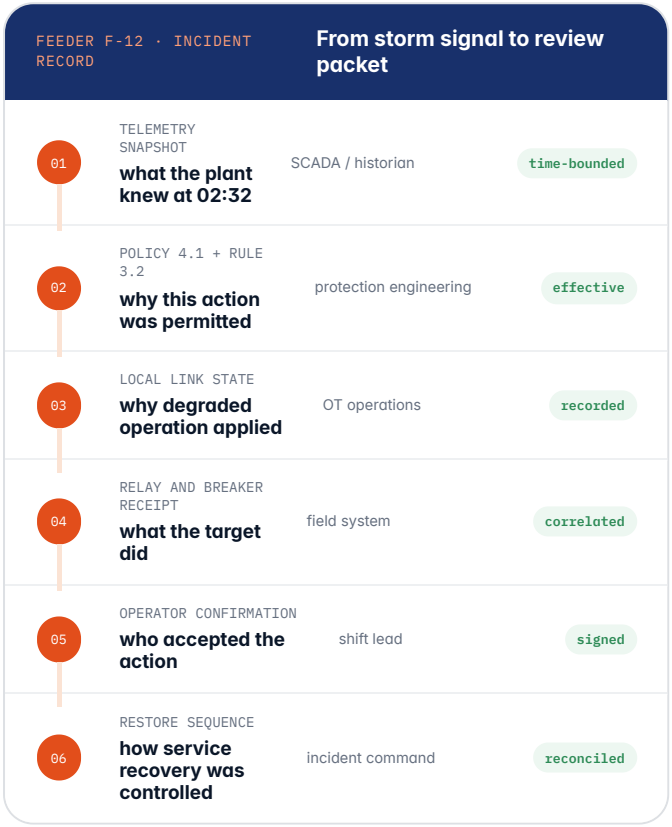
- the declared degraded-mode procedure and policy version
- the minimum telemetry and asset context allowed to support it
- operator identity, role, and action capability
- local keys, package integrity, time, and event storage
- the receipt and reconciliation state for every external effect

When the link returns, the plant should not blindly replay every queued intention. It should compare what the field did, what the operator confirmed, what the target reports, and what the incident record expects.

THE MORNING-AFTER WITNESS

The incident record is created during the shift

The regulator should not have to ask the operator to rebuild the night from a screenshot, a radio note, and a historian query.



The packet separates source truth, policy authority, physical effect, and human responsibility.

Ledger can retain the system event history, Selvedge can preserve the verified execution transcript, and AION can provide a portable decision certificate for the selected proof. Those layers answer different questions. A chain seal cannot establish that a sensor was truthful, and a correct relay receipt cannot prove that the wrong policy was appropriate.

The review packet should answer

- Which asset and topology were involved?
- What value, quality, age, and clock were available?
- Which procedure and policy version applied?
- What did the operator or relay do, and what did the field target report?
- What remained uncertain, and how was restoration closed?

INDEPENDENT CHECK

The reviewer should be able to verify the packet without granting the verifier authority over the OT system.

02

RESILIENCE UNDER PRESSURE

Prove the system when the comfortable assumptions disappear

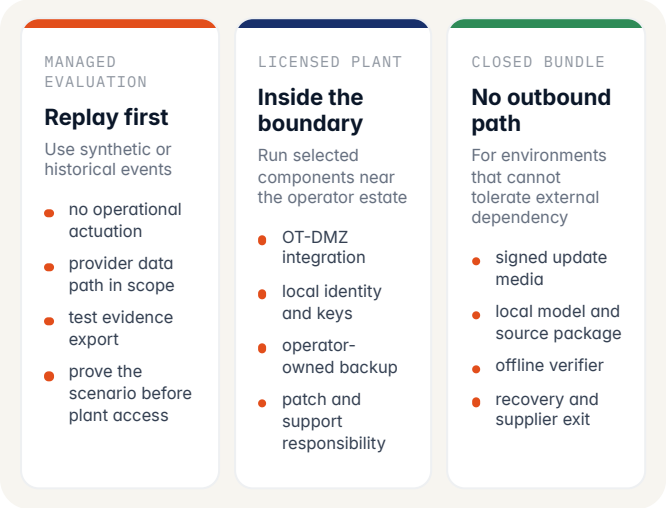
A critical-infrastructure proof is not complete because the normal dashboard works. It is complete when the plant can operate, stop, recover, and explain itself under the conditions that matter.

Resilience means preserving safe meaning, not merely preserving uptime.

DEPLOYMENT POSTURE

Local first, not cloud-shaped

The operating posture changes the controls. Managed evaluation, licensed plant deployment, and a closed isolated bundle are different commitments.



A label such as on-premises does not prove where a model, key, update, or support path actually travels.

The first operational proof should be a replay or shadow workflow. Only after the operator, engineering authority, security owner, and incident process trust the evidence should the scope approach a live consequence boundary.

Measure the posture, do not describe it

- egress and dependency test during normal operation
- local behaviour when the WAN and OT-DMZ links are unavailable
- signed package, update, rollback, and recovery exercise
- time source, key custody, telemetry retention, and verifier availability
- support path that does not smuggle administrative access into the plant

DEPLOYMENT ACCEPTANCE

The same semantic case may travel across postures. The operating responsibility does not become identical by changing the hosting label.

THREAT AND FAILURE MATRIX

Attack the assumptions that hold the plant together

The useful failure test is specific to the field system, the consequence boundary, and the evidence that must remain after recovery.

CONDITION	WHAT CAN GO WRONG	SAFE RESPONSE
Stale telemetry	Old current appears to be live	Show age and quality; hold or use declared local bound
Topology change	Feeder identity no longer matches current plant state	Stop the action and resolve the asset graph
Poisoned procedure	A document changes the apparent protection rule	Reject, quarantine, and route to policy authority
Compromised node	A local component emits a false event or receipt	Limit capability, isolate, and preserve incident evidence
Target timeout	Relay or breaker state is unknown after request	Do not retry blindly; reconcile field state
Operator absence	No authorised person is available for a non-automatic action	Enter the approved degraded state and escalate
Restore	Link returns with conflicting histories	Merge by authority and time; retain the conflict

A good failure response names the state and owner instead of hiding behind a generic retry.

Security is also an evidence problem

Segmented networks, signed packages, access controls, and local keys protect the plant. The review packet must also show when a trust boundary was crossed, which capability was denied, what support path was used, and whether the resulting record is complete.

NO BROAD TELEMETRY SHORTCUT

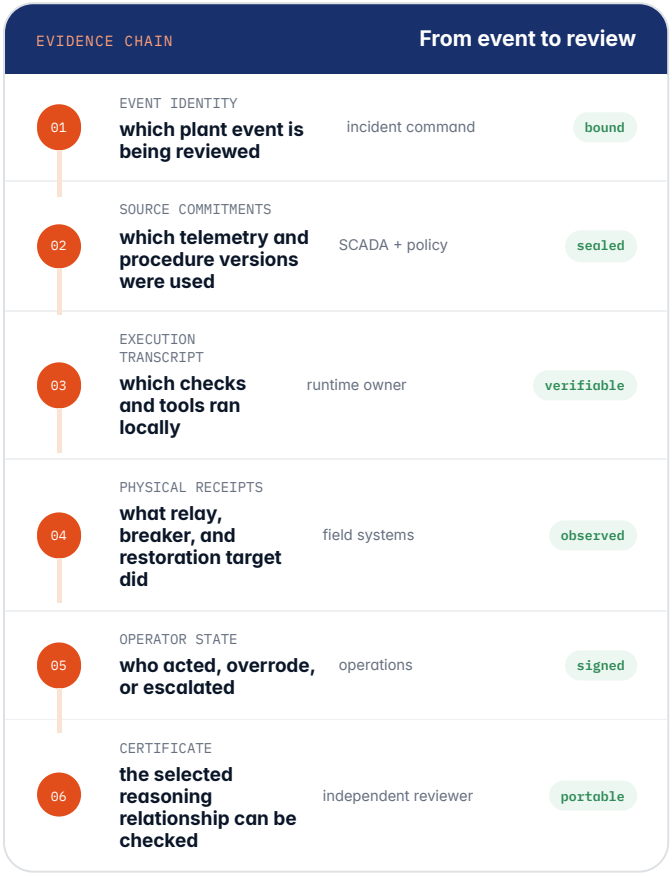
Do not export raw operational data to make a service easier to operate unless the plant has approved the purpose, path, retention, and disclosure.

The incident team should be able to investigate without giving every operator, supplier, or model runtime the same view of the plant.

INDEPENDENT REPLAY

The morning-after review must stand alone

The reviewer needs a portable answer to the event, not a temporary login into the system that created it.



A replay packet should make uncertainty visible rather than erase it for presentation.

The reviewer should be able to reproduce the declared rule path and inspect the packet without reconnecting the runtime to the live plant. If a value is intentionally unavailable because it was not retained, the packet should say so. “Not found” and “not applicable” are different findings.

What replay cannot prove

- that the sensor was physically calibrated unless calibration evidence is included
- that an engineering policy was appropriate merely because it was applied
- that service impact was acceptable because the incident closed
- that an unavailable source had no effect

PORTABLE DOES NOT MEAN PUBLIC

Independent checking still follows the operator’s classification, disclosure, and safety boundaries.

THE OPERATOR-OWNED CORPUS

Acceptance begins with the ugly cases

Normal storm response is only one slice. The proof must include stale, conflicting, missing, malicious, and recovered conditions.

TEST SLICE	INCLUDE	EXPECTED RESULT
Normal event	F-12 signal, policy 4.1, operator confirmation	action and packet close together
Link loss	02:31 comms drop with last snapshot	degraded state is visible and bounded
Bad quality	stale, conflicting, or invalid measurement	hold, refuse, or route to a local procedure
Topology change	maintenance or switching changes the asset graph	old target is not silently reused
Target uncertainty	command accepted but breaker state unknown	no duplicate action; reconciliation opens
Security event	poisoned document or compromised local node	capability is limited and incident evidence remains
Recovery	link return, restore, replay, and oversight export	histories reconcile with conflicts retained

The operator should choose the corpus and consequence boundary. This table is a starting shape.

Measure operating truth

- telemetry freshness and quality at every decision
- time from signal to authorised action without hiding human review
- target receipt and reconciliation after degraded operation
- availability of the local procedure, keys, verifier, and recovery path
- packet completeness and independent replay verdict
- access denial, malicious-input response, and incident hand-off

Do not reduce resilience to a single uptime number. A plant can be available and still be unable to establish whether an action is safe, authorised, or complete.

GO, NARROW, HOLD, OR STOP

The production decision belongs to the operator

A proof ends with a recorded operating decision, not with a successful screen demonstration during good weather.

The accountable group decides whether the selected workflow may cross into a live consequence boundary, under which assets, procedures, telemetry conditions, operator roles, target systems, deployment posture, service objectives, recovery, and disclosure rules. Operations, control engineering, OT security, safety, incident command, resilience, procurement, and oversight may each own a condition.

OPERATING PRODUCTION RECORD	Feeder F-12 proof decision	
WORKFLOW	**Storm trip assessment and controlled restoration**	BOUNDED
ASSETS	**Named feeder, substation, topology, and test cohort**	SCOPED
INPUTS	**Telemetry + quality + clock + procedure + asset state**	LINKED
AUTHORITY	**Relay path + operator role + escalation**	REVIEWED
RECOVERY	**Target reconciliation, restore, incident, verifier**	OWNED
EXIT	**Export, rollback, local support, and stop trigger**	DATED
DECISION	**Go / narrow / hold / stop**	SIGNED

The record must remain useful to the next shift, the incident team, and the reviewer who was not present at 02:32.

The smallest credible next exercise

Replay the F-12 event, then introduce one boundary failure chosen by the operator: stale telemetry, lost target receipt, topology change, or link restoration with conflicting histories. Make the shift lead, protection engineer, OT security owner, and incident reviewer inspect the same packet.

PRIMARY ACCEPTANCE CRITERION

The operator can identify the exact asset, telemetry state, policy/version, action authority, physical target state, restoration result, and replay verdict for every selected event.

That proves one operating slice. It does not authorise generalisation across every plant, asset class, procedure, or consequence.

FIND A SUBJECT

Subject index

Page references point to the substantive explanation, worked example, control, boundary, or decision record, not merely to a passing label.

SUBJECT INDEX CONTINUED

Subject index · S–W

Terms are grouped alphabetically. Consecutive page references are collapsed into ranges.

CLOSING RECORD

Exercise the failure before it becomes the incident

Choose one operational workflow, name the authority that can stop it, and prove that the plant remains safe and explainable when its comfortable assumptions disappear.

Write the asset identity, topology and operating mode, telemetry quality and clock, applicable procedure and effective version, model or solver boundary, permitted action, operator authority, target receipt, restoration sequence, packet, verifier, deployment posture, recovery, retention, and stop conditions.

Then choose the failure you most dread explaining. It may be a stale value, a lost link, a topology change, a compromised node, a denied operator action, an unknown breaker state, or a recovery that produces two histories. The field guide is useful when the difficult case can be run before the storm.

ASSET

One bounded operational decision

Do not begin with the whole plant

AUTHORITY

Named operator, relay, engineering, and incident owners

Control must be real

QUESTION

Can the next morning's record be independently checked?

Not merely narrated

STATE

Input, action, target, restoration, and uncertainty

Each with its own status

DECISION

Go, narrow, hold, or stop

Signed with conditions and triggers

THE CONTROL-ROOM STANDARD

A dashboard can show that something happened. A defensible operating record shows what the plant knew, what it was allowed to do, what it did, and how it recovered.