



ASTRA

AEROSPACE STANDARD

PROCEDURE

Cyber Incidents, Evidence Recovery and Service Continuity

AF-AST-PR-020

FIRST EDITION

30 September 2026 | English master text

Aviation / Space / Defense / Future systems

Publication identity and use

Control	Publication information
Code and title	AF-AST-PR-020 — Cyber Incidents, Evidence Recovery and Service Continuity
Edition and publication date	FIRST EDITION 30 September 2026 English master text
Accountable function	Information and Security Manager
Controlling technical basis	AF-AST-STD-001 / AF ASTRA-100:2026; supplied 248-page FIRST EDITION, Clauses 0–80 and Annexes A–AR.
Source fingerprint	fe0f775b3f57e43c7ad6b3d4ab17ac0ff872d3ce8c88fcd9ae9a0116b23209b1
Portfolio	108 retained document codes; F01–F08; 68 retained technical subjects. All-space and verification domains are applicability tags, not additional families.
Publication and operation	Prepared publication. Actual technical approval, consultation, institutional adoption, operational effectivity and individual scope activation require separate authentic records.

Purpose and application

Defensive incident handling for engineering, production, assessment and public-status systems. No intrusive security testing is authorised by this procedure.

Source requirements and added implementation detail

The controlling ASTRA source is identified above by content fingerprint. Numbered source clauses and annexes retain their own authority. The retained operating material is restructured and expanded with implementation methods, additional profile controls, worked synthetic examples, decision diagrams and record contracts. Added implementation detail is not presented as an earlier institutional approval or as a change to the supplied core standard. Any additional binding criterion requires the applicable technical adoption process.

The displayed publication date identifies the edition; it is not a fabricated authoring, test, approval or operational date. Actual records retain genuine event times and controlled versions. No named outside organisation or standard is incorporated as a normative reference. AF internal instruments and separate legal or contractual duties remain applicable within their actual scope.

Acceptance boundary

A positive grant requires every applicable mandatory condition to PASS, every N/A to have independent justification, every in-scope nonconformity to be verified closed, and competent independent authority. HOLD, unknown state, missing evidence, a favourable average, a signature image or a completed form cannot substitute for those conditions.

Contents

Publication identity and use	2
Purpose and application	2
Source requirements and added implementation detail	2
Contents	3
1 Scope, trigger and responsibility	5
2 Operating sequence	5
PR-020 — Cyber Incidents, Evidence Recovery and Service Continuity	5
3 Completion, holds and handover	6
Decision and authority boundary	6
4 Timing and escalation	7
5 Worked application and failure response	7
E1 Explicit acceptance and evidence contract	8
E2 Source-to-implementation crosswalk	8
E3 Detailed operating extensions	9
AF-AST-PR-020 — Cyber Incidents, Evidence Recovery and Service Continuity	9
E4 Application-specific parameter completion	10
P01 — Mission and scope	10
P03 — Requirements and acceptance	10
P11 — Communication and timing	10
P14 — Software, AI and models	10
P15 — Security and command authority	10
P18 — Decision, continuity and terminal duties	10
E5 All-space applicability and bounded responsibility	10
E6 Workflow and evidence relationships	11
E7 Calculations, assumptions and synthetic charts	12

AM.Q03 Positive-decision conjunction and essential failure	13
AM.Q09 Availability is not output correctness	13
AM.Q16 Outage data storage with overhead	14
AM.Q17 Clock uncertainty and maximum data age	15
AM.Q25 Reliability architecture and common-cause sensitivity	16
E8 Adverse cases and independent replay	17
Appendix A — Controlling source requirements	18
Appendix B — Local adoption, validation and receiving acceptance	21

1 Scope, trigger and responsibility

Defensive incident handling for engineering, production, assessment and public-status systems. No intrusive security testing is authorised by this procedure.

Trigger: A cyber/data incident, suspected compromise, service interruption or recovery exercise affects assurance records or operations.

Accountable process owner: Information and Security Manager. Actual named appointments and deputies are recorded separately. The process owner coordinates execution; technical review, independent conformity decisions and operational permissions retain their separate mandates.

Input	Output / destination
Actual request or triggering event, scope and current technical basis	A traceable process record linked to its case/object and the required form modules.
Competence, conflict, authority and access evidence	Approved assignment and lawful access before affected work begins.
Original observations, technical results, limitations and prior history	Reasoned accept/hold/escalation decision; preserved adverse evidence and recipient communications.
Controlling clocks and genuine event timestamps	Actual due/completion records in SC-003 and the relevant register; no administrative reset.

2 Operating sequence

PR-020 – Cyber Incidents, Evidence Recovery and Service Continuity

Trigger: A cyber/data incident, suspected compromise, service interruption or recovery exercise affects assurance records or operations.

1. Identify and preserve the event

The incident owner records awareness, original evidence, affected systems, deployed versions, users and initial uncertainty. Preserve relevant logs and source records through authorised means. Separate a detection alert from a confirmed cause and from the technical effect on assured outputs.

2. Contain within actual authority

Stop or restrict compromised access, data use or connected work using safe authorised arrangements. Coordinate with operational technical authorities so that a security response does not defeat an essential safety function. Apply urgent critical notices and status controls when their actual triggers are met.

3. Trace affected evidence and outputs

Map compromised records, machine programmes, configurations, software updates, reports, credentials and recipients. Establish the last demonstrated trustworthy state. Include downstream decisions made using wrong or unavailable information, not only the system named in the incident ticket.

4. Plan correction and trusted recovery

Select the recovery point, authentic sources, permitted configuration and required checks. Preserve post-recovery-point events and identify reconciliation needs. Approve patches and other changes for safety, timing and qualification compatibility; a security fix is also a technical change.

5. Restore service separately from assurance

Record when the system becomes available, but do not declare assured return yet. Verify data identity, versions, units, time basis, permissions, evidence links and current/historical status. Missing original evidence stays unavailable rather than being reconstructed as an invented favourable record.

6. Challenge prohibited transitions

Safely test wrong profiles, duplicate keys, expired roles, open findings, stale imports, interrupted updates and suspended/expired status. Use synthetic fixtures isolated from live holders. Expected outcomes come from the controlling requirements, not whatever the application happens to display.

7. Authorise return and correct recipients

The competent technical function accepts restored integrity and actual operating restrictions. The independent status function separately decides credential effects. Notify affected recipients and correct earlier reports or public claims when unsupported. Successful backup restoration is not itself the approval.

8. Verify learning and continued control

Repeat failed tests after correction and relevant regression after changes. Review occurrence and escape causes, supplier dependencies and recovery performance. Record residual limitations, owners and follow-up. Retain originals, incident chronology and actual decision history.

Hold / escalation: Broken configuration/evidence links, unreconciled later events, compromised permissions or unresolved critical defects prevents assured return even when the service is online.

Record handover: AF-AST-FR-012, AF-AST-FR-016, AF-AST-FR-026, AF-AST-FR-028.

3 Completion, holds and handover

Broken configuration/evidence links, unreconciled later events, compromised permissions or unresolved critical defects prevents assured return even when the service is online.

Decision and authority boundary

A positive grant, renewal or extension requires valid scope, every applicable criterion fulfilled, sufficient usable evidence, closure of every in-scope nonconformity, current competent independent decision authority and effective required permissions. No score, majority vote, membership status or future corrective promise replaces a missing gate. An operational technical release, a programme outcome and an administrative publication are separate actions.

Required record	Capture responsibility
AF-AST-FR-012	Finding, containment and corrective action
AF-AST-FR-016	Suspension, restriction, restoration and withdrawal
AF-AST-FR-026	Digital evidence, incident and recovery
AF-AST-FR-028	Programme change, transition and closure

The performer hands the actual record to the designated owner or reviewer. The receiving function verifies scope, version, usable evidence, open conditions, original dates and the action it may take. Sending an email, completing a form or setting a database flag is not acceptance of that handover.

4 Timing and escalation

Control / source	Trigger and interval	Required response
Critical protection Core 14.2	Recognition of credible concern Immediately	Stop or contain affected work; preserve evidence.
Holder critical notice Core 14.2	Awareness Within 24 hours	Earlier applicable duties remain in force.
Operator critical status action Core 14.2	Substantiated critical concern Within 24 hours	Suspend or independently justified effective restriction.
Assessment and decision records Core 10.6	Last relevant decision At least 7 years	Longer where obligations, life or a hold require; reconcile legally required alternative handling.

Use actual awareness, notification, completion, decision, issue and expiry timestamps with a declared time zone. Days are calendar days unless explicitly stated otherwise. Month intervals end on the corresponding date, or month-end where that date does not exist. Earlier applicable duties prevail. Source: Annex H.

5 Worked application and failure response

Synthetic example: A synthetic restored database contains all expected record counts but links one decision to the wrong configuration. Service availability is restored; evidence integrity is not. Dependent claims stay held until the relationship is corrected and verified.

Before closure, challenge a missing essential input, an expired or conflicted role, wrong configuration, contradictory evidence and an incomplete receiving handover where applicable. Record expected and actual behaviour. A completed synthetic exercise tests reasoning or workflow only; it cannot replace required technical witnessing.

E1 Explicit acceptance and evidence contract

Apply the following logic to the exact evaluated object and responsible function. A procedural checkpoint, product characteristic, competence decision and public credential are different objects. Their states shall not be collapsed into one score. Source: ASTRA 62.1–62.7 and Annex AL.

State	Sufficient basis	Required next action
PASS	Applicable; current approved predicate met by valid, purpose-specific evidence.	Retain the original evidence and bounded inference. Other mandatory gates still apply.
FAIL	Applicable; valid evidence demonstrates that the approved predicate is not met.	Contain affected use; retain the failure; assess cause, extent and required corrective verification.
HOLD	Applicability, criterion, method, evidence, uncertainty or authority is unresolved.	Resolve the missing basis. Do not manufacture a value, favourable default or product-defect conclusion.
N/A	Activity trigger and retained responsibility are absent; independent exclusion approval exists.	Retain the scope-specific reason and reassess when activity or responsibility changes.
UNSET	Only an uncompleted field in this PDF; not a conformity state.	No conclusion is recorded. Complete review before the field can support a decision.

For a compound source clause, create a child-condition ledger containing every separately testable condition, location, phase and operating mode. A sentence-level checkpoint is a navigation aid, not permission to merge unrelated predicates. Each child receives an ID, responsible owner, criterion, method, source evidence, uncertainty where relevant, current state and independent review. The parent cannot PASS while any mandatory child is FAIL, HOLD or UNSET.

An acceptable measurement interval and an acceptable authority chain are independent prerequisites. Use finite, unit-consistent, unrounded values; negative uncertainty, reversed limits, unknown version or wrong-object evidence produce HOLD. For inclusive [L,H] and accepted interval [a,b], PASS requires $a \geq L$ and $b \leq H$; FAIL requires $b < L$ or $a > H$; otherwise HOLD. Approved one-sided or exclusive boundaries retain their own declared predicate.

Positive-decision conjunction

Every applicable mandatory child is PASS AND each N/A is independently justified AND every in-scope nonconformity is verified closed AND scope, competence, independence and actual authority are valid AND required panel participation and voting rules are satisfied. No average, majority preference or payment supplies missing evidence.

E2 Source-to-implementation crosswalk

The references below use the supplied 248-page FIRST EDITION. Each row retains the original clause identifier and source page. The operating instructions in this document elaborate implementation; they do not replace the full source condition or its applicable annexes. A reference to a whole chapter requires selection of every triggered subclause, not only the examples printed here.

ASTRA ID / page	Source subject	Implementation use
10.3 / 21	Digital tools and calculations	Requirement, objective evidence and local child predicates
10.6 / 22	Recovery, retention and closure	Requirement, objective evidence and local child predicates
14.2 / 25	Immediate protection and notifications	Requirement, objective evidence and local child predicates
47.1 / 70	Safety-security dependency analysis	Requirement, objective evidence and local child predicates

ASTRA ID / page	Source subject	Implementation use
47.4 / 71	Connected production and operational technology	Requirement, objective evidence and local child predicates
47.5 / 71	Update trust and cryptographic transition	Requirement, objective evidence and local child predicates
47.6 / 71	Incident recovery and assured return	Requirement, objective evidence and local child predicates
56.4 / 81	Validation and prohibited cases	Requirement, objective evidence and local child predicates
56.5 / 81	Export, migration and meaningful recovery	Requirement, objective evidence and local child predicates
66.7 / 97	Outage, recovery and service evidence	Explicit verification and acceptance predicate
67.6 / 99	Anomaly response and safe restoration	Explicit verification and acceptance predicate
78.5 / 121	Security and trusted updates	Explicit verification and acceptance predicate
78.7 / 121	Recovery and semantic portability	Explicit verification and acceptance predicate
79.3 / 122	Loss of contact and uncertain physical state	Explicit verification and acceptance predicate
79.4 / 122	Affected populations and historical decisions	Explicit verification and acceptance predicate

E3 Detailed operating extensions

AF-AST-PR-020 – Cyber Incidents, Evidence Recovery and Service Continuity

Implementation basis: 10.6 (p. 22); 47.6 (p. 71); 56.4 (p. 81); 56.5 (p. 81); 66.7 (p. 97); 67.6 (p. 99); 78.5 (p. 121); 78.7 (p. 121); 79.3 (p. 122); 79.4 (p. 122)

X20.1 Contain the actual evidence dependency

Identify affected configuration, identities, source records, products, commands and decisions. Preserve raw evidence and isolate tests from live assets.

Completion / hold: Service availability alone does not establish trustworthy operation or exclude impact.

X20.2 Select a recoverable trusted baseline

Record recovery point, accepted schema/configuration, permissions, source links and missing or later events. Preserve the source for reconciliation.

Completion / hold: A backup job success is not acceptance of recoverable semantic evidence.

X20.3 Restore and reconcile meaning

Check record identity, source access, units, event time, versions, relationships, adverse states and independent decision instruments after restoration.

Completion / hold: Equal file counts or application startup cannot close missing relationships; dependent conclusions remain HOLD.

X20.4 Authorise return and remaining restrictions

Obtain technical return authority separately from registry/status decisions, inform affected recipients and retest original failure paths plus regression.

Completion / hold: No retrospective validation of outputs issued while essential integrity was unknown.

Record contract: the actor records the input baseline, actual work, deviations, result and evidence link; the named receiving function acknowledges access and the permitted next action. A returned or incomplete handover retains the original event history. Use the associated FR modules and RG record links; no document or database field confers actual authority.

E4 Application-specific parameter completion

These are required information groups from Annex AO, not pre-approved engineering limits. For every triggered group, populate actual values or observable attributes before evaluation, with unit, inclusivity, phase/mode, technical derivation, uncertainty/dependence, method version, owner, independent review, authentic approval and change trigger. An absent trigger requires an approved exclusion; an unsupported or missing essential value is HOLD.

P01 — Mission and scope

Legal owner, performer, family/module, object, domain, configuration, location, duration and modes.

Derivation and evidence: Scope tuple and mission concept; approved applicability matrix.

Completion test: No undefined essential object, duty, phase or exclusion.

P03 — Requirements and acceptance

Stable ID, owner, characteristic, units, bound inclusivity, predicate, observation and essential-step marker.

Derivation and evidence: Requirement baseline and Annex AL decision rule.

Completion test: Every condition is evaluable before observations are judged.

P11 — Communication and timing

Distance, frequency/wavelength, gain/loss, noise, rate, margin, latency, event time, age, clock error and outage.

Derivation and evidence: Validated end-to-end budget and adverse service tests.

Completion test: Required quality, delay and integrity conditions all pass.

P14 — Software, AI and models

Purpose/domain, source/build/weights/data, dependencies, target, errors, uncertainty, prohibited behaviour and change limits.

Derivation and evidence: Independent verification and model/use validation.

Completion test: Essential scenarios and target conditions pass; experimental outputs remain separate.

P15 — Security and command authority

Identities, roles, privileges, keys/trust, target, validity window, command sequence, integrity and interruption response.

Derivation and evidence: Written test authorisation and deployed workflow validation.

Completion test: No prohibited authority or unverified command state is accepted.

P18 — Decision, continuity and terminal duties

Closed findings, reviewer competence, independence, authority, status clocks, final-state criteria, custody and open obligations.

Derivation and evidence: Authenticated decisions and verified terminal/transfer evidence.

Completion test: Every mandatory gate is complete; incomplete or unknown terminal state remains explicit.

E5 All-space applicability and bounded responsibility

The following Annex AK tags are selected because the document can support these responsibilities. Applicability is decided for the actual case. Tags do not expand a family, create an operating permission or place a whole mission inside a supplier's limited scope. Resolve domain, phase, mode, environment and retained duty before accepting a claim.

Domain / source page	Coverage	Required boundary
AK02 / 187 Test facilities and technical providers	Environmental, structural, materials, calibration and inspection services, including mobile and remote work.	Actual method competence and valid result evidence are separately demonstrated.
AK10 / 189 Constellations and formation services	Distributed functions, inter-satellite links, fleet management and shared ground support.	Distributed performance and independent redundancy assumptions are validated.
AK11 / 189 Orbital traffic and tracking support	Tracking, conjunction information, data services and inter-operator coordination.	A metric is accepted only for its validated data/model scope; missing data are not zero risk.
AK12 / 189 Cooperative docking and servicing	Authorised inspection, connection, transfer, repair and service interventions.	All essential interface and completion states are independently supported.
AK21 / 192 Interplanetary cruise and deep-space missions	Spacecraft, relays, science operations and long-delay mission support.	Human and autonomous actions are feasible within actual timing and resource limits.
AK24 / 192 Interstellar precursor and future distant systems	Bounded research and demonstrable capabilities for very long-range or novel concepts.	Research promise is not an operational grant; unsupported capability stays in development.
AK26 / 193 Planetary protection and sample return	Forward/backward contamination, scientific cleanliness, samples and receiving chain.	No dependent commitment precedes complete protection and receiving evidence.
AK30 / 194 Ground, communication and navigation services	Mission control, RF/optical links, timing, data processing, relays and PNT support.	Availability, correctness, authority and completion are separately demonstrated.
AK31 / 194 Digital and autonomous space systems	Software, programmable hardware, AI, models, twins and defensive security.	All essential behaviours and prohibited transitions are verified for the actual deployment.
AK32 / 194 Retirement and long-term stewardship	Disposal, passivation governance, loss-of-contact states, records and residual obligations.	Final-state claims are truthful and every unresolved duty has an accepted owner.

E6 Workflow and evidence relationships

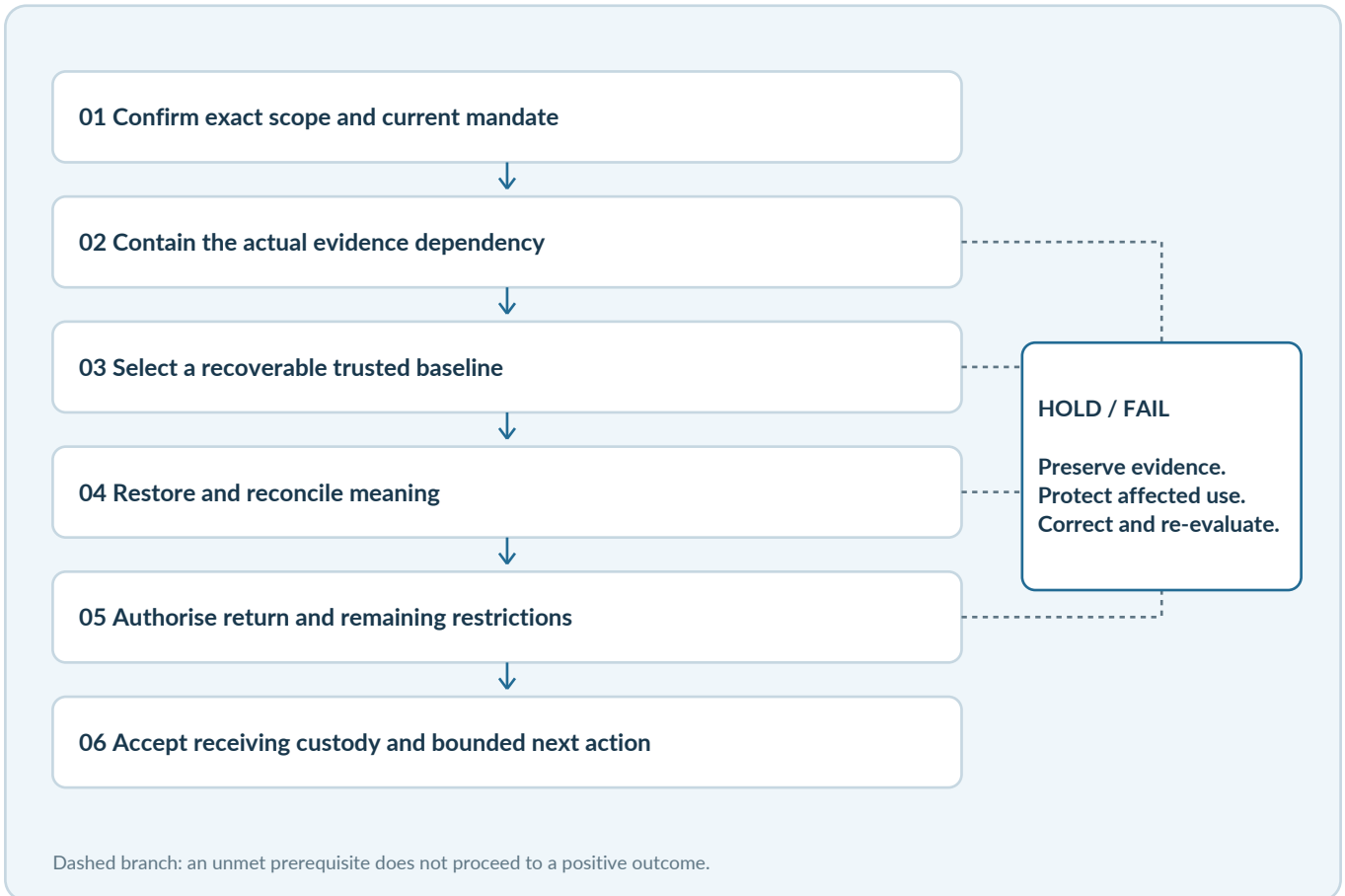
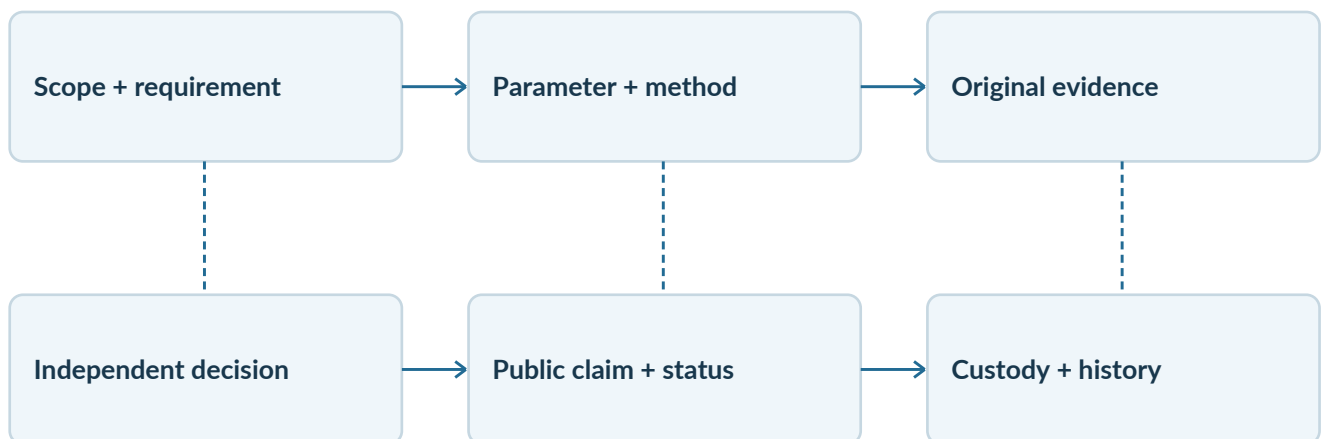


Figure — Implementation sequence for AF-AST-PR-020. Explanatory diagram; the source prerequisites and actual authority remain controlling.



Each relationship carries object identity, controlled version, actual event time and purpose-specific validity.

Figure — Scope-to-custody evidence relationships. A relationship is validated for its decision purpose, not merely because two identifiers exist.

E7 Calculations, assumptions and synthetic charts

The worked calculations below reproduce the supplied standard's Annex AM examples. Charted extensions are newly computed synthetic illustrations of those equations, not measured mission performance or new universal limits. A result is usable only when the actual inputs, model, units, uncertainty and approved application predicate are valid. A successful arithmetic check is not field validation.

AM.Q03 Positive-decision conjunction and essential failure

Source: ASTRA Annex AM, Q03, page 202. All numerical inputs in this example are synthetic.

$$G = S \wedge P \wedge E \wedge F \wedge C \wedge I \wedge A$$

Requirement completion = completed applicable rows / all applicable rows

Variables and units

S=valid scope; P=all predicates passed; E=adequate valid evidence; F=all in-scope findings closed; C=competence; I=independence; A=actual authority.

Example inputs

A synthetic file has 200 applicable rows; 190 are complete. One remaining row concerns an essential protective control. Six other gate groups are true.

Calculation and checks

1. Completion = $190/200 = 0.95 = 95\%$.
2. The unverified essential row makes P false and E false for the requested conclusion.
3. $G = \text{true false false} \dots = \text{false}$.

Decision interpretation: No positive grant. The completion percentage is a planning measure only. A conditional development permission is a separate bounded action, not a conformity certificate.

Validity limits: No averaging, vote or commercial action can change a false mandatory gate. N/A requires independent approval of the absent trigger; it is not a way to remove unfinished work.

ASTRA connections: 15.2; Annex G.1; 62.5; 80

Completion is not the grant decision

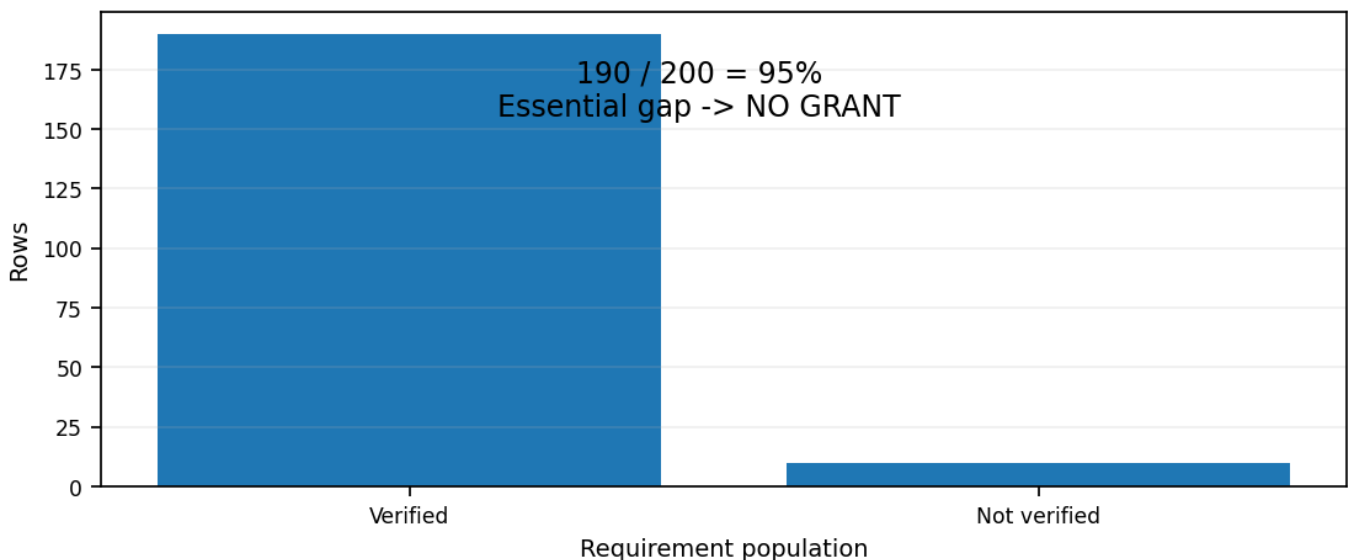


Figure Q03 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

Local replay record: retain the actual input manifest, source versions, calculation version, unit checks, independent recomputation, expected/observed boundary results, limitations and decision authority. Do not overwrite the teaching inputs as though they were operational data.

AM.Q09 Availability is not output correctness

Source: ASTRA Annex AM, Q09, page 208. All numerical inputs in this example are synthetic.

$$A_{\text{observed}} = T_{\text{available}}/T_{\text{window}}$$

$$\text{Correct-service fraction} = T_{\text{available_and_correct}}/T_{\text{window}}$$

Variables and units

All categories shall use the same declared window and explicit downtime and integrity definitions. Missing time is separately recorded.

Example inputs

Synthetic window=1,000 h; available=960 h; unavailable=40 h. Of the available time, 20 h produced unacceptable information.

Calculation and checks

1. Availability = $960/1,000 = 96\%$.
2. Available-and-correct time = $960-20 = 940$ h.
3. Correct-service fraction = $940/1,000 = 94\%$.

Decision interpretation: The 96% availability value does not prove correctness during every available hour. The two measures support different requirements.

Validity limits: The service boundary, outages, correctness test, unknown intervals and planned exclusions must be established in advance. A high uptime percentage cannot close an integrity failure.

ASTRA connections: 51.4; 55.1; 66.7; 78.7

Availability and correct service are different

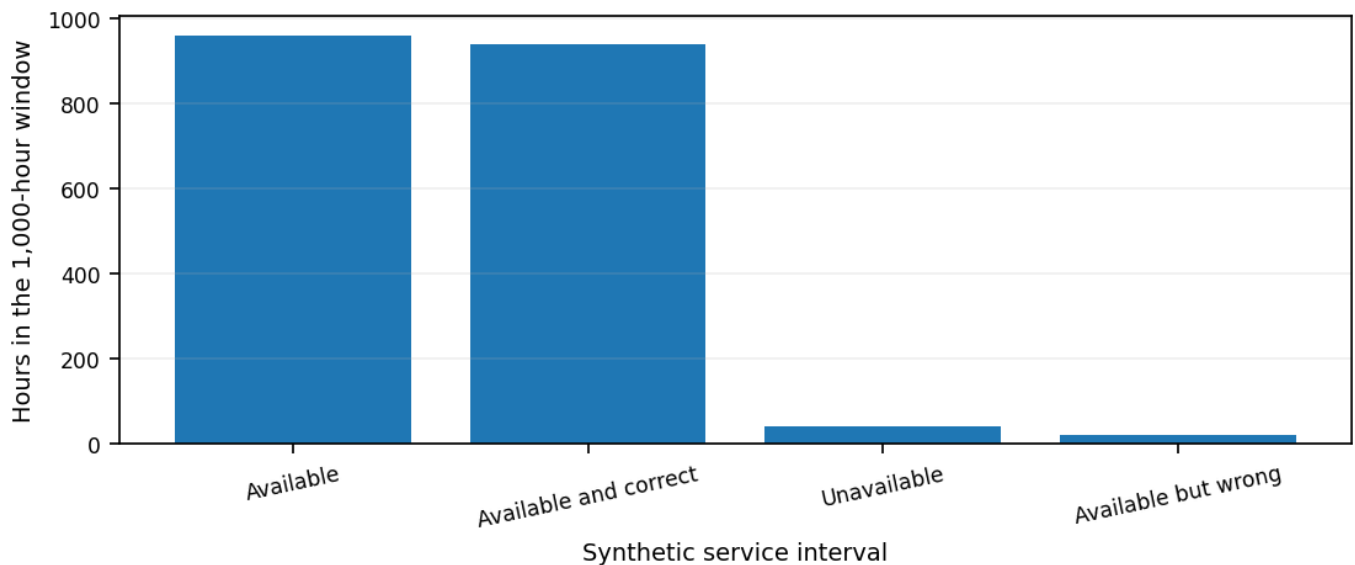


Figure Q09 — Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

Local replay record: retain the actual input manifest, source versions, calculation version, unit checks, independent recomputation, expected/observed boundary results, limitations and decision authority. Do not overwrite the teaching inputs as though they were operational data.

AM.Q16 Outage data storage with overhead

Source: ASTRA Annex AM, Q16, page 215. All numerical inputs in this example are synthetic.

$$B_{\text{required}} = R_{\text{data}} \times t_{\text{outage}} \times f_{\text{overhead}}$$

1 byte = 8 bits

Variables and units

Use a defined payload rate and explicit overhead, reserves and decimal/binary storage conventions. Avoid mixing Mbit/s and MB/s.

Example inputs

Synthetic 2.0×10^6 bit/s, 6 h outage, overhead factor=1.25; usable storage= 64×10^9 bit.

Calculation and checks

1. Outage duration= $6 \times 3,600 = 21,600$ s.
2. Required capacity= $2.0 \times 10^6 \times 21,600 \times 1.25 = 54 \times 10^9$ bit.
3. In decimal bytes this is 6.75×10^9 bytes = 6.75 GB.
4. Headroom= 10×10^9 bit; headroom/required=18.5185185%.

Decision interpretation: The example quantity fits in the stated usable capacity. Data priority, integrity and required extra reserve still need their own criteria.

Validity limits: Do not credit unvalidated compression, unavailable storage blocks or capacity already allocated elsewhere. Tests must include overflow, power interruption, duplicate delivery and recovery.

ASTRA connections: 66.3; 67.4; 78.7

Outage storage including the stated overhead

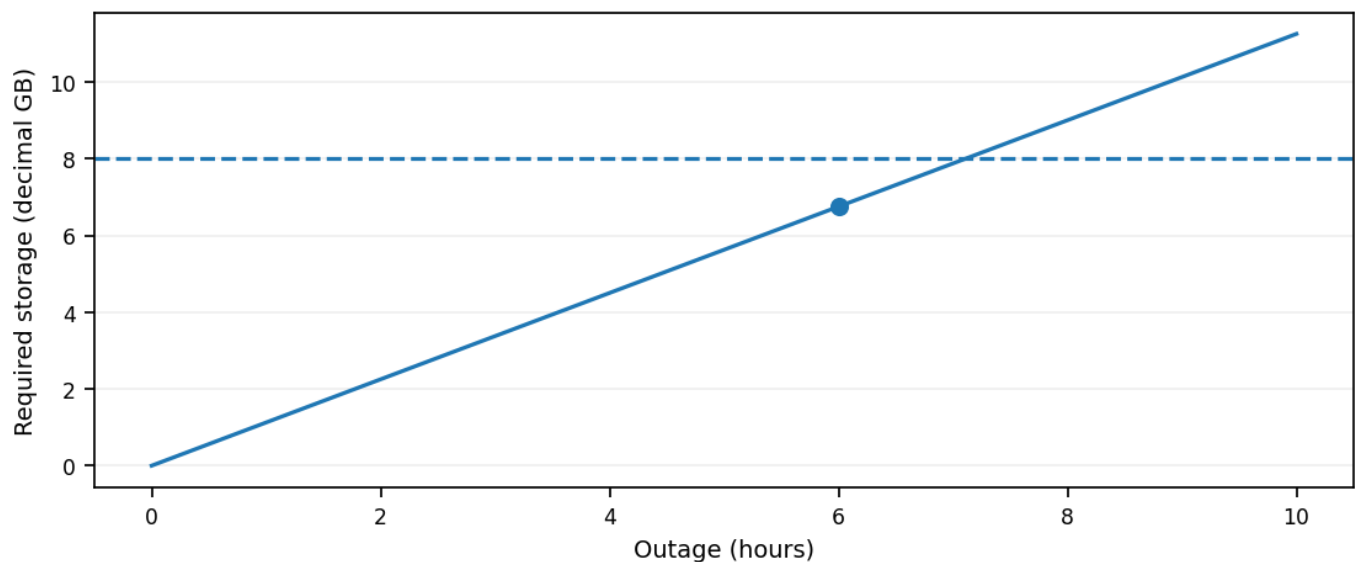


Figure Q16 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

Local replay record: retain the actual input manifest, source versions, calculation version, unit checks, independent recomputation, expected/observed boundary results, limitations and decision authority. Do not overwrite the teaching inputs as though they were operational data.

AM.Q17 Clock uncertainty and maximum data age

Source: ASTRA Annex AM, Q17, page 216. All numerical inputs in this example are synthetic.

$u_t = \sqrt{u_{\text{event}}^2 + u_{\text{sync}}^2}$ for justified independence

$U_t = k u_t$

Upper age endpoint = age_estimate + U_t

Variables and units

Time components refer to the same event and time basis. Correlation and systematic conversion errors require appropriate treatment.

Example inputs

Synthetic standard components 3 ms and 4 ms; illustrative $k=2$; maximum inclusive permitted data age=100 ms.

Calculation and checks

1. $u_t = \sqrt{3^2 + 4^2} = 5$ ms; $U_t = 10$ ms.
2. At age estimate 95 ms, interval=[85,105] ms: HOLD under the full-interval rule.
3. At age estimate 80 ms, interval=[70,90] ms: PASS for this age criterion.

Decision interpretation: A recently received packet can still contain stale event data. The 95 ms estimate is not rounded down into acceptance.

Validity limits: This calculation does not account automatically for unrecorded queueing, an incorrect epoch or an unknown time scale. Such validity defects cause HOLD before the age predicate is evaluated.

ASTRA connections: 66.4; Annex G; 77.6

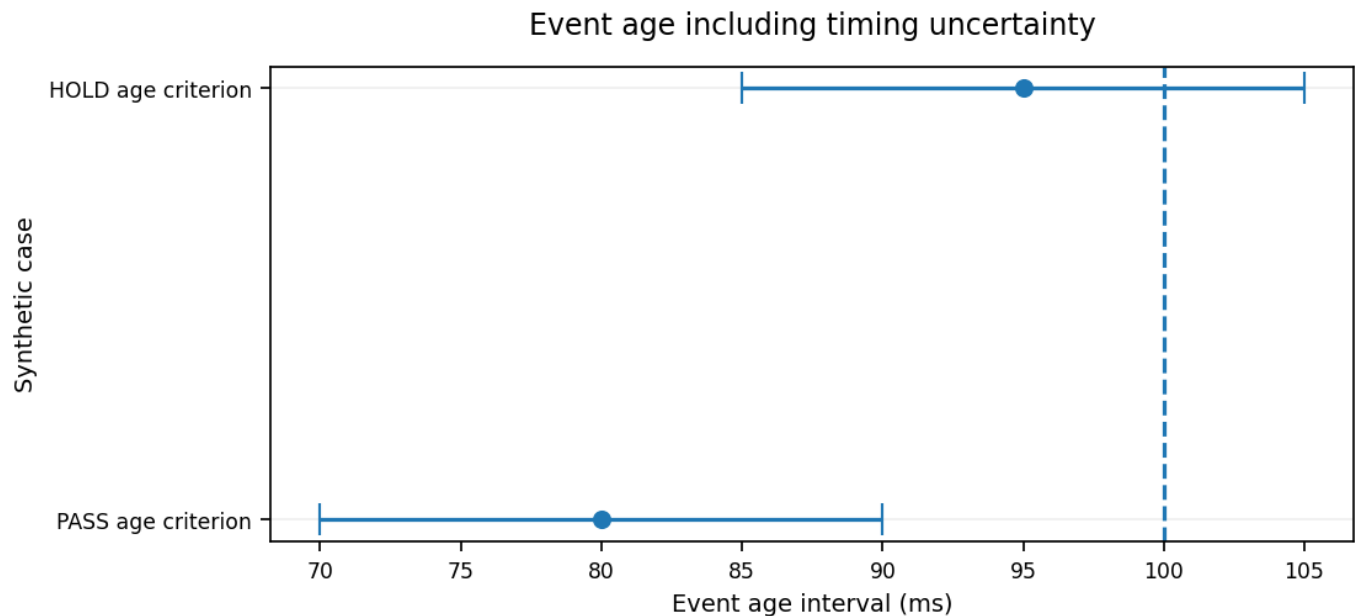


Figure Q17 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

Local replay record: retain the actual input manifest, source versions, calculation version, unit checks, independent recomputation, expected/observed boundary results, limitations and decision authority. Do not overwrite the teaching inputs as though they were operational data.

AM.Q25 Reliability architecture and common-cause sensitivity

Source: ASTRA Annex AM, Q25, page 224. All numerical inputs in this example are synthetic.

$R_{\text{series}} = R_1 R_2$ for independent required elements

$R_{\text{parallel}} = 1 - (1 - R_1)(1 - R_2)$ for independent full-capability alternatives

$R_{\text{with_common_event}} = (1 - q) R_{\text{parallel}}$

Variables and units

R_1 and R_2 refer to the same mission duration and domain. q is an illustrative independent probability of a common event defeating both alternatives. Perfect switching is assumed only for this example.

Example inputs

Synthetic $R_1 = 0.98$, $R_2 = 0.99$; illustrative common-event probability $q = 0.01$.

Calculation and checks

1. Series result $= 0.98 \times 0.99 = 0.9702$.
2. Ideal independent parallel result $= 1 - (0.02 \times 0.01) = 0.9998$.

3. With the stated common event: $0.99 \times 0.9998 = 0.989802$.

Decision interpretation: The architecture and common-dependency assumptions materially change the result. Component figures alone cannot establish system reliability.

Validity limits: Unequal functions, imperfect switching, dormant failures, shared software, maintenance or external resources require a different model. The example probabilities are not actual mission data or prescribed targets.

ASTRA connections: 55.2; 68.1–68.2; 76.5

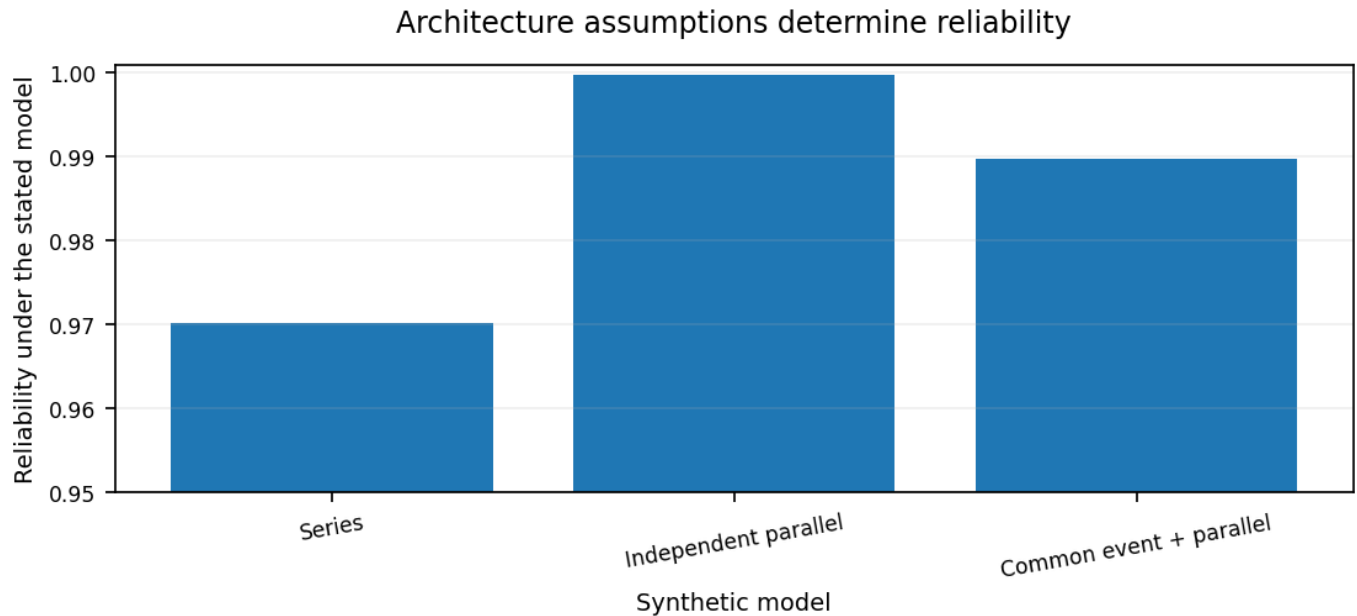


Figure Q25 — Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

Local replay record: retain the actual input manifest, source versions, calculation version, unit checks, independent recomputation, expected/observed boundary results, limitations and decision authority. Do not overwrite the teaching inputs as though they were operational data.

E8 Adverse cases and independent replay

Challenge	Expected handling	Evidence retained
PR-020: Contain the actual evidence dependency — required basis missing	Service availability alone does not establish trustworthy operation or exclude impact.	Original input, unresolved value, affected requirement and scope; named action owner.
PR-020: Authorise return and remaining restrictions — handover or review incomplete	No retrospective validation of outputs issued while essential integrity was unknown.	Expected and observed state; independent replay; correction/retest; receiving acknowledgement.

Before local reliance, also select every relevant AP01–AP48 challenge in the core. Keep fictional tests isolated from live credentials, commands and recipients. For each test define the requirement, precondition, expected response, execution steps, actual observations, evidence, defect consequence, correction, retest and acceptance. This publication supplies test designs and examples, not completed local validation records.

Appendix A — Controlling source requirements

The following text is reproduced from the supplied ASTRA FIRST EDITION. The clause identifier and page refer to that 248-page source. These excerpts and their evidence fields must be read with all triggered normative annexes. Newly authored implementation steps elsewhere in this document do not amend the core standard.

10.3 — Digital tools and calculations

Source: AF-AST-STD-001, page 21.

Validate decision-support tools, spreadsheets, interfaces and automated scoring against their intended use. Test correct, boundary, missing, invalid and prohibited states, including expired authority, a mismatched configuration and an open critical finding. Control versions, formula changes, permissions and deployments. Formula accuracy does not establish input truth or model suitability. The accountable user shall verify the actual dataset and limitation before relying on a computed result.

Required evidence: Tool inventory; known-answer/prohibited-case tests; version approval; input review.

10.6 — Recovery, retention and closure

Source: AF-AST-STD-001, page 22.

Maintain protected backups and test restoration of data, identity, configuration links and current status. Meeting recovery-time objectives does not establish restored evidence integrity. Retain assessment and decision evidence for at least seven years after the last relevant decision, or longer when justified by applicable obligations, service life or a hold; reconcile any legally required alternative handling without concealing the decision basis. Separate unnecessary personal copies and dispose of them under approved controls.

Required evidence: Restore/integrity tests; retention basis; legal holds; secure disposal and closure transfer.

14.2 — Immediate protection and notifications

Source: AF-AST-STD-001, page 25.

Upon a credible critical concern, the responsible organisation shall protect people and affected work immediately, preserve evidence and notify required recipients. A holder shall notify its operator within 24 hours of awareness; earlier applicable duties remain. On a substantiated critical concern, the operator shall suspend the affected status or impose an effective evaluated restriction within 24 hours. An independent duty function with a pre-existing mandate may act urgently, followed by prompt independent review.

Required evidence: Awareness and action times; containment; notification/acknowledgement; status decision.

47.1 — Safety-security dependency analysis

Source: AF-AST-STD-001, page 70.

The organisation shall identify assets, trust boundaries, suppliers, users and interfaces whose loss of integrity, availability, authenticity or confidentiality can affect assured outcomes. Threat and safety analyses shall be coordinated where protective measures can interfere with emergency or degraded operation. Engineering records, machine programmes, maintenance data and product updates shall be included, not only office systems. Assumptions about shared infrastructure and external services shall have named owners and demonstrable controls.

Required evidence: Asset and trust-boundary inventory; joint hazard/threat review; dependency ownership; approved protective controls.

47.4 — Connected production and operational technology

Source: AF-AST-STD-001, page 71.

Connected equipment shall protect authorised machine programmes, process parameters, monitoring data and essential functions. Segmentation, access, backup, monitoring and degraded operation shall be selected according to the actual process risk. Patches and security tools shall be assessed for compatibility with timing, safety and production qualification. When immediate change is inappropriate, a documented compensating-control decision shall have an owner, limits and review. Operational continuity shall not excuse unbounded unsupported risk acceptance.

Required evidence: Operational-technology architecture; authorised configuration; patch review; compensating controls; restoration tests.

47.5 – Update trust and cryptographic transition

Source: AF-AST-STD-001, page 71.

Updates shall verify origin, integrity, authority, compatibility and intended target configuration. The organisation shall control signing and other trust dependencies, key custody, expiry, revocation and migration. A future algorithm transition shall be planned according to product life and actual risk; this standard does not declare a particular algorithm universally suitable. Recovery and rollback shall not silently reintroduce an unacceptable vulnerability. Evidence-preservation needs shall be considered separately from live-system authentication.

Required evidence: Update trust model; key and certificate governance; interruption/rollback tests; migration and archival-validation plan.

47.6 – Incident recovery and assured return

Source: AF-AST-STD-001, page 71.

Incident handling shall preserve evidence, contain affected use, identify impacted products and decisions, notify responsible parties and control restoration. Returning a service to availability shall be separated from verifying its data and configuration integrity. Exercises shall test recovery objectives and the meaning of restored records. Missing original evidence shall remain a gap in the dependent conclusion. An incident closure shall include the actual technical return authority and follow-up actions, not only a completed support ticket.

Required evidence: Incident and affected-output record; integrity checks; recovery exercise; authorised return and continuing actions.

56.4 – Validation and prohibited cases

Source: AF-AST-STD-001, page 81.

Local validation shall cover normal, boundary, missing, invalid and prohibited inputs in the actual deployment. Tests shall include open findings, expired authority, wrong profiles, broken evidence links, suspended status, duplicate imports and interrupted changes. Expected outcomes shall be defined from the controlling requirements before execution. Synthetic fixtures shall be isolated from live claims. Correction shall be followed by repetition of the original failed test and relevant regression, not merely an assurance that the code was changed.

Required evidence: Local validation baseline; expected/observed cases; defect and retest history; actual acceptance and limitations.

56.5 – Export, migration and meaningful recovery

Source: AF-AST-STD-001, page 81.

Transfer shall preserve readable evidence, identities, versions, field semantics, units, time zones, approvals, relationships and current and historical status. Reconciliation shall examine meaning as well as counts; equal file totals may conceal substitutions or missing links. Recovery shall distinguish availability from integrity and reconcile events after the selected recovery point. A sent archive is not accepted custody. The receiving function shall demonstrate usable access and acknowledge continuing duties before dependent cutover.

Required evidence: Export manifest; semantic reconciliation; preserved source; recovery integrity; receiving acceptance and custody.

66.7 – Outage, recovery and service evidence

Source: AF-AST-STD-001, page 97.

The operator shall reconcile lost data, delayed messages, incomplete transfers and state changes after an outage. Recovery shall restore meaning, configuration, authority and history as well as network availability. Report actual service measures with time windows, excluded outages and missing data. A service restoration shall not retrospectively validate dependent decisions made with unavailable or corrupted information.

Verification: Review outage timelines, replay/reconciliation logs and receiving acceptance.

Acceptance / hold rule: All necessary state and data integrity checks are complete before assured use resumes; remaining gaps are carried into the affected claims.

67.6 – Anomaly response and safe restoration

Source: AF-AST-STD-001, page 99.

The operations team shall classify anomalies, preserve raw evidence, control affected commands and follow authorised mission-specific protective procedures. Restoration shall establish current physical and digital state, cause disposition, remaining restrictions and separate technical return authority. A restarted computer or renewed communication link does

not prove that the spacecraft or remote process is safe to resume.

Verification: Examine adverse rehearsals and actual restoration records where available.

Acceptance / hold rule: Required state, integrity and protection checks pass before resumed dependent action; unresolved essential uncertainty retains a restriction.

78.5 – Security and trusted updates

Source: AF-AST-STD-001, page 121.

Protect source, build, machine instructions, operational data, identities and updates according to the actual threat and safety model. Update acceptance shall verify origin, integrity, authority, target, compatibility and interruption behaviour. Reversion to an earlier load shall not reintroduce an unacceptable defect without explicit technical disposition. Security testing requires written safe authorisation.

Verification: Review trust dependencies and execute isolated permitted and prohibited update tests.

Acceptance / hold rule: All required integrity and protective gates pass; a valid signature alone does not establish functional safety or compatibility.

78.7 – Recovery and semantic portability

Source: AF-AST-STD-001, page 121.

Export and recovery shall preserve identities, scope, configuration, evidence states, decisions, history, units, time basis, permissions and relationships. Equal file counts do not establish equal meaning. Reconcile events after the recovery point and obtain receiving acceptance before cutover. Service availability and evidence-integrity acceptance are separate.

Verification: Execute missing-link, wrong-version, interrupted-write, expired-authority and restore tests.

Acceptance / hold rule: All essential records and relationships are usable and correct; unresolved evidence loss keeps dependent decisions on HOLD.

79.3 – Loss of contact and uncertain physical state

Source: AF-AST-STD-001, page 122.

The operator shall define the distinction between missing data, confirmed failure, safe dormant state, lost asset and completed disposition. Preserve last valid observations, their age and uncertainty. The absence of an alarm or signal shall not establish safe state. An inference shall identify its model and limits and shall not be presented as direct observation.

Verification: Review the state-classification record against raw evidence and observability limits.

Acceptance / hold rule: Only a supported state is assigned; uncertain essential conditions retain UNKNOWN in operational records and HOLD in dependent acceptance.

79.4 – Affected populations and historical decisions

Source: AF-AST-STD-001, page 122.

An event shall be traced to affected configurations, fleet members, materials, methods, software, personnel, reports and prior decisions. Determine both occurrence and escape causes and test competing explanations. Changing a supplier, restarting a service or training one person shall not by itself close a shared systemic cause.

Verification: Inspect end-to-end dependency and look-back analysis with actual notifications.

Acceptance / hold rule: All materially dependent outputs are addressed; no valid adverse history is erased by later correction.

Appendix B — Local adoption, validation and receiving acceptance

Gate	Required evidence	Outcome when incomplete
Authority and identity	Actual operator, scoped mandate, permissible result class, named owner, independent decision and remedy functions.	No live scope release.
Requirement population	All applicable clauses and annexes mapped to child conditions, with reasons and independent approval for exclusions.	HOLD the affected conclusion.
Parameters and methods	Prospective values/attributes; technical basis; valid methods; representativeness; calibration, uncertainty and approved predicates.	No dependent acceptance.
People and evidence	Current demonstrated competence; conflict clearance; original usable source evidence; actual configuration and event times.	Reassign or obtain sufficient evidence.
Local tools and tests	Actual deployment tested with positive, boundary, missing, invalid and prohibited inputs; original failed cases retested.	No consequential reliance on unaccepted tools.
Independent closure	Every mandatory requirement PASS, approved N/A, all in-scope nonconformities verified closed, panel rules where required.	No grant, renewal or extension.
Claims and continuity	Decision-linked scope/status; source history; genuine custody, receiving access, retention, urgent notices and terminal duties.	Restrict publication or transfer until resolved.

Record authentic approval and activation in AF-AST-FR-001 and AF-AST-SC-004 or an equivalent controlled record. The edition label is not an effective date for a particular case. Preserve historical decisions under their actual controlling basis; a newer document does not retroactively create missing competence or evidence. Source: Clauses 4, 31, 61, 62 and 80; Annexes P and AR.

PDF recording limits: text fields may scroll beyond their visible area. A printed or flattened copy shall include controlled continuations whenever the full response is not visible. A typed name is not a certificate-based authenticated signature. An actual signed instrument or authenticated workflow shall establish approval. Record custody and privacy are implemented by the receiving organisation, not by this PDF alone.