



ASTRA

AEROSPACE STANDARD

OPERATIONS MANUAL

Registry and Evidence Administration Manual

AF-AST-HB-005

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-HB-005 — Registry and Evidence Administration Manual
Edition and publication date	FIRST EDITION 30 September 2026 English master text
Accountable function	Assurance Programme 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

Administration of source records, evidence-purpose states, relationships, event chronology, decision-linked credentials, public status, access, local tool validation, migration, recovery and custody.

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 Operating model and responsibility	6
Decision and authority boundary	6
2 Case and outcome architecture	7
3 End-to-end operating pathways	7
PR-001 — Document, Record and Version Control	7
PR-004 — Scope Definition, Applicability and Evidence Reuse	8
PR-019 — Privacy, Confidentiality and Controlled Access	8
PR-020 — Cyber Incidents, Evidence Recovery and Service Continuity	9
PR-021 — Credential, Registry and Mark Approval	9
PR-028 — Change, Transition, Transfer and Programme Closure	9
5 Continuing controls and chronology	11
Worked cases and challenge questions	12
Synthetic case — Document, Record and Version Control	12
Synthetic case — Scope Definition, Applicability and Evidence Reuse	12
Synthetic case — Privacy, Confidentiality and Controlled Access	12
Synthetic case — Cyber Incidents, Evidence Recovery and Service Continuity	12
E1 Explicit acceptance and evidence contract	13
E2 Source-to-implementation crosswalk	13
E3 Detailed operating extensions	18
AF-AST-PR-001 — Document, Record and Version Control	18
AF-AST-PR-004 — Scope Definition, Applicability and Evidence Reuse	18
AF-AST-PR-012 — Technical Reporting, Amendments and Report Review	19

AF-AST-PR-019 — Privacy, Confidentiality and Controlled Access	20
AF-AST-PR-020 — Cyber Incidents, Evidence Recovery and Service Continuity	20
AF-AST-PR-021 — Credential, Registry and Mark Approval	21
AF-AST-PR-028 — Change, Transition, Transfer and Programme Closure	21
E4 Application-specific parameter completion	22
P01 — Mission and scope	22
P02 — Environment and exposure	22
P03 — Requirements and acceptance	22
P04 — Geometry and reference systems	22
P06 — Test article and fixtures	22
P07 — Measurement and uncertainty	22
P08 — Structure, life and mechanisms	22
P11 — Communication and timing	22
P13 — Contamination and samples	23
P14 — Software, AI and models	23
P15 — Security and command authority	23
P17 — Logistics and environmental claims	23
P18 — Decision, continuity and terminal duties	23
E5 All-space applicability and bounded responsibility	23
E6 Workflow and evidence relationships	25
E7 Calculations, assumptions and synthetic charts	26
AM.Q01 Measurement uncertainty and covariance	27
AM.Q02 Inclusive limits and four distinct measurement outcomes	28
AM.Q03 Positive-decision conjunction and essential failure	28
AM.Q04 Committee arithmetic and accreditation panels	29
AM.Q06 Random detection sample size	30
AM.Q09 Availability is not output correctness	31
AM.Q16 Outage data storage with overhead	32

AM.Q17 Clock uncertainty and maximum data age	33
AM.Q23 Material genealogy, yield and retained work	34
AM.Q25 Reliability architecture and common-cause sensitivity	35
E8 Adverse cases and independent replay	37
Appendix A – Controlling source requirements	39
Appendix B – Local adoption, validation and receiving acceptance	58

1 Operating model and responsibility

Administration of source records, evidence-purpose states, relationships, event chronology, decision-linked credentials, public status, access, local tool validation, migration, recovery and custody.

Record completeness, source truth, model validity, system validation and an authorised conformity decision are separate achievements. A PDF register records them but is not a deployed automated platform.

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.

Function	Responsibility and boundary
Scheme / institutional authority	Maintains actual instruments, resources, permissible outcomes and scoped delegations; does not order favourable case results.
Programme and case owner	Coordinates live-scope review, assignments, evidence, deadlines, handovers and communications.
Technical specialists and evaluators	Determine method validity and scope coverage, observe actual work, retain adverse evidence and state limitations.
Independent review / decision	Review the versioned dossier and apply every mandatory gate independently of the original evaluation.
Registry / custody	Implement only authenticated decisions, maintain scope and history, control access, retention and usable recovery.
Independent remedies and oversight	Review complaints, appeals, conflicts and operator performance through unimplicated competent functions.

2 Case and outcome architecture

Required identity or field	Content and interpretation
Record ID	Unique persistent identifier; do not reuse a withdrawn or superseded identifier for a different record.
Template / schema version	Identify this form version and any controlled continuation or equivalent record mapping.
Case and evaluated object ID	Connect to the actual application, asset, person, programme, method or statement.
Legal entity and actual performer	Distinguish accountable organisation, issuer, applicant and subcontracted performer.
Family / module and outcome class	Use the retained family/module and correct accreditation, recognition, qualification, certification, verification or validation class.
Scope / technical profile ID and version	Identify the exact version; a title alone is insufficient.
Site / station / delivery mode	Record physical, remote, mobile and partner-delivery boundaries that affect this record.
Configuration / method / statement version	Identify the actual technical baseline and conditions evaluated.
Creation date and time basis	Use the actual creation date; state time zone when a clock or sequence depends on time.
Relevant event / awareness / decision dates	Keep distinct dates separate. Use a linked chronology where more than one event exists.
Accountable author and role	Identify who recorded the information and within which task authority.
Reviewer / approver and authority	Identify the responsible review or approval function; blank does not mean approved.
Evidence references and versions	Link accessible original evidence, including adverse, missing or superseded items.
Record status and purpose	Use the relevant allowed states; evidence status and conformity status are separate.
Access / confidentiality class	Record authorised access; do not put protected operational detail in a public field.
Retention basis / custody / hold	Name the controlling retention rule, custodian and any preservation hold.
Correction / supersession history	Link the original, reason, person, actual date and affected downstream records.

Case progression is enquiry/application, admission, evaluation, review and actual decision. Holder status is separately active, restricted, suspended, expired, withdrawn or a historical instance result. Evidence may be received without being accepted for a purpose. A system must not force missing evidence into “conforming” or “not applicable”.

3 End-to-end operating pathways

PR-001 – Document, Record and Version Control

Trigger: A new document, revised requirement, completed record, correction, import or retirement is proposed.

Classify the object

The Quality Manager identifies whether the item is normative text, implementation guidance, a blank capture tool, a completed record or a public copy. Record its owner, intended users, dependencies and approval path. Do not let a guide or form change a requirement through wording, a default value or a dropdown.

Review before issue

Use technically competent reviewers for the affected subject. Check every internal reference, required field, authority boundary and actual record link. Compare a rendered PDF with its intended content, including tables, formulas, page continuations and form fields. Resolve a defect that could change a decision before dependent issue.

Transfer and retain meaning

Before migration or closure, reconcile record identities, versions, units, timestamps, approvals and relationships. Test retrieval under the receiving permissions. Confirm retention and preservation holds with the receiving custodian. Equal file counts and a successful upload are not acceptance of a complete dossier.

Hold / escalation: A missing source, unresolved changed requirement, unidentified approver or broken evidence relationship prevents the dependent release. Preserve a controlled working copy and assign the exact corrective action.

Record handover: AF-AST-FR-010, AF-AST-FR-026, AF-AST-FR-028.

PR-004 – Scope Definition, Applicability and Evidence Reuse

Trigger: A scope is first defined, an exclusion is proposed, evidence is reused or the requested boundary changes.

Identify the actual decision object

Distinguish the organisation, process window, product configuration, person, educational programme, service capability, assessment body and environmental statement. Record what the receiving user will be entitled to conclude. A brand-wide label cannot replace that decision definition.

Review exclusions substantively

For each claimed non-applicability, establish which activity and retained responsibility are absent and why the desired result remains valid. Small size, budget, another certificate or lack of evidence is not a sufficient exclusion. Refer material exclusions to a competent technical reviewer.

Carry scope through every record

Check the same tuple in the plan, observations, reports, findings, review, decision, certificate instruction and public record. When the scope changes, preserve the earlier request and assessment history. Do not silently remove a failed activity merely to present the remaining work as an unrestricted success.

Hold / escalation: Unclear outcome class, missing configuration, unsupported exclusion or inaccessible essential reused evidence holds the dependent conclusion until an independently reviewable boundary exists.

Record handover: AF-AST-FR-002, AF-AST-FR-003, AF-AST-FR-004, AF-AST-FR-010.

PR-019 – Privacy, Confidentiality and Controlled Access

Trigger: Personal, confidential, proprietary or controlled technical information is collected, accessed, shared, published or retired.

Define the purpose and necessary data

The information owner identifies the decision or obligation the information supports. Collect only necessary fields and source records. Separate personal identifiers, protected technical detail and public scope data. A broad application request is not an unlimited permission to reuse data.

Arrange sufficient protected review

Use authorised reviewers and secure access that permits examination of essential evidence. Redaction must not remove the material needed for the conclusion. Where adequate lawful review is impossible, retain the gap, limit scope or decline the result rather than accept an assertion by reputation.

Respond to incidents and access changes

Contain unauthorised disclosure, preserve logs, determine affected data and decisions and use the applicable notification process. Review privileges promptly when duties end. Verify integrity and receiving authority before restored or transferred records support a conclusion.

Hold / escalation: Unlawful access, excessive disclosure, inadequate protected evidence or unsupported transfer authority holds the affected processing and dependent conclusion.

Record handover: AF-AST-FR-008, AF-AST-FR-010, AF-AST-FR-017, AF-AST-FR-026.

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.

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.

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.

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.

PR-021 – Credential, Registry and Mark Approval

Trigger: An independent result is ready for issue, public status changes or an AF mark/claim is proposed for use.

Accept only an authentic instruction

The Registry Manager verifies the issuer, independent decision authority, actual decision date, reviewed dossier and exact authorised outcome. A prepared certificate template, payment receipt or signed application is not a grant instruction.

Prepare public and protected views

Publish the fields necessary for honest scope verification while protecting detailed configuration, sensitive locations or personal information under approved arrangements. Keep adequate independent evidence access. Applicant and pilot records are not displayed as accredited holders.

Maintain verification during disruption

Provide a controlled alternative status channel during outage, tied to authentic current decisions. Test recovery of scope, restrictions, expiry and history. An unavailable registry does not extend a credential or make a stale cached page authoritative.

Hold / escalation: No authentic decision, mismatched scope, missing mark permission, expired/suspended status or unlawful public disclosure means no affected publication or current mark use.

Record handover: AF-AST-FR-013, AF-AST-FR-014, AF-AST-FR-016, AF-AST-FR-018.

PR-028 – Change, Transition, Transfer and Programme Closure

Trigger: A programme/profile version, transfer, provider cessation, scope withdrawal or closure affects controlled work.

Identify the actual change and boundary

The programme manager states old/new versions, reasons, entities, profiles, locations, methods, configurations and affected stakeholders. Distinguish document version from technical transfer, operating-authority change and complete closure.

Set prospective implementation conditions

Specify actual effective versions, owners, permitted work, prohibited claims, notices, required additional assessment and verification. Do not waive immediate safety duties. Conditions on development progression do not authorise a conformity certificate with unmet mandatory criteria.

Record completion and residual duties

The actual authorised function decides transition, transfer or closure for an exact scope and date. Keep unresolved notifications, warranties, remedies and custody duties assigned. Closing a project or changing an issuer must not erase failure history or imply continuous authority that never existed.

Hold / escalation: Unresolved essential compatibility, missing receiving capability, abandoned learner/customer duties or an incomplete evidence transfer prevents a supported closure or new-scope release.

Record handover: AF-AST-FR-001, AF-AST-FR-012, AF-AST-FR-015, AF-AST-FR-016, AF-AST-FR-018, AF-AST-FR-028.

5 Continuing controls and chronology

Control / source	Trigger and interval	Required response
Ongoing outcome Core 16.1	Independent conformity decision Maximum 24 months	Shorter profile permitted; AF 9100 retains its own controlling rules. Instance results have no invented ongoing validity.
Routine surveillance Core 16.2	Decision / last completed surveillance Maximum 12 months	Complete evaluation; booking is not completion.
High-consequence / novel / integrity exposure Core 16.2	Decision / last completed surveillance Maximum 6 months	Use the shortest triggered interval for inseparable mixed scopes.
Corrective-action plan Core 14.4	Original finding notification 30 calendar days	Immediate protection is separate. Do not reset the original clock.
Major finding closure Core 14.4	Original finding notification 60 calendar days	Verify implementation and effectiveness; review continued conformity immediately.
Minor finding closure Core 14.4	Original finding notification 90 calendar days	All in-scope nonconformities closed before grant, renewal or extension.
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.
Registry status update Core 15.5	Actual status decision Within 2 calendar days	Urgent holder communication does not wait for public update.
Suspension resolution Core 16.5	Suspension decision Maximum 90 calendar days	Restore on evidence, restrict independently unaffected scope or withdraw.
Final evaluation report Core 13.5	Evaluation closure Within 14 calendar days	Explain exceptional delay; existing finding clocks stay unchanged.
Unplanned non-critical material change Core 16.3	Awareness Within 5 calendar days	Expanded claim still requires prior evaluation and decision.
Planned material change Core 16.3	Before implementation / expanded claim Early enough for required prior review	No generic grace period for unassessed scope.
Complaint / appeal acknowledgement Core 27.2	First receipt Within 5 calendar days	Where a reply channel exists; immediate urgent triage.
Control / source	Trigger and interval	Required response
Initial substantive complaint response Core 27.4	First receipt Within 30 calendar days	Not a substitute for immediate protection.
Appeal submission Core 27.3	Notice of contested decision Normally within 30 calendar days	Reasoned good-cause late admission remains available.
Complaint / appeal determination Core 27.4	First receipt Normally within 60 calendar days	Necessary extension: reasons, revised target and progress at least every 30 days.

Control / source	Trigger and interval	Required response
Programme internal audit and formal review Core 29.1; 29.2	Active operation At least annually	Performance and risk reviewed quarterly.
Independent accrediting-operator review Core 29.3	Before launch / last review No more than 36 months	Earlier after serious concerns; no reciprocal self-approval.
Rule/profile suitability review Core 4.6	Issue / last suitability review No more than 3 years	Earlier after material evidence; version is distinct from an interpretation.
Substantive public consultation Core 4.3	Published proposed normative text At least 60 calendar days	Actual comments, dispositions and valid technical approval required.
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.

Worked cases and challenge questions

Synthetic case – Document, Record and Version Control

A fictional report is reissued because the specimen serial was transposed. The custodian retains the original, verifies the correct serial from custody records, reviews any affected conclusion and informs recipients. The reissue date does not become a new test date.

Review challenge: identify the exact affected object, requirement, missing or adverse evidence, accountable action, independent decision and historical record. A fictional example is not a real applicant or evidence of a completed pilot.

Synthetic case – Scope Definition, Applicability and Evidence Reuse

A synthetic component has bench evidence but a new installation changes power and cooling. The unchanged material evidence is reused; installation compatibility remains open and requires new verification. The component result does not become an installed-system result.

Review challenge: identify the exact affected object, requirement, missing or adverse evidence, accountable action, independent decision and historical record. A fictional example is not a real applicant or evidence of a completed pilot.

Synthetic case – Privacy, Confidentiality and Controlled Access

A fictional public registry can show a bounded method description while the detailed configuration is restricted. The independent reviewer still receives legitimate access to the protected dossier. A public redaction does not become a waiver of technical review.

Review challenge: identify the exact affected object, requirement, missing or adverse evidence, accountable action, independent decision and historical record. A fictional example is not a real applicant or evidence of a completed pilot.

Synthetic case – Cyber Incidents, Evidence Recovery and Service Continuity

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.

Review challenge: identify the exact affected object, requirement, missing or adverse evidence, accountable action, independent decision and historical record. A fictional example is not a real applicant or evidence of a completed pilot.

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
1.3 / 10	Object and responsibility tuple	Requirement, objective evidence and local child predicates
1.5 / 11	Activity-based applicability	Requirement, objective evidence and local child predicates
2.1 / 11	Accreditation and competence	Requirement, objective evidence and local child predicates
2.2 / 11	Recognition, qualification and certification	Requirement, objective evidence and local child predicates

ASTRA ID / page	Source subject	Implementation use
2.3 / 11	Verification and validation	Requirement, objective evidence and local child predicates
2.4 / 12	Programme name and public designations	Requirement, objective evidence and local child predicates
2.5 / 12	Evidence, witnessing and technical profile	Requirement, objective evidence and local child predicates
2.6 / 12	Requirement status and uncertainty	Requirement, objective evidence and local child predicates
9.7 / 20	Technical reporting and amendments	Requirement, objective evidence and local child predicates
10.1 / 21	Records and provenance	Requirement, objective evidence and local child predicates
10.2 / 21	Confidentiality, personal data and controlled technology	Requirement, objective evidence and local child predicates
10.3 / 21	Digital tools and calculations	Requirement, objective evidence and local child predicates
10.4 / 21	Artificial intelligence and generated material	Requirement, objective evidence and local child predicates
10.5 / 21	Remote access and live evidence	Requirement, objective evidence and local child predicates
10.6 / 22	Recovery, retention and closure	Requirement, objective evidence and local child predicates
11.3 / 22	Existing evidence and reuse	Requirement, objective evidence and local child predicates
13.5 / 25	Closing and report	Requirement, objective evidence and local child predicates
16.1 / 27	Duration and basis	Requirement, objective evidence and local child predicates
16.2 / 28	Surveillance frequency and coverage	Requirement, objective evidence and local child predicates
16.3 / 28	Material change and notification	Requirement, objective evidence and local child predicates
16.4 / 28	Renewal and interruption	Requirement, objective evidence and local child predicates
16.5 / 28	Suspension, restoration and withdrawal	Requirement, objective evidence and local child predicates
16.6 / 28	Transfer and cessation	Requirement, objective evidence and local child predicates
28.1 / 45	Mandatory scope content	Requirement, objective evidence and local child predicates

ASTRA ID / page	Source subject	Implementation use
28.2 / 46	Truthful public wording	Requirement, objective evidence and local child predicates
28.3 / 46	AF marks and authorised use	Requirement, objective evidence and local child predicates
28.4 / 46	Registry states and authenticity	Requirement, objective evidence and local child predicates
28.5 / 46	Registry security, correction and availability	Requirement, objective evidence and local child predicates
30.2 / 48	Controlled transition	Requirement, objective evidence and local child predicates
30.4 / 48	Scope withdrawal and learner/customer protection	Requirement, objective evidence and local child predicates
31.1 / 48	Minimum records and equivalent systems	Requirement, objective evidence and local child predicates
31.2 / 48	Document hierarchy and phased development	Requirement, objective evidence and local child predicates
31.3 / 49	Actual adoption record	Requirement, objective evidence and local child predicates
31.4 / 49	Implementation and verification	Requirement, objective evidence and local child predicates
31.5 / 49	Review of this edition	Requirement, objective evidence and local child predicates
44.1 / 66	Lifecycle and architectural assurance	Requirement, objective evidence and local child predicates
44.2 / 66	Source, build and loaded configuration	Requirement, objective evidence and local child predicates
44.3 / 67	Verification and target representativeness	Requirement, objective evidence and local child predicates
44.4 / 67	Tool and generated-output reliance	Requirement, objective evidence and local child predicates
44.5 / 67	Release and update integrity	Requirement, objective evidence and local child predicates
44.6 / 67	Long-term support and digital retirement	Requirement, objective evidence and local child predicates
45.1 / 67	Intended use and prohibited use	Requirement, objective evidence and local child predicates
45.2 / 68	Data provenance and evaluation independence	Requirement, objective evidence and local child predicates
45.3 / 68	Performance and uncertainty	Requirement, objective evidence and local child predicates

ASTRA ID / page	Source subject	Implementation use
45.4 / 68	Human oversight and safe fallback	Requirement, objective evidence and local child predicates
45.5 / 68	Release, drift and bounded adaptation	Requirement, objective evidence and local child predicates
45.6 / 68	Assurance decisions remain attributable	Requirement, objective evidence and local child predicates
46.1 / 69	Decision purpose and model authority	Requirement, objective evidence and local child predicates
46.2 / 69	Verification, validation and uncertainty	Requirement, objective evidence and local child predicates
46.3 / 69	Twin synchronisation and stale state	Requirement, objective evidence and local child predicates
46.4 / 69	Replacement or reduction of physical work	Requirement, objective evidence and local child predicates
46.5 / 69	Model-based maintenance and remaining life	Requirement, objective evidence and local child predicates
46.6 / 70	Reproducibility and independent access	Requirement, objective evidence and local child predicates
47.1 / 70	Safety-security dependency analysis	Requirement, objective evidence and local child predicates
47.2 / 70	Identity, access and privileged actions	Requirement, objective evidence and local child predicates
47.3 / 70	Supply-chain and dependency integrity	Requirement, objective evidence and local child predicates
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
56.1 / 80	Distinct entities and authoritative records	Requirement, objective evidence and local child predicates
56.2 / 80	Evidence states and requirement conclusions	Requirement, objective evidence and local child predicates
56.3 / 81	Decision and publication safeguards	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

ASTRA ID / page	Source subject	Implementation use
61.1 / 86	Publication identity	Explicit verification and acceptance predicate
61.2 / 86	Retained text and authored additions	Explicit verification and acceptance predicate
61.3 / 86	Dependent documents and compatibility	Explicit verification and acceptance predicate
61.4 / 86	Actual approval and activation	Explicit verification and acceptance predicate
61.5 / 87	Correction, custody and file integrity	Explicit verification and acceptance predicate
62.1 / 88	Atomic requirement record	Explicit verification and acceptance predicate
62.3 / 88	Evidence validity before conformity	Explicit verification and acceptance predicate
62.4 / 88	Four requirement states	Explicit verification and acceptance predicate
62.5 / 89	No compensation or favourable default	Explicit verification and acceptance predicate
62.7 / 89	Decision replay and consistency	Explicit verification and acceptance predicate
63.1 / 90	Domain selection without geographic omission	Explicit verification and acceptance predicate
63.2 / 90	Object and activity rather than a universal label	Explicit verification and acceptance predicate
63.3 / 90	Environment, phase and mode matrix	Explicit verification and acceptance predicate
63.6 / 91	Interface and lifecycle closure	Explicit verification and acceptance predicate
64.5 / 92	Heritage and similarity	Explicit verification and acceptance predicate
65.6 / 95	Payload function and scientific or service output	Explicit verification and acceptance predicate
66.7 / 97	Outage, recovery and service evidence	Explicit verification and acceptance predicate
67.1 / 98	Configuration and operational baseline	Explicit verification and acceptance predicate
67.3 / 98	Receipt, execution and completion	Explicit verification and acceptance predicate
67.6 / 99	Anomaly response and safe restoration	Explicit verification and acceptance predicate
68.7 / 101	Status and long-term custody	Explicit verification and acceptance predicate
73.7 / 111	Medical capability and health-data boundaries	Explicit verification and acceptance predicate
74.4 / 112	Sample identity and custody	Explicit verification and acceptance predicate
74.6 / 113	Anomalies, unknown state and release of information	Explicit verification and acceptance predicate
74.7 / 113	Disposition and residual responsibility	Explicit verification and acceptance predicate
75.7 / 115	Handover, resource claims and closure	Explicit verification and acceptance predicate
77.5 / 118	Original data and invalid tests	Explicit verification and acceptance predicate
77.8 / 119	Independent campaign closure	Explicit verification and acceptance predicate
78.3 / 120	Evaluation data and model credibility	Explicit verification and acceptance predicate
78.5 / 121	Security and trusted updates	Explicit verification and acceptance predicate

ASTRA ID / page	Source subject	Implementation use
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
79.5 / 122	Terminal evidence and responsible transfer	Explicit verification and acceptance predicate
80.1 / 124	One complete application schedule	Explicit verification and acceptance predicate
80.2 / 124	Domain and verification completeness	Explicit verification and acceptance predicate
80.4 / 124	Bounded claim and publication	Explicit verification and acceptance predicate
80.5 / 124	Continuing conformity and change	Explicit verification and acceptance predicate

E3 Detailed operating extensions

AF-AST-PR-001 – Document, Record and Version Control

Implementation basis: 56.1 (p. 80); 56.2 (p. 80); 56.5 (p. 81); 61.1 (p. 86); 61.3 (p. 86); 62.1 (p. 88); 62.7 (p. 89); 78.7 (p. 121); 80.4 (p. 124)

X01.1 Freeze the publication and requirement baseline

The custodian records document code, edition identity, file digest, controlled version, approved applicability and the exact source clause. Keep the public FIRST EDITION label separate from mutable technical configuration and actual approval events.

Completion / hold: PASS requires a uniquely retrievable source and an authorised effective version; a matching filename is insufficient.

X01.2 Reconcile corrected and superseded records

Keep original values, reason, author, event time, receiving acknowledgement and all dependent requirement links. Assess whether changing text, units, relationships or a drawing invalidates earlier decisions.

Completion / hold: HOLD applies when the earlier decision cannot be reconstructed or a required original is inaccessible.

X01.3 Prove semantic transfer

Compare record identities, field meaning, units, configurations, attachments, permissions and adverse status before retiring the source system. Reconcile later events after the selected recovery point.

Completion / hold: Matching counts without matching identities and meanings fails transfer acceptance.

X01.4 Issue and withdraw controlled copies

Notify affected users of actual changes, retain the prior edition basis and remove only unapproved current-use claims. Do not backdate implementation from the printed publication date.

Completion / hold: Release needs authentic authority, a complete distribution record and tested retrieval of both current and historical evidence.

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.

AF-AST-PR-004 – Scope Definition, Applicability and Evidence Reuse

Implementation basis: 1.3 (p. 10); 1.5 (p. 11); 11.3 (p. 22); 62.1 (p. 88); 62.4 (p. 88); 63.1 (p. 90); 63.3 (p. 90); 63.6 (p. 91); 64.5 (p. 92); 80.1 (p. 124); 80.2 (p. 124)

X04.1 Resolve every applicable domain

Compare the mission concept with AK01-AK32 and the actual activity with F01-F08. Record each phase, mode, duration, interface and retained responsibility.

Completion / hold: Unknown applicability is HOLD; absent equipment or budget never establishes N/A.

X04.2 Establish a defensible similarity argument

Compare object identity, design, sources, environment, software, prior exposure and observability. Assign reused evidence to specific unchanged requirements only.

Completion / hold: Every material difference has accepted new evidence or an explicitly limited conclusion.

X04.3 Maintain separate outcome tuples

A combined case may share provenance and visits but keeps separate methods, criteria, sites, instances, reviewers and independent decisions.

Completion / hold: No shared dossier creates a blanket mission, tenant, supplier or fleet approval.

X04.4 Approve exclusion and re-open triggers

An independent technical reviewer checks the absent trigger and retained duty, names the supported excluded boundary and records conditions that would re-open it.

Completion / hold: Only independently justified exclusions receive N/A; an unexamined consequential interface remains HOLD.

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.

AF-AST-PR-012 – Technical Reporting, Amendments and Report Review

Implementation basis: 9.7 (p. 20); 13.5 (p. 25); 28.1 (p. 45); 62.3 (p. 88); 62.4 (p. 88); 65.6 (p. 95); 67.3 (p. 98); 74.6 (p. 113); 77.5 (p. 118); 77.8 (p. 119); 80.4 (p. 124)

X12.1 Reconcile output identity and basis

Confirm actual item, configuration, method, site, period, performer, conditions, raw evidence, corrections and authorised signatory.

Completion / hold: A report title or customer description cannot substitute for verified identity and scope.

X12.2 Separate observed result from interpretation

Label measured, model-derived, declared and unknown information; state uncertainty, detection/access limits and the justified population.

Completion / hold: Qualification, provider competence, scientific inference and operational permission are not interchangeable report conclusions.

X12.3 Control adverse and amended reports

Keep earlier issued versions, exact correction reason, affected characteristics, original failures and recipients who may have relied on them.

Completion / hold: A replacement favourable report cannot erase a valid adverse result or make a missing observation contemporaneous.

X12.4 Review publication against authority

Compare report, scope schedule, registry and public claim with the actual independent decision. Use the printed edition date only as publication identity.

Completion / hold: Every communicated result retains its actual event history and no unsupported broader scope.

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.

AF-AST-PR-019 – Privacy, Confidentiality and Controlled Access

Implementation basis: 10.2 (p. 21); 10.6 (p. 22); 62.3 (p. 88); 67.1 (p. 98); 73.7 (p. 111); 74.4 (p. 112); 78.3 (p. 120); 78.7 (p. 121); 80.4 (p. 124)

X19.1 Classify purpose and necessary data

Define why each technical, personal or controlled item is needed, who may use it and which public representation is sufficient.

Completion / hold: Collecting more sensitive material than needed is not a substitute for better technical evidence.

X19.2 Verify actual access rights

Assign person and service identities, role, scope, event-time authority, permitted transfer and expiry. Control emergency access with attribution and review.

Completion / hold: A shared credential or later permission cannot authenticate an earlier unapproved action.

X19.3 Enable sufficient protected technical review

Provide a lawful detailed or appropriately redacted review path without making essential evidence inaccessible to the competent reviewer.

Completion / hold: HOLD or limit the result when sufficient independent review cannot be achieved; secrecy is not a favourable default.

X19.4 Preserve custody and authorised disposal

Retain necessary originals, record legal/technical holds, test recovery and obtain receiving acceptance at transfer. Separate unnecessary personal copies from decision evidence.

Completion / hold: Disposal cannot conceal a required historical decision basis or erase unresolved access and correction duties.

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.

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.

AF-AST-PR-021 – Credential, Registry and Mark Approval

Implementation basis: 28.1 (p. 45); 28.2 (p. 46); 28.3 (p. 46); 28.4 (p. 46); 28.5 (p. 46); 56.3 (p. 81); 62.5 (p. 89); 63.2 (p. 90); 80.4 (p. 124)

X21.1 Reconcile credential instruction to the decision

Verify exact holder, issuer, outcome class, object, configuration, family/module, domain/site, criteria and genuine dates.

Completion / hold: A profile title or cover image does not authorise a wider claim.

X21.2 Maintain independent state domains

Keep application, evidence acceptance, technical requirement state, credential status, operational asset state and mark permission distinct.

Completion / hold: Received or reviewed evidence cannot automatically become PASS or an active credential.

X21.3 Control artwork and public projection

Use approved AF artwork, legible identifiers and precise scope wording; provide sufficient public boundaries without disclosing protected detail.

Completion / hold: Public text must not imply unassessed all-space coverage, governmental permission or unevidenced recognition.

X21.4 Test correction and adverse events

Challenge expired/suspended reprints, stale imports, duplicate identities, missing decisions and pending appeals. Retain history and timely notices.

Completion / hold: Only an authentic authorised decision changes status; a new file date never revives authority.

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.

AF-AST-PR-028 – Change, Transition, Transfer and Programme Closure

Implementation basis: 30.2 (p. 48); 30.4 (p. 48); 31.3 (p. 49); 56.5 (p. 81); 61.3 (p. 86); 62.7 (p. 89); 68.7 (p. 101); 74.7 (p. 113); 75.7 (p. 115); 78.7 (p. 121); 79.5 (p. 122); 80.5 (p. 124)

X28.1 Map the complete change population

Identify affected requirements, profiles, objects, configurations, sites, people, calculations, fields, interfaces and public claims.

Completion / hold: A cosmetic filename or edition-label change cannot hide a changed technical basis.

X28.2 Establish retained and additional evidence

Record what remains valid, what is invalidated, required new demonstration, compatible tools and actual competence. Keep mandatory protective duties active during transition.

Completion / hold: No automatic grandfathering, retrospectively applied requirement or unsupported transfer of scope.

X28.3 Accept custody and local implementation

Reconcile semantic records, permissions, actual receiving capability, remaining learners/customers, open cases, notices and independent decisions.

Completion / hold: Sending an archive or signing a commercial handover does not establish accepted technical custody.

X28.4 Close without abandoning terminal duties

Preserve unknown final states, original status gaps, hazardous inventories, unresolved remedies and actual receiving owners.

Completion / hold: Only demonstrably complete obligations are closed; remaining duties stay assigned after programme or provider cessation.

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.

P02 — Environment and exposure

Quantity, spatial/temporal boundary, distribution or bound, source/model, uncertainty and coupled effects.

Derivation and evidence: Mission environment baseline and qualified specialist rationale.

Completion test: Selected conditions bound each claimed use; unknown critical mechanisms remain HOLD.

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.

P04 — Geometry and reference systems

Frame origin/orientation, epoch, time scale, coordinate units, transformation and covariance.

Derivation and evidence: Validated transformation and independent known-answer checks.

Completion test: Correct frame and time are maintained through every interface.

P06 — Test article and fixtures

Article pedigree, differences from delivered object, mounting, boundary conditions, operating state and exposure history.

Derivation and evidence: Approved representativeness and cumulative-test analysis.

Completion test: No material difference or prior damage invalidates the intended inference.

P07 — Measurement and uncertainty

Measurand, instrument/range, corrections, sensitivity, covariance, coverage, time/space sampling and calibration.

Derivation and evidence: Complete measurement model; valid raw data.

Completion test: Uncertainty and detection capability are fit for the approved decision rule.

P08 — Structure, life and mechanisms

Loads, allowables, factors, life, geometry, material state, mechanisms, detectability and approved reserve.

Derivation and evidence: Qualified structural/life model and representative evidence.

Completion test: Each prospectively defined margin and essential mechanism predicate passes.

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.

P13 – Contamination and samples

Relevant substances/particles, pathway, limit, method/detection, custody, cleanliness, containment and receiving.

Derivation and evidence: Mission-specific technical/protection basis.

Completion test: Required integrity and scientific cleanliness are demonstrated for the actual sample/use.

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.

P17 – Logistics and environmental claims

Identity, amount, units, condition, losses, allocation, lifecycle boundary, factor provenance and exclusive attributes.

Derivation and evidence: Reconciled custody/quantity records and separate suitability/statement evaluation.

Completion test: Quantity and claim integrity pass independently of technical eligibility.

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
AK01 / 187 Terrestrial engineering and supply	Design offices, manufacturing, material sources, procurement and integration.	Every delivered characteristic and essential supplier interface is traceable to accepted evidence.
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.
AK03 / 187 Launch sites and spaceports	Site infrastructure, handling, ground services, emergency interfaces and actual permissions.	No site outcome is used as vehicle, launch or mission permission.
AK04 / 187 Launch and deployment interfaces	Vehicle/payload integration, handling, ascent environment, separation and commissioning.	Every required integration and protective condition is met before the actual commitment.

Domain / source page	Coverage	Required boundary
AK05 / 188 Reusable launch and return articles	Cumulative exposure, refurbishment, thermal protection, hidden damage and life decisions.	Reuse is based on actual history and accepted condition, never a reset life.
AK06 / 188 Low Earth orbit systems	Satellites, stations and services in the declared near-Earth operating environment.	Environment-specific qualification and end-of-life capability support the bounded mission.
AK07 / 188 Medium, geosynchronous and high Earth orbits	Navigation, communication, relay and other specified orbit-dependent services.	No lower-orbit or nominal-link evidence automatically covers a different environment.
AK08 / 188 Highly elliptical and transfer regions	Missions crossing materially different exposure, geometry and communication regimes.	Every phase and transition has a supported envelope and verification path.
AK09 / 189 Cislunar and libration-region systems	Lunar vicinity, relays, gateways, transportation interfaces and regional services.	The exact operating domain and service dependencies are technically complete.
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.
AK13 / 190 On-orbit assembly and manufacture	Assembly, additive or other production, finishing and output verification in space.	Process execution is not substituted for evidence of required output properties.
AK14 / 190 Stations and inhabited orbital platforms	Habitation, payload integration, visiting vehicles, occupants and support.	Integrated human protection and resources are accepted independently of mission success.
AK15 / 190 Extravehicular and isolated crew work	Individual equipment, user/task, environment, support and rescue dependencies.	Essential individual and integrated protective tasks pass without averaging.
AK16 / 190 Lunar surface systems	Landers, rovers, infrastructure, observation and processing on the Moon.	Destination-specific evidence bounds the actual region, phase and operating mode.
AK17 / 191 Planetary landers and surface vehicles	Surface exploration, scientific instruments, mobility and handling.	Terrestrial analogy is justified; unknown critical surface conditions remain restricted.
AK18 / 191 Atmospheric and buoyant exploration	Planetary atmospheric vehicles, balloons, aircraft and relevant instruments.	All relevant environment-specific structural and functional predicates pass.
AK19 / 191 Small-body and comet operations	Observation, cooperative contact, sampling and resource demonstrations.	Uncertain body/interaction properties are not treated as established terrestrial conditions.
AK20 / 191 Subsurface and ocean-world exploration	Subsurface, liquid, ice and extreme-pressure exploration systems and their interfaces.	Specialist boundary and contamination evidence precedes dependent use.
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.
AK22 / 192 Solar and heliophysics missions	Solar observations and missions with relevant thermal, plasma and radiation extremes.	Protection and data-quality evidence cover the actual mission envelope, not a screening equation alone.

Domain / source page	Coverage	Required boundary
AK23 / 192 Outer-system and distant observatories	Low-flux, long-life, long-delay science and infrastructure applications.	Required lifetime and survival margins are met with credible continuity and data integrity.
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.
AK25 / 193 Human exploration and surface habitats	Crew transport interfaces, habitation, exploration support and emergency protection.	Every essential human protection and feasibility predicate is supported by specialists.
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.
AK27 / 193 Resource utilisation and remote processing	Resource characterisation, processing, quality, storage, use and residues.	Resource yield, product eligibility and permission remain distinct.
AK28 / 193 Space logistics and distributed supply	Warehousing, transfer, spares, custody, condition, receiving and service continuity.	Only physically or otherwise validly confirmed accepted usable inventory supports mission budgets.
AK29 / 194 Specialised energy infrastructure	Generation, storage, conversion, remote delivery and controlled high-hazard power interfaces.	Performance never substitutes for safety, source authority or terminal accountability.
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

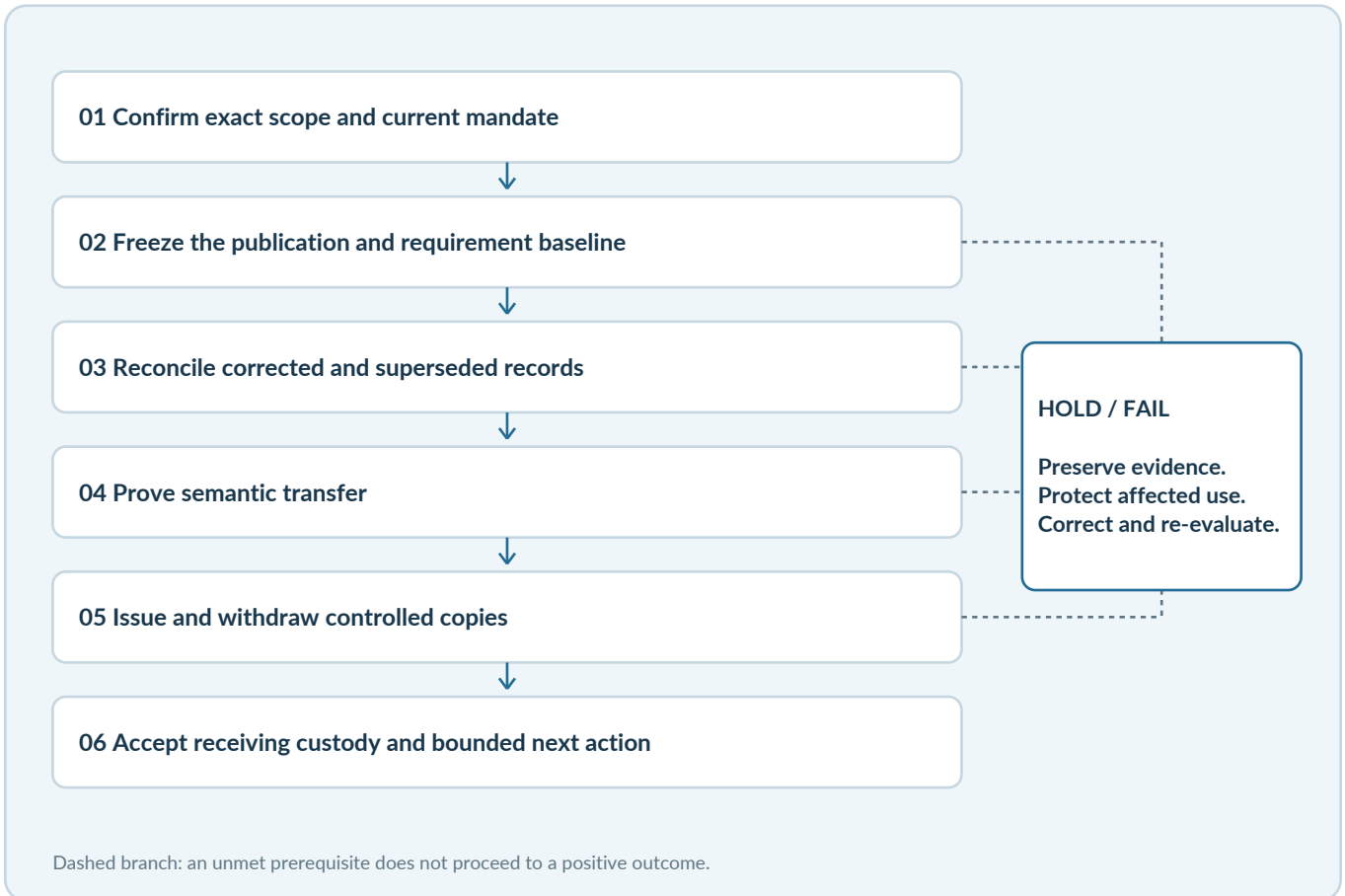
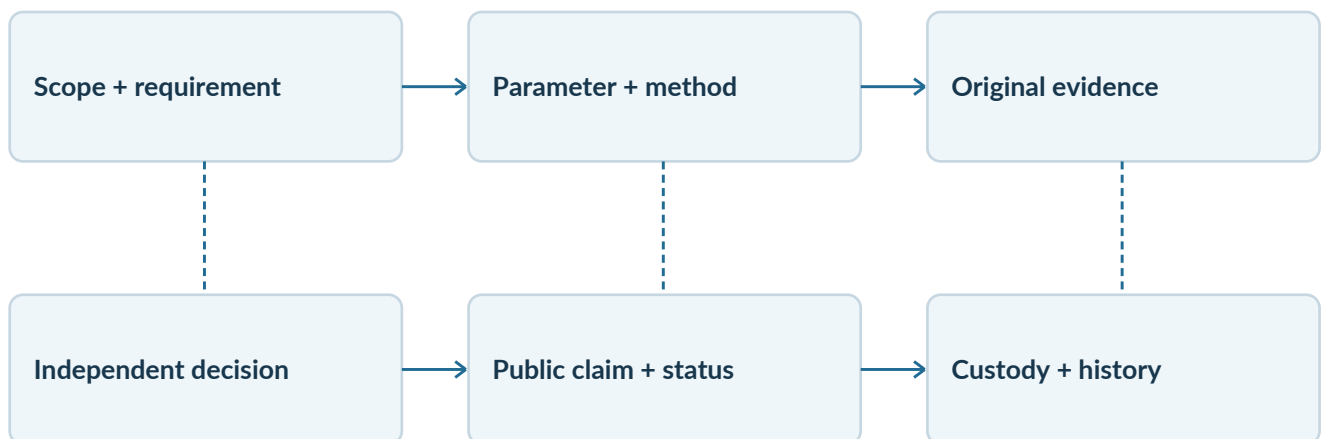


Figure — Implementation sequence for AF-AST-PR-001. Explanatory diagram; the source prerequisites and actual authority remain controlling.



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.Q01 Measurement uncertainty and covariance

Source: ASTRA Annex AM, Q01, page 200. All numerical inputs in this example are synthetic.

$$u_c^2 = \sum (c_i^2 u_i^2) + 2\sum (i < j) (c_i c_j \text{cov}_{ij})$$

$$U = k u_c$$

Variables and units

u_i is a standard uncertainty; c_i is a sensitivity coefficient; cov_{ij} is covariance; k is the justified coverage factor. Variance terms carry squared output units.

Example inputs

Synthetic direct sum: $c_1=c_2=1$; $u_1=0.003$ mm; $u_2=0.004$ mm. First assume independence, then correlation $\rho=0.5$. Illustrative $k=2$.

Calculation and checks

1. Independent variance = $0.003^2 + 0.004^2 = 0.000025$ mm².
2. $u_c = 0.005$ mm; $U = 0.010$ mm for the stated k .
3. Correlated covariance = $0.5 \times 0.003 \times 0.004 = 0.000006$ mm².
4. Correlated variance = $0.000025 + 2 \times 0.000006 = 0.000037$ mm².
5. Correlated $u_c = 0.0060827625303$ mm; $U = 0.0121655250606$ mm.

Decision interpretation: The correlated model produces a larger uncertainty. No PASS/FAIL follows until an approved specification and decision rule are applied.

Validity limits: The linear propagation model requires a valid measurement function and adequate approximation. $k=2$ is not a universal guarantee of 95% coverage. Known bias requires correction or explicitly justified treatment; uncertainty does not conceal missing requirements.

ASTRA connections: 9.4–9.5; Annex G; 62; 77

Standard and expanded uncertainty

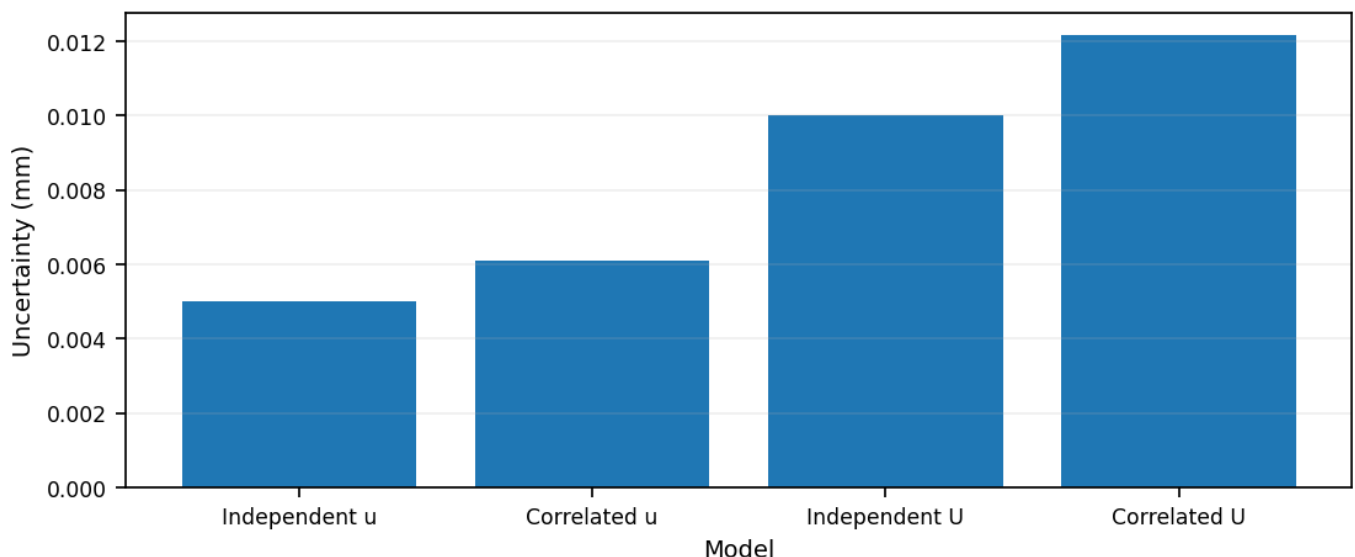


Figure Q01 — Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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.Q02 Inclusive limits and four distinct measurement outcomes

Source: ASTRA Annex AM, Q02, page 201. All numerical inputs in this example are synthetic.

PASS: $y - U \geq L$ AND $y + U \leq H$

FAIL: $y + U < L$ OR $y - U > H$

Otherwise: HOLD; invalid evidence also results in HOLD

Variables and units

L and H are inclusive specification limits; y is a corrected result; U is a non-negative expanded uncertainty with stated coverage.

Example inputs

Synthetic specification [49.970, 50.030] mm; U=0.004 mm. Results y=50.024, 50.028, 50.036 and 50.026 mm.

Calculation and checks

1. $50.024 \pm 0.004 \rightarrow [50.020, 50.028]$ mm: PASS.
2. $50.028 \pm 0.004 \rightarrow [50.024, 50.032]$ mm: HOLD, interval overlaps the upper limit.
3. $50.036 \pm 0.004 \rightarrow [50.032, 50.040]$ mm: FAIL, interval entirely above the limit.
4. $50.026 \pm 0.004 \rightarrow [50.022, 50.030]$ mm: PASS; equality is inside the inclusive upper bound.

Decision interpretation: Neither the overlapping interval nor an invalid run is rounded into acceptance. N/A is an applicability decision, not a measurement outcome.

Validity limits: Use actual endpoints for asymmetric intervals. For an upper-only limit, PASS requires the upper endpoint at or below the limit and FAIL the lower endpoint above it. A coverage interval is not automatically a probability that this particular item conforms.

ASTRA connections: Annex G; 62.3–62.5; 77.6

Inclusive full-interval decisions

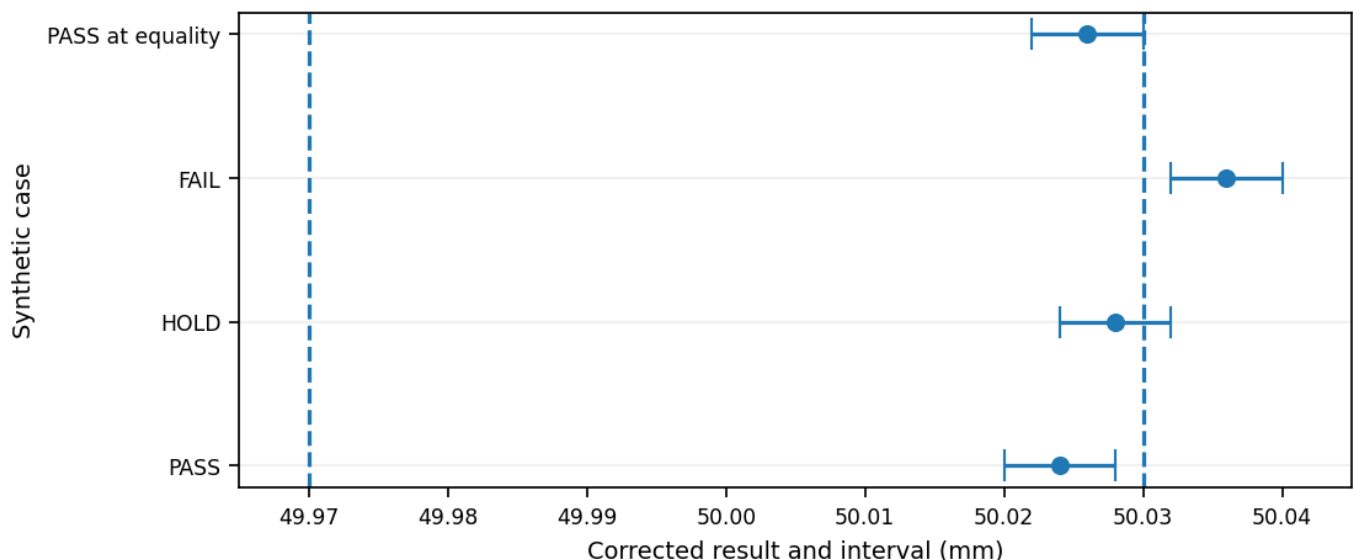


Figure Q02 — Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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.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

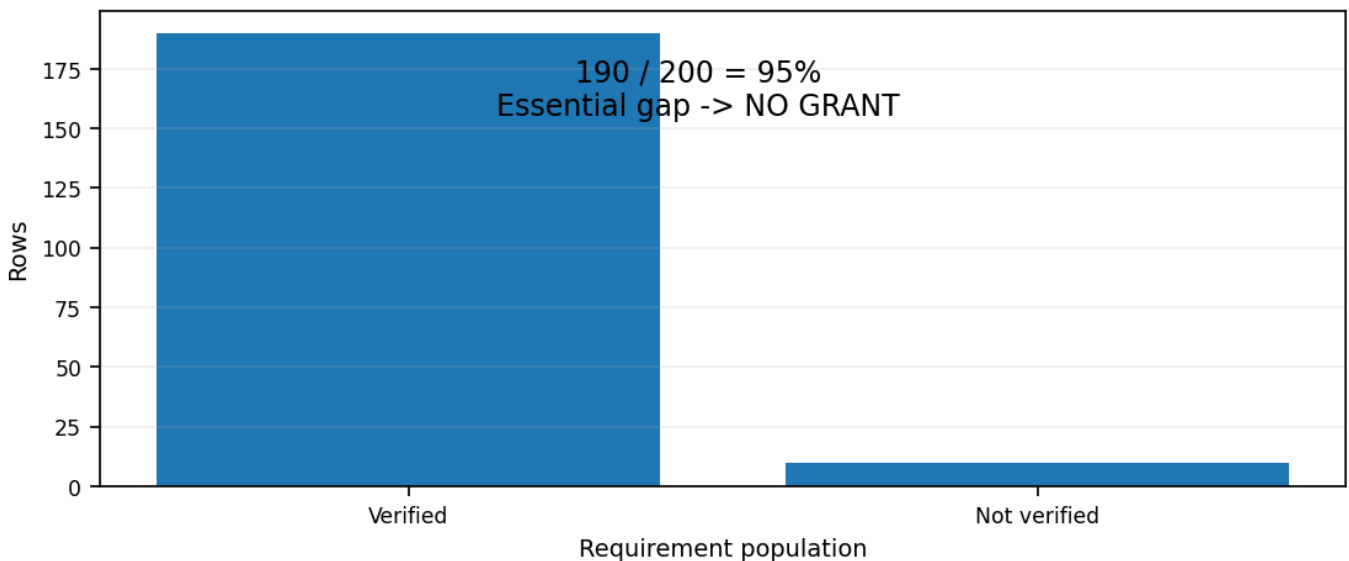


Figure Q03 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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.Q04 Committee arithmetic and accreditation panels

Source: ASTRA Annex AM, Q04, page 203. All numerical inputs in this example are synthetic.

Substantive participation minimum = $\text{ceil}(2N/3)$

Affirmative minimum = $\text{ceil}(2V/3)$

Variables and units

N is the eligible committee population; V is the number of substantive yes/no votes. These equations concern the technical committee, not an applicant panel.

Example inputs

Synthetic committee: N=9, V=6, yes=4, no=2. Separate accreditation panel: three eligible members, two affirmative and one adverse.

Calculation and checks

1. Participation: $\text{ceil}(2 \times 9/3) = 6$; actual V=6 meets it.
2. Affirmative: $\text{ceil}(2 \times 6/3) = 4$; actual yes=4 meets it.
3. Accreditation panel: all three must participate; at least two support and all technical gates must pass.
4. Two participating panel members voting yes do not form a valid three-person panel.

Decision interpretation: The committee arithmetic passes for the stated case. The separate panel can decide positively only if technical gates and eligibility are all established.

Validity limits: Abstentions are not substantive committee yes/no votes. Rounding is upward. A mathematical majority never resolves missing technical evidence or an ineligible member.

ASTRA connections: 3.4; 4.3; 15.3; Annex B

Committee participation threshold

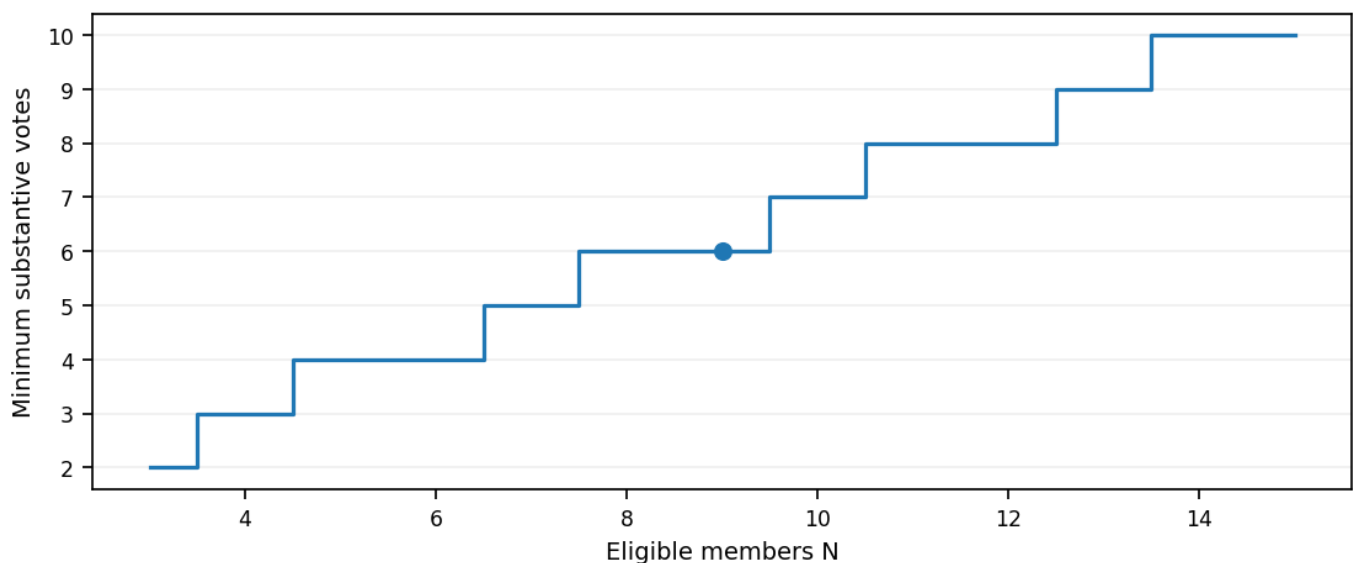


Figure Q04 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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.Q06 Random detection sample size

Source: ASTRA Annex AM, Q06, page 205. All numerical inputs in this example are synthetic.

$$P(\text{at least one detection}) = 1 - (1-p)^n$$

$$n_{\min} = \text{ceil}[\ln(1-C)/\ln(1-p)]$$

Variables and units

p is a fixed issue probability per independent representative observation; C is the selected target detection probability; n is a positive integer.

Example inputs

Synthetic $p=0.10$ and $C=0.95$.

Calculation and checks

1. $\ln(0.05)/\ln(0.90) = 28.433158...$; round upward to $n=29$.

2. $P(\text{detection at } n=29) = 1 - 0.9^{29} = 0.9528987130$.

3. At $n=28$, $P = 0.9476652367$, below the specified target.

Decision interpretation: 29 is the minimum integer sample for the stated independent model; the demonstration does not certify 95% conformity.

Validity limits: This calculation is invalid for unexamined dependence, changing p , biased selection or a judgemental sample represented as random. Detection is also conditional on an effective observation method.

ASTRA connections: 9.3; Annex F.5; 55.3

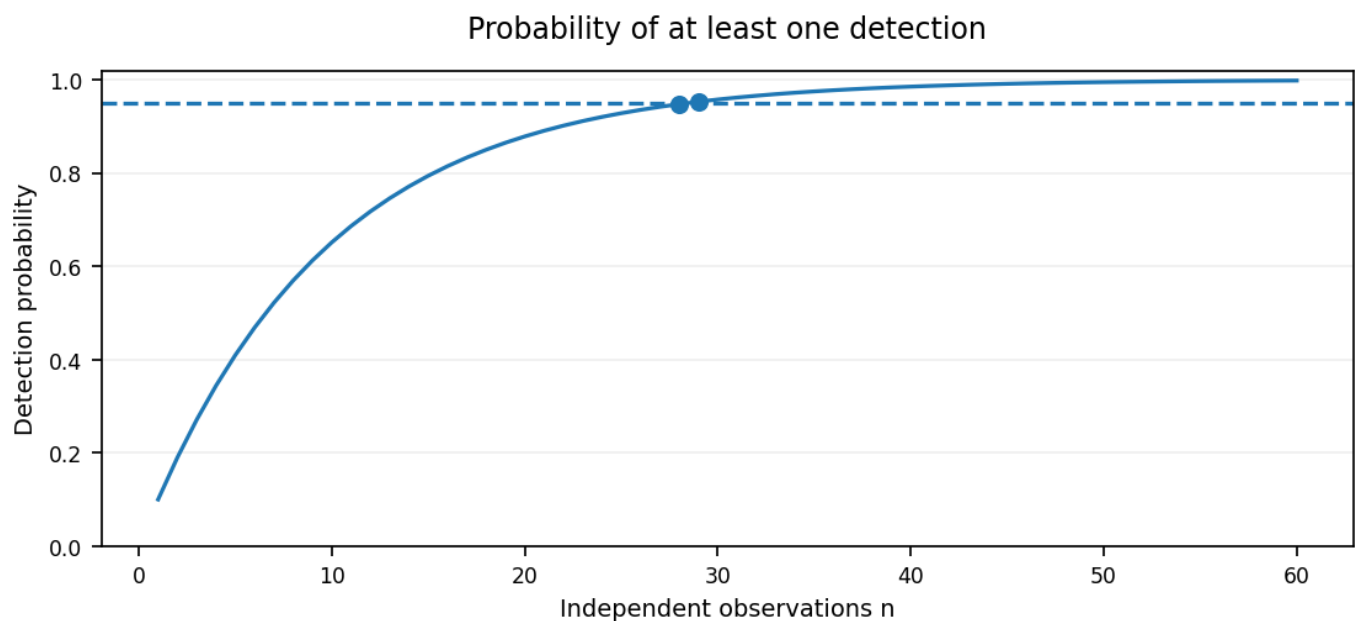


Figure Q06 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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

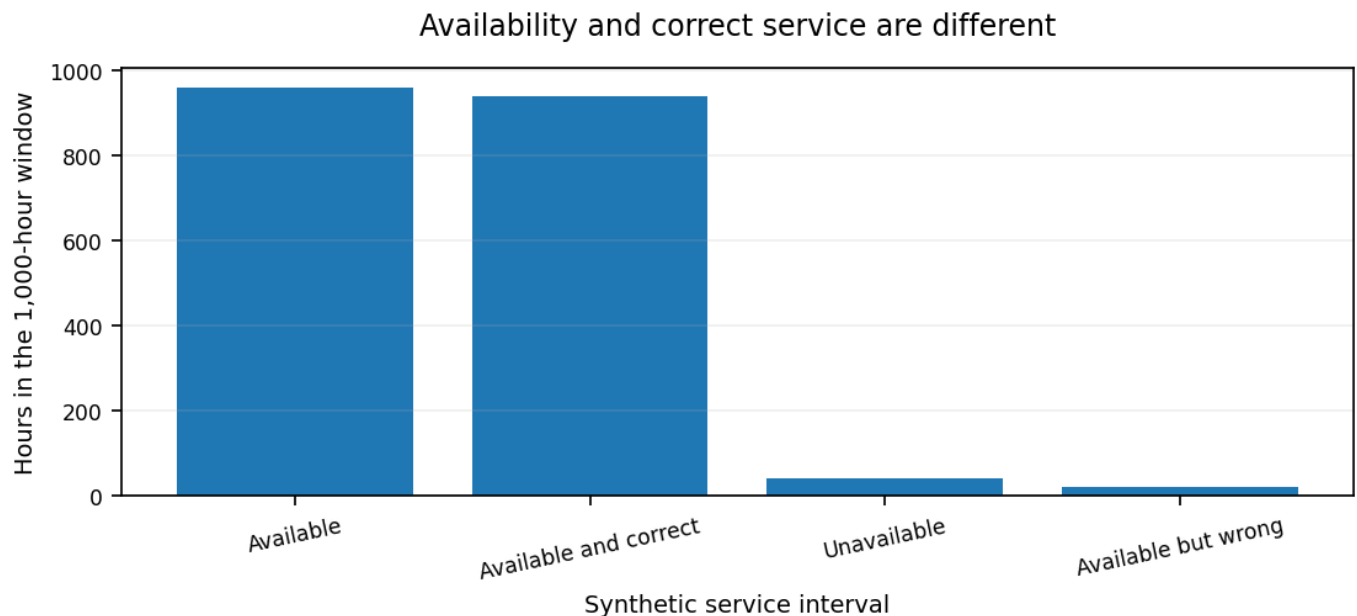


Figure Q09 — Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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.

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

$$1 \text{ byte} = 8 \text{ bits}$$

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

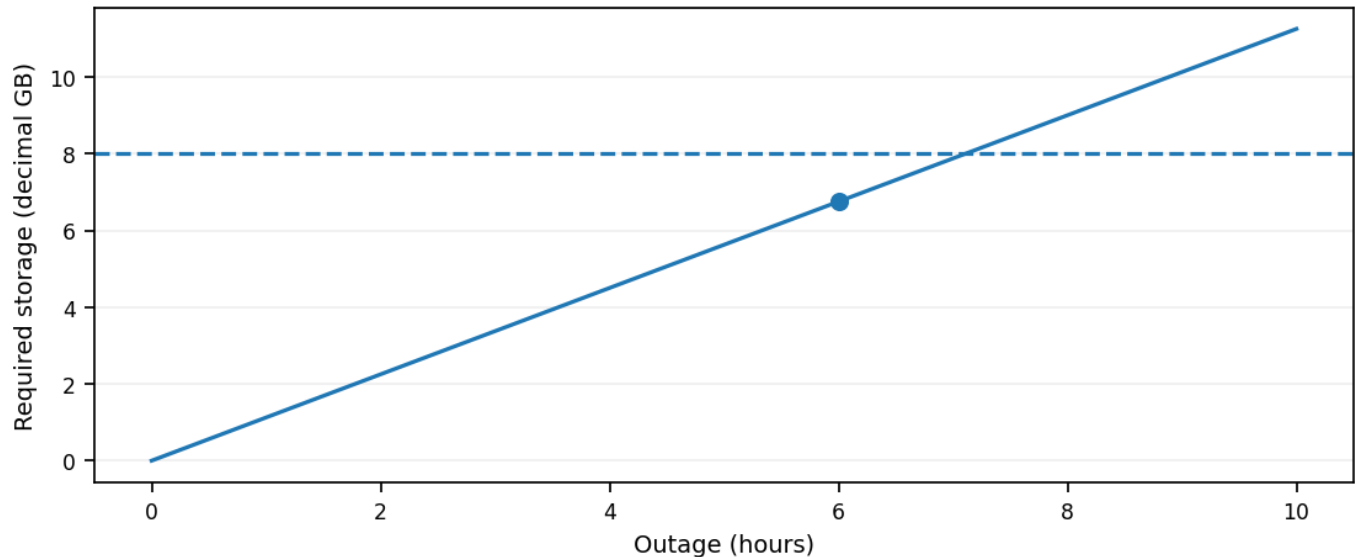


Figure Q16 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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

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

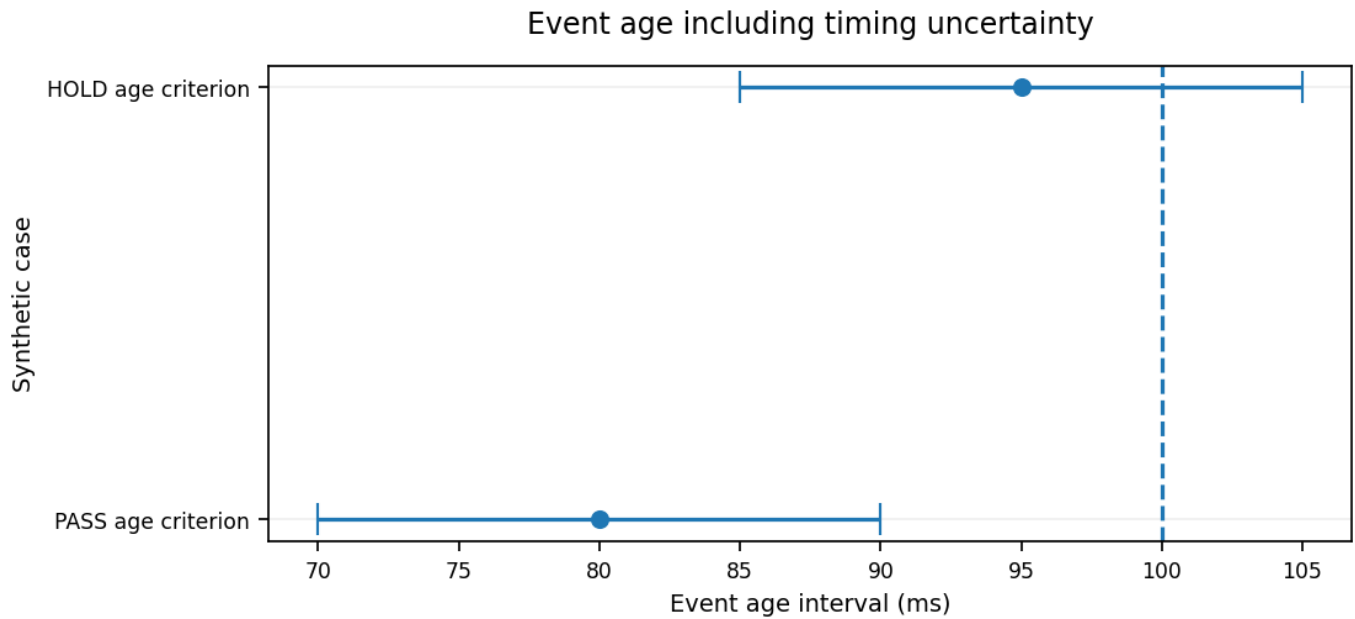


Figure Q17 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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.Q23 Material genealogy, yield and retained work

Source: ASTRA Annex AM, Q23, page 222. All numerical inputs in this example are synthetic.

Input = good + reject + tests + losses + work_in_progress

First-pass yield = accepted_first_pass_output/input

Variables and units

All quantities shall use a consistent lot and period. Recovered material remains linked to its origin and is not counted twice as new production.

Example inputs

Synthetic input=500 units; good first-pass=410; reject=30; destructive tests=10; process losses=20; work in progress=30.

Calculation and checks

1. Reconciliation=410+30+10+20+30=500 units.
2. First-pass yield=410/500=82%.
3. If 20 rejected units are later recovered, the recovery does not increase original input or first-pass output.

Decision interpretation: The quantity balance closes. Technical identity, condition and acceptance evidence still determine whether the 410 outputs are eligible.

Validity limits: A closed balance does not prove authenticity, completeness or material quality. Mixing quantities with different units or unverified scrap/recovery transfers invalidates the reconciliation.

ASTRA connections: 18.4; 48.4; Annex AC; 75.4

Original input reconciliation

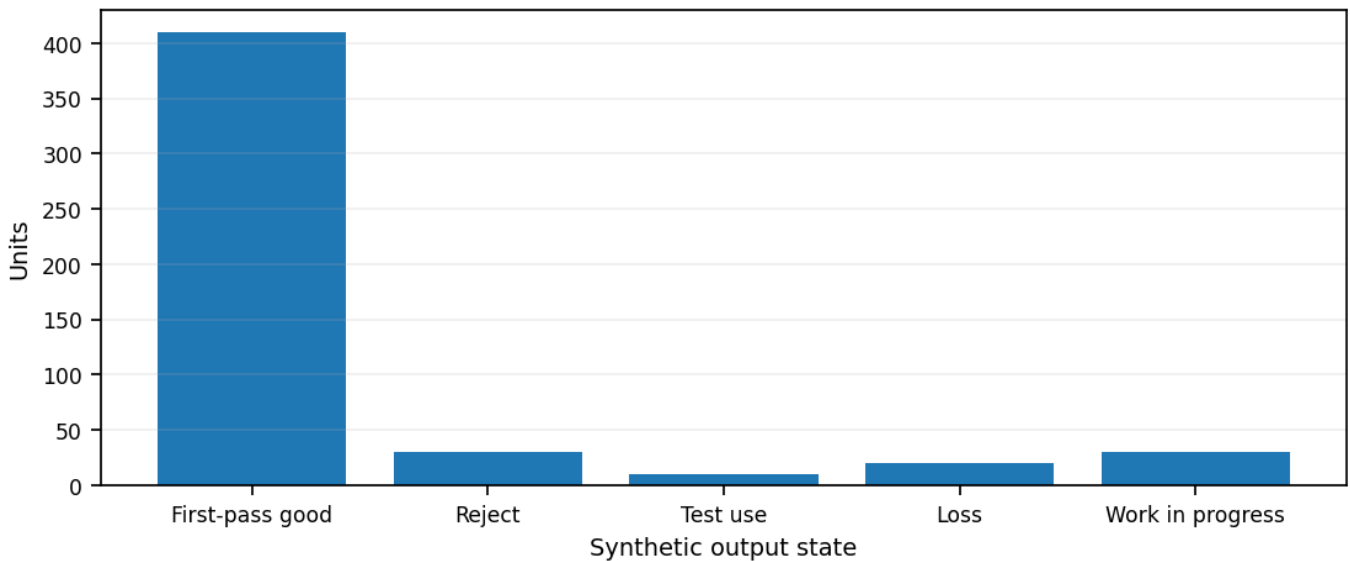


Figure Q23 – Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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

Architecture assumptions determine reliability

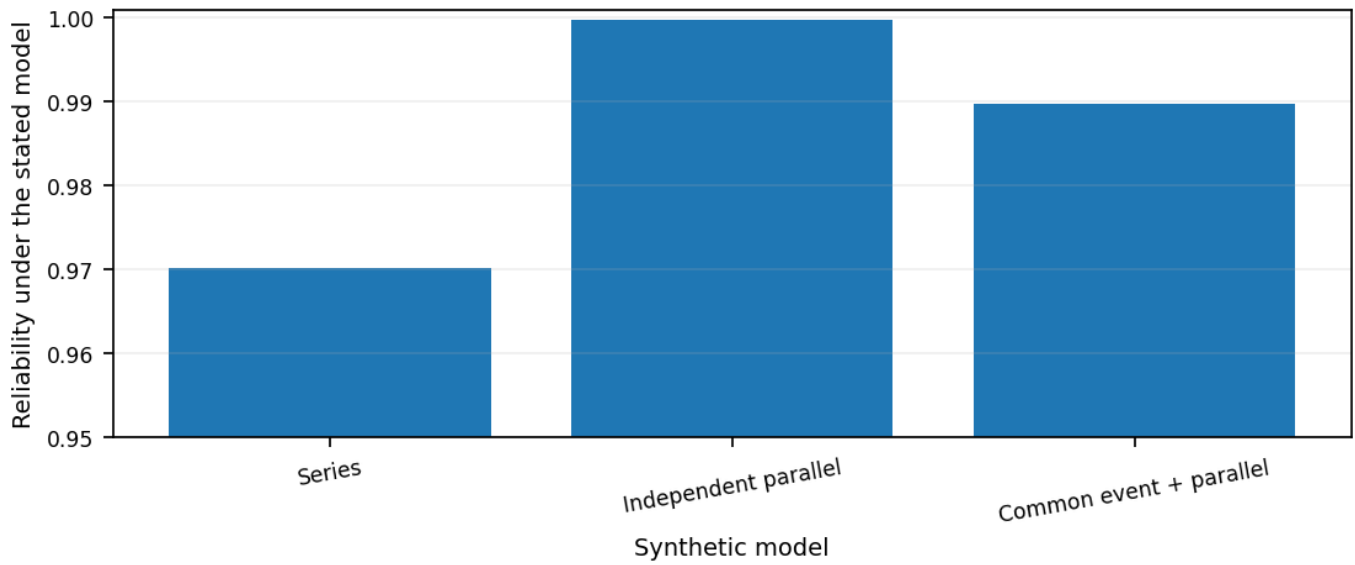


Figure Q25 — Synthetic visualisation. The axes and stated scenario define the quantity; no graph is an accreditation score, approved operating envelope or evidence of a real mission.

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-001: Freeze the publication and requirement baseline — required basis missing	PASS requires a uniquely retrievable source and an authorised effective version; a matching filename is insufficient.	Original input, unresolved value, affected requirement and scope; named action owner.
PR-001: Issue and withdraw controlled copies — handover or review incomplete	Release needs authentic authority, a complete distribution record and tested retrieval of both current and historical evidence.	Expected and observed state; independent replay; correction/retest; receiving acknowledgement.
PR-004: Resolve every applicable domain — required basis missing	Unknown applicability is HOLD; absent equipment or budget never establishes N/A.	Original input, unresolved value, affected requirement and scope; named action owner.
PR-004: Approve exclusion and re-open triggers — handover or review incomplete	Only independently justified exclusions receive N/A; an unexamined consequential interface remains HOLD.	Expected and observed state; independent replay; correction/retest; receiving acknowledgement.
PR-012: Reconcile output identity and basis — required basis missing	A report title or customer description cannot substitute for verified identity and scope.	Original input, unresolved value, affected requirement and scope; named action owner.
PR-012: Review publication against authority — handover or review incomplete	Every communicated result retains its actual event history and no unsupported broader scope.	Expected and observed state; independent replay; correction/retest; receiving acknowledgement.
PR-019: Classify purpose and necessary data — required basis missing	Collecting more sensitive material than needed is not a substitute for better technical evidence.	Original input, unresolved value, affected requirement and scope; named action owner.
PR-019: Preserve custody and authorised disposal — handover or review incomplete	Disposal cannot conceal a required historical decision basis or erase unresolved access and correction duties.	Expected and observed state; independent replay; correction/retest; receiving acknowledgement.
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.
PR-021: Reconcile credential instruction to the decision — required basis missing	A profile title or cover image does not authorise a wider claim.	Original input, unresolved value, affected requirement and scope; named action owner.

Challenge	Expected handling	Evidence retained
PR-021: Test correction and adverse events – handover or review incomplete	Only an authentic authorised decision changes status; a new file date never revives authority.	Expected and observed state; independent replay; correction/retest; receiving acknowledgement.
PR-028: Map the complete change population – required basis missing	A cosmetic filename or edition-label change cannot hide a changed technical basis.	Original input, unresolved value, affected requirement and scope; named action owner.
PR-028: Close without abandoning terminal duties – handover or review incomplete	Only demonstrably complete obligations are closed; remaining duties stay assigned after programme or provider cessation.	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.

1.3 — Object and responsibility tuple

Source: AF-AST-STD-001, page 10.

Each application shall identify the responsible legal entity, actual performer, object type, family and module, sites and remote functions, configuration or programme version, lifecycle role, applicable period, criticality, profile and exclusions. Products, services, processes, people, supplier scopes, educational programmes, assessment providers and environmental statements are separate objects. A combined dossier may share evidence but shall provide a separate conclusion and status history for each claimed object. Where a duty is outsourced, the record shall identify both the performer and the organisation retaining accountability.

Required evidence: Complete scope tuple; separate requested outcomes; actual-performer map.

1.5 — Activity-based applicability

Source: AF-AST-STD-001, page 11.

The applicant shall make a reasoned applicability decision for every common and family requirement. Non-applicability requires the actual activity and retained responsibility to be absent, without undermining a claimed outcome. Small size, another certificate, customer nomination or outsourcing alone does not justify exclusion. A provider that changes from distribution to repair, or from laboratory testing to product certification, shall reassess its scope before making the broader claim. Technical reviewers shall approve material exclusions and record the supporting evidence.

Required evidence: Approved applicability matrix; technical rationale; review triggers and version history.

2.1 — Accreditation and competence

Source: AF-AST-STD-001, page 11.

Accreditation within the current AF framework is an independently decided attestation that a conformity-assessment body is competent, impartial and consistently operated for specified assessment activities. Competence concerns demonstrated ability to perform a defined task and reach valid conclusions, including recognising limitations. A broad sector title, legal registration, quality manual or equipment list does not demonstrate competence. The accredited scope shall identify activity, object or method family, range or conditions, location, resources and limitations sufficient to prevent a misleading interpretation.

Required evidence: Technical competence scope; witnessed performance; independent accreditation decision.

2.2 — Recognition, qualification and certification

Source: AF-AST-STD-001, page 11.

Recognition records that a specified institutional, educational, operational or service capability meets its approved criteria. Qualification records a demonstrated task, process or supply capability under defined conditions. Certification records conformity of a stated product, service, process, system or person to specified requirements. The relevant record shall name the result actually reached. None of these labels is interchangeable with accreditation of the body producing the result, membership, attendance, an award, a professional licence or a public operating permission.

Required evidence: Outcome classification; exact criterion set; approved statement and limitations.

2.3 — Verification and validation

Source: AF-AST-STD-001, page 11.

Verification of a statement examines whether its historical information and assertions are supported for the declared boundary and period. Validation examines the reasonableness of assumptions, methods and prospective claims for an intended future use; it does not establish that a forecast will occur. Laboratory method validation is a separate technical activity demonstrating method fitness. The engagement shall state which meaning applies. A favourable review of a transition plan shall not be published as an achieved emissions reduction, and an accredited verifier is not automatically the holder of a verified environmental claim.

Required evidence: Engagement objective; statement identity; historical/prospective classification; bounded conclusion.

2.4 – Programme name and public designations

Source: AF-AST-STD-001, page 12.

AF ASTRA may be described as an accreditation and assurance programme. An individual outcome shall use its precise class from Annex A. Under the present protected AF instruments, educational and operational applicants use the relevant programme or capability recognition route unless an expressly adopted higher-instrument change permits a different qualified designation. The programme name shall not be abbreviated in a way that implies every participant is accredited. No certificate or registry flag shall apply an expanded accreditation title merely because it appeared in an earlier planning heading.

Required evidence: Permitted-claims register; terminology clearance; applicable authorisation for any changed title.

2.5 – Evidence, witnessing and technical profile

Source: AF-AST-STD-001, page 12.

Evidence is information capable of competent verification and relevant to a stated condition. Witnessing is attributable observation of representative work under known conditions, including necessary setup, execution and conclusion. A technical profile is a controlled definition of the object, intended use, requirements, methods, acceptance rules, limitations and continuing controls. A curated presentation is not equivalent to an end-to-end witness unless its representativeness is justified. Hashes, signatures, video and artificial-intelligence summaries can support integrity or access but do not prove that the original observation is correct.

Required evidence: Profile; evidence-purpose links; witness identity and limitations; provenance records.

2.6 – Requirement status and uncertainty

Source: AF-AST-STD-001, page 12.

Requirement conclusions shall distinguish conforming, nonconforming, approved non-applicability and not yet demonstrated. Evidence status shall separately distinguish planned, received, reviewed, accepted for a purpose, rejected, superseded and unavailable. An indeterminate measurement or inaccessible essential record shall not be changed to non-applicable merely to close a checklist. Confidence in a model, coverage of an uncertainty interval, probability of detection and percentage of completed checklist rows are different quantities and shall not be reported as interchangeable assurance scores.

Required evidence: Controlled status dictionary; recorded transitions; uncertainty and decision interpretation.

9.7 – Technical reporting and amendments

Source: AF-AST-STD-001, page 20.

Reports shall identify issuer, client, actual item, scope, method/version, conditions, dates, results, units, uncertainty where needed, deviations, decision rule, conclusion, limitations and authorised signatory. Identify subcontracted results and opinions separately. A report shall not imply that untested characteristics or future production were examined. Amendments shall preserve the original, state the reason and affected conclusion, and reach recipients who relied on an incorrect result.

Required evidence: Attributable report; raw-data linkage; subcontracted-result identity; amendment and recipient log.

10.1 – Records and provenance

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

Records shall connect each requirement to actual work, configuration, performer, method, data, review and decision. Maintain unique identifiers, units, time basis, versions, status and change history. Corrections shall preserve the earlier information and reasons. Evidence shall remain distinguishable from forecasts, simulations and generated text. An imported record shall be checked for completeness and semantic mapping; a readable file without its essential relationships is not a complete transferred dossier.

Required evidence: Evidence index; version/provenance; change audit trail; migration checks.

10.2 – Confidentiality, personal data and controlled technology

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

Collect only information needed for the authorised purpose and apply suitable access, transfer, retention and disposal controls. Agree legally sufficient confidential review of proprietary or restricted evidence. Public registry fields shall be separated from protected technical and personal records. A security or secrecy restriction shall not lead to a favourable conclusion based on inaccessible essential evidence. Use authorised reviewers, a bounded scope or refusal when adequate lawful review cannot be achieved.

Required evidence: Data classification; permissions; secure review; retained evidence and public-field separation.

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.

10.4 – Artificial intelligence and generated material

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

AI may assist search, classification, drafting and anomaly identification only within an approved use, data boundary and human review. Material conclusions shall retain verifiable underlying evidence; generated citations, transcripts, images or observations shall not be passed off as authentic records. Evaluate data rights, bias, failure modes, confidentiality and model changes. An automated system shall not independently grant, renew, suspend or restore an ASTRA outcome. The authorised decision maker remains accountable.

Required evidence: Approved AI use; validated limitations; verified outputs; human decision and audit trail.

10.5 – Remote access and live evidence

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

Before remote assessment, verify identity, connection security, permissions, camera or sensor adequacy, observation continuity and independent selection of evidence. Record interruptions, inaccessible areas and substitutions. Prerecorded material shall be identified and shall not be represented as live observation. Where physical or practical capability cannot be established remotely, arrange on-site or appropriately controlled witnessed work. Remote convenience shall not reduce scope coverage, time, competence or critical observation.

Required evidence: Remote suitability review; consent/access; live-session record; supplementary coverage.

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.

11.3 – Existing evidence and reuse

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

Review prior reports, approvals and certificates for authenticity, issuer competence, actual method, site, period, conditions and configuration. Identify precisely which requirement and decision use they support and what remains to be evaluated. Include adverse results and restrictions. Another outcome shall not be declared equivalent solely from a similar title or scope label. Evidence reuse may reduce repeated document requests but cannot remove necessary local implementation, witnessing or independent decision.

Required evidence: Reuse matrix; authenticity/scope checks; residual gaps; controlled access to original evidence.

13.5 – Closing and report

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

Communicate evidence-based findings, affected scope, immediate protection and the distinction between team recommendation and final decision. Acknowledge factual corrections without erasing valid adverse evidence. Issue the final evaluation report within 14 calendar days of evaluation closure; exceptional delay shall be explained without moving an already notified finding clock. The report shall state actual time, methods, samples, sites, witnesses, criteria, limitations, findings and recommendation.

Required evidence: Closing record; findings and original notification dates; final actual-coverage report.

16.1 – Duration and basis

Source: AF-AST-STD-001, page 27.

Ongoing ASTRA recognition, qualification, certification or CAB accreditation under this common framework shall have a maximum 24-month period from the independent conformity decision, subject to a shorter profile interval and continued fulfilment. AF 9100 cases retain their controlling provisions. An instance result identifies its lot, serial, event, test or historical statement and does not acquire a universal two-year technical validity. Credential duration never extends an equipment life limit, calibration, statutory authorisation or qualified process window.

Required evidence: Ongoing/instance classification; exact dates; linked technical limits.

16.2 – Surveillance frequency and coverage

Source: AF-AST-STD-001, page 28.

Complete ongoing surveillance at intervals no greater than 12 months, reduced to six months for high-consequence, materially novel or significant competence/integrity exposure. Apply the AF 9100 C0–C3 rules when that standard is used. Mixed scopes follow the shortest triggered interval unless genuinely separated. Reassess actual operation, technical witnessing, changes, adverse results and controls; a document check or booked visit alone is not completed surveillance. Missing required completion triggers affected suspension.

Required evidence: Risk-based timetable; completed technical coverage; changed-scope review; overdue action.

16.3 – Material change and notification

Source: AF-AST-STD-001, page 28.

Planned changes shall be notified early enough for required prior review and before using an expanded claim. Unplanned non-critical material changes shall be notified within five calendar days after awareness; critical concerns follow the 24-hour rule. Evaluate ownership, responsible entity, location, methods, key personnel, digital platforms, aircraft/task capability, educational delivery and environmental boundaries. An unchanged commercial name shall not conceal a different technical basis.

Required evidence: Change notification; impact; prior approval; updated scope and evidence.

16.4 – Renewal and interruption

Source: AF-AST-STD-001, page 28.

Plan renewal sufficiently early to complete evaluation, closure, independent review and decision before expiry; initiation at least 90 days beforehand is recommended, not a guarantee. If the renewal decision occurs after expiry, a visible gap remains and the new status starts no earlier than the actual decision. Relevant prior work may inform the review but not substitute for current demonstrated capability. No payment or appeal automatically extends validity.

Required evidence: Renewal plan; current evidence; closed findings; actual dates and disclosed gap.

16.5 – Suspension, restoration and withdrawal

Source: AF-AST-STD-001, page 28.

A suspension shall state scope, reason, prohibited claims, required actions and a resolution deadline no later than 90 days from the decision. Restore only after verified correction, affected-output review and a valid current basis; otherwise restrict to independently unaffected scope or withdraw. Repeated administrative resets are prohibited. Restoration without full renewal preserves the original expiry and does not validate the suspended interval. Technical containment and reporting continue independently of certificate administration.

Required evidence: Status notices; verified restoration; unaffected-scope rationale; historical continuity.

16.6 – Transfer and cessation

Source: AF-AST-STD-001, page 28.

A receiving operator shall verify authenticity, scope, criteria, decision history, findings, surveillance, authority and technical evidence before accepting a transfer, and perform additional evaluation where necessary. Suspended or unsupported status cannot be made valid by changing issuer. Operator cessation shall preserve records, pending remedies, current status, holder communication and lawful access. Transfer of files does not itself transfer accreditation, AF operating authority or a wider technical scope.

Required evidence: Transfer review; additional work; continuity agreement; accurate issuer/status history.

28.1 – Mandatory scope content

Source: AF-AST-STD-001, page 45.

Each outcome shall state holder and responsible issuer, unique identifier, exact class, family/module, criteria and version, evaluated object, site, technical activity, conditions/ranges, configuration or delivery version, period, decision/issue dates, status and restrictions. Identify ongoing expiry or instance boundary appropriately. The scope schedule forms part of the outcome and shall be available for verification without disclosing protected technical detail. Annex I supplies the minimum schema.

Required evidence: Decision-linked scope schedule; claim class; criteria/version; public/private split.

28.2 – Truthful public wording

Source: AF-AST-STD-001, page 46.

Public wording shall distinguish accredited assessment competence, recognised educational or operational capability, certified conformity and verified historical statements. A label shall not imply statutory approval, all-sector authority, guaranteed safety or recognition by an unevidenced third party. Group logos and commercial package titles shall not conceal excluded sites, tasks or programmes. Every claimed recognition or acceptance arrangement shall be supported by its actual written scope and current terms.

Required evidence: Approved claim; actual acceptance arrangement where claimed; limits clearly communicated.

28.3 – AF marks and authorised use

Source: AF-AST-STD-001, page 46.

Use only authorised AF artwork and approved scope-specific wording. Preserve shape, proportions, legibility and the required identifier; do not create an apparent new certification symbol or apply an organisational mark to imply product approval. Permission shall identify holder, purpose, media, period and restrictions. Suspension or withdrawal shall end affected current claims promptly. Historical factual statements shall state the actual period and status without presenting withdrawn authority as current.

Required evidence: Mark licence; approved artwork/use; monitoring; correction of misuse.

28.4 – Registry states and authenticity

Source: AF-AST-STD-001, page 46.

Maintain separate entity, application, profile, technical scope, decision, credential, authorisation and statement records. Public states shall distinguish active, restricted, suspended, expired, withdrawn and historical instance results. Applicant or pilot records shall not appear in a list of accredited holders. Validate signatures or other authentication, current status and permitted scope rather than treating a scanned certificate image as conclusive. Preserve corrections and prior states.

Required evidence: Validated registry; authenticated decision linkage; separate application/live status; history.

28.5 – Registry security, correction and availability

Source: AF-AST-STD-001, page 46.

Protect registry integrity through least-privilege access, attributable updates, version history and tested recovery. Update status within two calendar days of a decision and communicate urgent restrictions without waiting for a routine update. Correct misleading duplicates, stolen identities and altered certificates through controlled investigation. Provide an alternative verified status channel during outage without extending expiry. The existence of a digital record demonstrates

a recorded decision, not universal technical truth.

Required evidence: Access/update logs; two-day control; recovery; corrected misuse and alternative verification.

30.2 – Controlled transition

Source: AF-AST-STD-001, page 48.

For a new profile or substantive version, identify affected holders, evidence gaps, changed methods, competence, system updates, communications and effectivity. Set a technically justified transition that does not waive immediate safety duties. Preserve the basis of previous decisions and state when additional assessment is needed. Neither indefinite grandfathering nor automatic retrospective invalidation is presumed. A future requirement is not applied as though it had governed an earlier decision.

Required evidence: Transition plan; holder impact; competence/tool updates; actual effective versions.

30.4 – Scope withdrawal and learner/customer protection

Source: AF-AST-STD-001, page 48.

Before closing a profile or provider operation, identify active holders, open cases, pending appeals, unresolved findings, learners, records, status, contracts and financial duties. Notify affected parties and arrange lawful transfer or teach-out as relevant. A closure shall not erase adverse evidence or imply continued authority. Preserve access to historical decisions and correction channels. If urgent cessation is required, prioritise protection and accurate communication while completing residual obligations.

Required evidence: Closure plan; affected-party notices; transfer/teach-out; retained records and remedies.

31.1 – Minimum records and equivalent systems

Source: AF-AST-STD-001, page 48.

The records in Annex M shall be created when their triggering activity applies. They may be combined in a database or controlled document if identities, required fields, relationships, signatures, access and history remain intact. Templates are capture tools, not completed evidence. The programme shall not invent applicants, calibration results, witnesses, student attainment, emissions figures, appointments or approvals. Blank fields shall remain visibly incomplete until authentic information is entered.

Required evidence: Record dictionary; equivalent-system mapping; genuine data and approvals.

31.2 – Document hierarchy and phased development

Source: AF-AST-STD-001, page 48.

The master documentation plan shall distinguish this prepared standard from planned manuals, procedures, technical profiles, checklists and forms. A planned document code does not mean a file exists or a programme is ready. The standard and its applicable normative annexes state the core requirements; implementation documents translate them without adding unapproved duties. Each released technical profile shall have the complete operating and record set required for its scope before activation.

Required evidence: Document catalogue; actual file/version status; dependency and release checks.

31.3 – Actual adoption record

Source: AF-AST-STD-001, page 49.

Record the authenticated legal operator, technical approval, consultation completion, competent institutional adoption, signatories, effective date, applicable instruments and any necessary compatibility amendments. Keep edition date distinct from legal or operational effectivity. Uncompleted approval fields shall not be filled with assumed names or dates. Programme-wide adoption alone shall not activate every listed technical scope; each profile requires the independent readiness and scope decision in Annex P.

Required evidence: Authentic adoption; completed compatibility conditions; individual scope activation.

31.4 – Implementation and verification

Source: AF-AST-STD-001, page 49.

Implement in the following order: settle authority and permissible outcomes; release core operating controls; validate forms, tools and registry states; establish qualified teams and independent decision functions; complete technical profiles and checklists; conduct representative controlled pilots; close findings; and authorise exact live scopes. Annex Q assigns documentation work packages without imposing an invented calendar promise. Maintain an open-action register and verify that every active dependency is actually available.

Required evidence: Implementation programme; verified dependencies; pilot/closure; exact live-scope notice.

31.5 – Review of this edition

Source: AF-AST-STD-001, page 49.

Maintain a controlled master, version history, interpretation register and distribution record. Reassess suitability at least every three years and sooner after material safety, technical, legal or implementation evidence. Technical changes shall undergo the appropriate normative approval process; editorial changes shall preserve meaning. Retain the actual original and revised decision bases. Publication, arithmetic checks and visual review do not by themselves establish independent field validation or external recognition.

Required evidence: Maintenance programme; actual versions; controlled corrections; verified publication integrity.

44.1 – Lifecycle and architectural assurance

Source: AF-AST-STD-001, page 66.

The organisation shall define requirements, architecture, implementation, integration, verification, release, maintenance and retirement for software and programmable hardware. Assurance depth and independence shall be matched to consequence and actual obligations. Architecture shall address interfaces, timing, resource limits, partitioning, fault containment and recovery where relevant. The absence of physical wear shall not be used to dismiss systematic defects, configuration errors, data corruption or environmental change. Purchased artefacts shall remain within the same assigned assurance responsibility.

Required evidence: Digital lifecycle plan; allocated requirements; architecture and consequence review; supplier responsibilities.

44.2 – Source, build and loaded configuration

Source: AF-AST-STD-001, page 66.

Source, generated code, logic, configuration, tools, dependencies and build instructions shall have controlled identities and attributable changes. The released artefact shall be linked to the reviewed baseline and the actual loaded target. Reproducibility shall be demonstrated where necessary for the intended assurance claim. Unapproved dependencies and embedded secrets shall be controlled. A software version label alone shall not establish which settings, data, model weights or external services influenced the delivered behaviour.

Required evidence: Source and review records; build/dependency manifest; artefact identity; loaded-configuration verification.

44.3 – Verification and target representativeness

Source: AF-AST-STD-001, page 67.

Verification shall address requirements, interfaces, boundaries, invalid inputs, timing, resource exhaustion, failure handling and regression. Coverage criteria shall be justified by the technical basis rather than an unexplained universal percentage. Differences between host, simulated and deployed execution shall be assessed. Uncovered behaviour, unresolved anomalies and tool limitations shall remain visible. Passing tests shall not establish completeness when the test set omits an essential condition or was not executed on a representative target.

Required evidence: Verification plan; traced test results; coverage and target-difference analysis; anomaly disposition.

44.4 – Tool and generated-output reliance

Source: AF-AST-STD-001, page 67.

Tools whose failure can create or conceal a defect shall be assessed for intended use, consequence and independent detection. Validation shall include known-answer, boundary, missing-input and prohibited-state cases. Generated calculations, code, technical statements and references shall receive competent verification before becoming controlled evidence. The organisation shall prevent unauthorised disclosure to external services. Neither successful tool execution nor a convincing generated explanation establishes the truth of the input, physical model or engineering conclusion.

Required evidence: Tool-risk and validation record; verified generated outputs; access controls; accountable technical approval.

44.5 – Release and update integrity

Source: AF-AST-STD-001, page 67.

A release shall identify approved functionality, configuration, dependencies, unresolved limitations, installation conditions and support obligations. Updates shall verify origin, integrity, compatibility and intended target before use. Interruption, failed installation, rollback and restoration shall be evaluated for the actual architecture. A security fix shall also be assessed for effects on timing, safety and qualification. The organisation shall not assume that changing a version number closes the original defect or retrospectively validates affected earlier outputs.

Required evidence: Release and update manifest; compatibility review; interrupted-update tests; rollback limits; affected-output decisions.

44.6 – Long-term support and digital retirement

Source: AF-AST-STD-001, page 67.

Long-life digital systems shall have a plan to preserve source or equivalent support access, build environments, licences, technical knowledge and records necessary for maintenance. Dependence on a cloud service or supplier shall be assessed before commitment. Migration, replacement or emulation shall preserve required behaviour and evidence meaning. Retirement shall address data custody, residual vulnerabilities, user notification and prevention of unauthorised reuse. Cryptographic signing alone shall not guarantee permanent readability or technical validity.

Required evidence: Support and obsolescence plan; access arrangements; migration tests; retirement and record-custody decisions.

45.1 – Intended use and prohibited use

Source: AF-AST-STD-001, page 67.

Each AI use shall have an accountable owner, intended purpose, operational domain, affected decisions, permitted authority and prohibited applications. The organisation shall examine foreseeable harms, security exposure, human limitations and whether a simpler, more verifiable method can meet the need. Development and experimental uses shall be separated from released operational use. A vendor's capability claim or a benchmark result shall not establish the suitability of the deployed system for a high-consequence application.

Required evidence: AI use-case register; alternatives and consequence review; domain and authority limits; release boundary.

45.2 – Data provenance and evaluation independence

Source: AF-AST-STD-001, page 68.

Datasets shall retain collection sources, rights, versions, labelling methods, relevant populations, operating conditions and known limitations. Training, tuning and evaluation partitions shall prevent leakage or unjustified overlap. The organisation shall preserve difficult, rare and adverse conditions needed for the intended use. Synthetic data shall be identified and its representativeness justified. A large dataset or overall accuracy score shall not establish coverage of a materially different population, environment or critical failure scenario.

Required evidence: Dataset manifest; partition and labelling controls; scenario coverage; synthetic-data limitations; independent evaluation design.

45.3 – Performance and uncertainty

Source: AF-AST-STD-001, page 68.

Acceptance criteria shall be fixed before evaluation and define relevant errors, denominators, exposure, uncertainty and essential protective conditions. Results shall be examined by meaningful operating condition or subgroup rather than only in aggregate. False acceptance, missed detection, unavailable output and indeterminate behaviour shall be distinguishable. A model confidence score is not automatically a calibrated probability of correctness or a probability of safe operation. Material evidence gaps shall prevent the dependent positive conclusion.

Required evidence: Prospective performance criteria; stratified results; uncertainty and calibration review where relevant; essential-failure record.

45.4 – Human oversight and safe fallback

Source: AF-AST-STD-001, page 68.

The organisation shall demonstrate that responsible people have sufficient information, time, competence and technical ability to intervene. Fallback shall be feasible in the actual operating environment and shall not rely on a failed common resource without justification. Invalid, missing, adversarial or out-of-domain inputs shall be considered under the approved threat and hazard model. A nominal manual-override button or requirement to review every result shall not count as an effective control without representative evidence.

Required evidence: Oversight task analysis; intervention and fallback tests; abnormal-input response; validated operating restrictions.

45.5 – Release, drift and bounded adaptation

Source: AF-AST-STD-001, page 68.

Model weights, preprocessing, dependencies, thresholds, sensor configuration and deployment conditions shall form an identifiable released baseline. Monitoring shall define relevant drift, changed exposure, failure indicators and accountable response. Adaptation outside the approved envelope requires renewed impact review and verification before reliance. The organisation shall retain earlier versions and explain the validity of previous conclusions after a change. An autonomous improvement claim shall not remove the need to demonstrate continued fulfilment of essential requirements.

Required evidence: Model release card; drift and response plan; adaptation boundary; change approvals; retained historical baselines.

45.6 – Assurance decisions remain attributable

Source: AF-AST-STD-001, page 68.

AI may support search, document review, classification and anomaly detection within validated limitations. It shall not independently grant, renew, suspend or restore an ASTRA outcome. The authorised decision maker shall have access to verifiable source evidence, understand material limitations and record the reasoned decision. Generated transcripts, images or observations shall not be presented as authentic events. Independent reviewers shall challenge automation bias and the risk of several tools repeating the same unsupported source.

Required evidence: Approved decision-support use; source verification; human review and decision; generated-content identification; independence checks.

46.1 – Decision purpose and model authority

Source: AF-AST-STD-001, page 69.

Every relied-upon model shall identify its owner, decision purpose, physical or operational target, version, inputs, outputs and authorised use boundary. The organisation shall distinguish an illustrative model, an engineering prediction, a synchronised digital twin and an acceptance model. Visual realism or a common data format shall not establish technical credibility. A model validated for one output or range shall not automatically support a different decision, configuration or environment.

Required evidence: Model identity and purpose; authority and use limits; target/configuration association; versioned assumptions.

46.2 – Verification, validation and uncertainty

Source: AF-AST-STD-001, page 69.

The organisation shall verify the implementation and validate the model against relevant observations for the claimed use. It shall evaluate input quality, numerical effects, calibration, sensitivity, dependence and uncertainty as appropriate. Calibration and validation evidence shall be distinguishable. Material discrepancy shall be investigated rather than concealed through repeated tuning to the same evidence. The final conclusion shall state the limits of the demonstrated domain and the consequences of relying on extrapolation.

Required evidence: Verification and validation plan; independent comparison data; sensitivity and uncertainty; discrepancy and extrapolation review.

46.3 – Twin synchronisation and stale state

Source: AF-AST-STD-001, page 69.

A digital twin shall maintain a traceable association with the actual asset and identify the source and age of updates. The system shall detect relevant missing, stale, inconsistent or wrong-configuration information. Maintenance and replacement shall update both physical and model records without erasing prior states. The organisation shall define what decisions remain permissible when synchronisation is lost. A visually current dashboard shall not be treated as proof that the underlying configuration is current.

Required evidence: Asset-twin identity; update and timestamp controls; stale-state response; configuration reconciliation.

46.4 – Replacement or reduction of physical work

Source: AF-AST-STD-001, page 69.

Where modelling replaces or reduces physical testing, inspection or practical observation, the organisation shall provide a prospective equivalence argument. It shall address failure mechanisms, validated domain, uncertainty, independent review and the material properties or behaviours that remain unobserved. The actual technical and legal obligations shall be checked before removal of a required activity. Cost, speed or model convenience alone shall not justify a reduction in necessary evidence.

Required evidence: Test-replacement rationale; validated equivalence; residual physical evidence; approval and restrictions.

46.5 – Model-based maintenance and remaining life

Source: AF-AST-STD-001, page 69.

A predictive or remaining-life output shall identify the asset history, degradation mechanism, observable inputs, model assumptions and uncertainty. The organisation shall validate the output for the intended maintenance decision and retain mandatory inspection or life-limit obligations. Absence of an alert shall not establish integrity where the model cannot detect the relevant mechanism. A new duty, repair, missing history or changed sensor shall trigger reassessment before the model supports an extended use decision.

Required evidence: Asset-history linkage; degradation and model validity; uncertainty; interval/life decision; changed-duty review.

46.6 – Reproducibility and independent access

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

The evidence dossier shall retain sufficient model definition, input data, parameter settings, tool version and execution records to reconstruct the conclusion. Proprietary restrictions shall be managed through authorised access without accepting an inaccessible essential model by reputation. Independent review shall address the engineering relevance as well as computational correctness. Export and migration shall preserve units, field meaning, relationships and known limitations. A successful file transfer shall not establish successful model transfer.

Required evidence: Reproducible execution package; lawful independent access; engineering review; semantic migration checks.

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.

47.2 – Identity, access and privileged actions

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

Access shall follow verified identities, necessary privileges and actual roles. Human, machine and service identities shall be controlled throughout their lifecycle. Privileged release, maintenance and status actions shall have authentication and attribution appropriate to consequence. Emergency access shall be bounded, logged and reviewed. Shared credentials shall not obscure who performed an action. Changes in employment, supplier access or responsibilities shall promptly trigger the relevant permission review and removal.

Required evidence: Access and role matrix; identity lifecycle; privileged approvals; emergency logs; event-time authority checks.

47.3 – Supply-chain and dependency integrity

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

The organisation shall maintain a relevant inventory of digital components and dependencies, their provenance, supported versions and channels for vulnerability information. Disposition shall consider actual exposure, exploitability, safety consequences and available protection. An inventory is not proof that every component is secure. Supplier changes,

unsupported software and inaccessible update mechanisms shall trigger technical and continuity review. The organisation shall identify the actual party responsible for remediation and for informing affected users.

Required evidence: Dependency inventory; provenance; vulnerability assessment; support commitments; remediation and notification records.

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.

56.1 – Distinct entities and authoritative records

Source: AF-AST-STD-001, page 80.

The information model shall distinguish organisations, people, profiles, applications, assignments, evidence, findings, decisions, credentials, permissions, appeals and status events. Each record shall have a unique identity, version, accountable origin, scope and relevant time basis. A case may support several outcomes, but the conclusion and history of each outcome shall remain separate. Copies and public projections shall identify their relationship to the authoritative source rather than become competing unexplained masters.

Required evidence: Entity dictionary; source-of-record map; relationships; scope and time conventions; controlled projections.

56.2 – Evidence states and requirement conclusions

Source: AF-AST-STD-001, page 80.

Evidence receipt, review, purpose-specific acceptance, rejection, supersession and unavailability shall remain distinct from conformity conclusions. A missing essential source shall not become non-applicable because a database field requires a value. Accepted evidence shall state the requirement and configuration it supports and its limitations. An imported identifier shall not be presumed to refer to the correct object or version. Contradictory evidence shall remain visible through the independent review process.

Required evidence: Evidence-purpose links; controlled state dictionary; missing/wrong-version checks; reasoned requirement conclusions.

56.3 – Decision and publication safeguards

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

The workflow shall test valid scope, complete evidence, fulfilled criteria, closed findings, current competence, case independence and actual authority before publishing a positive outcome. Where a three-person panel is required, all eligible participation and votes shall be recorded. An automated check may flag or block a proposed instruction but shall not create the independent technical decision. Public information shall match the authorised decision and preserve restrictions, expiry and historical gaps.

Required evidence: Decision preflight; authentic decision instrument; panel record where required; public/private reconciliation.

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.

61.1 – Publication identity

Source: AF-AST-STD-001, page 86.

The display title shall be ASTRA with AEROSPACE STANDARD directly beneath it. The standard identifier shall remain AF ASTRA-100:2026 and the document code AF-AST-STD-001. The displayed edition shall be FIRST EDITION and the displayed publication date 30 September 2026. These labels shall not be substituted for an actual technical approval, contract effectivity, operational permission or conformity-decision date.

Verification: Compare cover, identity page, headers, metadata and controlled publication record.

Acceptance / hold rule: Identity fields agree. A publication date alone provides no evidence of adoption or operational authority.

61.2 – Retained text and authored additions

Source: AF-AST-STD-001, page 86.

Clauses 0–60 and Annexes A–AH retain the source architecture, subject identifiers and operational controls, subject to the editorial identity changes stated in Annex AI. This clause, Clauses 62–80 and Annexes AK–AR develop explicit all-space coverage, decision logic, calculations and evidence controls. They shall not be represented as records of completed field evaluation or as proof that the complete consolidated text existed on the displayed edition date.

Verification: Review the internal authorship boundary in Annex AJ and the actual approval dossier.

Acceptance / hold rule: Source-derived requirements and newly authored material are distinguishable; no invented approval, validation or prior effectivity is asserted.

61.3 – Dependent documents and compatibility

Source: AF-AST-STD-001, page 86.

The responsible custodian shall identify every affected profile, manual, procedure, checklist, form and register before use of this text. Existing 108-title architecture and F01–F08 codes shall remain stable. Newly added requirements shall be mapped to the actual dependent documents; a previous checklist shall not be assumed to cover them. Actual constitutional and legal obligations remain separately applicable.

Verification: Reconcile the dependency register against selected requirements and operating versions.

Acceptance / hold rule: Every required operating document is available, consistent and authorised for the intended use. Unresolved conflicts place dependent use on HOLD.

61.4 – Actual approval and activation

Source: AF-AST-STD-001, page 86.

The adoption dossier shall retain the proposed text, consultation, comment dispositions, valid technical decision, institutional authority, operator identity and exact scope activation. Real signatories and event timestamps shall be recorded when the events occur. A blank, generated or copied signature shall not be used as an approval. Technical and institutional release shall remain separate from the acceptance of a particular applicant.

Verification: Trace the authorisation chain and independently verify each necessary approval.

Acceptance / hold rule: All triggered gates in Clause 4 and Annex P are satisfied before live scope use; otherwise the affected scope remains unavailable.

61.5 – Correction, custody and file integrity

Source: AF-AST-STD-001, page 87.

The custodian shall retain controlled source versions, change reasons, affected requirements and distribution records even though no numbered change label appears on the publication. Corrections shall not erase historical decisions. The issued PDF shall have complete content, readable figures, working navigation and an identifiable master. Removal of publication labels shall not remove record timestamps, method versions or technical configuration controls.

Verification: Reconcile the final file with its manifest and inspect content, navigation and correction records.

Acceptance / hold rule: No missing section, contradictory edition field or unreadable essential figure; the original evidence and actual history remain retrievable.

62.1 – Atomic requirement record

Source: AF-AST-STD-001, page 88.

Each assessed requirement shall have a stable identifier, one accountable owner, an applicability trigger, defined object and configuration, required behaviour or characteristic, observable conditions, verification method and acceptance predicate. Compound statements shall be separated into individually testable rows without deleting any condition. Terms such as adequate, suitable, promptly or representative shall be resolved through the explicit records in this clause before they support an acceptance decision.

Verification: Inspect each requirement row and its linked method, boundary and predicate.

Acceptance / hold rule: Every applicable row is evaluable without inventing an object, limit, observation or decision role. Unresolved essential terms result in HOLD.

62.3 – Evidence validity before conformity

Source: AF-AST-STD-001, page 88.

The evaluator shall first determine whether evidence belongs to the correct object, configuration, period, method and authorised performer and whether it is usable for the intended inference. Only valid relevant evidence shall enter a conformity predicate. Rejected, corrupted, missing, unobservable or wrong-version evidence shall remain identified. Evidence may be valid and show failure; an invalid test is not a valid pass or a valid proof of product failure.

Verification: Check provenance, configuration, method capability, original data and uncertainty separately from result classification.

Acceptance / hold rule: Validity is established before PASS or FAIL is assigned; otherwise use HOLD with an explicit invalidity or evidence-gap reason.

62.4 – Four requirement states

Source: AF-AST-STD-001, page 88.

A requirement state shall be PASS, FAIL, HOLD or N/A. PASS means the approved predicate is satisfied by valid evidence. FAIL means valid evidence demonstrates that the predicate is not satisfied. HOLD means applicability, method, evidence, uncertainty or authority is not sufficiently resolved. N/A means the trigger and retained responsibility are absent and independent approval of that exclusion is recorded. Missing equipment, budget, access or time shall not justify N/A.

Verification: Execute the truth table in Annex AL using actual scope and evidence.

Acceptance / hold rule: Exactly one current state is assigned with reason and traceable evidence. All earlier states are retained.

62.5 – No compensation or favourable default

Source: AF-AST-STD-001, page 89.

A positive conformity decision shall require PASS for every applicable mandatory requirement, closure of every in-scope nonconformity, valid independent competence and actual authority. N/A rows shall have approved reasons; HOLD and FAIL rows shall not contribute a favourable default. Weighted scores, averages, majority votes, programme membership or good results in another discipline shall not compensate for an unmet condition.

Verification: Reconcile the complete requirement population with the decision dossier; test missing and negative cases.

Acceptance / hold rule: The Boolean conjunction in Annex AL is true. Otherwise no positive grant, renewal or extension is permitted.

62.7 – Decision replay and consistency

Source: AF-AST-STD-001, page 89.

A decision shall be reproducible from the same frozen requirements, parameter values, original evidence, calculation version, uncertainty model and role assignments. Two competent reviewers reaching different results shall identify the differing input, predicate, assumption or expertise before closure. Interpretation records may clarify a term but shall not change limits after results are known. Equation inputs shall retain unrounded values.

Verification: Independently replay a selected boundary case and reconcile every difference.

Acceptance / hold rule: The replay produces the same supported state, or the case remains HOLD pending a controlled technical resolution.

63.1 – Domain selection without geographic omission

Source: AF-AST-STD-001, page 90.

The mission owner shall assess every domain in Annex AK and record applicable, not applicable or not yet determined. The scope shall include terrestrial preparation, launch and recovery interfaces as well as the in-space activity. Earth orbit, cislunar and libration-region operations, solar and planetary missions, small bodies, ocean-world exploration and interstellar precursor concepts shall not be excluded solely because they differ from conventional satellite operations.

Verification: Compare the mission concept and responsibility map with all Annex AK domain rows.

Acceptance / hold rule: Every domain has a reasoned disposition. Any unassessed domain that can affect a required outcome remains HOLD.

63.2 – Object and activity rather than a universal label

Source: AF-AST-STD-001, page 90.

The claimed object shall be identified as a system, subsystem, component, material, process, service, facility, software artefact, person, educational programme, assessment provider or statement. Record what is designed, built, tested, operated, maintained or retired, by whom and where. A phrase such as all space, space-qualified or complete mission assurance shall not replace the exact boundaries and limitations of the evaluated object.

Verification: Compare application, technical schedule, evidence and proposed public wording.

Acceptance / hold rule: The object and activities agree throughout the dossier; unsupported sector-wide or geographically unlimited claims are prohibited.

63.3 – Environment, phase and mode matrix

Source: AF-AST-STD-001, page 90.

For each applicable domain, define mission phase, operating mode, intended duration, exposure, interfaces, repairability, accessible evidence and credible degraded states. Include dormant storage, transport, separation, commissioning, routine service, communication outage, servicing, retirement and loss-of-mission conditions when relevant. A qualification for one phase shall not automatically cover another phase with different loads, resources or observability.

Verification: Review the complete phase-by-mode matrix and its verification links.

Acceptance / hold rule: Every safety-, mission- or claim-relevant cell has accepted evidence or an explicit restriction; no essential unexamined cell is passed by analogy.

63.6 – Interface and lifecycle closure

Source: AF-AST-STD-001, page 91.

The scope shall include relevant upstream and downstream duties, including supplied design data, ground services, communications, receiving facilities, environmental custody and long-term records. Transfers shall identify the sender, receiver, evidence and acceptance. A contractor delivering one subsystem shall not be made responsible for unrelated mission duties, but an integrator shall not exclude duties it retains because they are performed by others.

Verification: Trace each interface to an accountable performer and retained owner.

Acceptance / hold rule: No essential responsibility, evidence handover or terminal obligation is orphaned.

64.5 – Heritage and similarity

Source: AF-AST-STD-001, page 92.

A heritage argument shall compare actual design, materials, manufacturing source, mission exposure, software, interfaces and life history. Identify unchanged evidence, invalidated evidence and new demonstration. Successful service of a related design shall be accepted only for characteristics and mechanisms it actually supports. Lack of a recorded failure shall not prove performance of an unmonitored critical characteristic.

Verification: Review a difference matrix and trace each retained conclusion to applicable original evidence.

Acceptance / hold rule: Every material difference has a technical disposition and sufficient evidence before the new claim is accepted.

65.6 – Payload function and scientific or service output

Source: AF-AST-STD-001, page 95.

Payload requirements shall identify intended outputs, calibration, dynamic range, contamination sensitivity, pointing or timing needs, processing and delivered data quality. Instrument performance, system suitability and scientific interpretation are separate conclusions. Changes in compression, processing or calibration shall retain raw or reconstructable data and algorithm identity. Marketing resolution or accuracy figures shall state the tested conditions and limitations.

Verification: Reconstruct selected output products from identified inputs, calibration and processing.

Acceptance / hold rule: Output criteria are met for the stated domain; unsupported scientific or service claims are not inferred from a functioning instrument.

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.

67.1 – Configuration and operational baseline

Source: AF-AST-STD-001, page 98.

The ground baseline shall identify deployed hardware, software, databases, operational procedures, configuration dictionaries, simulation models, keys, operators and external services. The controlled baseline shall be linked to each supported flight configuration. A simulator or training installation shall be segregated from live commanding.

Verification: Reconcile installed versions and target mappings with approved release records.

Acceptance / hold rule: Every live mission interface uses an accepted compatible baseline; training or stale configuration cannot be selected as a live authority.

67.3 – Receipt, execution and completion

Source: AF-AST-STD-001, page 98.

The record shall distinguish command prepared, approved, transmitted, received, accepted, started, completed, failed and unknown. A transmission log or acknowledgement shall not be treated as verified physical completion. Completion criteria shall identify telemetry or other evidence, timing, confidence limits and independent checks needed for the actual action.

Verification: Trace a command through its full event and evidence history.

Acceptance / hold rule: Only evidence satisfying the approved completion predicate supports completed status; missing terminal evidence remains unknown or partial.

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.

68.7 – Status and long-term custody

Source: AF-AST-STD-001, page 101.

Closure shall record whether an asset is operating, restricted, dormant, disposed, lost or unknown using verified evidence and defined meanings. Loss of communication shall not be labelled successful disposal. Assign remaining notices, monitoring and records to an actual custodian. A closed commercial contract does not close an unresolved technical or environmental obligation.

Verification: Trace final-state evidence and accepted transfer of residual duties.

Acceptance / hold rule: Terminal claims match observed or explicitly bounded inferred states, and every continuing duty has a receiving owner.

73.7 – Medical capability and health-data boundaries

Source: AF-AST-STD-001, page 111.

The mission shall identify the qualified health functions, equipment and support access required for its actual population and duration. Engineering assurance shall verify availability, integration, power, maintenance, communication and privacy without inventing treatment protocols or clinical certification. Health information shall be restricted to authorised purposes and handled separately from public conformity records.

Verification: Check actual health-support arrangements, equipment integration and protected data access.

Acceptance / hold rule: Required support functions are demonstrably available and usable within the mission limits; undocumented specialist capacity is not credited.

74.4 – Sample identity and custody

Source: AF-AST-STD-001, page 112.

Each sample shall retain origin description, collection event, container, seal or interface identity, mass or quantity where known, conditions, contamination history, transfers, subdivisions and authorised access. Unknown provenance shall remain unknown. Splitting or pooling shall preserve parent-child links and shall not create duplicate inventories.

Verification: Reconcile original collection, custody, receiving and subdivision records.

Acceptance / hold rule: The sample and its history are unambiguous and usable for the claimed purpose; missing essential links block the dependent sample conclusion.

74.6 – Anomalies, unknown state and release of information

Source: AF-AST-STD-001, page 113.

Loss of containment indication, unverified seal condition, missing samples or unexplained contamination shall trigger preservation, restriction and qualified review. Do not equate absent alarms with demonstrated integrity. Technical data and scientific interpretations shall retain limitations; public statements shall not imply a sample is harmless or pristine solely because its custody form is complete.

Verification: Examine anomaly decisions, actual observations and bounded reporting.

Acceptance / hold rule: Only supported technical conclusions are released; uncertainty and unresolved protection duties remain visible.

74.7 – Disposition and residual responsibility

Source: AF-AST-STD-001, page 113.

Final disposition shall identify sample, container, residue, facility, record and long-term custody obligations. Transfer shall include receiving acceptance and usable evidence. Mission completion shall not terminate a continuing protection or scientific-record duty. The custodian shall preserve genuine access conditions and correction channels after organisational closure.

Verification: Trace final-state evidence and accepted residual duties.

Acceptance / hold rule: No required custody or protection obligation is abandoned and no unverified disposal is claimed complete.

75.7 – Handover, resource claims and closure

Source: AF-AST-STD-001, page 115.

The final claim shall state actual production, quality, quantity, conditions, uncertainty, exclusions and accepted receiving responsibility. Demonstration of a resource process creates no ownership, extraction right or operating permission. Waste, residues, hazardous inventories and long-term custody shall have accepted disposition.

Verification: Reconcile reported outputs, accepted products, rights/permissions and final-state evidence.

Acceptance / hold rule: The claim is bounded to measured and accepted achievement; undeveloped scale-up and unknown disposition remain separate.

77.5 – Original data and invalid tests

Source: AF-AST-STD-001, page 118.

Retain actual setup, input and response histories, environmental conditions, interruptions, alarms, raw files, corrections, uncertainty and validity classification. An invalid run shall state what evidence remains usable and which requirement is not demonstrated. A repaired or changed article shall not silently replace the originally failed configuration.

Verification: Reconstruct a selected run from raw data and contemporaneous records.

Acceptance / hold rule: The run is independently interpretable and no failed, invalid or missing evidence is concealed.

77.8 – Independent campaign closure

Source: AF-AST-STD-001, page 119.

The final dossier shall reconcile configuration, criteria, valid results, adverse evidence, untested characteristics, uncertainty, concessions and open duties. Qualification, article acceptance, laboratory competence and ASTRA conformity shall retain separate decisions. A technical concession shall not be relabelled as fulfilment of the original criterion.

Verification: Perform independent requirement-by-requirement closure with actual decision authority.

Acceptance / hold rule: Every applicable gate for the exact claimed object passes; counts, percentages or programme completion dates alone cannot release the object.

78.3 – Evaluation data and model credibility

Source: AF-AST-STD-001, page 120.

Evaluation shall retain data provenance, rights, labelling, representative populations, partitions, leakage checks, synthetic contribution and adverse cases. Model verification, calibration and independent validation shall be distinguished. A high aggregate score, large dataset or visual twin is not evidence of every rare or safety-critical condition.

Verification: Inspect data partitions and independently reproduce selected performance and model-validation results.

Acceptance / hold rule: Prospective scenario-specific criteria are met with disclosed uncertainty and limitations; unsupported extrapolation remains HOLD.

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.

79.5 – Terminal evidence and responsible transfer

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

Terminal-state claims shall specify the exact intended condition, permitted inference, observation method, resources and residual duties. Transfer shall preserve custody and receiving acceptance of records, hazardous inventory, notices, monitoring and unresolved remedies. A file sent or contract ended is not accepted closure.

Verification: Reconcile final-state evidence, inventory and recipient acknowledgement.

Acceptance / hold rule: Every required terminal criterion is demonstrated or openly limited, and every remaining duty has an actual receiving owner.

80.1 – One complete application schedule

Source: AF-AST-STD-001, page 124.

The schedule shall join the object tuple, F01–F08 selection, Annex AK domains, phase/mode matrix, required methods, parameter records, competence, evidence, independent decisions and continuing controls. All triggers in Annex AO shall be resolved. Shared records may be reused after relevance review, but shall not merge distinct objects, outcome classes or actual authority.

Verification: Reconcile the full schedule with Clauses 1, 4, 62 and 63 and Annex C.

Acceptance / hold rule: No essential scope, parameter, responsibility or evidence field remains undefined before a positive decision.

80.2 – Domain and verification completeness

Source: AF-AST-STD-001, page 124.

Map every applicable domain and requirement to valid verification and to an accountable conclusion. Treat domain counts, test counts and completed checklist percentages as planning measures only. Annex T is not exhaustive of all future methods; a newly discovered material mechanism shall create a controlled additional requirement and evidence task before the affected claim proceeds.

Verification: Perform forward and reverse traceability and inspect omitted-domain reasons.

Acceptance / hold rule: Every applicable condition passes or has a justified approved N/A; no HOLD or FAIL is hidden by a coverage percentage.

80.4 – Bounded claim and publication

Source: AF-AST-STD-001, page 124.

The outcome shall identify legal holder, issuer, object, configuration, family/module, domain, site or remote responsibility, criteria, limitations, actual dates and ongoing or instance basis. Public wording shall not imply unrestricted coverage of all space, universal safety, statutory permission or external recognition without evidence. The approved cover and edition label do not change those boundaries.

Verification: Compare the actual decision with credential, registry and all proposed public representations.

Acceptance / hold rule: Published scope and status exactly match the authorised decision and preserve every material restriction.

80.5 – Continuing conformity and change

Source: AF-AST-STD-001, page 124.

Maintain surveillance, technical validity, people, resources, configuration, monitoring and actual state history under the controlling clocks. Mission, environment, population or technology changes shall trigger impact review before expanded reliance. Restoration shall preserve expiry unless a full renewal has occurred and shall not validate the suspended interval.

Verification: Audit actual completion, change and status records rather than scheduled dates alone.

Acceptance / hold rule: The current claim remains fully supported; overdue or invalidated conditions trigger the applicable restriction, suspension or withdrawal.

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.