



AF 9200

Aerospace Safety & Operational Assurance

Space / Aviation / Defense

FIRST EDITION

Document status and authority

FIRST EDITION MANUSCRIPT - Prepared for publisher review

Field	Declared position
Identifier	AF 9200
Title	Aerospace Safety & Operational Assurance
Organization	Aerospace Federation
Edition	FIRST EDITION
Language	English master text
Approval and effective date	Not assigned in this manuscript
Content	Clauses 0-28 and Annexes A-Z
Normative status	Proposed requirements, subject to controlled publisher approval

Normative status at a glance

Content	Status
Main clauses 0-28	Requirements are identified by shall; guidance and explanations remain distinguishable.
Annexes A-R	Normative supporting controls; explicitly identified filled examples are informative.
Annexes S-X and Z	Informative calculations, cases, comparisons, diagrams, challenges and navigation.
Annex Y	Normative proposed publication-control process; completion is not asserted.

This manuscript is prepared for Aerospace Federation review. It does not assert completed consultation, technical validation, publication approval or an effective date. FIRST EDITION is the intended edition designation. The publisher controls the transition to an approved publication under Annex Y.

Publication, conformity assessment, residual-risk acceptance and operational permission are separate decisions. Applicable legal and competent-authority obligations remain independently binding. No blanket safety guarantee is created by this document.

Quick-start guide

Define the activity, complete the parameters, demonstrate the controls and keep the decision current.

1 Define the object and responsibility

Use Clauses 1-4 and Annex A. Identify actual activities, sites, configurations, lifecycle phases, exposed populations, outsourced duties and essential interfaces. Select every technical module triggered by the work.

2 Complete the decision criteria

Use Annex B before acceptance. Define operating limits, risk criteria, assurance level, barrier performance, competence, release prerequisites, response clocks, evidence validity and review triggers. Unset essential parameters cause HOLD.

3 Build the safety argument

Apply Clauses 7-11 and Annexes C-E. Trace hazards to requirements, controls, valid evidence and residual-risk decisions. Include common causes, human performance, uncertainty and independent challenge.

4 Release and maintain the operation

Apply Clauses 12-16 and Annexes F-J. Verify actual readiness, issue a bounded decision, monitor barrier health and assumptions, control change and learn from occurrences.

5 Add the relevant technical controls

Use Clauses 17-26 and Annexes K-O for aviation, ground services, maintenance, unmanned systems, space, defense, industrial, digital, supplier and energy interfaces.

6 Evaluate and communicate truthfully

Use Clauses 27-28 and Annexes P-R. Preserve PASS, FAIL, HOLD and approved N/A. State the exact scope and authority. Use Annexes S-X for worked methods and Annex Z for navigation.

Decision principle: No score compensates for a failed mandatory condition. A release remains valid only while its configuration, controls, evidence and assumptions remain valid.

Contents - clauses and annexes

Entries are clickable. PDF bookmarks also locate subclauses and technical examples. Page numbers refer to this file.

0 Introduction and application principles	11
1 Scope, boundaries and conformity model	13
2 Application, precedence and the AF framework	14
3 Terms, definitions and conventions	15
4 System definition and lifecycle context	18
5 Leadership, governance and safety culture	19
6 Safety planning and assurance depth	21
7 Hazard identification and the lifecycle hazard register	22
8 Risk analysis, evaluation and accountable acceptance	23
9 Safety requirements and engineered controls	25
10 Safety cases, evidence and independent challenge	26
11 Human performance, competence and safety communication	27
12 Operational planning, release and continuing control	28
13 Degraded, abnormal and emergency conditions	30
14 Change, configuration and controlled transition	31
15 Occurrence reporting, investigation and learning	32
16 Performance assurance, audit and management review	33
17 Aviation operations and airspace interfaces	34
18 Aerodromes, ground operations and aviation support services	35
19 Maintenance and continuing operational integrity	36
20 Unmanned systems, advanced air mobility and autonomy	37

21 Space systems, missions and ground support	39
22 Defense aerospace and dual-use safety interfaces	40
23 Design, manufacture, testing and commissioning	41
24 Software, cybersecurity, data and AI safety interfaces	42
25 Suppliers, partners and joint operations	43
26 Energy, facilities and lifecycle protective controls	44
27 Records, digital workflow and evidence integrity	45
28 Evaluation, conformity decisions and truthful claims	46
Annex A - Activity-based applicability and boundary closure	48
Annex B - Mandatory parameters and common record payloads	51
Annex C - Consequence, assurance depth and risk governance	55
Annex D - Hazard and barrier records	57
Annex E - Safety-case architecture and evidence acceptance	59
Annex F - Readiness, release, emergency and restart records	61
Annex G - Change and combined-condition assessment	63
Annex H - Human performance and competence evidence	64
Annex I - Occurrence, investigation and corrective-action records	65
Annex J - Performance indicator dictionary and review rules	67
Annex K - Engineering, testing and digital assurance matrices	69
Annex L - Aviation, ground, maintenance and unmanned operational matrices	71
Annex M - Space, defense and critical-infrastructure matrices	73
Annex N - Digital record and workflow validation	75
Annex O - Supplier and interface assurance package	76

Annex P - Assessment planning, competence and decision independence	77
Annex Q - Findings, corrective action and continuing status	79
Annex R - Requirement coverage and claim control	80
Annex S - Quantitative methods and reproducible worked examples	81
Annex T - Integrated worked cases and decision trails	94
Annex U - Comparison matrices and prevention of false equivalence	101
Annex V - Diagram atlas: safety, evidence and decision workflows	103
Annex W - Boundary and adverse-case challenge suite	109
Annex X - Assessor evidence trails and activity starter profiles	112
Annex Y - Publication, interpretation and maintenance control	116
Annex Z - Navigation crosswalk and implementation sequence	118

Tables - technical controls and worked examples

Table 0-1. The AF 9200 assurance chain	11
Table 3-1. Core safety and assurance terms	15
Table 3-2. Abbreviations used in this document	18
Table A-1. Activity and responsibility triggers	48
Table A-2. Required boundary challenge	49
Table A-3. Informative examples of applying the normative selection rules	49
Table B-1. Safety and operational parameter schedule	51
Table B-2. Fields required for every controlled decision-bearing record	52
Table B-3. Record-specific minimum additions	53
Table C-1. Consequence categories to be made specific in the project profile	55
Table C-2. Minimum assurance architecture	55
Table C-3. Non-compensable decision conditions	56
Table D-1. Minimum hazard-log fields	57
Table D-2. Barrier challenge questions	57
Table D-3. Illustrative ground-equipment hazard record	58
Table E-1. Safety-case structure	59
Table E-2. Evidence disposition rules	59
Table F-1. Mandatory release prerequisites	61
Table F-2. Decision states	61
Table G-1. Change screening	63
Table H-1. Required task profile	64
Table H-2. Safety handover record	64
Table I-1. Occurrence intake record	65
Table I-2. Causal-analysis completeness check	65

Table J-1. Safety performance indicator structures	67
Table K-1. Engineering assurance controls	69
Table K-2. Test evidence validity checks	69
Table K-3. Digital safety controls	70
Table L-1. Aviation readiness and continuing assurance	71
Table L-2. Ground-service assurance	71
Table L-3. Maintenance safety evidence	72
Table L-4. End-to-end unmanned assurance	72
Table M-1. Space mission assurance by phase	73
Table M-2. Defense aerospace safety interfaces	73
Table M-3. Critical-support controls	74
Table N-1. Required workflow controls	75
Table O-1. Required supplier agreement content	76
Table P-1. Required evaluation plan	77
Table P-2. Role-specific competence	77
Table Q-1. Finding and decision implications	79
Table R-1. Claim payload	80
Table S-1. Failure-free exposure and the 95% upper rate bound	82
Table S-2. Zero-failure sample sizes at one-sided 95% confidence	83
Table S-3. Synthetic operational data	84
Table S-4. Dependency sensitivity	85
Table S-5. Branch contributions to severe outcome	86
Table S-6. Interval sensitivity under the simplified model	87
Table S-8. Decision outcomes under the stated rule	89
Table S-9. Response budget	90

Table S-10. Illustrative probability budget	91
Table S-11. Required reporting layers	92
Table S-12. Recovery acceptance checks	93
Table T-1. Case definition and initial evidence	94
Table T-2. Required decision trail	94
Table T-3. Maintenance case records	96
Table T-4. Closure and release logic	96
Table T-5. Unmanned-system case definition	97
Table T-6. Evidence needed before release	97
Table T-7. Mission case record	98
Table T-8. Gate disposition	98
Table T-9. Combined-condition case	99
Table T-10. Release and monitoring	99
Table T-11. Recovery case states	100
Table T-12. Recovery acceptance	100
Table U-1. Distinctions that preserve decision meaning	101
Table U-2. Selecting analytical methods	101
Table U-3. Common misleading substitutions	102
Table W-1. Requirement and evidence challenges	109
Table W-2. Authority and release challenges	109
Table W-3. Data, transfer and recovery challenges	110
Table W-4. Operational challenge examples	110
Table X-1. End-to-end evidence trail	112
Table X-2. Aircraft operator first-case evidence	112
Table X-3. Maintenance first-case evidence	113

Table X-4. Ground-service first-case evidence	113
Table X-5. UAS first-case evidence	114
Table X-6. Space mission first-case evidence	114
Table X-7. Supplier first-case evidence	114
Table Y-1. Document identity and status	116
Table Z-1. Questions and primary provisions	118
Table Z-2. Implementation sequence and evidence of completion	119

0 Introduction and application principles

AF 9200 establishes a connected approach to aerospace safety and operational assurance. Its purpose is to make the relationship between a defined operation, credible harm, preventive and protective controls, evidence, human authority and continuing performance explicit. Safety is demonstrated through a maintained argument supported by valid evidence; it is not inferred from a low event count, a completed checklist or an organizational title.

The framework covers aviation, space and defense aerospace activities and the industrial, digital and service interfaces on which they depend. The same principles apply at different scales, but the evidence needed for a workshop task is not identical to that needed for a crewed mission. The organization shall tailor the depth of demonstration to the consequence, complexity, uncertainty, exposure and reversibility of its activity while retaining every applicable requirement.

0.1 Purpose and intended outcomes

(a) The organization shall establish and maintain a safety and operational assurance system that identifies hazardous conditions, sets justified safety requirements, controls relevant exposure and verifies that controls remain effective throughout the claimed lifecycle.

(b) The system shall produce a traceable decision for every safety-significant transition: proceed within the authorized envelope, proceed with explicitly bounded restrictions, hold pending evidence, or stop and make safe. The decision shall identify its object, configuration, conditions, accountable authority and expiry or review trigger.

(c) Operational continuity, commercial delivery and mission success shall be assessed separately from safety. A successful mission with an uncontrolled hazardous condition shall not be recorded as evidence that the condition was acceptable.

Required evidence: Approved scope; safety programme; hazard register; control verification; release decisions; monitoring records; improvement actions.

0.2 The assurance chain

Table 0-1. The AF 9200 assurance chain

Stage	Required question	Demonstrable output
Define	What is operated, by whom, where, in which configuration and under what conditions?	Bounded system and operational profile
Understand	What can cause harm, including interactions and unexpected behavior?	Scenario-based hazard and dependency analysis
Control	Which measures prevent, detect, contain or recover the hazardous state?	Allocated requirements and barrier performance standards
Demonstrate	Why is each safety claim justified, and where does uncertainty remain?	Valid evidence, argument and independent challenge
Authorize	Who may accept residual risk and permit this particular transition?	Scoped, conditional and time-bounded decision
Maintain	What would invalidate that decision, and how will this be detected?	Monitoring, change control, reassessment and learning

0.3 Relationship between quality, safety and assurance

(a) Quality management establishes controlled and repeatable processes; safety assurance establishes whether the resulting system and operation satisfy the applicable safety objectives. Process conformity alone shall not be accepted as proof of safe behavior.

(b) AF 9100 may supply common controls for competence, documents, suppliers, configuration and improvement. An organization using those controls shall identify the shared records and demonstrate their adequacy for AF 9200. Duplicate records are unnecessary, but the AF 9200 safety conclusions shall remain explicit.

(c) A conformity assessment, an operational release and a statutory permission are different decisions. No conclusion under this document shall be presented as a substitute for a legally required authorization.

0.4 Requirement, evidence and decision states

(a) Each applicable requirement shall have one of four recorded states: PASS, FAIL, HOLD or approved N/A. PASS means conformity has been demonstrated for the defined object and conditions. FAIL means a requirement is not met. HOLD means the available evidence does not support a determination. N/A means the activity and retained responsibility that trigger the requirement are absent and the exclusion has been justified and approved.

(b) Evidence shall have its own state: planned, collected, under review, accepted for a stated purpose, rejected, superseded or unavailable. Evidence receipt shall not automatically set a requirement to PASS.

(c) A score, average, maturity rating or number of successful tests shall not compensate for a failed applicable requirement. Unknown risk, unresolved critical assumptions and unavailable essential evidence shall not be converted to low risk.

Decision control: An applicable FAIL or HOLD blocks the affected positive conformity claim. Operational decisions shall additionally satisfy the release and residual-risk controls in Clauses 8 and 12.

0.5 Language conventions and document status

In this document, "shall" expresses a proposed requirement, "should" expresses a recommendation, "may" expresses permission within the stated conditions, and "can" expresses possibility or capability. "Including" introduces examples and does not limit the required analysis. Tables identified as normative have the same force as the requirements that invoke them. Informative examples do not establish universal engineering limits.

This First Edition manuscript is prepared for Aerospace Federation publisher review. Its normative provisions describe the intended requirement set; approval, publication and effective dates have not been assigned in this manuscript. Document preparation does not demonstrate completed consultation, technical validation or approval. The status controls on page 2 and in Annex Y govern representation of the document.

0.6 Proportionality without loss of control

(a) Tailoring shall change the depth, method and frequency of assurance in response to justified conditions; it shall not remove an applicable safety objective. The organization shall document its rationale and obtain approval from the relevant technical authority before relying on a reduced assurance activity.

(b) Small organizations may combine roles where competence and independence requirements remain satisfied. For severe consequences or conflicts of interest, an independent competent reviewer shall be used.

(c) Novel technology, sparse operating data, uncertain models or irreversible transitions shall increase the required challenge and protective measures. An absence of historical failures shall not by itself

justify reduced assurance.

1 Scope, boundaries and conformity model

1.1 Activities within scope

This document specifies requirements for managing and demonstrating safety and operational assurance across concept development, design, integration, manufacture, testing, commissioning, operation, maintenance, modification, withdrawal and disposal. It applies to organizations performing work directly and to organizations retaining responsibility for outsourced work or essential interfaces.

The scope includes aircraft and installed systems; aerodromes and ground operations; maintenance and technical support; unmanned and remotely operated aircraft; advanced air mobility; launch and ground support; orbital, in-space and surface missions; defense aerospace and dual-use activities; and safety-relevant infrastructure, energy, software, data and supply-chain services. Applicability depends on actual activities and interfaces, not the organization's name.

1.2 Evaluated objects

- (a) The organization shall identify whether the evaluated object is an organizational safety system, a product or integrated system, an operation or mission, a service, a process, or a defined change. The claim shall state the object explicitly.
- (b) Personnel competence and assessment-provider competence are supporting controls. An individual shall not be required to demonstrate an entire corporate system merely to demonstrate a bounded task authorization. Conversely, a corporate certificate shall not be treated as individual task competence.
- (c) A product-level argument shall include the necessary operational assumptions and installation constraints. An operator shall verify that those assumptions hold in the actual operation before relying on the product argument.

Required evidence: Object definition; evaluated activities; sites; lifecycle phases; interfaces; responsibility matrix; claims and exclusions register.

1.3 Scope boundaries and exclusions

- (a) Boundaries shall identify physical systems, organizational authority, geography, operating conditions, time, external services, data inputs and affected people. The analysis shall include people outside the organization who may be exposed to harm.
- (b) A boundary shall not be placed so that a hazardous interaction, retained duty or essential dependency disappears from the assurance argument. A supplier's activity may be outside direct control while remaining an essential dependency requiring assurance.
- (c) Exclusions shall identify the absent activity, supporting evidence, approving authority and review trigger. Lack of access to a site, unavailable personnel, missing data or a failed result shall not be represented as non-applicability.
- (d) The scope shall distinguish safety of the aerospace activity from general business continuity. Supporting facilities and workplace conditions shall be included where they can affect the safety of people, operations or products within the defined scope.

1.4 Limits of the conformity model

- (a) A claim shall identify the controlled edition, applicable provisions, object, configuration, locations, lifecycle phase, evidence period and limitations. It shall distinguish a self-assessment from an independent assessment.
- (b) This document does not establish a statutory permission, operational license, airworthiness approval, mission authorization or authorization to conduct hazardous tests. Such decisions remain with

the competent authorities and accountable organizations.

(c) Safety controls for defense aerospace are included. Tactical effectiveness, targeting methods and weapon employment are outside the technical purpose of this document. Safety evidence shall address storage, handling, segregation, interfaces, maintenance and authorized operation without converting this framework into an operational instruction for weapon use.

(d) No claim of "zero risk", "universally safe" or equivalent unlimited assurance shall be made on the basis of this document.

1.5 Multi-organization and multi-site application

(a) Each participating organization shall identify its own decision rights and retained responsibilities. A lead integrator shall coordinate interface closure but shall not silently assume another party's legal authority.

(b) A common management system may support multiple sites. Site-specific hazards, infrastructure, personnel, emergency capabilities and operational restrictions shall still be evaluated.

(c) When sites or partners use different criteria, the interface agreement shall identify compatible units, severity meanings, exposure denominators, acceptance authorities and escalation rules. An unresolved incompatibility shall block the affected transition.

2 Application, precedence and the AF framework

2.1 Self-contained application

The main clauses and normative annexes form the AF 9200 requirement set. This document does not incorporate another organization's standard by reference. Applicable external obligations remain independently binding and shall be identified by each user in its obligation register. The absence of a named external reference in this document shall not be interpreted as exemption from those obligations.

2.2 Order of precedence

(a) The organization shall satisfy applicable law and competent-authority conditions, the declared AF 9200 requirements, and applicable contractual or programme commitments. These conditions are cumulative where they can be satisfied together.

(b) Where conditions conflict, the organization shall record the conflict, protect the affected activity, obtain a determination from the competent authority or contractual decision maker as relevant, and prevent an unsupported conformity claim. Internal preference shall not resolve a legal conflict.

(c) A project profile may specify a stricter limit than this document. It shall not weaken a mandatory control, erase a required evidence item or replace independent challenge with a commercial acceptance.

Required evidence: Obligation register; applicability matrix; conflict determinations; authorized profile; controlled interpretations.

2.3 Activity-triggered application

(a) Clauses 0-16 and 27-28 establish the common architecture and shall be applied to the extent of the evaluated responsibility. Clauses 17-26 shall be added whenever their activities or essential interfaces are present.

(b) Annex A shall be used to map activities to clauses. The organization shall review all technical modules rather than selecting only a preferred sector label.

(c) An emerging activity that is not named explicitly shall be assessed by function, exposure and lifecycle. It shall be assigned the relevant controls through a documented technical determination. New terminology shall not create an automatic exclusion.

2.4 Complementary AF publications

(a) Shared evidence with AF 9100 shall retain its original identity, configuration, purpose and acceptance status. The organization shall identify what additional safety argument is required for AF 9200.

(b) A concept-stage programme item shall not be treated as a published normative dependency. Future AF publications may be used only through an explicit controlled reference that identifies edition, status and relevance.

(c) ASTRA assessment arrangements, where separately authorized and applicable, remain distinct from product safety and operational release. Participation or membership does not establish either outcome.

2.5 Completed parameter schedules

(a) The organization shall complete Annex B before making a release or conformity decision that depends on a parameter. Every entry shall state the value or rule, unit, applicability, technical basis, owner, approver and review trigger.

(b) "As appropriate", "acceptable", "timely", "adequate" and equivalent terms shall be resolved into measurable criteria or explicit decision rules in the profile where the result affects acceptance.

(c) A missing parameter shall cause HOLD for the dependent decision. A value copied from an informative example shall not be accepted without evidence that it is suitable for the actual context.

Decision control: The profile shall be approved before the relevant analysis or test is used for acceptance. Retrospective changes designed only to make a result pass are prohibited.

3 Terms, definitions and conventions

3.1 Core terms

Table 3-1. Core safety and assurance terms

Term	Meaning in AF 9200
Safety	Condition in which the risk of harm is controlled to the criteria applicable to the defined activity and lifecycle.
Harm	Injury or loss of life, damage to property or environment, or other safety consequence defined in the approved profile.
Hazard	A condition, state or source with the potential to cause or contribute to harm.
Hazardous event	An occurrence or transition that realizes a hazard or moves the system toward a harmful outcome.
Scenario	A defined sequence or combination of conditions, actions, failures and outcomes, including relevant context.
Risk	Combination of consequence and the likelihood of a specified harmful outcome for a stated exposure and context.
Residual risk	Risk remaining after the credited controls and their limitations have been considered.

Term	Meaning in AF 9200
Uncertainty	Incomplete knowledge or variability affecting the interpretation, prediction or decision.
Exposure	Opportunity for a hazardous event, expressed with a defined population, activity or time basis.
Safety objective	Required safety outcome against which a defined system or activity is judged.
Safety requirement	Verifiable condition allocated to a system, process, person or interface to achieve a safety objective.
Barrier	A measure that prevents, detects, contains or mitigates a hazardous scenario.
Barrier performance standard	Defined function, capacity, response time, availability, integrity and verification criteria for a barrier.
Barrier impairment	A condition that reduces a credited barrier's ability to perform its required function.
Safety-critical element	An element whose failure, incorrect operation or absence can materially contribute to severe harm.
Safe state	A defined state that controls the relevant hazards for the stated conditions; it is not necessarily an unpowered state.
Operating envelope	Approved limits and conditions within which the safety argument remains supported.
Operational assurance	Continuing demonstration that an operation is controlled within its authorized envelope and assumptions.
Safety case	Structured argument, supported by evidence, explaining why stated safety claims are justified for a defined context.
Claim	A proposition whose validity is asserted for a stated object, scope and conditions.
Evidence	Information used to support or challenge a claim, with identified origin, configuration, method and acceptance purpose.
Defeater	A condition, observation or argument that could invalidate or materially weaken a claim.
Assumption	A condition treated as true for analysis or decision that requires justification, monitoring or subsequent confirmation.
Independent review	Competent examination with sufficient separation from the work and incentives being evaluated.
Common-cause failure	Failure of multiple elements due to a shared cause or dependency.
Common-mode behavior	Similar response of multiple elements to a condition, whether or not the elements share a physical component.

Term	Meaning in AF 9200
Latent condition	A condition that can remain undetected until combined with another event or demand.
Demand	An occurrence requiring a safety function to act.
Risk acceptance	An accountable determination that residual risk satisfies the approved criteria for a defined scope and period.
Operational release	Permission by the designated authority to begin or continue a specified activity under stated conditions.
Concession	Authorized disposition of a specified nonconformity; it does not change a failed AF 9200 requirement into conformity.
Change	An alteration to a system, operation, organization, interface or assumption that can affect the assurance basis.
Occurrence	An event or observation relevant to safety, including accidents, incidents, near misses and weak signals.
Just reporting culture	A reporting environment that protects good-faith disclosure while retaining fair accountability and lawful process.
Human performance	Human action and capability as influenced by task, tools, information, workload, fatigue and organizational conditions.
Competence	Demonstrated ability to perform a defined task under specified conditions.
Configuration baseline	Controlled description of the approved hardware, software, data, procedures and interfaces.
Recovery	Controlled restoration to an authorized condition after disruption, failure or protective action.
Readiness	Demonstrated satisfaction of the conditions required to enter a specified lifecycle phase or operation.
Continuing validity	Ongoing applicability of evidence and decisions as configuration, exposure, knowledge and conditions change.

3.2 Record and state conventions

(a) A record identifier shall be unique within the declared system and stable through its controlled history. Reuse of a retired identifier for another object is prohibited.

(b) Time records shall identify their time basis and, where sequence matters, clock synchronization and uncertainty. "Current" shall mean verified against the authoritative baseline at the relevant decision time.

(c) Each recorded conclusion shall distinguish an observed fact, an inference, a hypothesis and an assumption. A hypothesis shall not be promoted to fact merely because it appears in several reports.

(d) The word "closed" shall state what has closed: an action, a finding, a hazard-control verification task or an operational restriction. A hazard may remain present and controlled after its mitigation actions have closed.

3.3 Abbreviations

Table 3-2. Abbreviations used in this document

Abbreviation	Meaning
AF	Aerospace Federation
AL	Assurance level defined in Annex C
AI	Artificial intelligence
CCF	Common-cause failure
FMEA	Failure modes and effects analysis
FTA	Fault tree analysis
ODD	Operational design domain for a bounded automated function
O&M	Operations and maintenance
PFD	Probability of failure on demand
RACI	Responsible, accountable, consulted and informed role allocation
SMS	Safety management system
SPI	Safety performance indicator
UAS	Unmanned aircraft system
V&V	Verification and validation

4 System definition and lifecycle context

4.1 System and operation description

(a) The organization shall describe the system as operated, not only as designed. The description shall include intended functions, physical and digital architecture, personnel, procedures, supporting infrastructure, external services and affected populations.

(b) The description shall distinguish normal, abnormal, emergency, maintenance, test, storage, transport and decommissioned states. Transitions between states shall be analyzed where sequencing can create a hazard.

(c) Drawings and models shall identify their baseline and limitations. Simplified diagrams shall retain the interfaces that can affect safety, including shared power, timing, data, communications, cooling, access and human supervision.

Required evidence: System description; lifecycle map; interface register; state and transition model; affected-population analysis.

4.2 Operational concept and environment

- (a) The operational concept shall define mission or service objectives, users, staffing, operating locations, traffic or activity interactions, environmental conditions, duration, support arrangements and contingency expectations.
- (b) Environmental assumptions shall include foreseeable extremes and combinations relevant to the activity, such as temperature, weather, contamination, radiation, vibration, electromagnetic conditions, terrain, visibility, occupancy and access restrictions.
- (c) The organization shall identify how the operating environment is measured or otherwise confirmed. If an envelope boundary cannot be detected with sufficient confidence and time, the design shall provide additional protection or restrict the operation.

4.3 Interfaces and retained responsibilities

- (a) Each safety-relevant interface shall have a named owner on each side, a defined exchanged item or service, compatibility criteria, failure behavior, notification rules and a closure record.
- (b) Interface analysis shall include incorrect, missing, stale, delayed, repeated, reordered and contradictory information. A correct data value with the wrong timestamp or configuration shall be treated as a potentially unsafe input.
- (c) Unowned interfaces shall remain open. A lead party shall escalate unresolved ownership before the affected lifecycle gate.

Decision control: No release shall depend on an essential interface for which responsibility, operating limits or failure response remain undefined.

4.4 Stakeholders and obligations

- (a) The organization shall identify people and entities that supply safety inputs, bear exposure, control constraints or receive safety information. Consultation shall include operational personnel and maintainers with direct knowledge of the work.
- (b) An obligation register shall identify requirement origin, jurisdiction or contractual applicability, affected activity, accountable owner, evidence and change-monitoring source.
- (c) Restricted or classified evidence shall be handled through authorized access arrangements. Restrictions shall not justify an unsupported safety conclusion; the reviewer shall record what could be examined and any resulting limit on assurance.

4.5 Lifecycle boundaries and disposal

- (a) The lifecycle description shall include commissioning, service growth, modifications, life extension, ownership transfer, storage, reactivation, withdrawal and disposal where relevant.
- (b) Residual hazardous energy, contamination, software credentials, hazardous materials and incomplete records shall be addressed at transfer and retirement.
- (c) Long-duration or unattended systems shall include the loss of ground support, obsolete equipment, degraded communications and loss of organizational knowledge in their lifecycle assumptions.

5 Leadership, governance and safety culture

5.1 Accountable executive and technical authority

- (a) The organization shall appoint an accountable executive with authority to provide resources, resolve cross-functional conflicts and require protective action. Delegation shall identify its scope and shall not erase retained accountability.

(b) Technical authorities for system safety, operations, design, maintenance, digital systems and emergency coordination shall be defined as applicable. A decision requiring several authorities shall identify how disagreement is resolved.

(c) Safety decisions shall be protected from unauthorized commercial override. Where cost or schedule influences a selected option, the decision record shall distinguish that consideration from evidence that the option satisfies safety criteria.

Required evidence: Governance structure; signed delegations; competence and independence records; decision escalation records.

5.2 Policy and objectives

(a) The policy shall commit the organization to effective hazard control, truthful reporting, compliance with applicable obligations, protected escalation, competent work and learning from failure and weak signals.

(b) Objectives shall be measurable and linked to exposure and control effectiveness. Targets that discourage reporting or reward the absence of recorded events without checking reporting quality shall not be used as sole safety objectives.

(c) Leaders shall communicate the policy in forms understood by affected personnel and verify understanding through observed decisions, exercises and interviews.

5.3 Stop-work and protective authority

(a) Every person performing or supervising safety-relevant work shall have a clear route to report a concern and request that the activity be paused. The organization shall identify who can command an immediate protective state and who can authorize restart.

(b) Personnel shall not be penalized for a good-faith protective intervention. An urgent stop shall be documented as soon as practicable after protection is established; paperwork shall not delay immediate protective action.

(c) Restart shall require examination of the initiating concern, the condition of the system after the stop and the validity of the proposed controls. The person who demanded restart for delivery reasons shall not be the sole reviewer of an unresolved safety objection.

5.4 Independence and conflicts of interest

(a) Independence shall be determined by actual decision and reporting relationships, authorship, financial incentives and prior involvement. A different job title alone shall not establish independence.

(b) Reviewers shall disclose relevant conflicts. A material conflict shall be removed, controlled with documented justification, or assigned to another competent reviewer.

(c) For severe-consequence decisions and high-uncertainty novel systems, the review shall be sufficiently separate to challenge assumptions, access underlying evidence and recommend HOLD without retaliation.

5.5 Resources and organizational capacity

(a) The organization shall provide enough competent personnel, infrastructure, time and budget to perform required controls and maintain evidence. Resource shortfalls shall be recorded as safety-relevant conditions where they can degrade assurance.

(b) Workload, backlog, turnover, contractor dependence and loss of key competence shall be monitored. A capacity forecast shall be reviewed before major service growth or simultaneous projects.

(c) The executive shall resolve persistent control failures and overdue critical actions. Repeated extensions shall trigger a review of the adequacy of the safety programme and resource allocation.

5.6 Fair accountability and protected reporting

(a) The organization shall distinguish inadvertent error, system-induced error, capability limitations, reckless conduct and deliberate misconduct through a fair documented process. A harmful outcome alone shall not establish culpability.

(b) Reporting channels shall provide confidential handling, feedback and protection from retaliation, within applicable legal limits. Confidentiality shall not be promised beyond the organization's lawful ability to protect it.

(c) The safety investigation function and disciplinary decision function shall have defined boundaries. Safety-critical facts shall still reach those who need them to control risk.

6 Safety planning and assurance depth

6.1 Integrated safety programme

(a) The organization shall maintain a safety programme covering objectives, deliverables, methods, roles, competence, interfaces, resources, independent reviews and lifecycle gates. The programme shall be integrated with engineering and operational plans.

(b) Each deliverable shall identify its acceptance criteria, responsible author, reviewer, approver, required inputs and dependent decisions. A document completion date shall not be the sole measure of readiness.

(c) The programme shall identify iterative activities. Hazards, assumptions and controls shall be revisited as knowledge, design, exposure or operating conditions change.

Required evidence: Programme plan; deliverable schedule; gate map; assurance-level rationale; resource allocation; review records.

6.2 Assurance-level selection

(a) Assurance depth shall be assigned using Annex C. The determination shall consider the worst credible consequence, novelty, complexity, coupling, uncertainty, exposure and reversibility.

(b) The assigned level shall govern independence, analysis breadth, verification depth, operational demonstration, data confidence and continuing review. It shall not be used as a substitute for a quantified safety objective where such an objective is required.

(c) Multiple functions within one system may have different assurance levels. Shared resources and interactions shall be addressed at the level needed to protect the most demanding affected claim.

6.3 Lifecycle gates

(a) The programme shall establish gates for concept acceptance, requirements baseline, design commitment, test readiness, operational readiness, continuing operation, major change and retirement as applicable.

(b) Gate criteria shall include the configuration baseline, applicable requirements, hazard disposition, evidence validity, open issues, personnel readiness, emergency capability and authority conditions.

(c) Deferred work shall be identified with its consequence and dependency. Deferral shall not permit an activity that requires the missing evidence or control.

Decision control: A conditional gate decision shall state precisely what may proceed and what remains prohibited. Conditions shall be verified before the next dependent transition.

6.4 Planning for uncertainty and new knowledge

- (a) The programme shall identify major knowledge gaps and how they will be reduced or bounded. Planned tests shall be selected for their ability to challenge the decision, not only to confirm expected behavior.
- (b) Research results, simulations and service experience shall be evaluated for representativeness. Uncertainty shall remain visible when transferred between analyses.
- (c) A contingency budget shall include time, resources and alternate technical options where an adverse result could otherwise create pressure to waive a safety condition.

6.5 Review frequency and triggers

- (a) Scheduled reviews shall be defined in Annex B and justified by exposure, degradation mechanisms and the time available to detect and control deterioration.
- (b) Unscheduled review shall be triggered by an occurrence, changed operating envelope, significant personnel or supplier change, barrier impairment, new failure mechanism, cyber compromise, contradictory evidence or expiry of an essential assumption.
- (c) The next scheduled review date shall not delay action on a triggered condition. The activity owner shall determine immediate containment while the broader review proceeds.

7 Hazard identification and the lifecycle hazard register

7.1 Systematic identification

- (a) The organization shall identify hazards across the defined lifecycle, operating states and interfaces. Identification shall include intended use, reasonably foreseeable misuse, maintenance error, incorrect sequencing, loss of supporting services and combinations of failures or adverse conditions.
- (b) Analysis shall use more than one perspective where a single method can miss relevant interactions. Functional analysis, failure analysis, scenario review, operational observation, human-task analysis and structured expert challenge shall be selected according to the system.
- (c) Frontline personnel, maintainers, designers, suppliers and emergency responders shall participate where they possess knowledge relevant to the scenario. Participation shall be recorded with the boundaries of the review.

Required evidence: Hazard-identification plan; participant competence; system baseline; method rationale; scenario list; unresolved questions.

7.2 Hazard statements and causal structure

- (a) Each hazard record shall distinguish the hazardous condition from its causes, initiating events, exposed population, top event and consequences. A label such as "human error" or "equipment failure" without a defined mechanism shall be insufficient.
- (b) The scenario shall specify the operating state, environment, configuration, exposure unit and applicable assumptions. Consequence shall be evaluated for the credible outcome before crediting controls that the analysis is intended to verify.
- (c) Chains that share a cause, barrier or exposed population shall be linked. Repeated wording shall not create a false impression of independent risk contributors.

7.3 Normal operation, failure and emergence

(a) The organization shall examine hazardous behavior that can occur while individual components meet their specifications. Conflicting commands, incorrect timing, misleading information and incompatible control objectives shall be considered.

(b) Analysis shall include latent failures, common-cause failures, common-mode behavior, maintenance-induced faults and protection-system dependencies.

(c) Adaptive or learning systems shall be examined for behavior outside the validated domain, drift, unexpected interactions and inability to explain or reproduce a safety-relevant output.

7.4 Hazard register and ownership

(a) The hazard register shall contain the fields in Annex D. Every active hazard shall have an accountable owner, control owners, current risk basis, linked evidence, assumptions, actions and review triggers.

(b) Hazard acceptance shall not delete the hazard. The register shall retain the hazardous condition, credited controls, residual-risk decision and continuing monitoring obligation.

(c) Transferred hazards shall identify the receiving party, information supplied, acceptance of responsibility and unresolved limitations. A dispatch note or purchase order shall not by itself demonstrate accepted transfer.

Decision control: An unowned hazard with a credible severe consequence shall block the affected release until responsibility and protective action are established.

7.5 Completeness review

(a) Before a lifecycle gate, a competent reviewer shall compare the hazard set against the system functions, operating states, interfaces, energy sources, human tasks and failure experience.

(b) The review shall identify blind spots, excluded scenarios and the rationale for exclusion. A blank checklist item shall not mean "no hazard".

(c) New information shall reopen analysis where it changes a causal model, consequence, exposure, barrier credit or acceptance basis. Reopening shall preserve the prior record and the reason for the change.

8 Risk analysis, evaluation and accountable acceptance

8.1 Risk criteria before assessment

(a) The organization shall define and approve risk criteria before using them for acceptance. Criteria shall identify severity categories, likelihood basis, exposure denominator, uncertainty treatment, escalation thresholds and acceptance authority.

(b) The criteria shall distinguish technical acceptability from management attention. A color in a risk matrix shall not by itself authorize operation.

(c) Where mandatory quantitative objectives apply, qualitative categories shall supplement and shall not replace those objectives. The profile shall identify the applicable numerical units and aggregation rules.

Required evidence: Approved risk profile; analysis method; data sources; uncertainty register; independent review; residual-risk decisions.

8.2 Consequence and likelihood

- (a) Severity shall be assigned using the worst credible consequence for the scenario and the exposed populations. Different consequence dimensions shall be retained when a single category would hide a material effect.
- (b) Likelihood shall state whether it is a probability per demand, rate per operating hour, frequency per mission, conditional probability or another defined quantity. Values with different denominators shall not be directly compared or added.
- (c) Quantitative estimates shall identify data selection, model assumptions, dependence, censoring, confidence or uncertainty bounds and applicability to the configuration being assessed.
- (d) Sparse data or zero observed events shall not be treated as zero probability. Annex S provides illustrative calculations showing why exposure and confidence matter.

8.3 Risk reduction and option selection

- (a) The organization shall first consider eliminating the hazard or reducing it by design. Remaining controls shall prioritize robust engineering measures before relying solely on warnings, procedures or operator vigilance.
- (b) Options shall be compared using safety benefit, failure behavior, independence, maintainability, human workload, verification feasibility and lifecycle effects. A control that creates a new hazardous interaction shall be assessed before adoption.
- (c) The selected control set shall satisfy mandatory criteria and demonstrate that practicable further reductions have been evaluated using a recorded decision rule. Financial benefit shall not compensate for violation of an applicable safety requirement.

8.4 Barrier credit and combined risk

- (a) Barrier credit shall be supported by a verified performance standard and current evidence. Unverified future actions shall not be credited as implemented controls.
- (b) Multiplication of barrier failure probabilities shall be permitted only where conditional independence is justified for the scenario. Shared power, software, sensing, maintenance, environment, personnel and timing shall be evaluated.
- (c) Simultaneous concessions, temporary changes and degraded barriers shall be assessed together. Individually acceptable deviations shall not be assumed acceptable in combination.
- (d) Aggregate risk shall retain severe low-frequency contributors and exposure to different populations. Averaging across sites or missions shall not conceal an unacceptable local condition.

8.5 Acceptance authority and record

- (a) Residual risk shall be accepted by a person with defined authority, competence and accountability for the affected activity. Authority levels shall increase with consequence and uncertainty as defined in Annex C.
- (b) The acceptance record shall identify the exact configuration, scenario, controls, residual risk, evidence, assumptions, operational restrictions, monitoring, review date and invalidation triggers. Acceptance by an unauthorized role is invalid.
- (c) Acceptance shall require closure of applicable mandatory requirements. Where a separate authority permits a bounded deviation, the record shall preserve the AF 9200 nonconformity and limit the claim accordingly.
- (d) A decision maker shall record dissent and the resolution of material technical objections. Acceptance shall not be inferred from silence or attendance at a meeting.

8.6 Reassessment and expiry

- (a) Risk acceptance shall cease to support the affected activity when its configuration, conditions, essential evidence, barrier capability or authority basis is no longer valid.
- (b) The organization shall identify the safe response to expired or invalidated acceptance. Continued operation requires a fresh authorized decision before exposure continues, except immediate protective actions necessary to reach a safer state.
- (c) Temporary acceptance shall have a defined end condition and shall not renew automatically. Repeated extension shall trigger independent review of the permanent solution.

Decision control: Unbounded uncertainty in a severe-consequence scenario shall result in HOLD or a demonstrably protective restriction; it shall not be assigned the lowest likelihood category by default.

9 Safety requirements and engineered controls

9.1 Allocation and traceability

- (a) Safety objectives shall be translated into verifiable requirements allocated to hardware, software, people, procedures, infrastructure and interfaces. Each requirement shall identify the hazard or claim it supports.
- (b) Requirements shall define the triggering condition, required behavior, performance limit, response time, environmental range, failure response and verification method where relevant.
- (c) Traceability shall run in both directions: from hazard to control and evidence, and from each credited control to the hazard and decision it supports. Orphan controls and unsupported hazards shall be reviewed.

Required evidence: Safety-requirement register; allocation model; interface requirements; verification matrix; design review and independence analysis.

9.2 Robustness and independence

- (a) Safety-critical controls shall be protected from foreseeable single failures and common causes to the extent required by the approved safety objectives. The analysis shall identify what the architecture can and cannot tolerate.
- (b) Redundancy shall not be equated with independence. Separate channels using the same sensor, power source, software defect or maintenance process shall be evaluated for shared failure.
- (c) Diversity shall be justified by the failure mechanisms it addresses. Superficial differences in supplier or programming language shall not establish independence without analysis.

9.3 Protective functions and safe states

- (a) Every protective function shall have a defined trigger, operating range, detection capability, actuation time, persistence, reset conditions and fail behavior.
- (b) The selected safe state shall be demonstrated for the actual phase. Removing power may be appropriate for a ground asset and hazardous for an airborne or life-support function; the determination shall be specific.
- (c) Automatic protection shall consider false activation, missed activation, oscillation, repeated resets and conflict with other protective functions.
- (d) Manual intervention shall be credited only where detection, comprehension, decision time, access, training and workload have been demonstrated under representative conditions.

9.4 Verification and validation

- (a) Verification shall establish that the specified control has been implemented correctly. Validation shall establish that the control addresses the actual operational hazard and supports the intended use.
- (b) Test conditions shall cover relevant boundaries, adverse combinations, failure insertion, degraded states and recovery. The test plan shall define pass criteria and safety constraints before execution.
- (c) Test equipment, data acquisition, environmental conditions and uncertainty shall be suitable for the decision. A pass obtained with invalid equipment or an unrepresentative configuration shall not be accepted.
- (d) Failed tests and anomalies shall be preserved and dispositioned. Repeating a test until a pass occurs shall not erase earlier evidence.

9.5 Maintainability of safety controls

- (a) Controls shall be designed for inspection, proof testing, calibration, repair and restoration without introducing unacceptable hazards.
- (b) Hidden or dormant protective functions shall have a justified means of detecting degradation before the next relevant demand. Inspection intervals shall reflect the failure mechanism and exposure.
- (c) Temporary bypasses and overrides shall be visible, authorized, time-bounded and assessed for combined effects. The system shall prevent an unnoticed bypass from persisting into an incompatible operating state.

10 Safety cases, evidence and independent challenge

10.1 Structured argument

- (a) A safety case shall define its top-level claim, scope, configuration, operating envelope, assumptions, subordinate claims, supporting evidence, uncertainties and known limitations.
- (b) The argument shall explain why the evidence is sufficient, relevant and valid. A list of documents without reasoning shall not constitute a safety case.
- (c) The case shall distinguish design evidence, operational evidence and organizational controls. Strength in one category shall not conceal the absence of another category required by the claim.

Required evidence: Claim structure; evidence index; assumptions and defeaters; independent review findings; acceptance and maintenance records.

10.2 Evidence quality and provenance

- (a) Evidence shall identify who produced it, when, using which method and configuration, with what competence and equipment, and for what intended acceptance purpose.
- (b) Borrowed, reused or inherited evidence shall undergo an applicability assessment. Differences in environment, loads, software, population, operating procedure and lifecycle shall be addressed.
- (c) Evidence integrity shall include authenticity, completeness, traceability and protection from unauthorized alteration. A digital signature can support provenance but shall not by itself establish technical correctness.
- (d) Restricted access shall be managed with an authorized review route. Evidence that no competent authorized reviewer can inspect shall remain unavailable for the affected claim.

10.3 Assumptions, uncertainty and defeaters

- (a) Each essential assumption shall have an owner, justification, confirmation method, monitoring method and invalidation trigger. The case shall identify consequences if the assumption is false.

- (b) The organization shall actively seek contradictory evidence. Analysis shall consider known weaknesses, alternate explanations and credible failure of the assurance process itself.
- (c) Confidence shall not be expressed as an unsupported percentage. Where a numerical confidence statement is made, its statistical or analytical meaning and limitations shall be stated.
- (d) A material defeater shall cause the affected claim to be reopened. The prior acceptance shall be suspended or restricted when its support is no longer adequate.

10.4 Independent review and challenge

- (a) Reviewers shall have competence relevant to the system, methods and operational context. The review scope shall identify sampled and fully examined areas.
- (b) Review shall challenge hazard coverage, assumptions, barrier independence, quantitative reasoning, human performance, test representativeness and the credibility of recovery arrangements.
- (c) Findings shall identify the specific claim or requirement, observed evidence, consequence, required action and closure criterion. The author shall not unilaterally close a material independent finding.
- (d) A disagreement shall be recorded and escalated to a competent decision authority. The final disposition shall explain the technical basis and any restriction.

10.5 Living assurance

- (a) The safety case shall be maintained as configuration, operations and knowledge evolve. Monitoring shall be mapped to the assumptions and controls that sustain the case.
- (b) A change-impact query shall identify affected hazards, requirements, tests, training, operational limits and approvals. A document date change alone shall not demonstrate this analysis.
- (c) The operational user shall have access to the limitations, obligations and triggers needed to maintain the case, in a usable form appropriate to the task.

11 Human performance, competence and safety communication

11.1 Human-system integration

- (a) The organization shall analyze safety-relevant tasks in their actual context, including normal work, time pressure, abnormal conditions, handovers and recovery.
- (b) Interfaces shall support correct perception, comprehension and action. Alarm priority, mode awareness, display consistency, units, language, accessibility and error recovery shall be evaluated.
- (c) A safety argument relying on rapid operator response shall include demonstrated detection and response time with allowance for workload, ambiguity, fatigue and environmental conditions.

Required evidence: Task analysis; interface evaluation; workload and fatigue controls; competence records; exercise and communication results.

11.2 Competence and task authorization

- (a) Task requirements shall identify knowledge, practical skills, experience, limitations, supervision and currency. Training attendance alone shall not establish competence.
- (b) Competence shall be demonstrated using representative practical assessment, observation or other justified methods. Assessors shall be competent and sufficiently independent of the candidate's delivery pressure.

(c) Authorizations shall identify permitted tasks, system types, conditions, sites, limitations and expiry or review triggers. The organization shall verify authorization at the point of assignment.

(d) Changes in equipment, procedure, role, health-related fitness restrictions where lawfully applicable, or a prolonged absence shall trigger a reassessment appropriate to the task.

11.3 Staffing, workload and fatigue

(a) Staffing plans shall consider task demand, concurrent duties, supervision, breaks, reserve capability and abnormal workload. A minimum headcount shall not be assumed sufficient without task analysis.

(b) Fatigue controls shall consider duty patterns, night work, rest opportunity, commuting where relevant, cumulative workload and self-reporting. Medical details shall be handled only by authorized roles under appropriate confidentiality.

(c) Personnel shall have a route to report inability to perform safely. The response shall protect the activity and provide appropriate reassignment or relief.

(d) Introducing automation shall not justify reduced staffing until the changed monitoring, intervention and recovery tasks have been demonstrated.

11.4 Communication and handover

(a) Safety-critical communications shall identify sender, receiver, object, action, configuration and timing where relevant. Read-back or equivalent confirmation shall be required where misunderstanding can create severe consequences.

(b) Handovers shall communicate active hazards, degraded barriers, open work, temporary changes, restrictions, pending decisions and responsibility for monitoring.

(c) Translation and terminology shall be controlled where multilingual teams operate. Ambiguous abbreviations or mixed units shall be resolved before use.

(d) Loss of a communication channel shall trigger the defined fallback or safe response. A fallback shall be tested under representative conditions.

11.5 Safety promotion and learning

(a) The organization shall share lessons in a form that changes work practices, design or decision-making. Awareness messages alone shall not close a corrective action requiring technical change.

(b) Exercises shall test realistic difficulties, including incomplete information, conflicting indications and personnel replacement. Debriefs shall identify systemic conditions and improvement actions.

(c) Personnel shall receive feedback on reported concerns, subject to privacy and investigation constraints. Management shall monitor whether reporting routes are trusted and usable.

12 Operational planning, release and continuing control

12.1 Operational plan and envelope

(a) Each operation or repeatable class of operations shall have a controlled plan defining the object, configuration, operating envelope, roles, prerequisites, limits, monitoring, abnormal actions and termination conditions.

(b) Plans shall be available at the point of use. Personnel shall verify the applicable version and identify changes affecting their tasks.

(c) Repetitive operations may use a standing plan, but each execution shall verify the variable conditions that can invalidate it, including personnel, weather, equipment status, traffic, mission data

and temporary restrictions.

Required evidence: Operational plan; readiness checklist; release record; active restrictions; monitoring log; handover and termination records.

12.2 Readiness and release

- (a) The designated release authority shall verify the correct configuration, satisfied prerequisites, accepted residual risk, current competence, equipment serviceability, interface readiness and emergency capability.
- (b) Release criteria shall be defined before the decision. The decision record shall identify evidence references and the actual state of open issues.
- (c) A restricted release shall define permitted activity, prohibited activity, compensating controls, duration, monitoring and termination trigger. It shall not authorize a condition prohibited by an applicable mandatory requirement.
- (d) The release authority shall not accept a general assurance statement where a specific readiness condition remains unverified.

Decision control: No-go criteria shall be explicit and non-compensable. A favorable overall score shall not override a single no-go condition.

12.3 Execution and supervision

- (a) Personnel shall monitor the parameters and conditions needed to maintain the approved envelope. The plan shall define who watches each parameter and who acts on an exceedance.
- (b) Operational deviations shall be recorded with time, conditions, action and authority. An unplanned deviation shall trigger assessment of immediate protection and the continued validity of the release.
- (c) Supervisors shall control concurrent activities, access, permits, isolation boundaries and contractor interfaces. Local optimization shall not defeat a system-level barrier.

12.4 Temporary controls and deferred defects

- (a) A temporary control shall be technically justified, verified, assigned to an owner and given an expiry. It shall identify dependencies and the risk of human error or forgotten restoration.
- (b) Deferred defects shall be assessed individually and in combination. A defect permitted in one operating condition shall not be assumed permitted in another.
- (c) Outstanding temporary controls shall be reviewed at handover and before a change in operating phase. Expired controls shall trigger HOLD or a defined protective restriction.

12.5 Completion and return to a controlled state

- (a) Completion shall include confirmation of system state, residual energy, configuration, records, outstanding defects and responsibility for the next phase.
- (b) Unexpected events, limit exceedances and control activations shall be reviewed before the next operation where they could affect continued safety.
- (c) A completed operational task shall not automatically close the associated assurance obligations. Monitoring, inspection or data review required after the task shall remain assigned and visible.

13 Degraded, abnormal and emergency conditions

13.1 Defined degraded modes

- (a) The organization shall identify degraded conditions that can be tolerated, the conditions under which they are permitted, and the controls required to prevent escalation.
- (b) The analysis shall address combinations of degradations and the loss of monitoring itself. A system shall not remain in an unrestricted state merely because the data needed to detect deterioration are unavailable.
- (c) Entry to and exit from a degraded mode shall have clear criteria, authority and records. The effect on other organizations and shared infrastructure shall be communicated.

Required evidence: Degraded-mode catalogue; combined-condition analysis; emergency plan; exercises; recovery and restart decisions.

13.2 Emergency preparedness

- (a) Emergency plans shall identify credible scenarios, command roles, alerts, communications, protective actions, evacuation or shelter arrangements, rescue interfaces and resource dependencies.
- (b) Response arrangements shall be coordinated with the parties expected to provide assistance. Assumed availability shall be verified for the location, operating hours and hazard type.
- (c) Plans shall consider simultaneous loss of power, communications, access, personnel or supporting infrastructure where credible. An emergency plan shall not depend exclusively on the system whose failure creates the emergency.
- (d) Information needed by responders shall identify hazardous energy, materials, access restrictions, occupancy and isolation arrangements without exposing unnecessary sensitive information.

13.3 Exercises and response capability

- (a) Exercise scenarios shall be selected from the hazard analysis and shall test decision-making, communication, resource mobilization and protective actions.
- (b) Exercises shall include representative adverse conditions and personnel who actually hold the roles. Desk reviews alone shall not demonstrate physical response capability where it is essential.
- (c) Measured response times and failures shall be compared with the safety assumptions. Gaps shall cause corrective action and, where necessary, operational restrictions.

13.4 Immediate response and evidence protection

- (a) Protection of life and control of the hazardous state shall take priority over routine evidence collection. Actions shall be recorded when safe and practicable.
- (b) Once protection is established, relevant data, logs, physical evidence and witness accounts shall be preserved with provenance and access control.
- (c) Communications shall distinguish confirmed facts from preliminary interpretation. External notifications shall follow applicable obligations and authorized channels.

13.5 Recovery and restart

- (a) Recovery shall identify the target safe condition, restoration sequence, tests, inspections, data reconciliation, personnel readiness and external clearances required.
- (b) The organization shall verify that restoration has not introduced new hazards or reinstated the initiating defect. Recovery evidence shall be reviewed by an authorized person independent of the immediate pressure to resume.

(c) Restart shall have a fresh release decision with restrictions and enhanced monitoring where uncertainty remains. Repeated restart failures shall trigger broader system review.

14 Change, configuration and controlled transition

14.1 Change identification

(a) Safety-relevant change shall include hardware, software, data, operating limits, procedures, organization, staffing, suppliers, facilities, interfaces, mission objectives and external conditions.

(b) The change process shall detect cumulative effects of individually small changes. Informal workarounds and recurring temporary controls shall be treated as change signals.

(c) A change shall be categorized using its effect on hazards, assumptions, controls, evidence and authority conditions, rather than cost or size alone.

Required evidence: Change request; impact analysis; configuration comparison; verification plan; transition and rollback plan; updated release.

14.2 Impact analysis and authorization

(a) Before implementation, the organization shall identify affected requirements, hazard records, safety-case claims, interfaces, competence, maintenance, emergency plans and approved operating limits.

(b) The analysis shall consider transition states, mixed configurations and interaction with concurrent changes. A safe final configuration does not establish a safe transition.

(c) Required approvals shall be obtained before the change affects live operation. Emergency changes shall use a defined expedited route retaining technical review, traceability and protective controls.

14.3 Verification and transition

(a) The change shall be verified in a representative environment before live use to the extent required by consequence and reversibility.

(b) The transition plan shall identify prerequisites, responsible roles, timing, communications, data migration, synchronization, acceptance tests and stop points.

(c) Training and instructions shall be available before affected personnel perform changed tasks. Equipment or software labels shall match the approved baseline.

14.4 Rollback and recovery

(a) Rollback shall be evaluated for technical feasibility and safety. The prior state may no longer be safe if data, hardware, interfaces or external conditions have changed.

(b) A rollback plan shall identify its trigger, authority, compatible versions, preserved evidence, restoration tests and restrictions.

(c) Where rollback is impossible, the organization shall provide an alternate safe-state or containment strategy and demonstrate it before commitment to the irreversible step.

14.5 Post-change assurance

(a) Monitoring shall be enhanced for the defined stabilization period and targeted to the assumptions affected by the change.

(b) Unexpected behavior shall trigger reassessment and protective action. A delivery milestone shall not close a change while required operational evidence remains incomplete.

(c) The final change record shall link the implemented configuration, verified results, residual restrictions, updated safety case and lessons learned.

15 Occurrence reporting, investigation and learning

15.1 Reporting and triage

(a) The organization shall provide accessible routes for reporting accidents, incidents, near misses, hazards, barrier failures, abnormal behavior and concerns about evidence integrity.

(b) Reports shall be triaged by potential consequence and time available for protection, not only by actual outcome. A near miss with severe potential shall receive appropriate priority.

(c) Triage shall identify immediate containment, notification duties, investigation ownership, evidence preservation and affected operations. Annex B shall define reporting clocks and escalation rules.

Required evidence: Report register; triage decisions; preservation log; investigation plan; findings; corrective actions; effectiveness review.

15.2 Investigation scope and independence

(a) Investigation shall examine technical, human, organizational and interface conditions. It shall not stop at an individual's final action when upstream conditions materially contributed.

(b) Investigators shall have competence, access and independence appropriate to the event. Material conflicts shall be declared and controlled.

(c) The investigation plan shall identify questions, methods, evidence sources, uncertainties, stakeholder interfaces and reporting arrangements. Restricted evidence shall be handled through authorized routes.

15.3 Evidence and causal reasoning

(a) Original evidence shall be preserved where practicable. Derived data shall retain a link to originals, processing steps and known uncertainty.

(b) Causal conclusions shall distinguish facts, hypotheses and unresolved alternatives. Chronology alone shall not establish causation.

(c) The investigation shall examine why barriers failed, were absent, were bypassed or did not prevent escalation. Successful recovery actions and their limits shall also be recorded.

15.4 Corrective and preventive action

(a) Actions shall address the identified causal conditions and affected population. Each action shall have an owner, due date, completion evidence and effectiveness criterion.

(b) Training shall not be the default action for a design, workload, interface or governance deficiency. Where training is selected, the investigation shall explain why it addresses the cause.

(c) Similar systems, sites, suppliers and operations shall be reviewed for common exposure. The scope of the action shall reflect the mechanism, not only the location of the observed event.

15.5 Closure and learning

(a) Action implementation and action effectiveness shall be separate determinations. Closure shall require evidence that the action works over the specified conditions and observation period.

(b) If recurrence is too rare for event counts to demonstrate effectiveness, the organization shall use control verification, challenge testing or another justified leading measure.

(c) Lessons shall be integrated into hazard analysis, design, procedures, competence, supplier controls and management review. The record shall identify where the learning was applied.

16 Performance assurance, audit and management review

16.1 Monitoring architecture

(a) The organization shall monitor exposure, barrier health, operational deviations, reporting behavior, competence, maintenance and changes relevant to the safety case.

(b) Indicators shall include both outcomes and control performance. Definitions shall state numerator, denominator, population, time basis, data source, uncertainty, owner and response threshold.

(c) Data quality checks shall identify missing, duplicated, delayed, inconsistent or selectively excluded records. An apparently favorable trend with deteriorating reporting completeness shall be investigated.

Required evidence: Indicator dictionary; data-quality records; trend analysis; assurance programme; audit findings; management decisions.

16.2 Thresholds and response

(a) Alert and action thresholds shall be linked to the time available to control the hazard and to justified statistical or engineering criteria.

(b) Threshold exceedance shall trigger a recorded assessment and assigned action. Thresholds shall not be relaxed merely because they are repeatedly exceeded.

(c) Statistical stability shall not be equated with safety. A stable process outside an acceptable limit shall remain unacceptable.

16.3 Internal assurance and audit

(a) The assurance programme shall sample actual work, decisions and evidence trails across sites, shifts, suppliers and operating conditions. It shall include adverse and unsuccessful cases.

(b) Auditors shall have sufficient independence and technical support. The plan shall identify sampling limitations and activities requiring direct observation.

(c) Findings shall distinguish system deficiencies, product or operation conditions, and evidence gaps. The organization shall preserve the separate implications for conformity and operational safety.

(d) Remote review shall be used only where access, identity, evidence integrity and observation are adequate. Inability to observe a critical activity shall limit the conclusion.

16.4 Management review

(a) Management review shall evaluate the adequacy of the safety programme, risk profile, resources, competence, reporting culture, control performance, significant changes and the validity of continuing acceptance.

(b) Inputs shall include unresolved objections, repeated temporary controls, overdue actions, external changes, supplier performance and foreseeable future exposure.

(c) Outputs shall specify decisions, resources, owners, due dates and verification of effectiveness. Meeting attendance and presentation of metrics shall not constitute a completed review.

16.5 Continual improvement and assurance of the assurance system

- (a) The organization shall evaluate whether its assurance methods detect the problems they are intended to detect. Missed hazards, ineffective audits and invalid evidence shall trigger improvement of the assurance process.
- (b) Improvement shall preserve configuration and evidence history. A new metric or method shall be validated before it replaces one supporting an active decision.
- (c) Improvement claims shall state the baseline, measurement method, period, exposure and uncertainty. Lower reporting volume shall not be described as improved safety without supporting evidence.

17 Aviation operations and airspace interfaces

17.1 Applicability and operational definition

- (a) This clause shall apply to organizations controlling or supporting aircraft operations, including passenger, cargo, special-purpose, training, test and remotely supervised operations within their actual responsibilities.
- (b) The operational profile shall identify aircraft configuration, mission or service type, routes or areas, crew and support roles, operating environment, airspace interfaces, ground support and emergency arrangements.
- (c) Applicable operating permissions and aircraft limitations shall be verified separately from AF 9200 conformity. The organization shall not infer permission from a safety-case review.

Required evidence: Aviation operational profile; aircraft and mission configuration; crew authorization; dispatch criteria; airspace-interface agreements; occurrence and trend records.

17.2 Flight preparation and dispatch interfaces

- (a) Preparation shall verify the relevant aircraft status, loading and balance information, mission data, environmental conditions, operating limitations, crew readiness and supporting services.
- (b) Changes after release that affect these conditions shall be communicated and evaluated before the dependent operation. A dispatch document shall not remain valid merely because it was signed earlier.
- (c) The organization shall define how conflicting information is resolved, including aircraft technical records, planning systems, weather sources, notices, maintenance status and operational instructions.
- (d) Loading, fuel or energy planning and performance calculations shall use controlled data and methods appropriate to the configuration. Units, version, input plausibility and independent checks shall be addressed according to consequence.

17.3 Flight phases and abnormal conditions

- (a) Hazard analysis shall cover ground movement, departure, climb, cruise, descent, approach, landing and post-flight transitions where applicable. It shall include phase-specific workload and available recovery time.
- (b) Relevant scenarios shall include loss or degradation of essential systems, incorrect information, adverse weather, terrain or obstacle interaction, traffic conflict, loss of communications and loss of support capability.
- (c) Operational procedures shall identify who makes the decision to continue, divert, terminate or enter a protective condition and what information is required. This standard does not replace approved aircraft procedures or crew operating instructions.

17.4 Navigation, communication and surveillance dependencies

- (a) The safety case shall identify dependencies on positioning, timing, communication, surveillance and external traffic information. Performance limits shall include accuracy, integrity, continuity, availability and latency as relevant.
- (b) Loss, interference, spoofed or misleading data, stale information and inconsistent sources shall be considered. The organization shall define detection and fallback behavior.
- (c) Alternative capability shall be verified for the actual operating environment. A nominally independent service sharing the same infrastructure or timing source shall be evaluated for common cause.

17.5 Continuing operational assurance

- (a) Monitoring shall identify precursors, exceedances and control weaknesses, while respecting applicable privacy and reporting protections.
- (b) Trends shall be stratified where operating environments, fleet configurations or exposure differ materially. Aggregated favorable results shall not conceal a hazardous subgroup.
- (c) Technical findings shall feed the continuing-airworthiness interface, operational procedures and competence programme. The organization shall verify that safety information reaches the parties able to act.

Decision control: A conflict between actual aircraft status and an essential dispatch assumption shall block release until resolved or covered by a valid, specific authorization.

18 Aerodromes, ground operations and aviation support services

18.1 Integrated ground safety scope

- (a) This clause shall apply to aerodromes, heliports, vertiports and ground-support services to the extent that they affect aerospace operational safety.
- (b) The scope shall include movement areas, stands, passenger or cargo interfaces, servicing, vehicle movement, maintenance access, energy supply, rescue interfaces and concurrent construction or maintenance.
- (c) The operator shall coordinate activities across service providers and establish a common route for hazard notification and protective action.

Required evidence: Site operational map; service-provider interface matrix; movement and access controls; inspection records; emergency coordination; change and work-zone assessments.

18.2 Movement areas and infrastructure condition

- (a) The organization shall identify infrastructure characteristics and conditions that can affect safe operation, including surface condition, obstacles, markings, lighting, drainage, contamination and availability of essential services.
- (b) Inspection methods and intervals shall reflect deterioration mechanisms, operating exposure and the time required to impose restrictions. Observed defects shall be linked to operational significance and action.
- (c) Temporary works shall have segregated boundaries, access control, communication, inspection and reinstatement criteria. A construction completion certificate shall not replace an operational readiness check.

18.3 Ground handling and aircraft servicing

- (a) Ground tasks shall define equipment compatibility, positioning, access zones, communication, supervision and protection against unintended movement or activation.
- (b) Servicing shall control the identity, condition and quantity of materials or energy supplied and verify compatibility with the aircraft or ground asset.
- (c) Loading and unloading shall address restraint, segregation, damage, center-of-gravity implications, documentation and changes after acceptance within the organization's responsibility.
- (d) Foreign-object control shall address sources, detection, collection, tool accountability and effectiveness. A clean inspection record shall be challenged where the method cannot observe concealed or inaccessible areas.

18.4 Concurrent activities and shared responsibility

- (a) The organization shall evaluate conflicts between aircraft movement, passengers, vehicles, servicing, lifting, maintenance and construction. Scheduling separation shall be treated as a control requiring verification.
- (b) Each provider shall know the applicable stop conditions and communication route. Contract boundaries shall not prevent an immediate warning or protective intervention.
- (c) Loss of a shared service shall trigger a coordinated response. Local continuation shall be assessed for its effect on other operations.

18.5 Emergency and resilience interfaces

- (a) Emergency capability shall be matched to the actual operation, location, occupancy and credible hazards. Availability and response assumptions shall be verified with the responsible providers.
- (b) Access routes, isolation points, communication systems and safe assembly or shelter arrangements shall remain usable during the scenarios for which they are credited.
- (c) Service recovery after severe weather, infrastructure failure or emergency response shall include inspections and a fresh operational readiness decision.

19 Maintenance and continuing operational integrity

19.1 Maintenance assurance scope

- (a) This clause shall apply to maintenance, repair, overhaul, inspection, technical records and support activities that can affect safety within the declared scope.
- (b) The organization shall identify the approved technical basis, asset configuration, task limits, personnel authorizations, facilities, tools, parts and release responsibilities.
- (c) Applicable maintenance and airworthiness requirements shall remain independently applicable. AF 9200 does not authorize a maintenance organization or individual to issue a release beyond their actual authority.

Required evidence: Maintenance programme; task packages; configuration and life records; personnel and tooling status; independent inspections; release and defect records.

19.2 Task preparation and execution

- (a) Work shall use current applicable instructions and verified asset identity. The organization shall assess access, isolation, environmental conditions, parts availability, tools and human factors before starting.

(b) Task sequencing shall prevent incompatible work, incomplete restoration and unintended energization. Interrupted tasks shall identify their exact completion state and remaining actions.

(c) Safety-critical steps shall have the specified independent check or equivalent verified control. A signature shall identify the actual check performed and shall not be applied retrospectively without evidence.

(d) Unexpected conditions, damage or ambiguity in instructions shall be escalated to the authorized technical source before proceeding beyond the permitted boundary.

19.3 Parts, materials and tools

(a) Parts and materials shall have verified identity, applicability, condition, life or shelf status and traceability appropriate to their safety significance.

(b) Suspected unapproved, counterfeit, damaged or misidentified items shall be segregated and traced to affected installations and stock.

(c) Measurement and test tools shall be fit for purpose and within their control status. An out-of-tolerance tool shall trigger an impact review of prior work, using the period and direction of possible error.

19.4 Configuration, life limits and deferred work

(a) The organization shall maintain configuration and usage records needed to demonstrate continued eligibility. Missing life history for a life-limited item shall not be replaced by an unsupported assumption.

(b) Deferred defects and incomplete tasks shall be visible to the release authority and operational user. Their combined effect shall be evaluated.

(c) Repeated defects shall trigger investigation of the underlying mechanism. Repeated reset or replacement without understanding an unresolved safety-significant pattern shall not establish correction.

19.5 Release and return to service

(a) Release shall verify completed work, required inspections, configuration restoration, tool and material accountability, functional checks, records and remaining limitations.

(b) The release statement shall be limited to the work and authority actually held. It shall identify any operational restrictions and additional checks required before use.

(c) Post-maintenance operational anomalies shall be linked to the maintenance record and reviewed for wider affected populations.

Decision control: Incomplete critical work, missing required inspection or unresolved configuration identity shall block the affected release.

20 Unmanned systems, advanced air mobility and autonomy

20.1 System-of-systems boundary

(a) The UAS or advanced-air-mobility profile shall include the vehicle, control station, communications, navigation, payload, automated functions, human supervisors, maintenance, infrastructure and external services.

(b) The profile shall identify whether people are carried, the exposure of uninvolved people, operating geography, airspace interaction and the means of preventing operation outside the approved envelope.

(c) The number of vehicles per operator or supervisor shall be justified by task demand, automation behavior, abnormal workload and demonstrated intervention capability.

Required evidence: Operational design domain; end-to-end architecture; link and navigation performance; human-supervision assessment; contingency validation; configuration and data controls.

20.2 Command, control and navigation

(a) The organization shall define command authority, authentication, latency, continuity, integrity and lost-link behavior. Conflicting or stale commands shall have a defined disposition.

(b) Loss or corruption of navigation, timing, terrain or obstacle data shall be analyzed. A containment function shall not depend solely on the source whose failure can create the containment demand without additional justification.

(c) Recovery after link restoration shall prevent abrupt or inconsistent mode changes. Control ownership shall be unambiguous throughout handover.

20.3 Containment and contingency

(a) The safety case shall address flight beyond intended boundaries, loss of propulsion or energy, inappropriate automation behavior, degraded sensing and inability to reach a planned destination.

(b) Contingency options shall be evaluated for the actual environment and exposure. A return or landing function shall not be presumed safe under every failure or weather condition.

(c) Protective functions shall be tested for missed and false activation, timing, environmental limits and common dependencies. Operational restrictions shall compensate only where their effectiveness is demonstrated.

20.4 Autonomous and adaptive functions

(a) Each autonomous function shall have a defined purpose, authority boundary, validated domain, prohibited actions, monitor and fallback.

(b) Validation shall address representative variation and adverse combinations, not only average performance. The organization shall examine distribution shift, out-of-domain input and misleading confidence outputs.

(c) Online learning or adaptive changes affecting safety shall be controlled as changes. If the assurance basis cannot support unrestricted adaptation, adaptation shall be bounded, monitored or disabled for the safety-relevant function.

(d) Human supervision shall be credited only where the human has sufficient information, time, authority and demonstrated ability to intervene.

20.5 Infrastructure and public interaction

(a) Ground or vertiport interfaces shall address energy replenishment, passenger movement, rotor or propulsor hazards, loading, weather, rescue access and concurrent operations as applicable.

(b) Noise or environmental constraints shall be managed alongside safety without weakening essential protection. A route change intended to reduce one impact shall be assessed for other exposure.

(c) Public-facing claims shall identify the approved operational domain and limitations. Demonstration success shall not be generalized to unrestricted deployment.

21 Space systems, missions and ground support

21.1 Mission lifecycle and responsibility

- (a) The mission safety scope shall cover relevant ground processing, integration, transport, launch preparation, launch, deployment, commissioning, routine operations, contingency, end-of-mission and disposal phases.
- (b) The organization shall identify responsibility across mission owner, platform, payload, launch service, ground systems, communications and external services.
- (c) Safety acceptance shall be phase-specific. Acceptance for ground testing shall not imply acceptance for launch or on-orbit operation.

Required evidence: Mission profile; phase-specific hazard analysis; interface agreements; ground and flight configuration; mission rules; contingency and disposal evidence.

21.2 Ground processing and launch interfaces

- (a) Ground operations shall identify hazardous energy, pressure, stored mechanical energy, chemicals, propulsion interfaces, lifting, environmental control and access limitations.
- (b) Incompatible activities shall be separated by verified physical, procedural or temporal controls. Required isolation and restoration states shall be confirmed before personnel access or hazardous operations.
- (c) Launch-interface acceptance shall verify configuration, environmental compatibility, payload constraints, command inhibits, data exchange and responsibility for unresolved anomalies.
- (d) This standard does not define launch trajectories, ordnance procedures or operational launch permissions. Those activities require their own competent technical and authority controls.

21.3 Orbital and in-space operations

- (a) The safety case shall address power, thermal control, communications, navigation, attitude control, propulsion, autonomy and the consequences of loss or degradation of these functions.
- (b) Mission rules shall identify command authority, verification of critical commands, timing, constraints, inhibit removal and irreversible actions. Data latency and uncertain state estimation shall be incorporated into decisions.
- (c) Collision-avoidance and proximity-operation interfaces, where applicable, shall identify data quality, decision authority, coordination, maneuver constraints and response to uncertainty.
- (d) Unattended or long-duration operation shall include component aging, radiation effects, consumable depletion, degraded ground support and loss of expertise.

21.4 Crewed and life-support interfaces

- (a) Where people are carried or supported, the scope shall address habitability, life support, fire and contamination protection, emergency refuge, medical support interfaces, evacuation or rescue constraints and human workload.
- (b) Safety-critical consumables and protective functions shall have justified margins, monitoring and contingency capability for the mission context.
- (c) Isolation from immediate assistance shall be considered explicitly. A ground-based response assumption shall not be credited where communication delay or physical separation prevents timely action.

21.5 Surface operations and robotic interaction

- (a) Surface missions shall evaluate terrain, dust, lighting, temperature, communications, mobility, energy, robotic interaction and inability to recover a stranded asset where relevant.
- (b) Command and autonomy limits shall account for delay, intermittent visibility and uncertainty in environment models.
- (c) Interactions between robots, people, habitats and infrastructure shall be controlled with explicit authority and exclusion boundaries.

21.6 End-of-mission, re-entry and disposal

- (a) End-of-mission plans shall identify the intended terminal state, retained hazards, passivation or energy control where applicable, tracking and notification interfaces, and evidence that the plan is achievable.
- (b) Re-entry or disposal activities shall meet their applicable authority requirements and approved technical criteria. This document does not establish universal casualty-risk limits or permission for re-entry.
- (c) Loss of capability before planned disposal shall trigger a defined contingency review. Sustainability objectives shall not override protection of people or required operational constraints.

Decision control: An irreversible mission step shall remain on HOLD when the necessary configuration, authority, hazard disposition or recovery limitation is unresolved.

22 Defense aerospace and dual-use safety interfaces

22.1 Scope and controlled information

- (a) This clause shall apply to safety management of defense aerospace platforms, support systems and dual-use activities within the declared responsibility.
- (b) The organization shall identify authorized operating conditions, configuration, personnel roles, information controls and interfaces with the responsible operational authority.
- (c) Restricted information shall be reviewed by appropriately authorized competent personnel. A public summary may omit sensitive detail, but the underlying safety decision shall retain adequate evidence and traceability.

Required evidence: Bounded safety scope; authority matrix; authorized evidence-access plan; configuration controls; interface acceptance; emergency and recovery arrangements.

22.2 Mission changes and mixed configurations

- (a) Changes in role, payload, operating environment or support arrangement shall be assessed for safety effects even when the basic platform is unchanged.
- (b) Mixed fleets and rapid configuration changes shall have positive identification and compatibility controls. Procedures, training and maintenance instructions shall match the actual configuration.
- (c) Mission urgency shall not silently bypass a required safety decision. Any authorized exceptional disposition shall identify its authority, scope, conditions and effect on the conformity claim.

22.3 Hazardous stores and energy interfaces

- (a) Where hazardous stores or energetic systems are present, the assurance scope shall address authorized handling, segregation, environmental compatibility, prevention of unintended activation, maintenance boundaries and emergency coordination.

(b) Technical work shall be performed only by appropriately authorized personnel under applicable controlled instructions. This document provides governance requirements and does not supply assembly, activation or employment procedures.

(c) Transfer between organizations shall include verified identity, condition, restrictions and accepted responsibility for safety-critical interfaces.

22.4 Deployed and constrained environments

(a) The organization shall assess reduced infrastructure, limited maintenance support, communications interruption, environmental extremes, fatigue and uncertain external services.

(b) Controls credited in normal facilities shall be revalidated for the deployed setting. A reduced support environment shall not inherit an unrestricted assurance claim from a fully equipped facility.

(c) Recovery and withdrawal criteria shall be defined before the activity, including conditions in which continued operation no longer has a supported safety basis.

23 Design, manufacture, testing and commissioning

23.1 Design integration

(a) Safety requirements shall be incorporated into design baselines and reviewed at the same decision points as performance, cost and schedule requirements.

(b) Design analysis shall include interfaces, assembly tolerances, environmental susceptibility, maintenance access, inspection capability and foreseeable operational errors.

(c) Changes to materials, processes, suppliers or software tools shall be assessed for their effect on safety-critical characteristics and evidence applicability.

Required evidence: Safety requirements; design review; critical-characteristic controls; process qualification; test readiness; commissioning and handover records.

23.2 Production and critical processes

(a) The organization shall identify production characteristics and processes whose nonconformity can defeat a safety requirement. Controls shall address prevention, detection, traceability and escape containment.

(b) Special processes whose outputs cannot be fully verified afterward shall have qualified methods, personnel, equipment, parameters and requalification triggers.

(c) Manufacturing deviations shall be reviewed by competent design and safety authorities where they affect safety. A commercial concession shall not establish technical suitability.

(d) Traceability shall permit affected populations to be identified when a material, process, tool or supplier defect is discovered.

23.3 Test safety and readiness

(a) Each hazardous test shall have a safety assessment independent of the product acceptance objective. The plan shall protect personnel, facilities, environment and neighboring activities.

(b) Test readiness shall verify the configuration, containment, instrumentation, protective systems, personnel, communications, emergency capability and permitted envelope.

(c) Test limits and stop criteria shall be predetermined. An unexpected response shall be evaluated before expanding the envelope or repeating the test.

(d) Simulation shall not replace physical demonstration where the relevant failure mechanism or operational interaction is not adequately represented.

23.4 Verification data and anomalies

- (a) Test data shall retain raw observations, processing methods, calibration status, configuration and environmental conditions sufficient for independent review.
- (b) Anomalies shall be dispositioned for both test validity and product safety. A test-system fault can invalidate a result without proving the product unsafe; both conclusions shall remain distinct.
- (c) Outliers shall not be discarded solely because they prevent acceptance. Exclusion shall require a documented technical reason and preservation of the original data.

23.5 Commissioning and handover

- (a) Commissioning shall verify installed configuration, system interactions, protection functions, operating limits, training, maintenance and emergency readiness.
- (b) Handover shall identify accepted evidence, open issues, restrictions, residual risks, monitoring obligations and responsible recipients.
- (c) The receiving organization shall confirm that it can maintain the assumptions and controls on which acceptance depends.

Decision control: Product acceptance, test completion and operational commissioning shall remain separate decisions with their own criteria.

24 Software, cybersecurity, data and AI safety interfaces

24.1 Safety-related digital scope

- (a) Digital scope shall include software, programmable hardware, networks, data services, models, tools, updates and AI functions that can influence a safety-relevant action or conclusion.
- (b) The organization shall identify digital failure modes including incorrect output, missing output, timing errors, unintended commands, corrupted data and loss of availability.
- (c) Software behavior shall not be modeled as a random hardware failure rate without a justified basis. Systematic defects, specification errors and unsafe interactions require appropriate assurance methods.

Required evidence: Digital safety allocation; architecture and dependency analysis; V&V records; cyber-safety scenarios; controlled data and model baselines; update and recovery evidence.

24.2 Development and verification

- (a) Safety requirements shall be traced to design, implementation and verification. Reviews shall examine abnormal behavior, boundary conditions, timing, resource exhaustion and error handling.
- (b) Tools that can introduce or fail to detect a safety-relevant error shall be assessed for intended use, validation and independent checking.
- (c) Verification shall include interfaces and integrated behavior. Component testing alone shall not establish system safety.

24.3 Cyber-safety interaction

- (a) The organization shall identify how unauthorized access, malicious change, denial of service, false data or compromised identity could create or conceal a hazardous condition.
- (b) Protective measures shall be evaluated for their safety effects. Security controls shall not prevent timely emergency action without a justified alternative.

(c) Segregation, access control, integrity checks, monitoring and recovery shall be matched to the safety consequence and operating environment.

(d) A credible compromise of safety-relevant evidence or configuration shall trigger protective assessment and suspension of unsupported claims until integrity is restored.

24.4 Data and model governance

(a) Safety-relevant data shall have identified origin, units, timestamp, quality, applicability and change control. Missing or stale data shall have a defined operational disposition.

(b) Models shall state assumptions, calibration, validation range, numerical limitations and uncertainty. Agreement with one test case shall not establish validity across an operating envelope.

(c) AI evaluation shall use representative data separation, relevant subgroup and edge-case analysis, uncertainty evaluation and controls against unsafe extrapolation.

(d) A model's score shall not directly authorize a safety-critical operation unless the decision rule and its limitations have been independently demonstrated for that use.

24.5 Updates, restoration and evidence continuity

(a) Updates shall be authenticated, configuration-controlled and verified for compatibility before installation. The process shall prevent partial or mismatched versions from entering an unsafe state.

(b) Backup and restoration shall be tested for completeness, consistency and recovery time. Successful file transfer alone shall not demonstrate restoration of a safe operational state.

(c) Restored systems shall preserve incident evidence and reconcile logs, permissions, configuration and active restrictions before release.

25 Suppliers, partners and joint operations

25.1 Retained responsibility and selection

(a) Outsourcing shall not remove the commissioning organization's responsibility for the safety of its claimed activity. The organization shall identify what is delegated and what is retained.

(b) Supplier selection shall evaluate technical capability, competence, configuration control, evidence quality, occurrence reporting and ability to meet safety-critical requirements.

(c) Past approval for another product or scope shall not establish suitability for the current safety function.

Required evidence: Supplier criticality; qualification record; contractual flow-down; interface agreement; surveillance plan; accepted deliverables and change notifications.

25.2 Safety flow-down

(a) Agreements shall specify safety requirements, assumptions, operating limits, evidence deliverables, notification triggers, access rights, subcontracting controls and responsibility for defects.

(b) Requirements shall flow to the tier where the relevant work is performed. The organization shall verify understanding and implementation rather than relying only on contract text.

(c) Suppliers shall disclose limitations that could invalidate the integrator's safety case. A generic statement of compliance shall not replace configuration-specific evidence.

25.3 Integration and acceptance

(a) Incoming evidence shall be reviewed for completeness, authenticity, applicability and unresolved anomalies. Acceptance for procurement shall be distinguished from technical acceptance for safety use.

- (b) Integration tests shall address incompatible assumptions between suppliers, including units, timing, failure behavior, maintenance and environmental conditions.
- (c) If proprietary evidence cannot be released, an authorized independent review route shall be established. An inaccessible assertion shall not be treated as verified evidence.

25.4 Continuing supplier assurance

- (a) Surveillance shall be proportionate to safety significance, performance, changes and uncertainty. It shall include actual process or product evidence where necessary.
- (b) Supplier changes, obsolescence, financial or capacity disruption and loss of competence shall be assessed for safety implications.
- (c) Escapes shall trigger containment, affected-population analysis, notification and reassessment of prior acceptance. Requalification shall be required where the qualification basis no longer holds.

25.5 Joint operations

- (a) Joint operations shall have an agreed command structure, shared hazard picture, compatible decision criteria, communication, emergency coordination and stop authority.
- (b) Each organization shall retain traceability to its own approvals. A joint readiness meeting shall not replace a required independent permission.
- (c) Responsibility gaps shall be resolved before exposure begins. Where one party cannot meet an essential interface condition, the affected joint activity shall remain on HOLD.

26 Energy, facilities and lifecycle protective controls

26.1 Hazardous energy and facilities

- (a) The organization shall identify electrical, mechanical, thermal, pressure, chemical and other energy sources that can affect the defined aerospace activity.
- (b) Controls shall address normal use, isolation, stored energy, unintended release, re-energization and emergency access. Isolation shall be verified at the point required for the task.
- (c) Facility design and operation shall account for occupancy, segregation, ventilation, drainage, fire protection, environmental conditions and support-service failure as relevant.

Required evidence: Energy and facility hazard assessment; isolation controls; inspection and proof-test records; environmental limits; emergency and restoration plans.

26.2 Propulsion, batteries and energy replenishment

- (a) The organization shall assess the safety interfaces of propulsion and energy systems, including storage, handling, replenishment, charging, monitoring, containment and maintenance.
- (b) Abnormal temperature, leakage, pressure, electrical condition or physical damage shall have defined detection and action criteria based on the actual technology and approved technical data.
- (c) Compatibility of connectors, materials, fluids, software protocols and protective functions shall be verified. Similar appearance shall not establish compatibility.
- (d) Emergency arrangements shall be appropriate to the energy type and credible propagation mechanism. Generic response instructions shall not replace technology-specific competent planning.

26.3 Environmental and natural-hazard interfaces

- (a) The organization shall assess weather, flooding, lightning, extreme temperature, seismic effects and other site-relevant conditions where they can impair safety controls.

- (b) The assessment shall include coincident loss of utilities, access, communications and staffing. Dependencies shall be identified rather than counted as separate independent protections.
- (c) Environmental monitoring shall have defined validity, lead time and response. An unavailable sensor or warning service shall trigger the specified fallback.

26.4 Occupational and operational interfaces

- (a) Personnel protection, access control, lifting, confined work, working at height and hazardous substances shall be included where they affect the declared activity and remain subject to applicable obligations.
- (b) The organization shall coordinate task permits and operational state. A permit to perform one task shall not authorize conflicting work on a shared system.
- (c) Protective equipment shall not substitute for feasible engineered controls without a documented assessment of the alternatives and remaining risk.

26.5 Withdrawal, storage and reactivation

- (a) Withdrawal and storage shall preserve configuration, condition, records and control of residual hazards. The organization shall define inspections and maintenance required during inactivity.
- (b) Reactivation shall assess deterioration, expired items, obsolete instructions, changed external conditions and loss of competence.
- (c) Disposal or transfer shall communicate residual hazards and remove or control access credentials and unsafe reuse opportunities within the organization's authority.

27 Records, digital workflow and evidence integrity

27.1 Record architecture

- (a) Records shall use the common payload and entity relationships in Annex B. Each shall identify its object, scope, configuration, author, time, state, evidence links and approval history.
- (b) Hazard, requirement, evidence, finding, action, risk acceptance and operational release records shall remain distinct entities linked by stable identifiers.
- (c) The system shall preserve prior states and reasons for change. Deletion or overwriting shall not be used to conceal an adverse result or expired authority.

Required evidence: Data dictionary; access matrix; state-transition rules; audit trail; retention schedule; backup and recovery validation.

27.2 Access, protection and retention

- (a) Access shall be based on role, competence, authorization and need. Authors shall not obtain approval authority merely by having system administration rights.
- (b) Retention shall cover the period needed for lifecycle assurance, investigation, legal obligations and contractual commitments. Annex B shall identify the governing retention rules by record type.
- (c) Sensitive information shall be protected without preventing authorized technical review. Public summaries shall preserve the meaning and limits of the underlying decision.

27.3 Automated decisions and workflows

- (a) Automated workflows shall enforce role separation, prerequisite checks, expiry, configuration compatibility and prohibited transitions.

- (b) A workflow shall not convert evidence upload to acceptance, an action marked complete to verified effectiveness, or an expired decision to current status.
- (c) Overrides shall require authorized roles, a recorded reason, bounded scope and review. The audit trail shall identify the original and resulting state.
- (d) Changes to decision logic shall be verified against normal and adverse cases before deployment. Annex W provides a challenge suite.

27.4 Transfer, reconciliation and recovery

- (a) Data transfer shall preserve identifiers, relationships, state history, timestamps, access restrictions and evidence links. Checksums or equivalent controls shall support integrity but shall not replace semantic reconciliation.
- (b) Recovery testing shall demonstrate usable records and correct decision states, not only successful backup completion.
- (c) Records created during an outage shall be reconciled before automated release decisions resume. Conflicting versions shall be resolved by an authorized owner with preserved history.

28 Evaluation, conformity decisions and truthful claims

28.1 Evaluation purpose and scope

- (a) An evaluation shall state whether it examines an organizational system, a product, an operation, a service, a process or a change. The criteria and evidence shall match that object.
- (b) Evaluators shall identify their competence, independence, access and limitations. A safety assessor shall obtain technical support where the scope exceeds their personal competence.
- (c) Use of AF's name or marks, or claims of AF-issued recognition, shall require the separate authorization applicable to that claim. This document alone grants no issuing authority.

Required evidence: Evaluation plan; scope and criteria; competence and impartiality; sampled trails; findings; independent decision; claim text and status controls.

28.2 Evidence sampling and coverage

- (a) The plan shall cover all applicable requirements through a justified combination of review, observation, interviews, testing and trace sampling.
- (b) Sampling shall include high-consequence activities, changes, degraded operations, adverse results, outsourced interfaces and different sites or shifts where relevant.
- (c) A favorable sample shall not support an unlimited claim. The report shall identify the population, sampling basis and unexamined limitations.

28.3 Findings and decisions

- (a) Findings shall identify the requirement, objective evidence, affected scope, consequence and required closure criterion. FAIL and HOLD shall remain distinguishable.
- (b) The final decision shall be made by a competent authorized person sufficiently independent of the evaluated work and evidence gathering for the declared assessment route.
- (c) A positive conclusion shall require all applicable mandatory conditions within the claimed scope to be satisfied. A restricted conclusion shall identify the genuinely separable scope and shall not hide a failed interface needed by that scope.

(d) Operational permission shall remain separate from conformity. A compliant management system can still require an operation to be stopped because actual conditions have changed.

28.4 Continuing status, suspension and withdrawal

(a) Continuing status shall depend on the defined surveillance, change notification, incident response and evidence-validity conditions. This document sets no automatic universal validity period.

(b) Material loss of control, invalid evidence, unauthorized change or obstruction of necessary review shall trigger restriction, suspension or withdrawal of the affected claim as appropriate.

(c) Reinstatement shall require verified correction, evaluation of affected outputs and a new authorized decision. Expiry or suspension shall remain visible in the history.

28.5 Complaints and appeals

(a) The organization conducting an assessment shall provide an accessible route for complaints and appeals with acknowledgment, impartial review, evidence handling and a reasoned outcome.

(b) Reviewers shall not review their own disputed decision without an independent resolution mechanism. Retaliation against good-faith complainants is prohibited.

(c) An appeal shall not automatically restore a suspended operational or conformity status. Immediate protective conditions remain in force until an authorized decision changes them.

28.6 Publication and representation

(a) Claims shall identify the actual document status and shall not portray this manuscript as an already approved or independently validated publication.

(b) After controlled publication, the publisher shall maintain the identifier, edition, issue status, change history and access to authoritative information in accordance with Annex Y.

(c) Publication, technical validation, contractual adoption, independent assessment and statutory authorization shall be represented as separate facts.

Decision control: No certificate, promotional statement or digital status shall imply a broader scope, stronger independence or greater authority than the underlying record supports.

Annex A - Activity-based applicability and boundary closure

Status: Normative within the proposed requirement set.

A.1 Application procedure

The organization shall first define the evaluated object and retained responsibility, then select every activity row that applies. Rows are cumulative. An organization designing and operating an unmanned vehicle shall apply the design, digital, UAS and operational controls; a supplier label shall not remove its design responsibilities. Supporting clauses shall be applied wherever an interface can affect the claimed safety outcome.

The applicability record shall contain each clause and normative annex, its trigger, the corresponding activity, applicability state, rationale, owner, approving authority and review trigger. N/A shall require evidence of absent activity and absent retained responsibility. Selection of this matrix does not replace evaluation of the full requirements.

Table A-1. Activity and responsibility triggers

Activity or responsibility	Principal provisions	Boundary evidence
Organizational safety governance	0-16, 27-28; A-J, N-R	Legal entity, sites, authority, processes, exposure and retained duties
Product or system design	4, 6-10, 14, 23-24; C-E, K	Functions, configuration, installation assumptions and allocated controls
Aircraft operation	11-17; F, H-J, L	Fleet, mission, crew, dispatch, airspace and support interfaces
Aerodrome or ground service	12-18, 25-26; F, H, L	Site areas, movement, servicing, concurrent work and emergency response
Maintenance or technical support	9, 11-16, 19, 25; H, L	Task authority, asset identity, technical data, tooling and release scope
UAS or advanced air mobility	17-18, 20, 24; K-L	Vehicle, control station, link, domain, supervisors and ground exposure
Space mission or ground support	12-16, 21, 23-26; K-M	Mission phases, payload, ground, launch, orbital and disposal interfaces
Defense aerospace or dual-use	17, 19, 22-26; K-M	Platform, mission conditions, controlled information and safety authority
Manufacture or integration	9, 14, 23, 25-26; K, O	Critical characteristics, processes, traceability and integration assumptions
Testing or commissioning	9-10, 12-14, 23; E-F, K	Test object, facility, envelope, validity and separate test safety
Software, AI or data service	9-10, 14, 20, 24, 27; E, K, N	Function, data domain, tools, digital dependencies and safety interfaces

Activity or responsibility	Principal provisions	Boundary evidence
Supplier or outsourced service	4, 7-10, 14-16, 25, 27; O	Flow-down, evidence access, changes and retained integrator responsibility
Hazardous-energy or facility support	9, 12-14, 26; D, F, M	Energy, isolation, protection, occupancy and restoration
Independent evaluation	10, 16, 27-28; P-R	Criteria, competence, independence, scope, sampling and decision rights

A.2 Responsibility and object closure

For each lifecycle phase, the organization shall distinguish performer, accountable owner, technical reviewer, acceptance authority and operational release authority. A single person may hold more than one role only when the competence and independence requirements permit it. An external permission shall be recorded as a dependency, not as a role assigned by the organization.

Table A-2. Required boundary challenge

Question	Required disposition
Does an excluded activity provide an essential safety input?	Retain it as an assured dependency and name its owner.
Does outsourcing move work but leave acceptance responsibility?	Retain the applicable acceptance and supplier controls.
Is the claimed configuration identifiable at every site?	Resolve differences or separate the claims.
Can a hazard cross the declared physical or organizational boundary?	Extend interface analysis and coordinate protection.
Are data, communications or human supervision assumed reliable?	Define performance requirements, evidence and failure response.
Is a technical module absent only because evidence is unavailable?	Record HOLD; N/A is not permitted.

A.3 Illustrative scope determinations

Table A-3. Informative examples of applying the normative selection rules

Example	Appropriate scope decision
Airport provider operating electric ground equipment	Apply ground-service and energy controls; vehicle design controls apply only to retained design or modification responsibility.
Software supplier delivering a safety-relevant scheduling function	Apply digital, interface and supplier controls; evaluate the effect of timing errors on the integrated operation.

Example	Appropriate scope decision
Component workshop with no aircraft operating authority	Apply maintenance task and release controls; do not imply authority to release an entire aircraft.
Satellite payload owner using a contracted ground station	Apply mission, digital and outsourced-interface controls; ground-station performance remains an essential dependency.

Annex B - Mandatory parameters and common record payloads

Status: Normative within the proposed requirement set.

B.1 Parameter governance

Every parameter below shall be completed before the dependent decision. A value may be a number, a category boundary, a specified method or an explicit rule, provided that a competent reviewer can determine conformity without inventing missing criteria. Each parameter shall carry an identifier, unit, scope, technical basis, source owner, approver, effective condition and review trigger. Where a parameter is not applicable, the reason shall be approved under Annex A.

No numerical value in an informative annex shall become a project limit by copying alone. Project criteria shall derive from the actual system, obligations, hazard mechanisms and required confidence. An unresolved parameter shall remain "not established" and shall block the dependent acceptance.

Table B-1. Safety and operational parameter schedule

ID	Required parameter or rule	Minimum completion requirement
P01	Object and configuration	Unique object, sites, lifecycle, hardware/software/data/procedure baseline
P02	Operating envelope	Limits, units, environmental conditions, excluded states and detection method
P03	Exposed populations	People, property and environment; location and exposure basis
P04	Severity categories	Consequence definitions and treatment of multiple dimensions
P05	Likelihood categories	Numerical or qualitative boundaries, denominator and uncertainty treatment
P06	Risk acceptance	Permitted and prohibited regions, authority and escalation rules
P07	Quantitative objectives	Target quantity, unit, scope, aggregation rule and required confidence
P08	Assurance levels	Assignment rationale and required independence, analysis and verification
P09	Barrier performance	Function, capacity, response, availability, integrity and environmental range
P10	Proof test and inspection	Method, interval, coverage, acceptance limit and overdue response
P11	Human response	Detection and action time, workload assumptions and validation basis
P12	Staffing and competence	Task demands, authorization, supervision and currency rules

ID	Required parameter or rule	Minimum completion requirement
P13	Release criteria	Prerequisites, no-go conditions, restrictions and release authority
P14	Temporary control duration	Maximum period, monitoring, combined-effect review and extension authority
P15	Emergency capability	Response objectives, resources, location, provider and verification method
P16	Recovery and restart	Target state, sequence, tests, external clearances and independent review
P17	Reporting clocks	Start event, maximum interval, recipient, backup route and escalation
P18	Investigation and action	Priority rules, timetables, owner, effectiveness window and overdue response
P19	Performance indicators	Formula, denominator, data quality, alert/action rules and owner
P20	Review and surveillance	Scheduled interval and event-triggered review criteria
P21	Evidence acceptance	Validity, representativeness, uncertainty, provenance and expiration rules
P22	Model and simulation	Intended use, validation domain, error bounds and prohibited extrapolation
P23	Measurement decisions	Tolerance, uncertainty, guard band, indeterminate zone and retest rule
P24	Cyber and digital recovery	Integrity checks, restoration objectives, dependencies and release tests
P25	Record retention	Record classes, lifecycle/legal/contractual duration and disposal authority
P26	Supplier notification	Events, clocks, affected population, evidence and receiving authority
P27	Change thresholds	Classification, independent review and transition/rollback requirements
P28	Claim and status control	Scope wording, surveillance, expiry, suspension and reinstatement rules

B.2 Common payload

Table B-2. Fields required for every controlled decision-bearing record

Field	Required content
Record identity	Stable ID, record type, title and current controlled state
Object and boundary	Object ID, scope, site, phase, configuration and relevant interfaces
Ownership	Author, accountable owner, reviewer and approver as applicable
Time	Creation, observation, review and decision time with time basis
Requirement links	Applicable clauses, profile parameters and local requirements
Evidence links	Source IDs, versions, location, provenance and acceptance purpose
Reasoning	Facts, assumptions, inference, uncertainty and decision basis
Limitations	Exclusions, restrictions, unresolved issues and prohibited reliance
Validity	Effective condition, expiry, review trigger and invalidation trigger
History	Prior state, actor, timestamp, reason and linked superseding record
Protection	Access classification, retention rule and authorized disclosure

B.3 Entity relationships

The system shall support the following trace without relying on free-text similarity: object to configuration; configuration to hazard; hazard to safety requirement; requirement to control; control to verification evidence; evidence to acceptance purpose; requirement to state; residual risk to acceptance authority; and release to its prerequisites and current restrictions. Findings and changes shall link to every affected entity.

Table B-3. Record-specific minimum additions

Entity	Additional required fields
Hazard	Scenario, causes, consequence, exposure, initial and residual basis, control owners
Requirement	Trigger, required behavior, limit, allocation, method and state
Barrier	Demand, performance standard, dependencies, test status and impairment response
Evidence	Method, raw source, configuration, equipment, competence, uncertainty and validity
Finding	Criterion, observation, affected scope, consequence and closure test
Action	Cause addressed, owner, due date, implementation evidence and effectiveness test
Risk acceptance	Residual basis, authority, objections, conditions and review/expiry
Release	Exact activity, start/end conditions, prerequisite results and stop triggers
Change	Old/new baselines, impact set, verification, transition and recovery

B.4 Minimum quality checks

Before a decision, the record system shall verify that linked records exist, refer to compatible configurations, have authorized states and have not expired. A broken link, ambiguous identity or unresolved state conflict shall cause HOLD for the affected dependency. A human review may resolve the defect only through a documented correction preserving the original record.

Annex C - Consequence, assurance depth and risk governance

Status: Normative within the proposed requirement set. The category architecture below is an AF 9200 proposal; it is not a universal numerical risk tolerance.

C.1 Consequence categories

Table C-1. Consequence categories to be made specific in the project profile

Category	Consequence description	Required treatment
S5	Credible multiple fatalities, catastrophic loss with severe public exposure, or comparably severe environmental harm	Highest executive accountability; independent technical challenge; explicit severe-consequence argument
S4	Credible fatality, permanent disabling injury, or major loss with serious safety consequences	Senior accountable acceptance; independent review of controls and assumptions
S3	Credible serious injury requiring substantial treatment, major recoverable damage, or significant localized harm	Defined management acceptance and competent review
S2	Credible minor injury, limited damage or short-lived contained harm	Local authority within approved limits and verified controls
S1	Negligible safety consequence within the approved profile	Recorded basis; review if exposure or mechanism changes

The organization shall translate these descriptions into domain-specific criteria before use. More severe mandatory definitions shall govern where applicable. Severity shall not be reduced solely because the event is unlikely. Controls that only reduce likelihood shall not reduce the consequence category.

C.2 Assurance levels

Table C-2. Minimum assurance architecture

Level	Typical trigger	Required assurance emphasis
AL4	S5 or S4 with substantial novelty, uncertainty, coupling or irreversible exposure	Independent multidisciplinary review; explicit defeater analysis; representative adverse-case validation; executive risk decision
AL3	S4, or S3 with high uncertainty or complexity	Independent technical review; multiple analytical perspectives; verified barriers and operational demonstration
AL2	S3 with understood mechanisms, or S2 with complexity	Competent review separate from author where practicable; traceable requirements and representative verification
AL1	S1 or S2 with bounded understood conditions	Competent documented review; verified basic controls and continuing monitoring

S5 shall not be assigned below AL4. S4 shall not be assigned below AL3. Uncertainty, exposure or coupling may increase the level. Lowering an assigned level shall require new evidence and independent approval; a favorable risk-matrix color alone shall not justify reduction. These levels govern assurance effort and do not define acceptable failure probabilities.

C.3 Risk categories and authority

The profile shall define at least: prohibited risk requiring redesign or cessation; risk requiring reduction and senior acceptance before exposure; controlled risk within authorized conditions; and uncertainty requiring HOLD. Category boundaries shall be approved before assessment and shall use the applicable domain's exposure basis. A risk matrix may support prioritization but shall not multiply ordinal category numbers to claim a physical risk quantity.

Table C-3. Non-compensable decision conditions

Condition	Required result
Applicable mandatory safety requirement fails	No positive conformity claim for affected scope; operation controlled under its own authority rules
Severe consequence with essential evidence unavailable	HOLD or demonstrably protective restriction
Credited barrier not installed or verified	Remove barrier credit and reassess before release
Acceptance authority absent or conflicted	HOLD pending eligible authority
Essential assumption invalidated	Suspend reliance on affected acceptance and protect operation
Several temporary conditions interact	Combined-risk review before continued exposure

C.4 Independence depth

The review plan shall identify which technical disciplines must be independent, which artifacts require full examination, and which may be sampled. At AL4, the review shall include the system-level argument and significant interfaces, not only isolated component analyses. External reviewers may be used where internal separation is insufficient, but the accountable organization shall retain decision responsibility.

Annex D - Hazard and barrier records

Status: Normative within the proposed requirement set.

D.1 Hazard record content

Table D-1. Minimum hazard-log fields

Field group	Required detail
Identity and context	Hazard ID; object; configuration; phase; operating state; environment
Scenario	Hazardous condition; initiating event; causal factors; top event; exposed population; consequence
Analysis basis	Method; participants; data; assumptions; uncertainty; severity; likelihood and denominator
Control allocation	Preventive, detective and mitigative controls; requirement IDs; owners; dependencies
Verification	Evidence ID; configuration; acceptance criterion; result; reviewer; validity
Residual risk	Remaining scenario; credited controls; uncertainty; acceptance authority and conditions
Continuing control	Monitoring; proof tests; impairment response; change and review triggers
History	Actions; findings; prior decisions; transfer; reopening and supersession

D.2 Barrier performance standard

For each barrier credited in a safety decision, the organization shall define the required function, demand conditions, response time, capacity, environmental limits, availability or integrity criterion, dependencies, diagnostic coverage, inspection or proof-test method, owner and impairment response. A barrier description such as "operator checks" shall be expanded into observable actions and performance criteria.

Table D-2. Barrier challenge questions

Attribute	Required challenge
Function	Does the barrier interrupt the actual causal path or merely report it?
Timing	Can it act before the harmful state becomes unavoidable?
Capacity	Does it remain effective at the worst credited demand?
Independence	What shared cause can defeat it and another credited barrier?
Human reliance	Is detection, understanding and action demonstrated under workload?
Testability	Can degradation be detected before an unacceptable exposure?
Restoration	Does reset restore the protective function and the correct configuration?
Impairment	Who detects loss, limits exposure and authorizes return?

D.3 Status and closure

Hazards shall use lifecycle states that distinguish identified, under analysis, controls allocated, verification pending, controlled with accepted residual risk, suspended and retired from scope. Retirement shall require evidence that the hazard no longer applies to the claimed object or phase. A hazard shall not be retired merely because no event has occurred.

D.4 Filled record example

The following example is informative and uses invented identifiers and criteria; it is not an approved operating limit.

Table D-3. Illustrative ground-equipment hazard record

Field	Filled example
Hazard	H-GND-014: unintended motion of a powered service unit while personnel work in the interface zone
Context	Unit G-07, configuration C4; servicing state; occupied stand; dry and wet ground considered
Causes	Incorrect mode selection; motion command retained after reconnection; restraint not effective
Consequence	Personnel crushing or impact; severity S4 under the example profile
Controls	BR-01 motion inhibit in servicing mode; BR-02 verified restraint; BR-03 access-zone confirmation
Dependencies	BR-01 and motion control share a controller; no independent-failure credit without further analysis
Evidence	TEST-031 boundary/mode tests; INS-012 restraint inspection; HF-006 observed task trial
Open issue	Wet-surface restraint capability unverified; requirement R-018 remains HOLD
Decision	No wet-surface release; dry-surface use only if a separately justified restricted profile is accepted
Trigger	Restraint design change, unexpected movement, controller update or changed surface condition

Annex E - Safety-case architecture and evidence acceptance

Status: Normative within the proposed requirement set.

E.1 Required argument layers

Table E-1. Safety-case structure

Layer	Required content
Top claim	Defined object can perform the stated activity within the authorized envelope while meeting the applicable safety criteria.
Context	Configuration, lifecycle, users, environment, interfaces, exposure and authority conditions.
Hazard coverage	Why the hazard set and interaction analysis are sufficiently complete for the decision.
Control adequacy	How allocated requirements control each significant scenario, including common causes and human reliance.
Demonstration	Why analysis, tests, inspections and operational evidence support the required behavior.
Operational readiness	Why personnel, procedures, equipment, support and emergency arrangements can sustain the controls.
Continuing validity	How monitoring, change control, investigation and review detect invalidation.
Limitations	Open issues, uncertainty, dissent, prohibited use and conditions for suspension.

E.2 Evidence acceptance test

Evidence shall be accepted only when its identity, provenance, method, competence, configuration, representativeness, uncertainty and validity are adequate for the stated claim. Acceptance may be limited to a specified purpose. A test may demonstrate correct alarm activation without demonstrating that the operator can respond in time.

Table E-2. Evidence disposition rules

Observation	Disposition
Correct method, configuration and valid result for stated claim	Accept for that purpose with recorded limitations
Relevant result but different configuration	Require documented equivalence or additional verification
Missing raw data needed to assess a critical result	HOLD pending adequate evidence or alternate demonstration
Known invalid method or compromised provenance	Reject; review dependent decisions

Observation	Disposition
Contradictory credible result	Reopen claim and investigate the contradiction
Older evidence with unchanged validity basis	May remain accepted after documented continuing-applicability review
Signature or certificate without technical scope	Insufficient for an unbounded safety claim

E.3 Review record

The reviewer shall record the claims examined, methods used, evidence sampled, limitations, challenged assumptions, findings and recommendation. The decision authority shall record how material findings and dissent were resolved. Review completion and acceptance shall be separate states.

E.4 Argument maintenance

A safety-case change shall identify affected claims and evidence. The organization shall preserve the prior accepted case and the conditions under which it was valid. An operational dashboard shall link its status to the current case and shall not display a positive status after an essential dependency expires.

Annex F - Readiness, release, emergency and restart records

Status: Normative within the proposed requirement set.

F.1 Readiness gate record

Table F-1. Mandatory release prerequisites

Prerequisite	Required evidence	Failure response
Identity and configuration	Actual object and baseline match the authorized plan	HOLD until identity or baseline resolved
Requirements	Applicable mandatory conditions satisfied	No release relying on failed condition
Hazards and risk	Current residual-risk acceptance within authority	Reassess or obtain valid acceptance
People	Competence, authorization, staffing and fitness-for-task controls	Replace, supervise or restrict as justified
Equipment and barriers	Serviceability and proof tests current	Restore or assess an authorized restriction
Environment and interfaces	Conditions within envelope and essential services ready	Wait, restrict or use verified fallback
Emergency capability	Required response resources and communications available	No operation relying on unavailable capability
Open issues	Disposition, combined effects and expiry reviewed	HOLD affected scope
Release authority	Eligible and authorized decision maker	Escalate to valid authority

F.2 Decision payload

The release record shall identify the requested activity, authorized activity, configuration, location, start condition, validity period or completion condition, evidence snapshot, residual-risk acceptance, restrictions, no-go triggers, monitoring roles and decision maker. A standing authorization shall specify the variable conditions to be checked before each execution.

Table F-2. Decision states

State	Meaning
RELEASED	All applicable prerequisites satisfied for the stated envelope.
RELEASED WITH RESTRICTIONS	A separately justified narrower activity is permitted; prohibited conditions are explicit.
HOLD	Required evidence, authority or readiness is incomplete; no affected exposure may begin.

State	Meaning
STOP / PROTECT	Active conditions require cessation or transition to the defined protective state.
COMPLETED	Authorized activity ended and the resulting state and follow-up duties are recorded.

F.3 Emergency coordination record

The plan shall identify scenario, detection, alert authority, command succession, protective actions, internal and external communications, access, rescue or shelter, critical resources, alternate arrangements, exercise evidence and maintenance owner. Notification clocks shall define the start event and recipient. External response capability shall be confirmed rather than assumed.

F.4 Restart dossier

Restart shall require a description of the event and protected state; cause or bounded uncertainty; inspection and test results; repaired configuration; corrected procedures; restored people and support; residual risk; required external clearances; independent review; and a new operational release. A restart decision shall state enhanced monitoring and the conditions requiring another stop.

Annex G - Change and combined-condition assessment

Status: Normative within the proposed requirement set.

G.1 Change significance

Table G-1. Change screening

Question	Required action if yes
Does the change alter a safety objective, limit or authority condition?	Reassess the approval basis and obtain required authority decisions.
Does it affect a credited barrier or its independence?	Reanalyze relevant scenarios and verify the changed control.
Does it change a human task, staffing or supervision?	Update task analysis and demonstrate competence and workload.
Does it create a mixed or transitional configuration?	Analyze transition states and compatibility before implementation.
Does it change data, software, AI or a digital tool?	Reassess digital safety, validation and recovery.
Does it affect a supplier or shared service?	Reopen interface acceptance and flow-down.
Is rollback unsafe or impossible?	Demonstrate alternate containment before commitment.

G.2 Combined-condition register

The organization shall maintain a current list of temporary changes, deferred defects, impaired barriers, expired assumptions and restricted resources affecting each operation. Before release, it shall assess interactions among them. The assessment shall identify shared dependencies and whether one condition removes a control credited for another.

G.3 Required change dossier

The dossier shall contain the old and proposed baselines, reason, hazard impact, affected requirements and evidence, human and supplier effects, verification plan, transition states, emergency arrangements, rollback or containment, approvals, implementation evidence and post-change monitoring. The dossier shall identify what would invalidate its own acceptance.

G.4 Illustrative combined-condition example

Two individually permitted conditions can become unacceptable together: a temporary loss of an automatic alarm and reduced supervisory staffing. If the alarm-loss disposition credits manual monitoring, reduced staffing can invalidate that disposition. The combined review shall examine actual monitoring demand, response time and competing tasks. Independent approvals of the two conditions do not establish their compatibility.

Annex H - Human performance and competence evidence

Status: Normative within the proposed requirement set.

H.1 Task-level competence profile

Table H-1. Required task profile

Element	Required definition
Task boundary	Equipment, configuration, location, permitted actions and prohibited actions
Knowledge	Hazards, principles, limits, procedures and escalation routes
Practical capability	Observable performance under normal and relevant abnormal conditions
Preconditions	Experience, prerequisite qualifications, supervision and currency
Assessment	Method, representative scenarios, pass criteria and assessor competence
Authorization	Issuer, scope, restrictions, validity and withdrawal triggers
Maintenance	Practice, refresher activity, observation and reassessment criteria

H.2 Human-performance demonstration

A demonstration shall state the task, participants, representativeness, environment, workload, information quality and success criteria. It shall include errors, delays and near misses rather than reporting only average completion time. Where response time supports a safety claim, the analysis shall address variability and the chosen conservative decision basis.

H.3 Handover minimum content

Table H-2. Safety handover record

Item	Required information
Current state	Object, configuration, mode and work in progress
Restrictions	Deferred defects, bypasses, temporary controls and expiry
Hazards	Active concerns, barrier impairments and monitoring duties
Decisions	Pending authorizations, unresolved objections and no-go conditions
Resources	Personnel, tools, services and emergency capability changes
Acceptance	Sender, receiver, time, questions and explicit transfer of responsibility

H.4 Authorization controls

An expired or suspended authorization shall not be made current by assignment to a shift. Supervised work shall specify the supervisor's competence, presence, span of control and intervention capability. Reassessment following an event shall be based on the actual cause; it shall not assume that every occurrence demonstrates individual incompetence.

Annex I - Occurrence, investigation and corrective-action records

Status: Normative within the proposed requirement set.

I.1 Reporting and triage payload

Table I-1. Occurrence intake record

Field	Required content
Event identity	Unique report, date/time, location, reporter route and confidentiality needs
Object	Asset, operation, configuration, phase and participating organizations
Observation	What was observed, actual outcome, potential consequence and immediate uncertainty
Protection	Immediate actions, current safe state, restrictions and affected activities
Evidence	Logs, data, physical items, witnesses and preservation actions
Triage	Potential severity, urgency, required notifications, owner and investigation priority
Follow-up	Next action, responsible role, due time and feedback route

The triage record shall preserve the original report. Later corrections shall be attributable. Reports from several channels concerning one event shall be linked without destroying their distinct observations or chronology.

I.2 Investigation record

The investigation shall state its purpose, scope, competence, independence, methods, evidence provenance, chronology, causal analysis, unresolved hypotheses, barrier performance, systemic factors and conclusions. The report shall identify limitations caused by unavailable evidence. It shall distinguish a safety conclusion from a legal or disciplinary determination outside its remit.

Table I-2. Causal-analysis completeness check

Dimension	Required examination
Technical	Design, material, equipment, software, configuration and degradation
Human	Information, workload, competence, fatigue, interface and task conditions
Organizational	Resources, planning, incentives, oversight, handover and escalation
Interface	Supplier assumptions, shared services, authority gaps and communication
Assurance	Why analysis, inspection, testing, audit or monitoring did not prevent escape
Recovery	What limited consequences, whether it was reliable, and remaining vulnerabilities

I.3 Corrective action and effectiveness

Each action shall identify the causal condition addressed, affected population, responsible owner, implementation deadline, evidence, verification authority and effectiveness criterion. An action that only improves detection shall not be described as eliminating the cause. Where effectiveness requires a period of operation, interim protective controls shall remain active until the criterion is met.

I.4 Closure and dissemination

Closure shall include a review of similar exposure, updated hazard records, changed procedures or design, training where relevant, and communication to affected parties. Sensitive details may be restricted, but actionable safety information shall reach authorized recipients. Overdue actions shall trigger escalation according to consequence and remaining exposure.

Annex J - Performance indicator dictionary and review rules

Status: Normative within the proposed requirement set. Indicator examples define measurement structure, not universal target values.

J.1 Indicator specification

Each indicator shall have a name, purpose, owner, population, numerator, denominator, unit, period, source, data-quality check, uncertainty treatment, alert threshold, action threshold and required response. Definitions shall remain stable over a comparison period or changes shall be reconciled explicitly.

Table J-1. Safety performance indicator structures

Indicator	Calculation or observation	Required interpretation
Barrier test compliance	On-time valid tests / tests due	Report overdue critical barriers separately; do not hide them in the average.
Barrier demand performance	Successful demands / observed demands	State demand definition and confidence; small samples remain uncertain.
Operational exceedance rate	Relevant exceedances / defined exposure	Use consistent mission, hour, movement or task denominator.
Unverified release conditions	Count of releases with missing required evidence	Any such release requires investigation; a percentage alone can conceal seriousness.
Temporary-control exposure	Exposure accumulated under temporary controls	Stratify by consequence and expiry; monitor repeated extensions.
Corrective-action effectiveness	Actions meeting verified effectiveness criteria / actions due for review	Separate implementation completion from effectiveness.
Reporting completeness	Expected reportable events captured / independently identified reportable events	Estimate limitations; increasing reports may indicate improved reporting.
Competence currency	Personnel current for assigned tasks / assigned personnel	Identify critical task gaps and supervision limitations.
Change escape	Safety-relevant changes implemented without required acceptance	Investigate each event and affected configuration.
Evidence integrity defects	Invalid or inconsistent evidence items affecting decisions	Trace dependent releases and claims.
Recovery performance	Demonstrated recovery time and completeness against approved objectives	Include safe-state verification, not only IT uptime.
Hazard response timeliness	Time from validated trigger to effective protection	Define clock start, endpoint and uncertainty.

J.2 Trend and statistical rules

The organization shall distinguish random variation, changes in exposure, changes in reporting and changes in underlying risk. A trend shall not be inferred from an arbitrary number of points without a justified method. Control limits and acceptance limits shall remain distinct. A process can be statistically stable while failing a safety requirement.

J.3 Review and escalation

Thresholds shall identify both the action and the authority. An alert may trigger investigation while an action threshold may impose a restriction; these responses shall be specified in advance. Any credible severe hazard may trigger protective action regardless of whether a statistical threshold has been crossed.

J.4 Dashboard integrity

A dashboard shall display missing data, stale data, unresolved HOLD and expired decisions. Green status shall not be generated by excluding unknown records from the denominator. Aggregation shall allow users to inspect the site, configuration, operating state and severe-consequence contributors underlying the summary.

Annex K - Engineering, testing and digital assurance matrices

Status: Normative within the proposed requirement set.

K.1 Engineering evidence matrix

Table K-1. Engineering assurance controls

Domain	Required control	Minimum evidence and release blocker
Functional architecture	Allocate safety functions and define failure behavior	Functional model and hazard links; blocker: unallocated critical function
Structural and mechanical	Address relevant load, degradation, damage and inspection mechanisms	Approved analysis/test basis and life assumptions; blocker: unverified critical load case
Electrical and power	Address loss, transients, isolation, protection and common supply	Power/dependency analysis and tests; blocker: unsupported protective function
Pressure and fluids	Address containment, compatibility, leakage, isolation and stored energy	Design and test evidence with safe operating limits; blocker: unresolved containment criterion
Thermal and fire	Identify initiation, propagation, detection, containment and recovery	Scenario analysis and representative demonstration; blocker: credited protection unverified
Environmental compatibility	Define relevant conditions and combinations	Qualification profile, configuration and uncertainty; blocker: operation outside demonstrated range
Materials and processes	Control safety-critical characteristics and latent defects	Traceability and qualified process evidence; blocker: unknown origin or process status
Integration	Resolve interface timing, units, commands and failure behavior	Interface verification and anomaly disposition; blocker: essential incompatibility
Maintainability	Ensure safe access, isolation, inspection and restoration	Task trials and maintenance controls; blocker: critical control cannot be maintained

K.2 Test acceptance architecture

A test plan shall identify the requirement, object, configuration, facility, method, instrumentation, uncertainty, preconditions, sequence, safety limits, pass criteria, anomaly rules and evidence retention. The test safety assessment and product acceptance criteria shall be reviewed separately. A failed test shall trigger technical disposition before repetition; changing the criterion requires a justified controlled change independent of the desire to pass.

Table K-2. Test evidence validity checks

Check	Required demonstration
Representativeness	Tested configuration and environment support the intended claim.
Measurement	Range, resolution, calibration and uncertainty are adequate.
Coverage	Relevant boundaries, adverse combinations and failure states are exercised.
Repeatability	Variability is understood where repeated behavior matters.
Data integrity	Raw data, processing and excluded data are traceable.
Independence	Review and witness roles meet the assigned assurance level.
Anomalies	Unexpected results are explained or remain open with restrictions.
Transfer	Extrapolation to other configurations has an approved technical basis.

K.3 Digital and AI evidence matrix

Table K-3. Digital safety controls

Subject	Required evidence	Prohibited inference
Software requirements	Traceable behavior, abnormal cases and timing	Code completion proves safe operation.
Programmable hardware	Logic, timing, configuration and verification	Hardware form eliminates systematic defects.
Data pipeline	Provenance, units, timestamps, transformations and quality	Successful transfer proves valid meaning.
AI model	Intended domain, representative validation, edge cases and limitations	High average accuracy proves safety in every subgroup.
Autonomy	Authority boundary, monitor, fallback and human-task validation	A human supervisor can always intervene.
Cyber protection	Threat-to-hazard mapping, protective controls and recovery	A security test alone proves operational safety.
Simulation	Model validity, uncertainty and intended-use bounds	Visual realism proves predictive accuracy.
Update	Authenticity, compatibility, interrupted-update behavior and rollback	Correct package signature proves functional compatibility.

K.4 Tool and model reliance

A tool shall be evaluated according to the error it can introduce or fail to detect. The organization shall define checks independent of the tool where necessary. A model shall not be used beyond its validated domain without a justified uncertainty treatment and approval. Reuse of a model shall include the configuration of its data, solver, parameters and processing code.

Annex L - Aviation, ground, maintenance and unmanned operational matrices

Status: Normative within the proposed requirement set.

L.1 Aviation operation controls

Table L-1. Aviation readiness and continuing assurance

Activity	Required assurance	Stop or hold trigger
Planning	Current aircraft, route/area, environment, loading and energy basis	Essential input missing, inconsistent or outside approved bounds
Crew and supervision	Task authorization, staffing, briefings and abnormal capability	Required role unavailable or not competent for assigned task
Aircraft status	Configuration, defects, maintenance and limitations reconciled	Technical and operational records conflict materially
Ground-to-flight transition	Handover, servicing completion and interface readiness	Unresolved ground task or unsafe concurrent activity
Airspace interface	Required communication, navigation and surveillance capability	Required capability unavailable without valid alternate
Abnormal operation	Defined authority, procedures and contingency support	Conditions exceed supported contingency envelope
Post-operation	Exceedance review, defects and record reconciliation	Unresolved event can invalidate next release

L.2 Ground-service controls

Table L-2. Ground-service assurance

Activity	Required assurance	Evidence
Aircraft approach and positioning	Compatible equipment, clearance, communication and motion control	Observed task, equipment status and interface procedure
Energy or fluid servicing	Correct identity, compatibility, connection and emergency isolation	Supply records, checks and protective-system tests
Loading and unloading	Identity, condition, restraint, segregation and information transfer	Loading record and independent checks where required
Passenger interface	Controlled routes, assistance, barriers and concurrent movement	Site plan, observations and incident feedback
Movement area inspection	Condition, obstacles, contamination, lighting and access	Inspection log and operational disposition
Activity	Required assurance	Evidence
Construction or maintenance	Work-zone boundaries, coordination and reinstatement	Change assessment, permits and readiness inspection

Activity	Required assurance	Evidence
Emergency support	Available capability for actual hazards and location	Agreements, exercises and response-time evidence

L.3 Maintenance controls

Table L-3. Maintenance safety evidence

Stage	Required evidence	Release blocker
Intake	Asset identity, configuration, history and requested work	Ambiguous identity or missing essential life history
Preparation	Applicable instructions, tools, parts, isolation and competence	Uncontrolled instructions or unavailable critical resource
Execution	Recorded steps, interruptions, findings and independent checks	Incomplete critical task or unresolved unexpected condition
Verification	Functional tests, inspections and tool accountability	Required verification not completed or invalid
Release	Authorized scope, completed work and explicit limitations	Signatory outside authority or unresolved configuration
Follow-up	Defect trends, escapes and affected-population review	Evidence invalidating previous release

L.4 UAS and autonomy controls

Table L-4. End-to-end unmanned assurance

Interface	Required definition and validation
Vehicle-control station	Command ownership, latency, integrity, loss and restoration behavior
Positioning and timing	Accuracy, integrity, continuity, interference response and common dependencies
Containment	Boundary definition, detection, response, environmental limits and failure cases
Human supervision	Workload, number of simultaneous tasks, alerts, intervention time and authority
Automated behavior	Domain, prohibited actions, monitor, fallback and data/model configuration
Ground exposure	Occupancy, access, emergency options and changing conditions
Multiple vehicles	Coordination, shared-service failure, workload and correlated behavior
Energy and infrastructure	Replenishment compatibility, condition monitoring and rescue interfaces

Annex M - Space, defense and critical-infrastructure matrices

Status: Normative within the proposed requirement set.

M.1 Mission phase evidence

Table M-1. Space mission assurance by phase

Phase	Required assurance	Transition blocker
Ground integration	Configuration, hazardous energy, compatibility, cleanliness where safety-relevant and access	Unverified isolation, incompatible interface or unresolved hazardous condition
Transport and storage	Environmental protection, restraint, monitoring and receiving inspection	Exposure outside qualified bounds without disposition
Launch interface	Payload constraints, inhibits, communications, authority and anomaly closure	Required interface acceptance or permission absent
Commissioning	Validated commands, telemetry, limits and recovery	Critical state uncertain beyond approved limits
Routine operation	Current mission rules, health monitoring and ground support	Essential assumption or control invalidated
Proximity or maneuver	Coordination, data quality, authority and contingency	Unresolved conflict or inadequate state knowledge
Crewed operation	Life support, habitability, refuge, medical and rescue interfaces	Required protective or survival capability unavailable
Surface operation	Environment, mobility, energy, communications and delayed intervention	Operation outside validated terrain/environment/domain
End-of-mission	Achievable terminal plan, residual hazards and required notifications	Disposal or terminal-state assumptions unsupported

M.2 Defense and controlled-information evidence

The safety dossier shall define the accessible evidence set, authorized reviewers, protected locations, handling rules and public-summary limits. Classified status shall not turn an unexamined claim into an accepted claim. The decision record shall identify the competent review route and any scope limitation caused by evidence restrictions.

Table M-2. Defense aerospace safety interfaces

Interface	Required safety evidence
Mission configuration	Positive identity, compatibility and changed hazard analysis
Authorized operating authority	Defined permissions, limitations, escalation and retained responsibility

Interface	Required safety evidence
Hazardous stores	Authorized procedures, segregation, compatibility and prevention of unintended activation
Deployed support	Demonstrated maintenance, competence, infrastructure and emergency capability
Mixed civil and defense interfaces	Compatible communications, responsibilities and operating constraints
Information restriction	Authorized technical review and preserved decision trace

M.3 Energy and facility evidence

Table M-3. Critical-support controls

Hazard source	Required control evidence
Electrical energy	Isolation, protection, condition, restoration and competent task performance
Stored pressure	Defined limits, containment, inspection, relief where required and safe isolation
Thermal energy and fire	Initiation/propagation analysis, detection, containment and response
Chemicals and fluids	Identity, compatibility, containment, exposure protection and emergency information
Mechanical movement and lifting	Capacity, stability, guarding, exclusion, communication and inspection
Battery or novel energy	Technology-specific abnormal behavior, propagation control and response capability
Natural hazards	Site-specific exposure, warning, structural/service dependencies and recovery
Loss of utilities	Safe state, backup independence, endurance and restoration verification

M.4 Irreversible transitions

For an irreversible transition, the dossier shall state why the prerequisites are sufficient, what uncertainty remains, what cannot be recovered, who accepts that limitation and how the remaining phase is protected. An irreversible step shall not be authorized on the assumption that missing evidence can be obtained afterward.

Annex N - Digital record and workflow validation

Status: Normative within the proposed requirement set.

N.1 State-transition rules

Table N-1. Required workflow controls

Transition	Required condition
Evidence collected to accepted	Competent review, purpose, configuration and validity recorded
Requirement HOLD to PASS	Accepted sufficient evidence and authorized determination
Requirement FAIL to PASS	Verified correction and closure of applicable criterion
Requirement to N/A	Approved absent-trigger rationale; no retained responsibility
Action implemented to effective	Defined effectiveness criterion demonstrated
Risk assessed to accepted	Eligible authority, current controls, residual basis and conditions
Readiness to released	All applicable release prerequisites satisfied
Released to suspended	Trigger recorded and affected users notified
Suspended to reinstated	Corrective evidence and fresh authorized decision
Record current to superseded	Successor linked, dependencies reviewed and history preserved

N.2 Prohibited shortcuts

The workflow shall prevent upload from acting as technical acceptance; administrator access from acting as risk authority; an expired record from appearing current; a failed requirement from being excluded from an average; and a missing record from being treated as N/A. Overrides shall be visible, authorized and reviewable.

N.3 Validation evidence

Validation shall use representative users, roles, records, configurations and adverse conditions. The test set shall cover incorrect state transitions, expired authority, broken links, concurrent edits, partial transfer, restoration from backup and conflicting offline records. The result shall show expected and actual behavior, defect disposition and retest evidence. Annex W gives informative scenario examples.

N.4 Migration and recovery

Migration shall preserve stable identity and relationships. Record counts and file checksums shall be supplemented with semantic checks of state, ownership, configuration and decision dependencies. Recovery shall be accepted only when a representative decision can be reconstructed correctly and prohibited releases remain blocked.

Annex O - Supplier and interface assurance package

Status: Normative within the proposed requirement set.

O.1 Supplier criticality and selection

Supplier criticality shall consider the function supplied, credible consequence, substitutability, detectability of defects, evidence access and retained integrator responsibility. A low commercial value shall not imply low safety significance. Qualification shall be scope-specific and shall be revisited after material change or performance deterioration.

Table O-1. Required supplier agreement content

Topic	Minimum obligation
Technical scope	Functions, configuration, interfaces, limits and deliverables
Safety requirements	Allocated requirements, assumptions and prohibited conditions
Evidence	Method, provenance, raw-data access where needed and acceptance criteria
Change	Prior notification and authorization for safety-significant changes
Occurrence	Prompt reporting rules, affected population and corrective cooperation
Subcontracting	Controlled flow-down and visibility of safety-critical tiers
Access	Authorized technical review, witness and inspection arrangements
Continuity	Obsolescence, support, data retention, transfer and exit arrangements
Claims	Accurate scope, status and prohibition of unsupported endorsements

O.2 Interface acceptance

Each party shall confirm the interface requirements and its own evidence. The integrator shall verify compatibility of assumptions and combined behavior. Interface closure shall identify configuration, remaining restrictions and the change triggers that reopen acceptance. One party's signature shall not stand in for another party's required acceptance.

O.3 Surveillance and escape response

Surveillance shall include the mechanisms most likely to affect safety: process changes, personnel capability, tooling, material origin, software/data versions and anomaly handling. When an escape is found, the organization shall identify affected delivered and in-process populations, contain exposure, notify recipients, assess prior decisions and verify corrective effectiveness.

O.4 Supplier exit and continuity

Exit planning shall preserve the information needed to maintain safe operation, including configuration, life history, software support, critical tooling, open anomalies and residual-risk obligations. If required support cannot be maintained, the operator shall restrict or withdraw the affected activity rather than assume indefinite continued validity.

Annex P - Assessment planning, competence and decision independence

Status: Normative within the proposed requirement set.

P.1 Evaluation plan

Table P-1. Required evaluation plan

Element	Required content
Purpose	Object and type of conclusion sought
Criteria	Controlled edition, applicable clauses, profile and additional obligations
Boundary	Sites, activities, phases, configurations and exclusions
Team	Competence, independence, technical support and conflicts
Methods	Review, observation, interviews, tests and trace sampling
Coverage	High-consequence work, changes, suppliers, shifts and adverse cases
Access	Evidence, locations, confidentiality and remote-method limitations
Schedule	Activities, resources, safety constraints and reporting milestones
Decision	Eligible decision authority, findings process and appeal route

P.2 Competence matrix

Table P-2. Role-specific competence

Role	Required demonstrated capability
Lead assessor	Scope planning, requirement interpretation, evidence evaluation and finding formulation
Technical specialist	Relevant system, hazards, methods and operating environment
Quantitative reviewer	Units, assumptions, data quality, dependence, confidence and model limitations
Human-factors reviewer	Task analysis, workload, interface and competence demonstration
Digital reviewer	Software/data/model assurance, cyber-safety and workflow integrity
Decision maker	Scope, acceptance rules, independence, limitations and status control

The team may combine roles when competence and independence are adequate. No person shall be assumed competent in every aerospace discipline by virtue of a general audit qualification. The record shall identify when specialist support was required and used.

P.3 Sampling and time

Evaluation effort shall be based on scope, consequence, complexity, sites, shifts, changes, evidence maturity and access. A fixed duration unrelated to these factors shall not establish adequate coverage. The plan shall identify sampling limitations and expand examination when findings indicate systemic weakness. Repeating more low-risk samples shall not compensate for omitting a critical interface.

P.4 Independent decision

The decision maker shall review scope, team competence, coverage, findings, closure, unresolved uncertainty and proposed claim wording. A positive decision shall not be made by a person who has a material conflict that prevents impartial judgment. The decision record shall retain the evidence basis and limitations rather than only a certificate number.

Annex Q - Findings, corrective action and continuing status

Status: Normative within the proposed requirement set.

Q.1 Finding classification

Table Q-1. Finding and decision implications

Condition	Required treatment
Failure of a mandatory condition	Record FAIL and prevent an affected positive conformity conclusion.
Incomplete or inconclusive evidence	Record HOLD and identify the evidence needed.
Immediate credible serious danger	Initiate protective escalation; do not wait for the assessment report.
Systemic loss of control	Expand impact review and consider restriction or suspension.
Isolated corrected defect	Verify cause, affected population and effectiveness before closure.
Improvement opportunity with no failed criterion	Record separately; do not mislabel as nonconformity.

Q.2 Finding closure

Closure shall verify the correction, cause analysis, affected population, implemented action and effectiveness. Evidence of a new procedure shall not demonstrate that actual work follows it. Where operational observation is necessary, closure shall remain pending until adequate evidence exists or the claim is narrowed to a separable supported scope.

Q.3 Continuing-status rules

The status plan shall define surveillance, change notification, occurrence reporting, expiry, restriction, suspension, withdrawal and reinstatement. There is no universal three-year validity rule in AF 9200. The validity of a decision shall depend on its own conditions and the applicable authorized scheme, where one exists.

Q.4 Appeals and complaints

The process shall identify access routes, acknowledgment, eligibility, confidentiality, conflict management, evidence handling, review timetable and reasoned determination. The complainant shall receive the outcome and available next route subject to lawful restrictions. The review shall address the substance of the complaint and not merely confirm that the original process was followed.

Annex R - Requirement coverage and claim control

Status: Normative within the proposed requirement set.

R.1 Requirement coverage register

The organization shall maintain a register linking every applicable clause and normative annex to its implementing process, owner, evidence, current requirement state and decision. Grouped evidence may support several requirements, but the register shall show why it is adequate for each. A completed checklist shall not substitute for the underlying evidence.

Table R-1. Claim payload

Field	Required content
Issuer	Actual organization and authority making the statement
Object	Defined organization, system, operation, service, process or change
Criteria	Controlled document identifier, edition, status and applicable provisions
Boundary	Configuration, sites, activities, phases and exclusions
Basis	Self-assessment or independent evaluation, method and evidence period
Outcome	Supported conclusion and unresolved limitations
Conditions	Restrictions, monitoring, validity and invalidation triggers
Verification	Authoritative record and current-status verification route

R.2 Non-compensable claim logic

A positive conformity statement shall require all applicable mandatory requirements in its scope to be PASS or approved N/A. A HOLD shall remain unresolved. A restricted claim shall be permitted only when the supported scope is technically separable and does not depend on the failed or unverified activity. Any supporting maturity score shall be displayed separately and shall not determine conformity.

R.3 Public wording

The claim shall not imply statutory approval, universal safety, third-party endorsement or AF authorization that has not been granted. Publication of this document shall not be cited as evidence that a particular organization, product or operation has been assessed. Membership, participation and technical contribution shall remain distinct from conformity.

R.4 Claim withdrawal and affected outputs

When a claim loses support, the issuer shall identify affected outputs, notify the relevant recipients, correct public status and retain the reason and history. Reinstatement shall require a fresh decision after the support has been restored. An appeal or commercial disagreement shall not keep an unsupported claim active.

Annex S - Quantitative methods and reproducible worked examples

Status: Informative. All numerical datasets, limits and decisions in this annex are synthetic teaching examples. They are not operating limits, evidence of an actual AF assessment or recommended universal risk targets.

S.0 Use of quantitative evidence

Calculations support a defined argument; they do not establish safety independently of the assumptions and evidence behind them. A calculation record should identify the question, model, inputs, units, data origin, assumptions, uncertainty, result, sensitivity and decision limitation. The examples below show methods and common interpretation errors. A real application must satisfy the normative controls in Clauses 8-10 and Annex B.

The examples use decimal points, hours (h), seconds (s) and dimensionless probabilities. A probability per demand is not a rate per hour. Independence, constant rates and representative sampling are assumptions to be demonstrated, not conveniences that may be silently adopted.

S.1 Zero observed failures: upper rate bound

Question: What does a failure-free exposure say about the event rate under a constant-rate Poisson model?

Assumptions: Events follow a homogeneous Poisson process; exposure is correctly counted; the tested population and conditions represent the intended claim; relevant events would be detected; and no event occurred. These assumptions are inappropriate for many systematic software defects, unobserved near misses and heterogeneous pooled populations.

$$P(N = 0 \mid \lambda, T) = \exp(-\lambda * T)$$

$$\lambda_{upper} = -\ln(\alpha) / T$$

For a one-sided confidence level of 95%, $\alpha = 0.05$. With $T = 12,000$ h and zero events:

$$\lambda_{upper} = 2.995732 / 12000 = 0.000249644 \text{ per h}$$

The point estimate is zero, but the 95% upper confidence bound is approximately 2.50×10^{-4} per hour. The data therefore do not demonstrate an event rate below an illustrative target of 1.00×10^{-5} per hour at that confidence under this model.

Table S-1. Failure-free exposure and the 95% upper rate bound

Failure-free exposure	Upper rate bound per h	Interpretation
1,000 h	2.9957×10^{-3}	Substantial uncertainty remains.
12,000 h	2.4964×10^{-4}	More exposure narrows the bound.
100,000 h	2.9957×10^{-5}	Still above the illustrative 10^{-5} target.
299,574 h	Approximately 1.0000×10^{-5}	Minimum whole-hour exposure meeting that target under the stated model.

The required exposure for a target rate λ_{target} is $T \geq -\ln(\alpha)/\lambda_{target}$. Rounding must increase the required exposure, not reduce it. A confidence bound is a property of the procedure under its assumptions; it is not a statement that this specific unknown parameter has a 95% probability of lying below the bound.

Decision implication: A low observed count with inadequate exposure remains insufficient evidence for a stringent rate claim. Design analysis, barrier verification and other evidence remain necessary.

S.2 Zero-failure demonstration on independent demands

Question: How many successful independent demands are required to support a reliability claim?

Assumptions: Each demand has the same success probability R , demands are independent, the success criterion is fixed before testing, and the test population is representative. Repeated tests on an unchanged deterministic software path do not automatically create independent evidence about all operational conditions.

$$P(\text{all } n \text{ demands succeed} \mid R) = R^n$$

$$R_{\text{lower}} = \alpha^{(1/n)}$$

$$n_{\text{required}} = \text{ceil}(\ln(\alpha) / \ln(R_{\text{target}}))$$

With 600 successful demands and no failures, at one-sided 95% confidence:

$$R_{\text{lower}} = 0.05^{(1/600)} = 0.99501956$$

$$p_{\text{failure_upper}} = 1 - R_{\text{lower}} = 0.00498044$$

Table S-2. Zero-failure sample sizes at one-sided 95% confidence

Target reliability per demand	Required independent successful demands
0.90	29
0.95	59
0.99	299
0.999	2,995
0.9999	29,956

These sample sizes are not a requirement of AF 9200. They illustrate how confidence and target reliability affect a particular demonstration plan. Any observed failure changes the appropriate calculation and requires disposition; deleting failed trials and counting only successful repeats is invalid.

Decision implication: The example with 600 successes supports the calculated lower bound under its assumptions, but not a 0.999 reliability claim at the same confidence.

S.3 Exposure-normalized rates and misleading aggregation

Question: Did performance improve when event counts increased but activity increased more?

Table S-3. Synthetic operational data

Period	Relevant events	Exposure	Rate per 1,000 h
Baseline	4	8,000 h	0.500
Later period	8	32,000 h	0.250
Pooled	12	40,000 h	0.300

$\text{rate} = \text{event_count} / \text{exposure}$

$\text{observed_rate_ratio} = (8 / 32000) / (4 / 8000) = 0.5$

The later count doubled, but the observed exposure-normalized rate halved. This arithmetic alone does not establish a statistically reliable improvement or a causal effect. The populations, reporting completeness, operating conditions and event definitions must be comparable, and uncertainty must be evaluated using an appropriate method.

A pooled rate can conceal a high-risk subgroup. If the later period consists mostly of easier operations, the aggregate improvement may not represent improvement within the more demanding activity. The analysis should stratify by relevant configuration, site, phase or exposure type before interpreting the result.

Decision implication: Report the count, exposure, rate, uncertainty and context together. Do not reward lower reporting or interpret a rising count without examining exposure.

S.4 Fault-tree logic and common-cause sensitivity

Question: How does a shared failure mechanism change the result for two nominally redundant protections?

For independent events A and B with probabilities $p_A = 0.002$ and $p_B = 0.003$ over the same exposure:

$$P(A \text{ OR } B) = p_A + p_B - p_A \cdot p_B = 0.004994$$

$$P(A \text{ AND } B) = p_A \cdot p_B = 0.000006$$

The AND result is valid only if the two events are independent for the modeled scenario. Now introduce a distinct common-cause event C with $p_C = 0.0004$. Assume C is independent of the branch containing A and B, and A and B describe the residual independent mechanisms. Then:

$$P(C \text{ OR } (A \text{ AND } B)) = p_C + p_A \cdot p_B - p_C \cdot p_A \cdot p_B$$

$$= 0.0004059976$$

Table S-4. Dependency sensitivity

Model	Top-event probability
Independent A and B only	6.0000×10^{-6}
Common-cause branch included	4.059976×10^{-4}
Ratio of second to first	Approximately 67.7

This is an illustrative event model, not a universal common-cause formula. If the component probabilities already include the common cause, adding it again would double count. Conditional probabilities and event definitions must be consistent.

Decision implication: Identical software, shared sensing, power, maintenance or environment can dominate a redundant architecture. Adding a second channel without evaluating shared causes can produce a misleading safety claim.

S.5 Event-tree calculation with conditional branches

Question: What is the modeled probability of a severe outcome after an initiating event?

Synthetic inputs: initiating event probability 0.02 per mission; detection success probability 0.98 conditional on the event; isolation success probability 0.95 conditional on detection; and mitigation success probability 0.90 conditional on an uncontrolled event. These values are illustrative and would require evidence in a real application.

The uncontrolled branch occurs if detection fails, or if detection succeeds and isolation fails. These branches are mutually exclusive:

$$P(\text{uncontrolled} \mid \text{initiating event}) = (1 - 0.98) + 0.98 \cdot (1 - 0.95) \\ = 0.02 + 0.049 = 0.069$$

$$P(\text{severe outcome per mission}) = 0.02 \cdot 0.069 \cdot (1 - 0.90) \\ = 0.000138 = 1.38 \times 10^{-4}$$

Table S-5. Branch contributions to severe outcome

Branch	Calculation	Contribution
Detection fails, mitigation fails	$0.02 \times 0.02 \times 0.10$	4.0×10^{-5}
Detection succeeds, isolation fails, mitigation fails	$0.02 \times 0.98 \times 0.05 \times 0.10$	9.8×10^{-5}
Total	Sum of mutually exclusive branches	1.38×10^{-4}

The calculation assumes the stated conditional probabilities apply to each branch. If mitigation performs differently after failed detection, a separate branch-specific probability is needed. The same physical measure must not be counted twice as independent detection and isolation without justification.

Decision implication: The result is a model output with input uncertainty, not a demonstrated universal risk level. The dominant branch helps identify where better evidence or control improvement is most valuable.

S.6 Proof-test interval and a simplified dormant failure model

Question: How does an ideal proof-test interval affect the average unavailability of a dormant protective function?

Assumptions: Dangerous undetected failures occur at constant rate λ_{DU} ; the function is restored as good as new at each perfect proof test; there is no repair delay, diagnostic detection, common cause or demand-induced failure; and the phase within the interval is uniformly distributed. This simplified model is not sufficient for a complete protective-system design.

$$PFD_{average} = 1 - (1 - \exp(-\lambda_{DU}T)) / (\lambda_{DU}T)$$

For small $\lambda_{DU}T$: $PFD_{average}$ approximately $\lambda_{DU}T/2$

For $\lambda_{DU} = 2 \times 10^{-6}$ per h and $T = 720$ h:

Approximation = 0.00072

Exact model value = 0.00071965

Table S-6. Interval sensitivity under the simplified model

Interval	Approximate average PFD
360 h	0.00036
720 h	0.00072
1,000 h	0.00100
1,440 h	0.00144

For an illustrative PFD budget of 0.001, the approximation gives $T \leq 1,000$ h. Real proof-test planning must also account for incomplete test coverage, repair time, maintenance-induced faults, common cause and the uncertainty of the failure-rate estimate. An overdue test can invalidate the credited barrier availability.

Decision implication: Test intervals need a technical basis. A convenient monthly calendar date does not itself demonstrate adequate protective performance.

S.7 Availability and why it is not safety

Question: What does a simple repairable-system availability calculation show?

Assumptions: A two-state system has mean up time of 1,200 h and mean down time of 8 h; the long-run alternating process is adequately represented by these means. The down time definition includes all delays intended by the calculation.

$$\begin{aligned}\text{Availability} &= \text{mean_up_time} / (\text{mean_up_time} + \text{mean_down_time}) \\ &= 1200 / 1208 = 0.99337748 = 99.337748\%\end{aligned}$$

$$\begin{aligned}\text{Expected unavailable hours in 8760 h} &= (1 - \text{Availability}) * 8760 \\ &= 58.013 \text{ h}\end{aligned}$$

A system can have high availability while failing dangerously when demanded. Conversely, a protective shutdown can reduce availability while improving safety. Availability therefore cannot substitute for a safety-function performance argument.

If the 8 h value excludes logistics, access or approval delays, the calculation does not describe operational availability. If failures are correlated with harsh conditions, average availability can also hide the period in which protection is most needed.

Decision implication: Define the metric and its denominator. Keep service continuity, safe-state availability and dangerous failure behavior separate.

S.8 Measurement uncertainty and a three-state decision rule

Question: How should uncertainty affect a decision against an upper temperature limit?

Synthetic profile: upper tolerance $L = 100.0$ degrees C. Independent standard uncertainty components are 0.4, 0.3 and 0.2 degrees C. The model is linear and the components are suitably represented as standard uncertainties.

$$u_{\text{combined}} = \sqrt{0.4^2 + 0.3^2 + 0.2^2} = 0.538516 \text{ degrees C}$$

$$U = k \cdot u_{\text{combined}} = 2 \cdot 0.538516 = 1.077033 \text{ degrees C}$$

For this example only, the pre-agreed rule is PASS when $y + U \leq L$; FAIL when $y - U > L$; otherwise HOLD. The coverage factor $k = 2$ does not automatically guarantee an exact 95% interval for every distribution and effective sample size.

Table S-8. Decision outcomes under the stated rule

Measured y	$y - U$	$y + U$	Result
98.7	97.623	99.777	PASS
99.2	98.123	100.277	HOLD
101.3	100.223	102.377	FAIL

HOLD is an indeterminate acceptance result, not proof of a physical defect. The organization may improve the measurement, obtain additional justified evidence or restrict the claim. It must not silently change the decision rule after seeing the result.

If the uncertainty components are correlated, covariance terms are required. Root-sum-square combination without considering correlation can underestimate uncertainty.

Decision implication: Record the measurement result, uncertainty, rule and outcome separately. A successful test procedure does not turn an indeterminate product result into PASS.

S.9 Response-time budget and usable margin

Question: Can a protective chain act before the harmful state becomes unavoidable?

Synthetic conditions: available response time is 12.0 s for a defined scenario. Conservative component budgets are detection 1.5 s, communication 0.8 s, decision 2.0 s, actuation 3.0 s and physical settling 1.2 s. An additional 1.0 s uncertainty allowance is reserved.

Required time = $1.5 + 0.8 + 2.0 + 3.0 + 1.2 + 1.0 = 9.5 \text{ s}$

Time margin = $12.0 - 9.5 = 2.5 \text{ s}$

Table S-9. Response budget

Element	Budget	Required evidence
Detection	1.5 s	Boundary-condition sensor and processing demonstration
Communication	0.8 s	Latency including credible congestion or retry
Decision	2.0 s	Logic or representative human-task demonstration
Actuation	3.0 s	Worst credited load and environment
Settling	1.2 s	Time until protective effect is achieved
Uncertainty allowance	1.0 s	Explicit basis and no double counting

Adding averages is not a conservative worst-case demonstration. Correlated delays, scheduling, time synchronization and failure behavior must be addressed. If detection and communication share a processor, a common overload can affect both budgets.

Decision implication: Positive arithmetic margin supports the argument only when each budget and the available-time estimate are valid. A human response credited at 2.0 s requires representative evidence, not an assumption.

S.10 Normalized risk allocation and dependency reserve

Question: How can a top-level budget be allocated without hiding interfaces?

Synthetic target: a probability budget of 1.0×10^{-4} per mission for a defined top event. Suppose disjoint scenario contributions are allocated as shown. The union bound can provide a conservative sum even when events overlap, but the allocation must not omit common causes or assume that a reserved number is an implemented control.

Table S-10. Illustrative probability budget

Contributor	Allocated budget per mission
Function A scenarios	2.0×10^{-5}
Function B scenarios	2.5×10^{-5}
Human and procedure scenarios	1.5×10^{-5}
Shared infrastructure and common causes	2.0×10^{-5}
Unallocated design reserve	2.0×10^{-5}
Total	1.0×10^{-4}

The assigned contributor budgets total 8.0×10^{-5} , leaving 2.0×10^{-5} reserve. A reserve is planning capacity, not evidence that unknown hazards are controlled. Each allocation requires its own demonstration, and actual system-level combinations must be reviewed.

If Function A's supported upper estimate becomes 3.0×10^{-5} , the change consumes 1.0×10^{-5} of reserve only after authorized reassessment confirms that the system model and other allocations remain valid. Automatic spreadsheet rebalancing is not risk acceptance.

Decision implication: Budgets improve traceability but do not justify independent treatment of dependent functions or conceal unmodeled scenarios.

S.11 Barrier-test compliance and hidden critical gaps

Question: Does a high aggregate compliance rate establish readiness?

Synthetic data: 98 of 100 scheduled barrier tests are valid and on time. Two overdue tests concern the only protective functions for severe-consequence scenarios.

Overall compliance = $98 / 100 = 98\%$

The 98% indicator is arithmetically correct. It is insufficient for release because the two missing tests may invalidate essential barrier credit. If the critical subset contains 10 tests, its on-time compliance is $8/10 = 80\%$, and the two specific gaps still require individual disposition.

Table S-11. Required reporting layers

Layer	Result	Use
Overall programme	98%	General planning and trend
Critical subset	80%	Prioritization and resource escalation
Barrier BR-07	Overdue	Specific readiness decision
Barrier BR-12	Overdue	Specific readiness decision

Decision implication: Aggregate metrics support management but cannot compensate for a failed or unknown mandatory condition. The release decision must evaluate the specific dependencies.

S.12 Recovery-time and data-consistency demonstration

Question: Does a successful backup restore demonstrate operational recovery?

Synthetic recovery objective: the defined operational service must reach a verified safe and usable state within 60 min. The demonstrated sequence is detection and decision 5 min, isolation 7 min, data restoration 18 min, integrity and configuration reconciliation 14 min, and release checks 10 min. The sequence is assumed serial for this example.

Total recovery time = 5 + 7 + 18 + 14 + 10 = 54 min

Margin against objective = 60 - 54 = 6 min

Table S-12. Recovery acceptance checks

Check	Example result
Files restored	Complete against the selected backup manifest
Record identities and links	Reconciled for the tested population
Decision states	Expired and suspended decisions remain blocked
Configuration	Hardware, software, data and procedures match the accepted baseline
Offline records	Conflicts resolved and history retained
Operational release	Authorized after functional and safety checks

An 18 min file restoration is not the 54 min operational recovery. The example does not demonstrate that every future recovery will meet 60 min; representative adverse cases, variability, resource availability and remaining uncertainty must be examined.

Decision implication: The recovery endpoint must be defined in operational and safety terms. A technically available system with incorrect release states is not a successfully recovered assurance system.

Annex T - Integrated worked cases and decision trails

Status: Informative. All organizations, assets, identifiers, data and decisions in these cases are invented. The cases illustrate application of the proposed requirements; they do not authorize an actual activity.

T.1 Ground-support equipment: a restricted release that remains bounded

A ground-service provider plans to use a modified powered service unit beside an aircraft. The modification changes the motion-control software. The evaluated object is the servicing operation using Unit G-07 in configuration C4, not the provider's entire organization. The claimed operating surface is dry or wet pavement.

Table T-1. Case definition and initial evidence

Item	Case record
Principal provisions	Clauses 7-14, 18, 23-24 and 26; Annexes D-G and K-L
Hazard	H-GND-014: unintended motion while personnel occupy the interface zone
Safety requirements	R-017 servicing-mode motion inhibit; R-018 restraint performance; R-019 clear mode indication
Evidence	TEST-031 software/mode checks; INS-012 restraint inspection; HF-006 task observation
Initial finding	Wet-surface restraint performance is unverified; R-018 is HOLD for wet operation
Dependency concern	Motion inhibit and drive control share a controller; independence is not assumed

The team first considers whether a dry-only activity is technically separable. It verifies that surface condition can be identified before use and monitored during operation, that the dry-surface restraint evidence is valid, and that a weather change can be detected in time to stop. If those conditions cannot be demonstrated, a dry-only label would not be an effective restriction.

The case assumes that the narrower profile is demonstrated. A competent reviewer verifies the dry-surface controls and the release authority issues REL-GND-021 for dry-pavement servicing only. Wet operation remains prohibited. The decision identifies the unit, configuration, servicing locations, authorized personnel, surface check, stop trigger and shift handover requirement. No statement of full wet-and-dry conformity is made.

Table T-2. Required decision trail

Record	State and reasoning
R-017	PASS for the tested configuration and modes; common-cause limitations retained
R-018 dry profile	PASS based on applicable dry-surface evidence
R-018 wet profile	HOLD; excluded from the restricted claim but retained as unresolved work
Risk acceptance	Restricted dry profile only, with monitoring and invalidation on surface change

Record	State and reasoning
Operational release	Dry-only activity; automatic expiry at configuration change or loss of required monitoring
Corrective work	Validate wet-surface capability or redesign restraint before extending the claim

A later software update reopens TEST-031 applicability and the release dependency. The old release does not remain valid simply because the physical restraint is unchanged. The worked case demonstrates that narrowing a claim requires a real technical boundary and effective controls, not a wording change.

T.2 Maintenance: a passed functional test does not close an uncertain configuration

A maintenance organization completes a component replacement on an aircraft system. The functional test passes, but the removed and installed part records show conflicting modification status. The task authority permits release of the maintenance work only within the applicable technical data and configuration.

Table T-3. Maintenance case records

Item	Case record
Object	Maintenance package MP-042 on Asset A-12
Configuration issue	Installed component identity is clear; modification compatibility is not demonstrated
Test	FT-088 passed for the tested functions
Requirement states	Functional behavior PASS for test scope; configuration compatibility HOLD
Immediate action	Prevent affected release and preserve parts and records
Owner	Maintenance technical authority with design-source interface

The passing test shows that the exercised functions behaved as required in that test. It does not prove compatibility in every relevant operating condition or establish the missing configuration history. The organization requests authoritative configuration evidence and reviews other assets receiving parts from the same source.

The case assumes that the source confirms the installed modification is incompatible with the intended baseline. The HOLD becomes FAIL for the configuration requirement. The organization removes the incompatible part, installs a verified eligible part, repeats the required inspections and functional tests, and checks for any secondary effects of the first installation.

Table T-4. Closure and release logic

Step	Evidence required
Correct configuration	Verified identity, modification status and applicability
Correct work	Completed task steps and required independent checks
Functional restoration	Valid tests for the restored configuration
Wider impact	Review of affected stock and previous installations
Cause correction	Receiving and configuration-control process corrected
Effectiveness	Representative later receipts and installations show the control works
Release	Authorized signatory records completed scope and limitations

Implementation of a receiving checklist closes an action only when the action's implementation criterion is met. It does not close effectiveness until the defined operational evidence is available. The aircraft or component release remains separate from the corrective-action effectiveness period; any permitted release must have its own complete safety and authority basis.

T.3 Unmanned inspection: correlated navigation and containment failure

An operator proposes automated inspection in a bounded area. The containment function and normal navigation both use the same positioning source. The supplier describes the two functions as independent because they run in different software modules.

Table T-5. Unmanned-system case definition

Item	Case record
Object	Operation OP-U17 with vehicle V-03, control station CS-02 and data baseline D8
Domain	Defined area, weather, visibility, occupancy and communication conditions
Hazard	Loss of reliable position can lead to operation outside the intended boundary
Proposed barriers	Navigation control and software containment
Defeater	Both barriers depend on the same corrupted position input
Initial decision	HOLD; the claimed independence is unsupported

The reviewer challenges the shared sensing and timing path. Successful nominal tests of each module do not address the common dependency. The team also reviews whether the human supervisor can detect and intervene before the boundary is exceeded. A claim of "human in the loop" is not accepted without information, timing, workload and authority evidence.

Possible corrective paths include a validated independent means of detecting the hazardous condition, a demonstrably protective operating restriction, or an architecture change. The case does not prescribe a technical design. The selected solution must be assessed against the actual environment and required safety objectives.

Table T-6. Evidence needed before release

Claim	Required demonstration
Domain remains bounded	Accurate boundary, monitored conditions and response before loss of containment
Shared dependency controlled	Analysis and representative fault cases for corrupted or lost input
Supervisor credit valid	Task trials with realistic delay, ambiguity and concurrent workload
Contingency appropriate	Safe behavior for the actual location and failure condition
Configuration current	Vehicle, station, software, data and procedures match the verified baseline

The operation remains on HOLD until the selected controls and their limitations are verified. A successful demonstration in a clear, unoccupied area does not establish suitability for populated or more complex environments. Any later expansion of the domain is treated as a change requiring fresh analysis.

T.4 Space mission: irreversible command with uncertain state

A robotic mission plans an irreversible deployment. Telemetry indicates a plausible but inconsistent state after an interrupted command sequence. The ground team has a procedure for normal deployment, but the current state is outside the assumptions of that procedure.

Table T-7. Mission case record

Item	Case record
Object	Mission phase MP-DEP-02, flight baseline F6 and ground baseline G9
Hazard	Deployment from an incompatible state can damage the system and remove recovery options
Essential assumption	Mechanism and command sequence are in the expected pre-deployment state
Evidence conflict	Two state indicators disagree after the interruption
Initial action	HOLD irreversible command; preserve logs and maintain the defined protective state
Authority	Mission operations authority with independent system-safety review

The team distinguishes telemetry observation from inferred physical state. It reviews command history, timing, data validity, sensor dependencies and alternate explanations. Repeating the irreversible command merely to see whether it succeeds is not an acceptable diagnostic method without a supported safety basis.

The case assumes that additional non-hazardous diagnostics can resolve the state. The diagnostics themselves are reviewed for side effects and authority. Their results establish a compatible state, and the relevant technical authorities verify the revised sequence and contingency limits.

Table T-8. Gate disposition

Prerequisite	Disposition
State knowledge	Demonstrated within the profile's required confidence and limitations
Command sequence	Controlled, independently reviewed and configuration-matched
Ground support	Current personnel, communications and monitoring capability
Residual risk	Accepted for the specific phase with irreversible consequences explicit
Release	New command authorization; prior normal-sequence approval not reused blindly
Post-action	Verification of resulting state and update of mission records

If the state cannot be resolved, the decision remains HOLD or the mission adopts a separately justified alternative that does not rely on the unsupported assumption. Schedule pressure and remaining mission value are recorded but do not supply missing technical evidence.

T.5 Aerodrome operations: simultaneous works and degraded communications

An aerodrome plans temporary maintenance near an operational area. A separate project has already approved a temporary communications degradation. Each project was assessed individually. The work-zone safety plan relies on the communication capability that is now degraded.

Table T-9. Combined-condition case

Condition	Individual disposition	Combined concern
Temporary work zone	Accepted with active coordination and rapid stop communication	Coordination channel degraded
Communications degradation	Accepted for routine operations with local fallback	Fallback not demonstrated for work-zone complexity
Increased vehicle movement	Planned within temporary-work arrangements	More coordination demand and conflict opportunities

The operational authority suspends the affected combined activity and opens a joint change review. The review considers physical separation, scheduling, alternate communication, staffing and emergency access. It does not assume that adding a second person or a radio automatically restores the required performance.

The case assumes that work can be rescheduled to a period with verified physical isolation from the relevant operation. The new plan defines the isolation boundary, access control, inspection, communication fallback and reinstatement criteria. Both project records link to the joint decision so that neither can later change independently without reopening the interface.

Table T-10. Release and monitoring

Record	Required result
Joint hazard analysis	Combined exposure and shared-control dependency addressed
Work authorization	Scope and timing match the isolated operating state
Inspection	Boundary, access and protection verified before work
Operational status	Affected activities restricted until reinstatement
Reinstatement	Surface, equipment, markings, communication and access checked
Learning	Change system updated to detect overlapping temporary conditions

The case illustrates why separate signatures are not a combined-risk assessment. The common operating picture must show all temporary conditions relevant to the release.

T.6 Digital restoration: a technically successful recovery with an unsafe status defect

An assurance registry is restored after a system outage. File checksums match the backup manifest. A functional test shows that users can log in and retrieve records. However, a suspended release appears active because the suspension was recorded after the backup and has not been reconciled from the outage log.

Table T-11. Recovery case states

Item	Observed state	Required conclusion
File integrity	Backup files match checksums	Technical transfer integrity demonstrated
User access	Login and retrieval operate	Basic availability demonstrated
Decision history	Recent suspension absent	Decision completeness not demonstrated
Release display	Incorrectly active	Safety-relevant workflow failure
Operational use	Could authorize unsupported activity	HOLD automated release use

The recovery team preserves the restored state for analysis, reconciles the offline and post-backup records, restores the suspension and verifies all affected decisions. It examines whether other expired, restricted or withdrawn records were also restored incorrectly.

The independent reviewer requires a representative adverse-case test set: expired credentials, suspended releases, missing evidence links, conflicting offline edits and partial data transfer. The corrected system must block prohibited transitions and preserve the history.

Table T-12. Recovery acceptance

Condition	Required evidence
Data completeness	Backup plus subsequent authorized records reconciled
Semantic integrity	Identities, relationships, states and configuration agree
Authority	Users retain only current authorized roles
Decision logic	Adverse cases produce the expected HOLD or block
Operational state	Affected users informed and incorrect outputs withdrawn
Fresh release	Authorized system owner and independent reviewer accept restored use

The case demonstrates why availability, file integrity and operational assurance are separate claims. Recovery is complete only when the service is usable in the correct controlled state.

Annex U - Comparison matrices and prevention of false equivalence

Status: Informative.

U.1 Different conclusions from different evidence

Table U-1. Distinctions that preserve decision meaning

Concept	What it can establish	What it does not establish alone
Quality-system conformity	Processes meet defined management requirements	Safe behavior in every operating condition
Product verification	Specified requirements were met in the verified scope	Suitability for every intended or changed use
Operational validation	Behavior is suitable in demonstrated conditions	Unlimited deployment beyond the tested domain
Safety-case acceptance	Argument and evidence support a bounded claim	Statutory permission or zero risk
Risk acceptance	Authorized residual-risk decision under stated criteria	Waiver of an unrelated mandatory obligation
Operational release	Permission for a specific activity and conditions	Permanent continuing validity
Accreditation or competence recognition	Competence within the separately evaluated scope	Approval of every output or operation
Publication	A document has been issued through its publication process	Field validation or independent acceptance of a particular application

U.2 Methods and their limitations

Table U-2. Selecting analytical methods

Method	Useful contribution	Limitation requiring other evidence
Functional hazard analysis	Identifies consequences of lost, incorrect or mistimed functions	Can miss detailed implementation and human context
FMEA	Examines component or process failure modes and local effects	Can miss interactions and non-failure hazardous behavior
Fault tree	Structures causal combinations for a defined top event	Depends on completeness, event definitions and dependency treatment
Event tree	Explores outcomes following an initiating event	Branch probabilities and conditional context must be justified
Barrier analysis	Makes preventive and mitigative controls visible	A diagram does not prove barrier performance or independence

Method	Useful contribution	Limitation requiring other evidence
Task analysis	Reveals human information, action and workload demands	Requires representative observation and operational validation
Simulation	Explores behavior and sensitivity in a model	Validity is bounded by model assumptions and data
Operational monitoring	Detects trends and invalidation in actual use	Sparse events and incomplete reporting can conceal risk

U.3 Scores, probabilities and decisions

A severity category is ordinal; multiplying category numbers does not create a physical probability or expected loss. A maturity score can help prioritize improvement but cannot convert a failed mandatory requirement into conformity. A probabilistic estimate can inform risk acceptance but cannot supply missing authority. These tools should remain visible as different kinds of information.

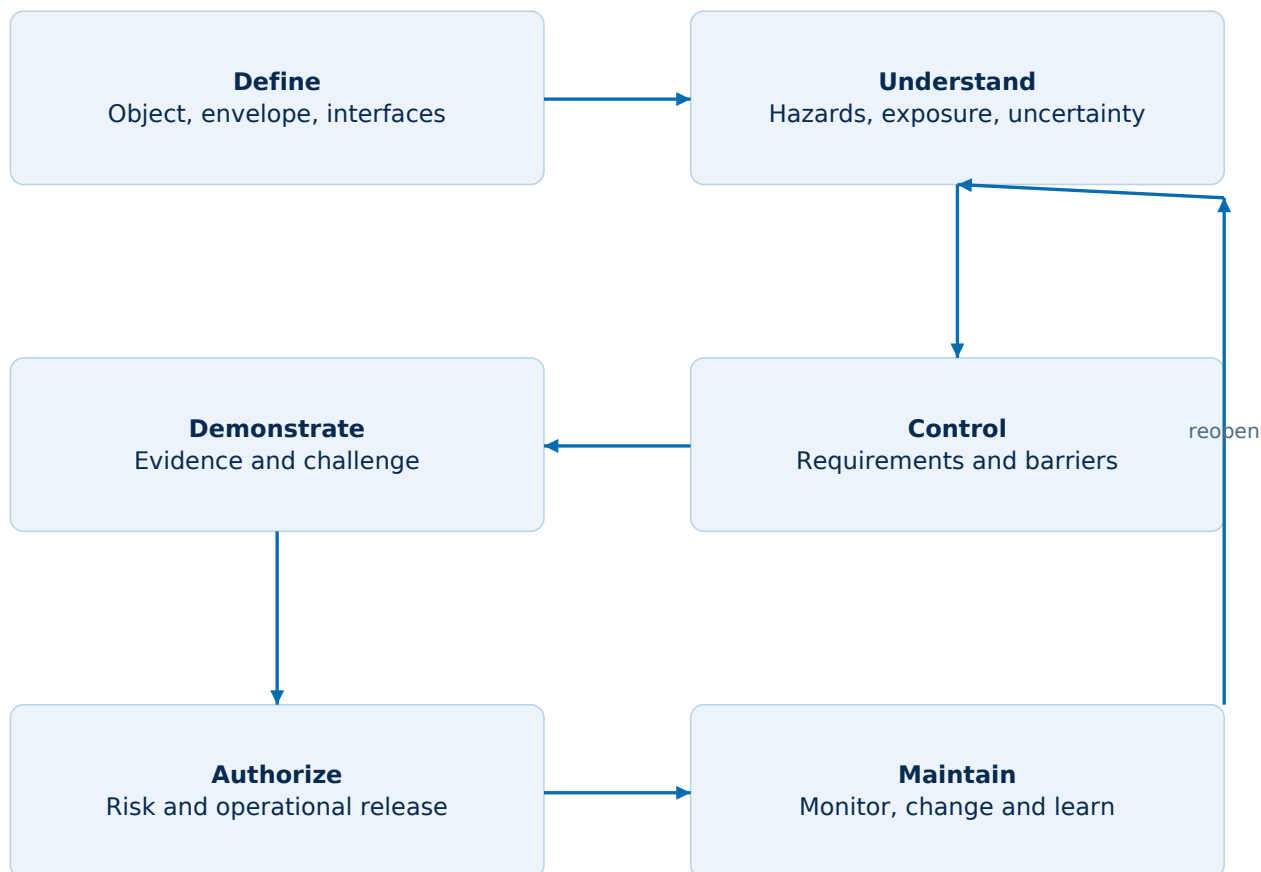
Table U-3. Common misleading substitutions

Substitution	Correct distinction
Two channels means independent protection	Shared causes must be analyzed.
No accidents means low risk is proven	Exposure, detection and uncertainty matter.
A signature means technical acceptance	Competence, purpose, evidence and authority must be established.
A successful restore means safe recovery	Decision states and operational configuration must be reconciled.
A trained person is authorized	Competence, task scope, currency and actual authorization differ.
A closed action means effective correction	Effectiveness needs its own criterion and evidence.
A restricted label makes an activity safe	The restriction must be enforceable and technically supported.

Annex V - Diagram atlas: safety, evidence and decision workflows

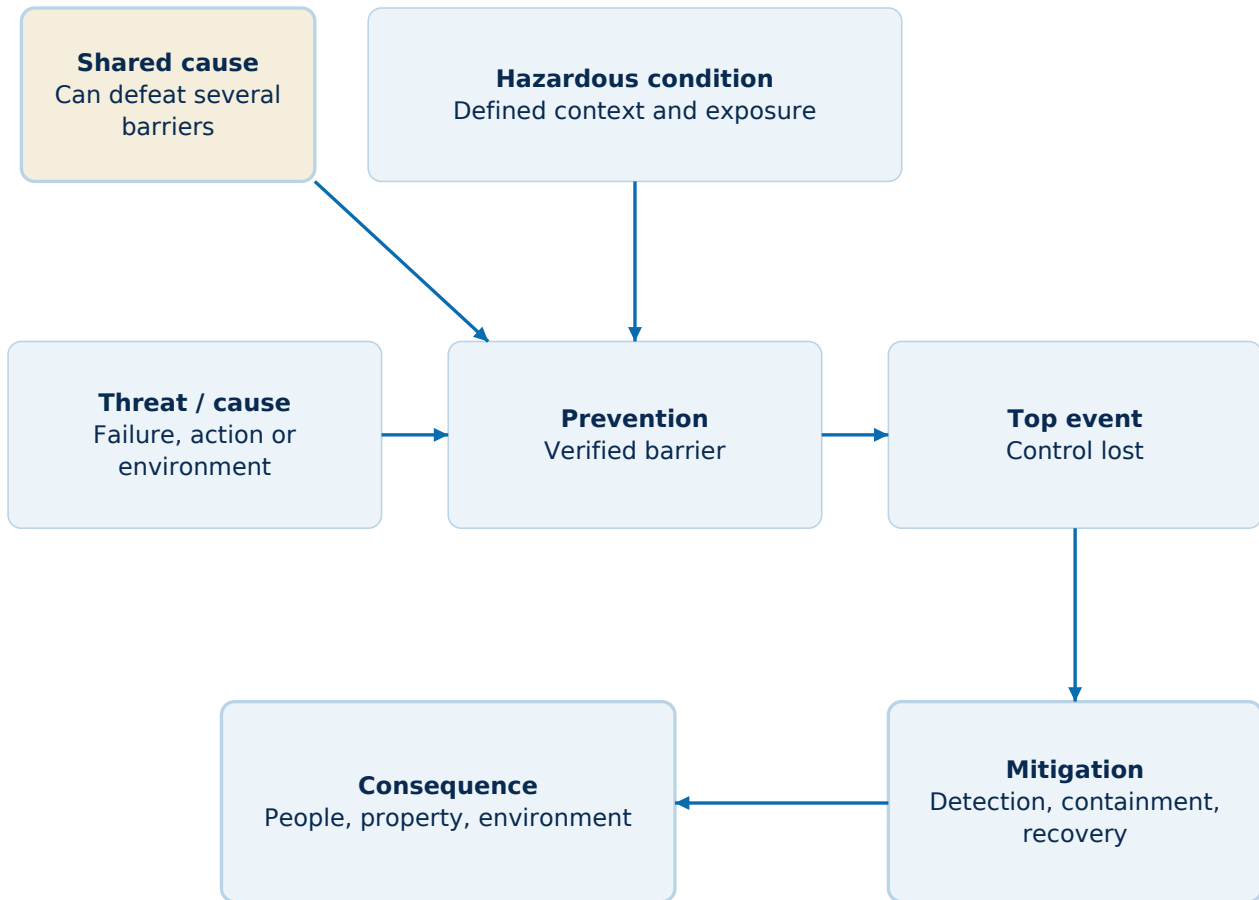
Status: Informative. Diagrams summarize the normative requirements and do not replace them.

V.1 Lifecycle assurance and feedback



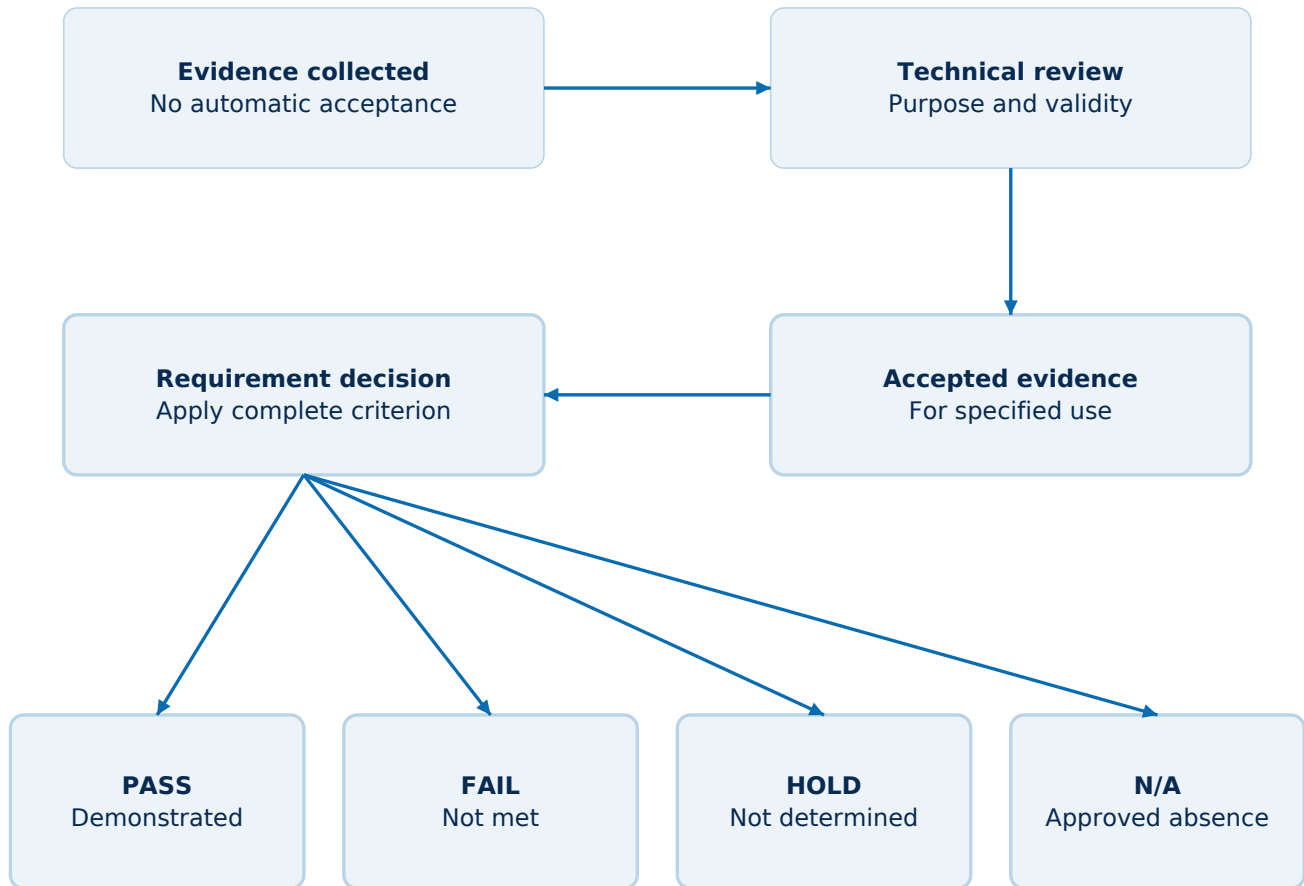
The lifecycle flow is iterative. Monitoring and occurrences can reopen the system definition, hazard analysis, control design or evidence. A release remains conditional on its supporting assumptions and current configuration.

V.2 Hazard, barrier and consequence structure



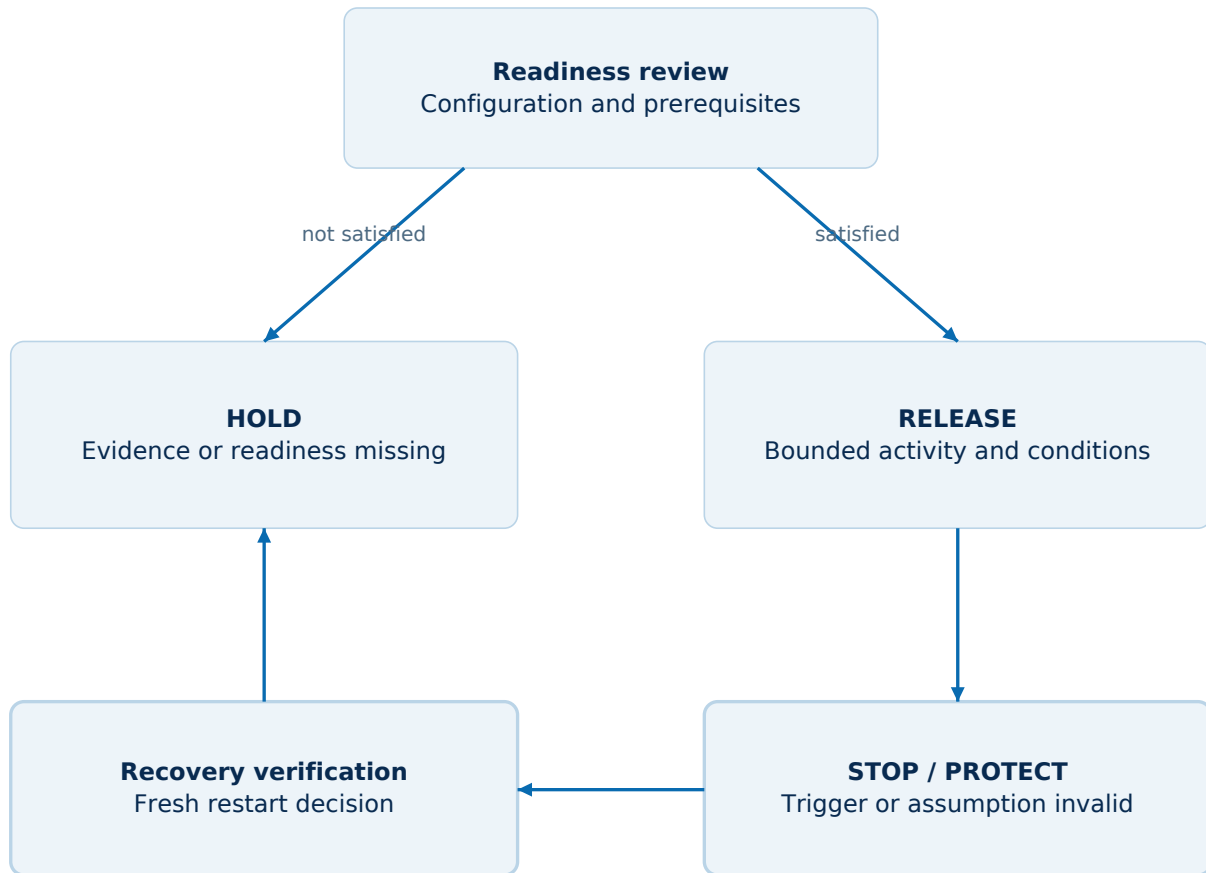
A barrier must interrupt a defined causal path or reduce a defined consequence. Shared dependencies can defeat several barriers simultaneously. The diagram should be read with the barrier performance standard, not as evidence of effectiveness.

V.3 Requirement and evidence states



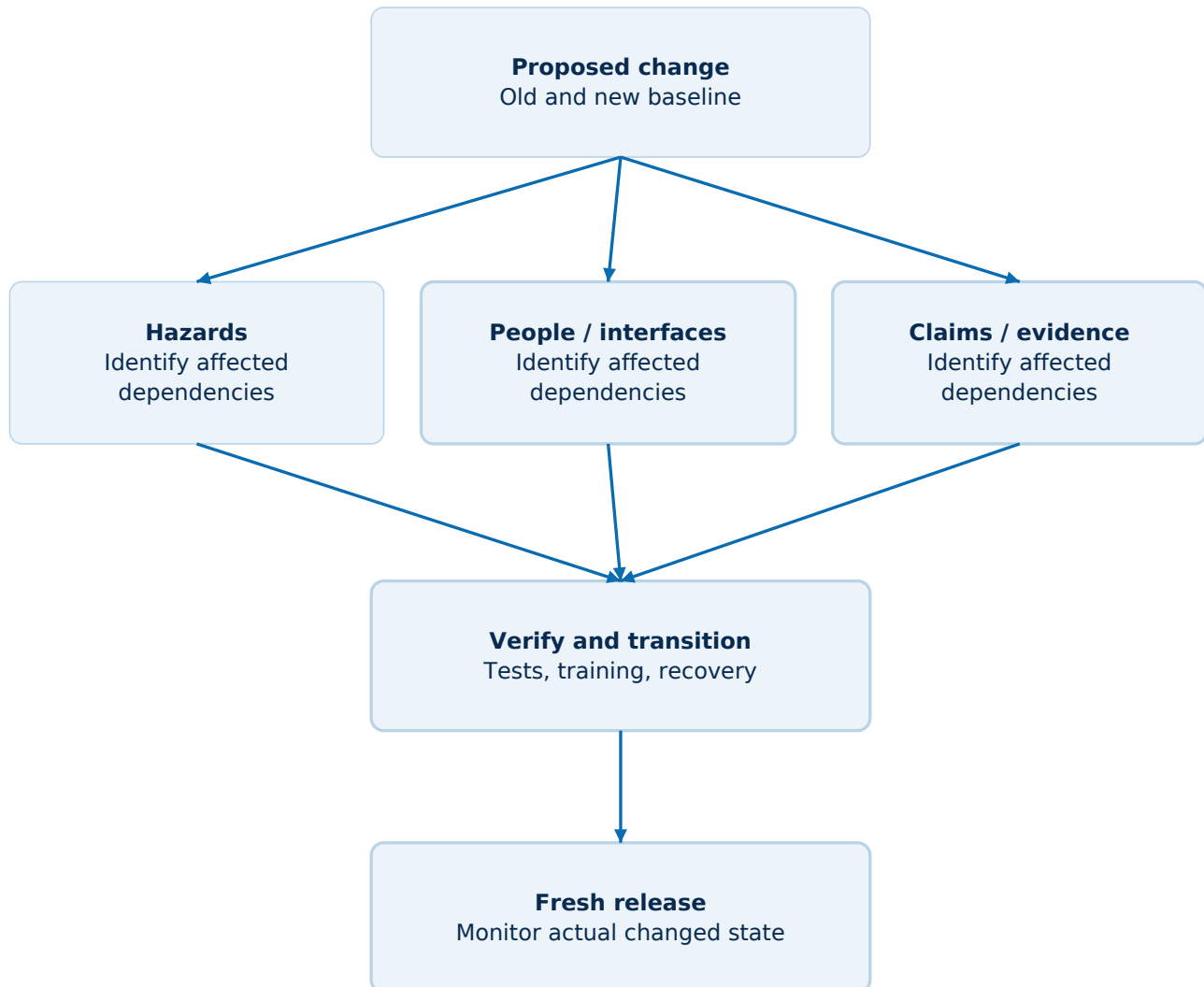
Evidence state and requirement state are distinct. Collected evidence awaits technical review. Accepted evidence supports a stated purpose; it does not automatically resolve every requirement. PASS, FAIL, HOLD and approved N/A preserve the actual determination.

V.4 Operational release and restart



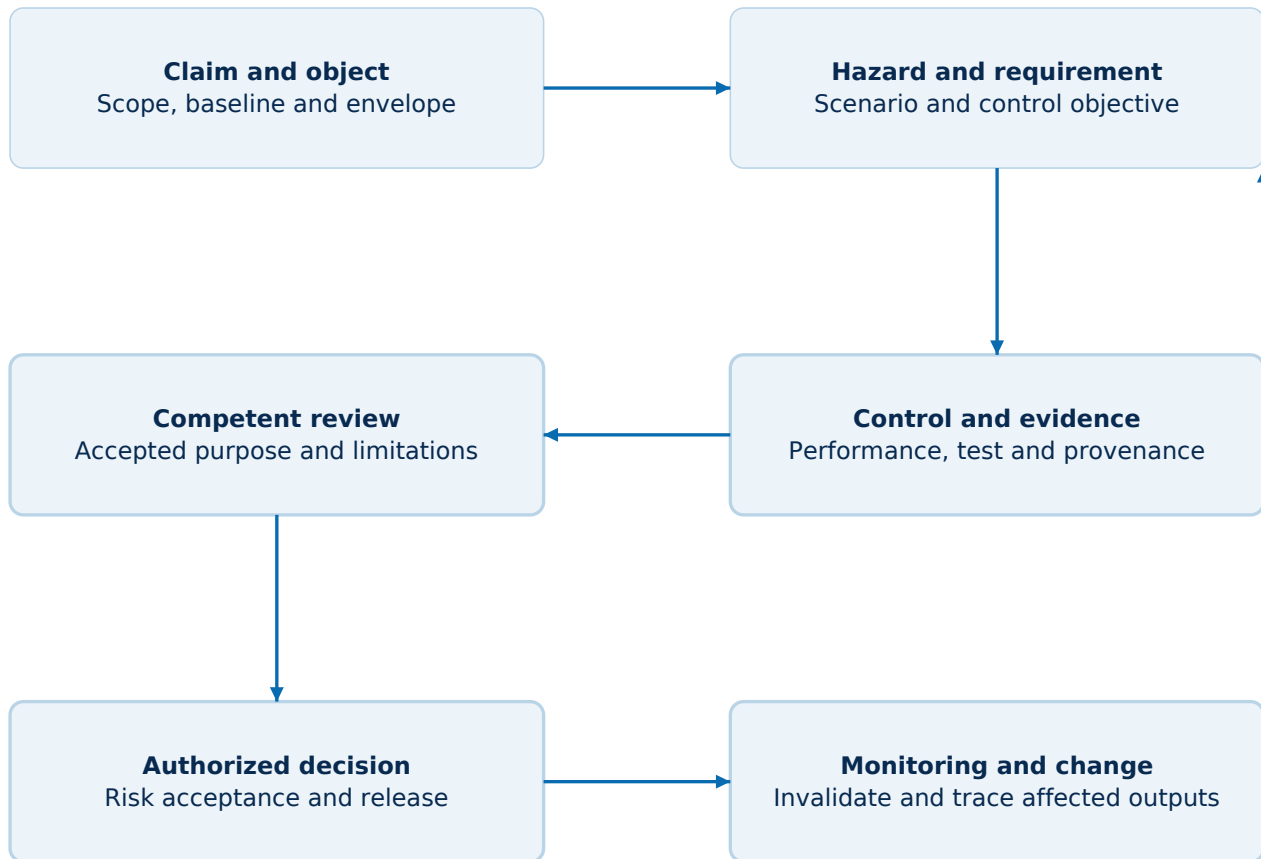
The release gate evaluates all applicable prerequisites. HOLD is a legitimate decision when evidence or readiness is incomplete. A stop creates a new need to verify condition and recovery; restart is a fresh decision.

V.5 Change propagation across the assurance case



A change can affect hazards, requirements, evidence, human tasks and supplier interfaces simultaneously. The impact set should be identified before implementation, then verified after the actual changed configuration is established.

V.6 Evidence trace and responsibility



Stable identifiers make the decision reproducible. A reviewer should be able to move from a claim to its hazard, control, evidence, accepted purpose and responsible authority, and back from adverse evidence to every affected decision.

Annex W - Boundary and adverse-case challenge suite

Status: Informative. The requirement to validate workflows is normative in Clause 27 and Annex N; the scenarios below are illustrative test cases to adapt and extend.

W.1 Use of the challenge suite

Each challenge should state preconditions, input, actor, expected state, expected notification, actual result and evidence. Passing these examples alone does not establish full workflow validation. The actual system should also be tested for its own rules, integrations, access restrictions and failure modes.

Table W-1. Requirement and evidence challenges

Test	Input condition	Expected behavior
W01	Evidence uploaded without review	Evidence remains collected/under review; requirement does not become PASS.
W02	Critical evidence link broken	Dependent claim becomes HOLD or is blocked from positive decision.
W03	Evidence belongs to another configuration	Applicability review required; automatic reuse blocked.
W04	Failed test followed by a passing repeat	Both results retained; failure disposition required.
W05	Measurement overlaps acceptance boundary	Apply pre-agreed rule; preserve HOLD if indeterminate.
W06	N/A requested because site access denied	Reject N/A rationale; record evidence limitation.
W07	One mandatory FAIL in an otherwise high score	Positive conformity decision blocked.
W08	Accepted evidence superseded by adverse result	Affected claims reopened and current decisions reviewed.

Table W-2. Authority and release challenges

Test	Input condition	Expected behavior
W09	Signatory's task authorization expired	Release blocked pending eligible authority.
W10	Administrator attempts risk acceptance without role	Action denied and logged.
W11	Reviewer has undeclared material authorship conflict	Independence review and reassignment/escalation.
W12	Release condition expires during operation	Defined warning and protective response triggered.

Test	Input condition	Expected behavior
W13	Temporary control extended repeatedly	Escalation and independent permanent-solution review.
W14	Two approved deviations share a weakened barrier	Combined-risk review required before continued exposure.
W15	Restart requested before recovery verification	Restart blocked.
W16	Restricted claim depends on failed excluded service	Restriction rejected as technically inseparable.

Table W-3. Data, transfer and recovery challenges

Test	Input condition	Expected behavior
W17	Duplicate identifiers refer to different objects	Conflict detected; dependent decisions held.
W18	Time sequence inconsistent across systems	Uncertainty identified; chronology reconciled.
W19	Partial migration preserves files but loses links	Semantic validation fails; operational use restricted.
W20	Backup restores a suspended release as active	Recovery rejected; state reconciled before use.
W21	Offline edit conflicts with current record	Authorized conflict resolution with both histories retained.
W22	Restricted evidence has no authorized reviewer	Evidence remains unavailable for the claim.
W23	Dashboard omits missing records from denominator	Data-quality defect detected; status corrected.
W24	Workflow logic changed without validation	Deployment blocked or rolled back under controlled change.

W.2 Physical and operational challenges

Table W-4. Operational challenge examples

Challenge	Question to demonstrate
Loss of monitoring	Does the activity enter the defined restriction rather than continue blindly?
False protective activation	Is the resulting state safe for the actual phase?
Delayed human intervention	Is the response-time claim still supported under workload?
Supplier evidence withdrawn	Can affected objects and releases be identified promptly?

Challenge	Question to demonstrate
Emergency responder unavailable	Is the operation blocked or supported by a verified alternate?
Environment crosses the boundary	Can the crossing be detected and acted on in time?
Mixed software/data baseline	Is incompatible operation prevented?
Irreversible step with uncertain state	Does the decision remain HOLD until a supported basis exists?

Annex X - Assessor evidence trails and activity starter profiles

Status: Informative. These profiles help select and examine requirements. They are not substitutes for the normative text or completed project parameters.

X.1 One complete evidence trail

An assessor should select an actual safety-significant operation and trace it from scope to current decision. The selected case should include a meaningful change, anomaly or temporary condition where possible. A perfectly prepared demonstration record may not reveal how the system handles real pressure and incomplete information.

Table X-1. End-to-end evidence trail

Step	Evidence to inspect	Challenge question
Scope	Object, activity, interfaces and exclusions	Does the boundary match the actual work?
Hazard	Scenario, exposure, causes and consequences	What could make this scenario worse or invalidate it?
Requirement	Allocated control and acceptance criterion	Is the requirement verifiable and complete?
Evidence	Method, configuration, data and review	Does it support this claim for this condition?
Risk	Residual basis, uncertainty and authority	Were all credited controls actually verified?
People	Task competence and authorization	Can the assigned people perform the required action?
Release	Prerequisites, restrictions and no-go rules	Was the real condition checked at decision time?
Monitoring	Indicators, barrier health and expiry	What would cause the release to lose support?
Change	Impact, transition and verification	Are current conditions still within the accepted case?
Learning	Occurrences and effective correction	Did findings change actual work and controls?

X.2 Aircraft operator starter profile

Define fleet and configurations, operation types, routes or areas, crew and support structure, dispatch authority, airspace dependencies and external services. Apply the common clauses, aviation controls and every triggered maintenance, ground, digital, supplier or energy interface. Prioritize evidence for actual dispatch decisions, abnormal operations, recent changes and repeated defects.

Table X-2. Aircraft operator first-case evidence

Priority	Evidence package
1	One current operational plan and its completed parameter profile
2	One severe-consequence hazard with verified controls and residual acceptance
3	One release record reconciled to actual aircraft, crew and environment
4	One change showing updated procedures, competence and safety case
5	One occurrence traced through effective corrective action

X.3 Maintenance organization starter profile

Define asset types, tasks, technical authority, release scope, facilities, personnel, parts, tooling and outsourced work. Trace a safety-critical maintenance task from intake through interruption, independent inspection, functional test and release. Include a record conflict or rejected part to examine whether the system preserves HOLD and FAIL rather than forcing completion.

Table X-3. Maintenance first-case evidence

Priority	Evidence package
1	Task and release-authority matrix
2	Applicable instructions and actual configuration
3	Personnel, tools and parts eligibility
4	Completed work with independent checks and anomaly disposition
5	Release, downstream information and repeat-defect learning

X.4 Aerodrome or ground-service starter profile

Define site boundaries, movement and servicing activities, contractors, shared infrastructure, emergency providers and concurrent works. Examine an actual shift handover and a temporary restriction. Confirm that essential services and emergency assumptions are available during the operating period, including nights or reduced staffing where relevant.

Table X-4. Ground-service first-case evidence

Priority	Evidence package
1	Site activity map and interface ownership
2	Servicing or movement hazard with barrier performance standard
3	Equipment condition and personnel task authorization
4	Temporary-work and combined-condition assessment
5	Emergency exercise and reinstatement decision

X.5 UAS or advanced-air-mobility starter profile

Define the entire system, operating domain, human supervision, communication, navigation, automated functions, ground exposure and contingency. Examine boundary tests and common dependencies. Compare the demonstrated domain with the actual deployment proposal. A pilot demonstration in easier conditions should not be used to infer unrestricted capability.

Table X-5. UAS first-case evidence

Priority	Evidence package
1	Operational design domain and enforceable limits
2	Lost/corrupted link and navigation safety analysis
3	Containment and contingency verification
4	Human workload and intervention demonstration
5	Current vehicle, station, software and data baseline

X.6 Space mission starter profile

Define the mission phases, interfaces, irreversible transitions, command authority, ground support and terminal state. Select a critical phase transition and reconstruct the evidence that supports it. Review what the team would do with uncertain state, conflicting telemetry or unavailable support.

Table X-6. Space mission first-case evidence

Priority	Evidence package
1	Phase-specific mission safety profile
2	Hazard and interface acceptance for a critical transition
3	Command, telemetry and configuration assurance
4	Contingency, ground-support and recovery limitations
5	End-of-mission feasibility and retained obligations

X.7 Design, digital or supplier starter profile

Define the supplied function, safety requirements, integrator assumptions, configuration, verification methods and change notifications. Trace one safety-relevant requirement through implementation, adverse-case testing, independent review and acceptance by the receiving party. Examine whether the supplier's limitations are actually reflected in the integrated safety case.

Table X-7. Supplier first-case evidence

Priority	Evidence package
1	Allocated requirements and interface assumptions
2	Configuration-specific design or digital evidence
3	Anomaly, uncertainty and limitation disclosure

Priority	Evidence package
4	Integrator acceptance and compatible operating conditions
5	Change, occurrence and support-continuity obligations

X.8 Assessment report structure

A useful report states the object, criteria, boundaries, team competence, methods, evidence coverage, findings, uncertainty, required actions and proposed conclusion. It distinguishes observations from interpretations and records inaccessible evidence. The report should allow a decision maker to understand why the scope is supported and where it is not.

Annex Y - Publication, interpretation and maintenance control

Status: Normative for the proposed publication-control process. This annex does not assert that the process has already been completed.

Y.1 Present manuscript status

Table Y-1. Document identity and status

Item	Declared position
Programme reference	AF 9200
Title	Aerospace Safety & Operational Assurance
Organization named in the manuscript	Aerospace Federation
Edition designation	FIRST EDITION
Language	English master text
Present document state	Complete proposed requirement manuscript prepared for publisher review
Publisher approval	Not recorded in this manuscript
Publication and effective dates	Not assigned in this manuscript
Technical validation and consultation	Completion is not asserted by preparation of this document
Intended normative content	Main clauses 0-28; Annexes A-R and Y, subject to their stated applicability
Informative content	Annexes S-X and Z; explicitly identified examples within normative annexes

Y.2 Publication decision dossier

Before issuing an approved edition, the publisher shall retain a dossier identifying the technical need, scope, competent contributors, interest declarations, review method, consultation arrangements, comments, dispositions, validation evidence where required, unresolved limitations and approving authority. The dossier shall identify the complete normative and informative content approved for issue.

The publisher shall assign the publication identifier and dates through its controlled decision. A programme reference shall not acquire an edition year merely because a manuscript exists. The cover and status page shall be updated together when the publication decision is recorded.

Y.3 Interpretation and change

Interpretations shall identify the question, affected provision, technical reasoning, authority and effective application. An interpretation shall not silently introduce a new requirement or weaken an existing mandatory condition. Substantive changes shall follow the applicable review and publication process, with impact and transition arrangements stated.

Y.4 Maintenance and withdrawal

The publisher shall monitor technical feedback, discovered errors, implementation difficulty, new hazards and changes affecting the technical basis. It shall determine whether correction, amendment, a new edition or withdrawal is necessary. Users shall be able to distinguish current, superseded and withdrawn material through the authoritative record.

Y.5 Truthful publication claims

Approval for publication concerns the document. It does not assert independent technical validation of every application, statutory approval, automatic conformity, accreditation or operational permission. Those conclusions require their own scope, evidence, authority and decisions. The publisher shall ensure that public descriptions preserve these distinctions.

Annex Z - Navigation crosswalk and implementation sequence

Status: Informative.

Z.1 Requirement-family crosswalk

Table Z-1. Questions and primary provisions

Practical question	Main clauses	Supporting annexes
What object and activities are covered?	1-4	A-B, R
Who owns safety and can stop or release work?	5-6, 12-13	C, F, P
How are hazards identified and maintained?	7	D, M
How are risk and uncertainty evaluated?	8	B-C, S
How are controls specified and demonstrated?	9-10	D-E, K
How are people prepared and authorized?	11	H
How is an operation released and monitored?	12-13, 16	F, J
How are changes controlled?	14	G, N
How are occurrences investigated?	15	I, Q
Which aviation and ground controls apply?	17-20	L, X
Which space and defense controls apply?	21-22	M, X
How are industrial and digital interfaces assured?	23-24	K, N
How are suppliers and facilities controlled?	25-26	M, O

Practical question	Main clauses	Supporting annexes
How are records and decisions protected?	27-28	B, N-R, W
How is publication status maintained?	0.5, 28.6	Y

Z.2 Practical implementation sequence

Table Z-2. Implementation sequence and evidence of completion

Stage	Work to complete	Evidence of completion
1 Define	Object, activities, interfaces, obligations and retained responsibility	Approved scope and applicability matrix
2 Govern	Authorities, competence, independence, reporting and stop-work	Named roles and usable escalation routes
3 Specify	Profile parameters, objectives, methods and lifecycle gates	Completed Annex B schedule
4 Understand	Hazard scenarios, dependencies, exposure and uncertainty	Reviewed hazard register
5 Control	Allocated requirements and barrier performance standards	Traceable control architecture
6 Demonstrate	Analysis, tests, human trials and independent challenge	Accepted purpose-specific evidence
7 Decide	Residual risk, readiness, restrictions and release	Authorized bounded decisions
8 Maintain	Monitoring, change, occurrence response and reassessment	Current safety case and effective learning

Z.3 Final completeness questions

Before relying on a conclusion, the user should be able to identify the exact object; the conditions under which the conclusion holds; every essential assumption; the evidence supporting the controls; the person authorized to decide; and the event that would invalidate the conclusion. If any of these cannot be answered, the assurance chain is incomplete.

The intended result of AF 9200 is a controlled relationship between technical evidence and real operational decisions. Its value depends on competent implementation, honest treatment of uncertainty and continuing verification in the actual environment.