



AF-IG-9200-002

Safety Case and Evidence Preparation Guide

Space / Aviation / Defense

FIRST EDITION

AF 9200 SUPPORTING DOCUMENT

Document identity and use

Field	Declared position
Code	AF-IG-9200-002
Title	Safety Case and Evidence Preparation Guide
Family	Companions
Organization	Aerospace Federation
Edition	FIRST EDITION
Relationship	Supporting material for AF 9200 - Aerospace Safety & Operational Assurance
Status	Prepared for publisher review; approval and effective dates not assigned
Language	English master text

Use and precedence

The AF 9200 standard contains the proposed requirements. This supporting document supplies guidance, model controls or records within its stated purpose. Complete the local scope, parameters, roles and authority before operational use. A completed template does not establish conformity or permission.

Applicable legal and competent-authority obligations remain independently binding. No AF recognition, accreditation, statutory approval or operational authorization is created by this document. Codes in this set are proposed identifiers for the newly prepared supporting collection.

Record completion

Where fillable fields are provided, use a PDF reader that supports interactive forms. Blank fields remain unresolved. Attach controlled evidence by identifier where space is insufficient. Typed names are not certificate-based digital signatures. Preserve the completed record and its history under the local retention rules.

Implementation control	Allocation
Responsible function	Safety-case owner
Primary AF 9200 anchors	7-10, 14, 28; Annexes C-E, K, P-R
Catalogue	AF-ML-9200-001; coverage: AF-CM-9200-001

Contents - clauses and annexes

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

1 Purpose and argument boundary	4
2 Claim decomposition	5
3 Evidence preparation	6
4 Assumptions, uncertainty and defeaters	7
5 Quantitative claim review	8
6 Independent review dossier	9
7 A compact example argument	10
8 Maintaining the case	11

1 Purpose and argument boundary

This companion explains how to prepare a safety case and evidence package for AF 9200. It is informative. The requirements remain in Clauses 7-10, 12, 14, 27-28 and Annexes B-E and P-R. A safety case is a reasoned argument for a defined object and conditions, not a collection of certificates or a promise of zero risk.

Start with one explicit top claim. State the object, configuration, lifecycle phase, activity, operating envelope, exposure and applicable criteria. Identify excluded activities and essential external dependencies. A reviewer should understand the claim without guessing which configuration or mission it concerns.

2 Claim decomposition

Decompose the top claim into the questions needed to support the decision. A useful structure examines hazard coverage, control adequacy, verification, operational readiness and continuing validity. Tailor the structure to the actual object rather than forcing every case into an identical diagram.

Table SG-1. Claim preparation questions

Claim area	Question	Typical evidence
Context	Is the actual system and environment bounded?	System description, configuration and interface register
Hazard coverage	Have credible scenarios and interactions been examined?	Hazard analysis, task review and independent challenge
Control adequacy	Do allocated controls address the scenario and its dependencies?	Requirements, architecture and barrier standards
Demonstration	Do valid results show the required behavior?	Analysis, tests, inspections and operational validation
Readiness	Can people and support sustain the controls now?	Competence, equipment, procedures and emergency evidence
Maintenance	Will invalidation be detected and acted on?	Monitoring, change, occurrence and review controls

Each claim should identify the argument connecting evidence to the conclusion. Avoid circular arguments such as "the system is safe because the safety process says it is safe". A process can improve confidence, but the technical behavior and operational conditions still need support.

3 Evidence preparation

3.1 Evidence identity

Assign an evidence ID and preserve the original source. Record author, date, method, configuration, equipment, competence, raw data, processing, uncertainty and intended purpose. A file name is not enough to establish provenance.

3.2 Reuse and equivalence

When reusing evidence, compare functions, design, interfaces, environment, exposure, procedures and failure mechanisms. State which differences are immaterial and why. Identify additional demonstration needed for material differences. Evidence accepted for one purpose may remain insufficient for another.

Table SG-2. Evidence review decisions

Result	Meaning
Accepted for stated purpose	Evidence is adequate for the identified claim and conditions.
Accepted with limitation	Only a specified portion or domain is supported.
Further evidence required	The claim remains HOLD pending completion.
Rejected	Evidence is invalid or inadequate; dependent decisions need review.
Superseded	A later controlled record replaces reliance while history remains.

4 Assumptions, uncertainty and defeaters

List essential assumptions separately from facts. Give each assumption an owner, justification, confirmation or monitoring method and invalidation trigger. An assumption about human response, supplier behavior or emergency availability needs the same discipline as an engineering assumption.

A defeater is a credible condition or argument that could undermine a claim. Examples include a common power source defeating two barriers, unrepresentative test conditions, stale mission data, or a model used outside its validated domain. Record the challenge and disposition rather than removing uncomfortable evidence from the package.

Table SG-3. Uncertainty treatment

Source	Appropriate treatment
Sparse events	Confidence bounds and complementary design/control evidence
Model limitations	Validated domain, sensitivity and bounded extrapolation
Unknown configuration	Resolve identity or restrict the claim
Human variability	Representative trials and conservative response assumptions
Supplier evidence limitation	Authorized review route or explicit HOLD
Changing environment	Monitoring, enforceable limits and revalidation triggers

5 Quantitative claim review

Verify units, exposure denominators, event definitions, dependence and uncertainty. Do not add probabilities referring to different exposures or multiply barrier probabilities without justified independence. Do not treat software systematic defects as random hardware failures without a defensible model.

Reproduce important calculations independently. Preserve input data and processing. Review sensitivity to uncertain inputs and identify dominant contributors. The examples in AF 9200 Annex S illustrate methods; their synthetic limits are not project acceptance criteria.

6 Independent review dossier

The dossier should contain the bounded claim, applicability matrix, completed profile, hazard and control registers, evidence index, open issues, assumptions, quantitative records, operational readiness basis and proposed decision. The reviewer needs access to the underlying evidence, not only summaries.

Table SG-4. Review record

Field	Required content
Review scope	Claims, configurations, phases and interfaces examined
Team	Competence, independence and conflicts
Method	Full review, sampling, observation, testing and limitations
Challenges	Assumptions, defeaters, contradictions and missing evidence
Findings	Requirement/claim, evidence, consequence and closure criterion
Disposition	Accepted, restricted, HOLD or rejected with reasoning
Decision	Eligible authority and conditions for continuing validity

7 A compact example argument

Synthetic claim: A defined servicing operation using Unit G-07 in dry conditions is supported within its approved profile. The scope excludes wet operation because restraint performance in wet conditions is unverified.

The argument identifies unintended movement as a hazard, allocates motion inhibition and restraint requirements, and links dry-condition tests and task observation. It acknowledges a shared controller dependency and does not claim two independent electronic protections. The operational plan verifies dry conditions and requires stopping if they change. Independent review confirms that the narrower boundary is enforceable.

The example's strength is its explicit limitation. If surface condition cannot be reliably detected or controlled, the restriction does not support the claim. The evidence package must then remain HOLD or adopt a different demonstrated control.

8 Maintaining the case

Map monitoring and change triggers to the claims they sustain. When a barrier fails a test, evidence is withdrawn, a supplier changes configuration or the operation expands, identify every affected decision. Preserve the prior accepted case and its validity conditions.

At each review, ask what has changed in the system, environment, people, data, knowledge and authority. Confirm that the current operation still matches the claimed object. A recently updated cover date does not establish a current safety case.