



AF-HB-9500-001

Aerospace Integration and Mission Assurance Handbook

Space / Aviation / Defense

FIRST EDITION

AF 9500 SUPPORTING DOCUMENT

Document identity and use

FIRST EDITION MANUSCRIPT - Prepared for Aerospace Federation review

Field	Controlled identity
Document	AF-HB-9500-001 - Aerospace Integration and Mission Assurance Handbook
Parent standard	AF 9500 - Aerospace Digital Systems, Software & Cybersecurity
Edition / language	FIRST EDITION / English master text
Family	Manuals
Primary source anchors	5-8, 17, 21-26, 29-37; Annexes C-D, H-J, L
Suggested local owner	Integration authority
Authority	Publisher approval and effective date are not assigned. Local use requires authorized adoption and completed parameters.

Use with the main standard

This document implements the identified AF 9500 clauses and annexes. Read the complete applicable requirements in the main standard. The source anchors are navigation references; a template does not replace technical judgement, evidence, permission or eligible approval.

AF-ML-9500-001 lists the complete supporting set. AF-CM-9500-001 maps the main clauses and annexes to working documents. AF-TP-9500-001 establishes the common local parameter baseline; add the relevant discipline profiles.

Record control

Identify the object, configuration, record owner and dates. Reference attachments by stable identifier and version. Keep superseded evidence and decisions traceable. Use the approved local retention, access and authentication arrangements. No technical limit, numerical limit, interval or acceptance value is assigned by a blank template.

Implementation model: Translate the stated responsibilities and controls into the actual organization. Informative examples remain explanatory; use approved programme-specific values for operational decisions.

1 Define the integrated function

Aerospace integration starts with intended behavior and consequences across the complete operational chain. Identify the airborne or remote platform, ground systems, payload, maintenance equipment, providers and users. Apply AF-PR-9500-001/002/004 to context, risk and architecture rather than assuming that component approvals add up to integrated approval.

1.1 Interface and authority model

Use AF-FR-9500-003/017. Define peers, commands, units, freshness, sequencing and failure responses. Separate operational, payload, passenger, enterprise and maintenance authority where relevant. Include temporary and privileged management paths. Review shared identity, time, power and update dependencies.

1.2 Timing and resources

Use AF-FR-9500-013 to reconcile end-to-end budgets. Include computation, communication, authentication, logging, actuation, jitter and interference under declared assumptions. Average latency or spare nominal capacity does not establish the worst relevant behavior.

2 Apply aviation-specific conditions

Use AF-TP-9500-003 and AF-FR-9500-019. Evaluate flight phases, ground connectivity, dispatch conditions, crew workload and operating permissions. A security rule that prevents unauthorized access can still create an unacceptable operational effect if it removes essential control.

2.1 Data loading and fleet state

Verify package identity, signer authority, target compatibility, permitted mode and recovery separately. Track actual installed configuration, maintenance changes and local overrides. Preserve restrictions for failed or unreachable targets. Ground-service or component evidence shall not imply approval of every aircraft installation.

3 Apply space and remote-mission conditions

Use AF-TP-9500-004. Define segments, contact windows, delays, constrained resources and physically inaccessible components. Command authority and freshness shall survive disconnection and reconnection without unsafe duplication or stale execution.

3.1 Remote evidence and autonomy

Distinguish sent, received, installed, active and confirmed states. Missing telemetry is uncertainty. Autonomous functions shall have approved constraints, monitoring and fallback. A human-intervention claim shall be realistic for contact delay, workload and available information.

3.2 Trust and long-life support

Plan key rotation, revocation, component support and algorithm migration for actual mission life. Assess how counters, data schemas and boot trust affect rollback. Demonstrate recovery before relying on it for an irreversible transition.

4 Demonstrate integrated adverse behavior

Use AF-PR-9500-011/019/023/027. Test representative lost links, invalid inputs, shared-service failure, interrupted update and restored-state reconciliation. Preserve limitations where test environments cannot represent actual conditions. Bridge evidence only through a documented technical argument.

4.1 Bounded operational decisions

Assemble AF-FR-9500-028 with exact platform, configuration, modes, target population and evidence. Keep safety assessment, cybersecurity acceptance, release and operating permission distinct. New threats or invalid assumptions shall reopen affected claims and operating restrictions.

Required evidence: An integrated phase-specific argument with actual interface, timing, trust, update and recovery evidence and explicit authority boundaries.