



AF-DM-9500-001

Software Development and Release Manual

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-DM-9500-001 - Software Development and Release Manual
Parent standard	AF 9500 - Aerospace Digital Systems, Software & Cybersecurity
Edition / language	FIRST EDITION / English master text
Family	Manuals
Primary source anchors	4-17, 28-30, 36; Annexes C-H, L
Suggested local owner	Development and release owner
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 Keep superseded evidence and decisions traceable.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 Establish the digital product basis

Use AF-PR-9500-001 and AF-FR-9500-001 to define the product, users, modes, retained responsibilities and consequence classification. Complete AF-TP-9500-001 and the P01-P44 parameter baseline. The development owner retains the authoritative requirements and identifies exact technical and operating authorities.

1.1 Risk and architecture

Use AF-FR-9500-002/004 for integrated safety-security scenarios, isolation, common causes and degraded modes. Identify what must happen when trust or availability is lost. Record architectural assumptions and who monitors them. A design boundary remains a claim until representative evidence supports it.

1.2 Requirements and planning

Use AF-FR-9500-003 for requirements and interface traceability and AF-FR-9500-005 for lifecycle gates, competence and independence. Define expected evidence before execution. Every essential gap retains an owner and blocked scope. Iterative development does not remove technical exit criteria.

2 Control inputs and implementation

Use AF-PR-9500-006/007 for suppliers, component inventories, configuration and changes. Bind the dependency inventory to actual artifacts. Agree support, findings and evidence access with providers. Preserve historical versions and relationships.

2.1 Code and generated content

Use AF-FR-9500-008 to record design rules, review and analysis. Examine boundary, error, resource and concurrency behavior. Generated code and AI-assisted work remain subject to the same necessary requirements and independent evidence. AF-PR-9500-021 defines assistance and action limits.

2.2 Tools and builds

Use AF-FR-9500-009/010 to control workers, source, caches, tools and output provenance. Evaluate tools for their exact intended use and independent error detection. Separate protected signing authority from uncontrolled execution. Reconstruct or compare outputs where required and explain nondeterminism.

3 Establish valid verification

Use AF-PR-9500-011/012 and the corresponding records. Define method capability, target representation, independent review, expected outcomes and acceptance rules. Security examinations require explicit authority, protective conditions and stop rules.

3.1 Coverage and anomalies

Retain complete denominators and actual PASS, FAIL, HOLD and N/A states. Test-data quality, labels and independence are part of evidence validity. Preserve original anomalies and failed or invalid runs. Correction requires affected-scope analysis and appropriate regression; a passing rerun does not erase unexplained behavior.

3.2 Timing and integration

Use AF-FR-9500-013 and the relevant profiles to establish end-to-end timing, concurrency and resource evidence. Include security and monitoring overhead. Verify actual platform, interface and operating-mode assumptions. Average performance and simulated behavior alone may not represent required target conditions.

4 Release and hand over the exact baseline

Use AF-FR-9500-028 to assemble the assurance case and reconcile claims, evidence, findings, residual risks and support conditions. The eligible authority decides the bounded release. Artifact authenticity, technical acceptance and operating permission remain separate.

4.1 Deployment and updates

Use AF-FR-9500-022/023 to verify target compatibility, secure configuration, operating window, interruption and recovery. Reconcile staged, active, confirmed, failed and unreachable targets. Operational handover includes known limitations, support, monitoring, competence and remaining dependencies.

4.2 Maintain the argument

Trace new vulnerabilities, incidents and compromised tools to affected releases. Reopen invalid assumptions and communicate restrictions. Preserve actual operating and historical evidence. Use AF-CM-9500-001 to navigate applicable requirements without treating a mapping as proof of implementation.

Required evidence: A complete requirement-source-build-verification-release-deployment trail with valid decisions and preserved adverse history.