AEROSPACE FEDERATION

AF-PR-9500-010

Tool, Model and Formal-Method Assurance

Space / Aviation / Defense

FIRST EDITION

AF 9500 SUPPORTING DOCUMENT

Aerospace Federation
af.org

Document identity and use

FIRST EDITION MANUSCRIPT - Prepared for Aerospace Federation review

Field	Controlled identity
Document	AF-PR-9500-010 - Tool, Model and Formal-Method Assurance
Parent standard	AF 9500 - Aerospace Digital Systems, Software & Cybersecurity
Edition / language	FIRST EDITION / English master text
Family	Procedures
Primary source anchors	14; Annex F
Suggested local owner	Procedure owner identified in execution table
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 Keep superseded evidence and decisions traceable.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 Purpose, trigger and inputs

A tool, model, solver, generator or service is introduced or changed.

Required inputs: Intended use, possible errors, consequence and independent detection.

Use the complete parent requirements at 14; Annex F. Assign an eligible owner to each step; retain the actual baseline and time of each significant action.

2 Controlled execution

Step / responsible role	Required action	Retained output
1 / Tool owner	Define exact intended use, version, options and error consequences.	Tool assurance assessment
2 / Validation lead	Exercise representative and adverse cases with known outcomes.	Validation evidence
3 / Model reviewer	Assess abstractions, assumptions and implementation relationships.	Model/proof scope argument
4 / Technical authority	Approve bounded use and change or fallback conditions.	Tool-use decision

Decision control: A vendor claim or formal result cannot establish properties outside its demonstrated assumptions and use.

2.1 Exceptions and escalation

Preserve the observed condition, affected object, evidence and decision state. Refer a deviation or anomaly to its eligible technical authority. Record why a departure is acceptable, what remains blocked and whether readiness, qualification, acceptance or release must be reconsidered.

3 Closure and handoff

A controlled tool/model baseline with valid evidence and historical interpretability.

The receiving owner verifies the outputs. Open items retain an owner, due basis and blocked scope; a due date does not authorize closure.

3.1 Working records

AF-FR-9500-010, AF-RG-9500-006, AF-CL-9500-009, AF-TP-9500-010. Consult AF-ML-9500-001 for titles and locations. Reopen affected steps when configuration, conditions, evidence validity or delegated authority changes. Verify the actual technical handoff during assurance review.