DO-333 Formal Methods Supplement Compliance

Overview

This document describes how the STUNIR DO-333 tools support compliance with DO-333 (Formal Methods Supplement to DO-178C).

DO-333 Objectives Matrix

FM.1: Formal Specification

ID	Requirement	Implementation	Evidence
FM.1.1	Define formal specifications	`formal_spec.ads` - Formal_Expression, Contract_Spec types	Unit tests
FM.1.2	Pre/postconditions	`spec_parser.ads` - Parse Pre/Post aspects	Parser tests
FM.1.3	Invariants	Invariant, Loop_Invariant, Type_Invariant support	Parser tests
FM.1.4	Ghost code	Ghost_Variable type, ghost detection	Parser tests
FM.1.5	Proof functions	Proof_Function type	Unit tests

FM.2: Formal Verification (Proofs)

ID	Requirement	Implementation	Evidence
FM.2.1	Mathematical proofs	GNATprove integration	SPARK proofs
FM.2.2	Multiple provers	Prover_Kind (Z3, CVC4, Alt-Ergo, CVC5)	Integration tests
FM.2.3	Proof strategies	Discharge_Strategy type	Unit tests
FM.2.4	Manual proofs	Manual_Proof_Record type	Evidence generator

FM.3: Proof Coverage

ID	Requirement	Implementation	Evidence
FM.3.1	PO coverage metrics	Coverage_Metrics type	Coverage reports
FM.3.2	VC coverage	VC_Coverage_Report type	Coverage reports
FM.3.3	Unproven analysis	Unproven_Analysis type	Analysis reports
FM.3.4	Coverage percentage	Coverage_Percentage function	Reports

FM.4: Verification Condition Management

ID	Requirement	Implementation	Evidence
FM.4.1	VC generation	GNATprove_Wrapper - Parse_VC_Results	Integration
FM.4.2	VC tracking	VC_Collection, VC_Tracker	Unit tests
FM.4.3	Complexity analysis	Complexity_Analysis type	Reports
FM.4.4	Status monitoring	VC_Status, Update_Status	Unit tests

FM.5: Formal Methods Integration

ID	Requirement	Implementation	Evidence
FM.5.1	Tool integration	SPARK_Integration package	GNATprove wrapper
FM.5.2	Configuration	SPARK_Config type	Config management
FM.5.3	DO-331 integration	Works with SysML 2.0 SPARK	Integration tests
FM.5.4	DO-332 integration	Works with OOP SPARK	Integration tests

FM.6: Certification Evidence

ID	Requirement	Implementation	Evidence
FM.6.1	PO reports	Generate_PO_Report	Report generation
FM.6.2	VC reports	Generate_VC_Report	Report generation
FM.6.3	Coverage reports	Gener-ate_Coverage_Report	Report generation
FM.6.4	Compliance matrix	Gener-ate_Compliance_Matrix	This document
FM.6.5	Justification	Gener-ate_Justification_Template	Evidence generator

Tool Qualification

Classification

Per DO-330, these tools are classified as:
- **TQL-5**: Development tools whose output is not part of airborne software

Rationale

The DO-333 tools:
1. Generate reports and analysis
2. Do not produce airborne software code
3. Provide certification evidence

Qualification Data

Artifact	Location
Tool Operational Requirements	This document
Software Requirements	HLI_DO333_IMPLEMENTATION.md
Test Cases	tests/*.adb
Test Results	SPARK proof reports

Self-Verification

All DO-333 tools are:

1. **Written in SPARK Ada** with `SPARK_Mode (On)`
2. **Formally verified** using GNATprove
3. **Guaranteed exception-free** via SPARK contracts
4. **Flow analysis clean** - no data flow issues

Evidence Generation

Report Types

Report	Purpose	Format
PO Report	List all proof obligations	Text, JSON, HTML
VC Report	List all verification conditions	Text, JSON, HTML
Coverage Report	Show verification coverage	Text, JSON
Compliance Matrix	Map to DO-333 objectives	Text, JSON
Justification Template	Document unproven VCs	Text

Sample Evidence


```
{
  "report_type": "compliance_matrix",
  "objectives": [
    {"id": "FM.1", "status": "Compliant"},
    {"id": "FM.2", "status": "Compliant"},
    {"id": "FM.3", "status": "Compliant"},
    {"id": "FM.4", "status": "Compliant"},
    {"id": "FM.5", "status": "Compliant"},
    {"id": "FM.6", "status": "Compliant"}
  ],
  "generated": "2026-01-29",
  "tool_version": "DO333 v1.0.0"
}
```


Integration with Certification

Plan for Software Aspects of Certification (PSAC)

The PSAC should reference:
- DO-333 as applicable supplement
- This compliance document
- Generated evidence artifacts

Software Verification Plan (SVP)

The SVP should describe:
- Formal verification approach
- SPARK tool usage
- Coverage criteria

Software Verification Results (SVR)

The SVR should include:
- PO reports
- VC reports
- Coverage reports
- Unproven VC justifications

Conclusion

The STUNIR DO-333 tools provide comprehensive support for formal methods verification per DO-333, including:

- ✅ Formal specification support (FM.1)
- ✅ Formal verification via SPARK (FM.2)
- ✅ Proof coverage analysis (FM.3)
- ✅ VC management (FM.4)
- ✅ Tool integration (FM.5)
- ✅ Certification evidence (FM.6)