STUNIR DO-333 Formal Methods User Guide

Introduction

The DO-333 Formal Methods Support provides tools for formal verification of avionics software, supporting certification under DO-178C with DO-333 Formal Methods Supplement credit.

Quick Start

Prerequisites

1. GNAT Ada Compiler (2020+)
2. SPARK Pro with GNATprove
3. Set environment variable: `export STUNIR_ENABLE_COMPLIANCE=1`

Building

```
cd tools/do333
make build      # Build tools
make prove      # Run SPARK proofs
make test       # Run all tests
```

Running

```
# Show help
./bin/do333_analyzer --help

# Run demo
./bin/do333_analyzer demo
```

Formal Specification

Supported Contract Types

Type	SPARK Syntax	Description
Precondition	`with Pre => ...`	Entry requirements
Postcondition	`with Post => ...`	Exit guarantees
Invariant	`with Invariant => ...`	Maintained property
Loop Invariant	`pragma Loop_Invariant (...)`	Loop property
Type Invariant	`with Type_Invariant => ...`	Type property
Ghost	`with Ghost`	Specification-only

Example

```
procedure Update_Altitude (Target : Altitude_Type)
  with Pre  => Target in 0 .. Max_Altitude,
       Post => Current_Altitude = Target;
```

Proof Obligation Management

PO Categories

- **Precondition**: Entry conditions
- **Postcondition**: Exit conditions
- **Range_Check**: Value range validity
- **Overflow_Check**: Arithmetic overflow
- **Loop_Invariant_Init**: Loop entry
- **Loop_Invariant_Preserv**: Loop iteration

PO Status

Status	Description
Proved	Automatically verified
Unproved	Requires attention
Timeout	Prover timeout
Manually_Justified	Accepted via review

Criticality Levels (DAL)

Level	Description	Action
DAL-A	Catastrophic	Must prove
DAL-B	Hazardous	Must prove
DAL-C	Major	Should prove
DAL-D	Minor	May prove
DAL-E	No Effect	Optional

Verification Conditions

Complexity Analysis

Category	Steps	Typical Time
Trivial	<10	<1s
Simple	10-100	1-5s
Medium	100-1000	5-30s
Complex	1000-10000	30s-5m
Very Complex	>10000	>5m

Manual Proofs

For VCs that cannot be automatically discharged:

1. Document justification
2. Perform code review
3. Optionally add tests
4. Get reviewer approval

SPARK Integration

Proof Modes

```
# Flow analysis only
gnatprove -P project.gpr --mode=flow

# Proofs only
gnatprove -P project.gpr --mode=prove

# Both (recommended)
gnatprove -P project.gpr --mode=all
```

Prover Selection

Supported provers:
- **Z3**: Fast, good for arithmetic
- **CVC4/CVC5**: Good for complex types
- **Alt-Ergo**: Good for floating point
- **All**: Try all provers (recommended)

Configuration

```
--  In .gpr file
package Prove is
   for Proof_Switches ("Ada") use (
      "--level=2",        -- Effort level (0-4)
      "--timeout=60",     -- Per-VC timeout
      "--prover=all",     -- Use all provers
      "--steps=10000"     -- Max proof steps
   );
end Prove;
```

Report Generation

Available Reports

1. **PO Report**: Proof obligation summary
2. **VC Report**: Verification condition details
3. **Coverage Report**: Combined coverage
4. **Compliance Matrix**: DO-333 objectives
5. **Justification Template**: Unproven VC form

Formats

- Text (`.txt`)
- JSON (`.json`)
- HTML (`.html`)
- XML (`.xml`)
- CSV (`.csv`)

Generating Reports

```
./bin/do333_analyzer report text
./bin/do333_analyzer report json
./bin/do333_analyzer report html
```

DO-333 Compliance

Objectives Coverage

Objective	Description	Status
FM.1	Formal Specification	✅
FM.2	Formal Verification	✅
FM.3	Proof Coverage	✅
FM.4	VC Management	✅
FM.5	FM Integration	✅
FM.6	Certification Evidence	✅

Troubleshooting

Common Issues

GNATprove not found

```
# Install SPARK Pro or community edition
which gnatprove
```

Proof timeout

```
# Increase timeout and steps
gnatprove -P project.gpr --timeout=120 --steps=50000
```

Complex VC not discharging

1. Add ghost code/lemmas
2. Simplify expressions
3. Use manual proof if necessary

Support

For issues, contact the STUNIR project team or consult the SPARK documentation.