RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington, D.C. 20036

Formal Methods Supplement to DO-178C and DO-278A

RTCA DO-333
December 13, 2011

Prepared by: SC-205
© 2011 RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc.

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This report was prepared by RTCA Special Committee 205 (SC-205) and EUROCAE Working Group 71 (WG-71) and approved by the RTCA Program Management Committee (PMC) on December 13, 2011.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Federal Advisory Committee and develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;

- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity, and efficiency;

- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders.

Since the RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

This Page Intentionally Left Blank

TABLE OF CONTENTS

FM.1.0 INTRODUCTION 1
FM.1.1 PURPOSE 2
FM.1.2 SCOPE 2
FM.1.3 RELATIONSHIP TO OTHER DOCUMENTS 2
FM.1.4 HOW TO USE THIS DOCUMENT 2
FM.1.5 DOCUMENT OVERVIEW 3
FM.1.6 CHARACTERISTICS OF FORMAL METHODS 3
FM.1.6.1 Formal Models 3
FM.1.6.2 Formal Analysis 4
FM.1.7 FORMAL METHODS AS A VERIFICATION TECHNIQUE 5

FM.2.0 SYSTEM ASPECTS RELATING TO SOFTWARE DEVELOPMENT 7

FM.3.0 SOFTWARE LIFE CYCLE 9

FM.4.0 SOFTWARE PLANNING PROCESS 11
FM.4.3 SOFTWARE PLANS 11

FM.5.0 SOFTWARE DEVELOPMENT PROCESSES 13

FM.6.0 SOFTWARE VERIFICATION PROCESS 15
FM.6.1 PURPOSE OF SOFTWARE VERIFICATION 15
FM.6.2 OVERVIEW OF SOFTWARE VERIFICATION PROCESS ACTIVITIES 17
FM.6.2.1 Considerations for Formal Methods 17
FM.6.3 SOFTWARE REVIEWS AND ANALYSES 17
FM.6.3.1 Reviews and Analyses of High-Level Requirements 18
FM.6.3.2 Reviews and Analyses of Low-Level Requirements 19
FM.6.3.3 Reviews and Analyses of Software Architecture 20
FM.6.3.4 Reviews and Analyses of Source Code 21
FM.6.3.5 Reviews and Analyses of the Outputs of the Integration Process 22
FM.6.3.6 Reviews and Analyses of the Formal Analysis Cases, Procedures, and Results for Requirements, Architecture, and Source Code 22
FM.6.4 SOFTWARE TESTING 22
FM.6.5 SOFTWARE VERIFICATION PROCESS TRACEABILITY 23
FM.6.6 VERIFICATION OF PARAMETER DATA ITEMS 23
FM.6.7 FORMAL ANALYSIS OF THE EXECUTABLE OBJECT CODE 23
FM.6.7.1 Principles of Coverage Analysis When Using Formal Methods 28
FM.6.7.2 Reviews and Analyses of the Formal Analysis Cases, Procedures, and Results for the Executable Object Code 30

FM.7.0 SOFTWARE CONFIGURATION MANAGEMENT PROCESS 33

FM.8.0 SOFTWARE QUALITY ASSURANCE PROCESS 35

FM.9.0 CERTIFICATION LIAISON PROCESS 37

FM.10.0 OVERVIEW OF CERTIFICATION PROCESS 39

FM.11.0 SOFTWARE LIFE CYCLE DATA 41

© 2011 RTCA, Inc.

FM.11.1 PLAN FOR SOFTWARE ASPECTS OF CERTIFICATION 41
FM.11.3 SOFTWARE VERIFICATION PLAN 41
FM.11.6 SOFTWARE REQUIREMENTS STANDARDS 41
FM.11.7 SOFTWARE DESIGN STANDARDS 42
FM.11.8 SOFTWARE CODE STANDARDS 42
FM.11.13 SOFTWARE VERIFICATION CASES AND PROCEDURES 42

FM.12.0 ADDITIONAL CONSIDERATIONS 43
FM.12.3.5 Coverage Analysis When Using a Combination of Formal Methods and Testing 43

ANNEX FM.A – PROCESS OBJECTIVES AND OUTPUTS BY SOFTWARE LEVEL IN DO-178C 45

ANNEX FM.B ACRONYMS AND GLOSSARY OF TERMS 57

ANNEX FM.C PROCESS OBJECTIVES AND OUTPUTS BY ASSURANCE LEVEL IN DO-278A 59

APPENDIX FM.A COMMITEE MEMBERSHIP A-1

APPENDIX FM.B FREQUENTLY ASKED QUESTIONS AND DISCUSSION PAPERS B-1

© 2011 RTCA, Inc.

LIST OF FIGURES

FIGURE FM.6-1 LEVEL A SOFTWARE VERIFICATION PROCESSES 16
FIGURE FM.6-2 POSSIBLE VERIFICATION PATHS FOR EXECUTABLE OBJECT CODE WITH RESPECT TO SOURCE CODE AND REQUIREMENTS 28
FIGURE FM.B.1-1 SOFTWARE LIFE CYCLE FOR UNIT PROOF B-8
FIGURE FM.B.1-2 PROOF PROCESS B-13
FIGURE FM.B.1-3 OVERVIEW OF REQUIREMENT ARTIFACTS B-19
FIGURE FM.B.1-4 SIMPLIFIED DISPLAY SYSTEM ARCHITECTURE B-20
FIGURE FM.B.1-5 WINDOW MANAGER TOP LEVEL SOFTWARE MODEL B-24
FIGURE FM.B.1-6 ANALYSIS PROCESS B-25

LIST OF TABLES

TABLE FM.A-1 SOFTWARE PLANNING PROCESS 46
TABLE FM.A-2 SOFTWARE DEVELOPMENT PROCESSES 47
TABLE FM.A-3 VERIFICATION OF OUTPUTS OF SOFTWARE REQUIREMENTS PROCESS 48
TABLE FM.A-4 VERIFICATION OF OUTPUTS OF SOFTWARE DESIGN PROCESS 49
TABLE FM.A-5 VERIFICATION OF OUTPUTS OF SOFTWARE CODING & INTEGRATION PROCESSES 50
TABLE FM.A-6 TESTING OF OUTPUTS OF INTEGRATION PROCESS 51
TABLE FM.A-7 VERIFICATION OF VERIFICATION PROCESS RESULTS 52
TABLE FM.A-8 SOFTWARE CONFIGURATION MANAGEMENT PROCESS 53
TABLE FM.A-9 SOFTWARE QUALITY ASSURANCE PROCESS 54
TABLE FM.A-10 CERTIFICATION LIAISON PROCESS 55
TABLE FM.C-1 SOFTWARE PLANNING PROCESS 60
TABLE FM.C-2 SOFTWARE DEVELOPMENT PROCESSES 61
TABLE FM.C-3 VERIFICATION OF OUTPUTS OF SOFTWARE REQUIREMENTS PROCESS 62
TABLE FM.C-4 VERIFICATION OF OUTPUTS OF SOFTWARE DESIGN PROCESS 63
TABLE FM.C-5 VERIFICATION OF OUTPUTS OF SOFTWARE CODING & INTEGRATION PROCESSES 64
TABLE FM.C-6 TESTING OF OUTPUTS OF INTEGRATION PROCESS 65
TABLE FM.C-7 VERIFICATION OF VERIFICATION PROCESS RESULTS 66
TABLE FM.C-8 SOFTWARE CONFIGURATION MANAGEMENT PROCESS 67
TABLE FM.C-9 SOFTWARE QUALITY ASSURANCE PROCESS 68
TABLE FM.C-10 SOFTWARE APPROVAL PROCESS 69
TABLE FM.B.1-1 REDUNDANCY MANAGEMENT SOFTWARE VERIFICATION RESULTS ... B-7
TABLE FM.B.1-2 WINDOW MANAGER REQUIREMENTS FORMALIZED IN CTL B-23
TABLE FM.B.1-3 WINDOW MANAGER ANALYSIS DATA B-26

© 2011 RTCA, Inc.

This Page Intentionally Left Blank

FM.1.0 INTRODUCTION

Formal methods are mathematically based techniques for the specification, development, and verification of software aspects of digital systems. The mathematical basis of formal methods consists of formal logic, discrete mathematics, and computer-readable languages. The use of formal methods is motivated by the expectation that, as in other engineering disciplines, performing appropriate mathematical analyses can contribute to establishing the correctness and robustness of a design. For example, formal methods, because of their mathematical basis, are capable of:

- Unambiguously describing requirements of software systems.
- Enabling precise communication between engineers.
- Providing verification evidence such as consistency and accuracy of a formally specified representation of software.
- Providing verification evidence of the compliance of one formally specified representation with another.

Formal methods are also capable of demonstrating properties of software systems such as:

- Freedom from exceptions.
- Freedom from deadlock.
- Non-interference between different levels of criticality.
- Worst case execution time.
- Bounds on stack size during execution.
- Freedom from unintended function.
- Correct synchronous or asynchronous behavior.

Since the publication of DO-178B, advances and experience have been gained in formal methods, their application, and tools. This supplement provides guidance for applicants and certification or approval authorities to facilitate the use of formal methods.

The adoption of formal methods into an established set of processes for development and verification can be an evolutionary refinement rather than an abrupt change of methodology. The extent to which formal methods are used to satisfy the objectives of DO-178C can vary according to aspects such as preferences of the program management, choice of techniques, and availability of specialized resources. Formal methods might be used in a very selective manner to partially address a small set of objectives, or might be the primary source of evidence for the satisfaction of many of the objectives concerned with development and verification.

© 2011 RTCA, Inc.

FM.1.1 Purpose

This supplement identifies the modifications and additions to DO-178C objectives, activities, explanatory text, and software life cycle data that should be addressed when formal methods are used as part of the software life cycle. This includes the artifacts that would be expressed using some formal notation and the verification evidence that could be derived from them.

FM.1.2 Scope

This supplement discusses the use of formal methods in the software life cycle for software that is produced in accordance with DO-178C. If the applicant is not planning to use formal analysis as defined in FM.1.6, then the applicant does not need to comply with this supplement.

FM.1.3 Relationship to Other Documents

This document supplements the guidance given in DO-178C and DO-278A. This document may be used in conjunction with any DO-178C-related supplements or other documents.

FM.1.4 How to Use This Document

This supplement should be used with and in the same way as DO-178C; however, the following should be noted:

- Section FM.1 contains explanatory text to aid the reader in understanding formal methods, and therefore is not to be taken as guidance.

- Annex FM.A of this supplement describes how the DO-178C objectives are revised in line with this formal methods guidance.

- Guidance from DO-178C should be used for all aspects of the software life cycle, apart from where formal methods are used. All guidance specific to formal methods is contained within this supplement.

- This supplement can be applied to DO-278A in the same manner as DO-178C. Applicants complying with DO-278A should be aware that the text within this supplement is based on DO-178C; thus, the DO-278A applicant needs to ensure that the proper DO-278A guidance is addressed. Annex FM.B of this supplement describes how the DO-278A, Annex A objectives are revised in line with the formal methods guidance in this supplement.

- In addition to the guidance contained in this supplement, a Discussion Paper is provided to clarify the guidance (see Appendix FM.B). The Discussion Paper contains no new or additional guidance.

- Major sections are numbered as FM.X.0 throughout this supplement. It should be noted that references to an entire section are identified as “section FM.X”; whereas, references to the content between section headers FM.X.0 and FM.X.1 are referred to as “section FM.X.0”.

© 2011 RTCA, Inc.