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

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

currently in preview, click buy full versi

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.

currently in preview, click buy full versi

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.

currently in preview, click buy full versi

This Page Intentionally Left Blank

currently in preview, click buy full versi

TABLE OF CONTENTS

© 2011 RTCA, Inc.

currently in preview. click buy full versi

currently in preview, click buy full versi

© 2011 RTCA, Inc.

LIST OF FIGURES

LIST OF TABLES

Currently in preview. click buy full versi

© 2011 RTCA, Inc.

This Page Intentionally Left Blank

currently in preview, click buy full versi

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.

currently in preview, click buy full versi

© 2011 RTCA, Inc.