FAS Topic Paper (FTP)

TITLE	REVISION	REVISION DATE
FTP1037 Formal Methods Objectives for Executable Object Code	1	03-Dec-2020

ABSTRACT/PURPOSE:

This FTP describes the use of Formal Methods to claim credit for Executable Object Code (EOC) against DO-333/ED-216 Annex FM.A Table FM.A-6 and Table FM.A-7 Objectives (and Annex FM.C Table FM.C-6 and Table FM.C-7 Objectives).

RELATED DO/ED DOCUMENTS:

____ DO-178C/ED-12C: SW Airborne Sys & Equip
____ DO-278A/ED-109A:SW (CNS/ATM) Systems
____ DO-248C/ED-94C: Supporting Information
____ DO-330/ED-215: Software Tool Qualification Considerations
____ DO-331/ED-218: Model Based Development & Verification Supplement
____ DO-332/ED-217: OO Technology and Related Techniques Supplement
_**X**__ DO-333/ED-216: Formal Methods Supplement
____ Other

For internal use only—This paper is based on internal FAS FTP1037 Revision 10

Any FAS Topic Papers released by FAS have been coordinated among the members of the FAS group and have been approved by the FAS executive management committee for release.

These papers do not constitute official policy or position from RTCA / EUROCAE or any regulatory agency or authority. These documents are made available for educational and informational purposes only

The present document was jointly developed by the EUROCAE / RTCA User Group ‘Forum for Aeronautical Software’ (FAS) and as such remains the exclusive intellectual property of EUROCAE and RTCA.

In order to maximize the use of the document and the information contained, the material may be used without prior written permission in an unaltered form with proper acknowledgement of the source.

FAS Team Definition and Goals:

The FAS user group monitors and exchanges information on the application of the following "software document suite" that was developed by joint RTCA/EUROCAE committee SC-205/WG-71:

- DO-178C/ED-12C - Software Considerations in Airborne Systems and Equipment Certification
- DO-278A/ED-109A - Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems
- DO-248C/ED-94C - Supporting Information
- DO-330/ED-215 - Software Tool Qualification Considerations
- DO-331/ ED-218 - Model Based Development & Verification Supplement
- DO-332/ED-217 - Object Oriented Technology and Related Techniques Supplement
- DO-333/ ED-216 - Formal Methods Supplement

The goals of the FAS user group are as follows:

1. To share lessons learned in the use of the RTCA/EUROCAE "software document suite" and to encourage good practices and promote the effective use of RTCA's and EUROCAE's publications.
2. To develop FAS Topics Papers (FTPs) relative to RTCA's and EUROCAE's publications or other related aeronautical software industry topics. These FTPs may include clarification to the "software document suite" or a discussion on a new topic.
3. To identify and record any issues or errata showing the need for clarifications or the need for modifications to the "software document suite".

The FAS user group does not have the authority to change the content of any approved RTCA/EUROCAE documents. Any publications of the FAS user group may be taken into consideration by a future RTCA/EUROCAE working group.

The text contained in this document is not to be construed as guidance, but is to be used for informational or educational purposes only.

Abstract / Purpose of the FAS Topic Paper:

This FTP describes the use of Formal Methods to claim credit for Executable Object Code (EOC) against DO-333/ED-216 Annex FM.A Table FM.A-6 and Table FM.A-7 Objectives (and Annex FM.C Table FM.C-6 and Table FM.C-7 Objectives).

FTP Discussion:

Question from Industry:

Within DO-333/ED-216, why are there additional objectives required for verification of the Formal Methods usage in every Annex FM.A table/Annex FM.C table where Formal Methods can be used (i.e., FM.A-3, FM.A-4, FM.A-5, FM.C-3, FM.C-4, and FM.C-5) but not for Annex Table FM.A-6/Table FM.C-6?

Response from FAS:

The use of Formal Methods to verify EOC does not change the objectives on the verification of the EOC which are described in Annex Table FM.A-6/Table FM.C-6 of DO-333/ED-216. But the use of Formal Methods to verify the EOC has an impact on Annex Table FM.A-7/Table FM.C-7 of DO-333/ED-216 which applies to the verification of the verification process results.

As with DO-178C/ED-12C and DO-278A/ED-109A where the Objectives of Annex Table A-7 apply to the artifacts and activities related to Annex Table A-6, the Objectives of Annex Table FM.A-7/FM.C-7 of DO-333/ED-216 apply to the artifacts and activities related to Annex Table FM.A-6/Table FM.C-6. Therefore, DO-333/ED-216 Objective FM-10 within Annex Table FM.A-7/Table FM.C-7 applies when the EOC is verified using Formal Methods versus the high-level requirements and/or low-level requirements.

The text contained in this document is not to be construed as guidance, but is to be used for informational or educational purposes only.