FAS Topic Paper (FTP)

TITLE	REVISION	REVISION DATE
FTP1053 Use of Supplements Clarifications	3	03-Dec-2020

ABSTRACT/PURPOSE:

This paper provides clarification on the use and assurance of Unmanned Aircraft System (UAS) products and systems with respect to the guidance in the supplements.

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
_**X**__ DO-331/ED-218: Model Based Development & Verification Supplement
_**X**__ 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 FTP1053 Revision 6

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.

Due to the amount of referenced text from published documents contained within this paper, this material may only be used with prior written permission from RTCA and EUROCAE.

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.

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 paper provides clarification on the use and assurance of Unmanned Aircraft System (UAS) products and systems with respect to the guidance in the supplements.

FTP Discussion:

The UAS community has expressed concerns related to the use of supplements listed below when developing software used in both air and ground segments of UAS:

- 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 UAS community should use the already published DO-248C/ED-94C, Section 5.13 that outlines the rationale for the supplements and provides an outline of each supplement. Additionally, the guidance material found in Federal Aviation Administration (FAA) Advisory Circular (AC) 20-115D and European Union Aviation Safety Agency (EASA)'s Acceptable Means of Compliance (AMC) 20-115D, Section 8.a, provides scope and clarification of the supplements.

The tailoring of the DO-178C/ED-12C and DO-278A/ED-109A objectives and the associated supplement objective for UAS is based on safety assessments as outlined in Section 2 of DO-178C/ED-12C and DO-278A/ED-109A.

The supplements should not be seen as an additional burden, but instead, they allow certification/approval credit to be taken for the use of techniques such as Model-based Development and Verification, Formal Methods, and/or Object-Oriented Technology.

The use of various constraints in the UAS development processes can allow the applicant to minimize the perceived burdens of the supplements. The supplements, just like the core documents DO-178C/ED-12C and DO-278A/ED-109A, contain many options for the developer, some of which are more technically challenging and thus necessitating greater oversight and scrutiny.

UAS developers can choose to avoid supplement processes that involve significant rationalization and proof. Examples include the use of formal model analysis as a replacement for testing, the use of multiple inheritances in an object-orient design, or the use of simulation to replace executable object code verification for model-based design. While the supplements are applicable to the extent indicated in the DO-178C/ED-12C and DO-278A/ED-109A Annex Tables and FAA AC 20-115D or EASA AMC 20-115D, the developer can chose among many methods to simplify their compliance.

The key for the UAS applicant is to select a development approach and then work with the certification authority to tailor their activities to maximize the benefits of the core document and the technology supplements. The UAS development approach should align with the developer's

experience-base, and align with the business objectives required to meet the safety guidelines and the product specifications.

The following are excerpts taken from DO-248C and ED-94C. The text in each document is technically identical except for the respective document name and references. This text is copyrighted by RTCA, Inc. and EUROCAE, and used with permission. The complete RTCA document and EUROCAE document referenced may be obtained from:

RTCA, Inc.
1150 18th Street NW
Suite 910
Washington, DC 20036
+1 (202) 833-9339
www.rtca.org

EUROCAE
9-23 rue Paul Lafargue
"Le Triangle" building
93200 Saint-Denis
France
www.eurocae.net/contact/

RTCA Document References:

The following text is an excerpt from DO-248C Subsection 5.13:

> "5.13 Rationale for TOOL QUALIFICATION DOCUMENT AND DO-178C/DO-278A SUPPLEMENTS
>
> Supplements were implemented to provide guidelines for technology advances in software engineering. When these technologies are used, it was not always clear how the objectives of the core DO-178C/DO-278A document are mapped to the terminology and approach used by a specific technology. Each Supplement adds, modifies, or deletes the DO-178C/DO-278A objectives to make the guidance more clear."

The following text is an excerpt from DO-248C Paragraph 5.13.2:

> "5.13.2 Rationale for "FORMAL METHODS SUPPLEMENT TO DO-178C AND DO-278A"
>
> Formal methods are mathematically based techniques for the specification, development, and verification of computer systems. The use of formal methods is motivated by the fact that performing rigorous mathematical analyses can contribute to establishing the correctness and robustness of software aspects of safety-critical systems. Such techniques are also highly applicable to complex hardware development assurance. The formal logic, discrete mathematics, and computer-readable languages underpinning formal methods, provide a solid and

defensible foundation for many of the development and verification activities required for avionics software. Nonetheless, the avionics industry at large has been hesitant to adopt formal methods, despite growing evidence of their benefits.

Since the introduction of formal methods as an alternative method in section 12.3.1 of DO-178B, advances and practical experience have been gained in techniques and tools supporting formal methods, to the extent that they have become sufficiently mature for application on today's avionics products. The Formal Methods Supplement was authorized, consequently, to provide guidance for applicants and certification/approval authorities to facilitate the use of formal methods. The supplement is based on the following key principles:

- A formal method is the application of a formal analysis to a formal model.
- A formal model must be in a notation with mathematically defined syntax and semantics.
- Formal methods may be used at different verification steps in the software life cycle, for all or part of a step and for all or part of the system being developed.
- A formal method must never produce a result which may not be true (that is, the formal analysis must be sound).
- It is possible to apply the results of formal analysis of Source Code to the corresponding object code by understanding the compilation, link, and load processes in sufficient detail.
- Test is always required to ensure compatibility of the software with target hardware and to fully verify the understanding of the relationship between source and object code."

The following text is an excerpt from DO-248C Paragraph 5.13.3:

"5.13.3 Rationale for "OBJECT-ORIENTED TECHNOLOGY AND RELATED TECHNIQUES SUPPLEMENT TO DO-178C AND DO-278A"

Object-oriented technologies (OOT) have been widely adopted in non-critical software development projects. The use of these technologies for critical software applications in avionics has increased, but a number of issues need to be considered to ensure the safety and integrity goals are met.

These issues are directly related to language features and to complications encountered with meeting well-established safety objectives. There are a number of additional language features that are part of OOT that need to be considered as well. Clarifying each issue will ease the application of object-oriented technology and related techniques (OOT&RT).

The OOT&RT Supplement was authorized, consequently, to provide guidance for applicants and certification/approval authorities to facilitate the use of OOT in the development process. The supplement addresses both object-oriented technology and related techniques and includes the following key elements:

- Basic concepts of OOT include classes and objects, types and type safety, hierarchical encapsulation, polymorphism, function passing and closures, and method dispatch.
- Related techniques include parametric polymorphism, overloading, type conversion, exception management, dynamic memory management, virtualization, and component-based development.
- Key features include inheritance, parametric polymorphism, overloading, type conversion, software exceptions and exception handling, and dynamic memory management.
- An annex is included to assist in vulnerability analysis for OOT&RT.
- Frequently asked questions are included in an appendix."

The following text is an excerpt from DO-248C Paragraph 5.13.4:

"5.13.4 Rationale for "MODEL-BASED DEVELOPMENT AND VERIFICATION SUPPLEMENT TO DO-178C AND DO-278A"

Model-based development and verification technology involves methods and techniques to represent requirements in the form of a model, typically a graphical model, to facilitate the development and/or verification of software. The model-based techniques are rarely, if ever, used as the sole means to develop or verify software since model-based techniques may not be the optimum choice for all requirements.

The use of model-based development and verification technology in safety-critical airborne applications pre-dates DO-178B and no special guidance was included in DO-178B to address the use of models. As tools and techniques have evolved with the use of models, auto-code generation, simulation, and test automation, there has not been a consistent understanding and application of how the DO-178B (and hence, DO-278) objectives mapped to the systems and software aspects of model-based requirements and associated verification activity.

The Model-based Development and Verification Supplement was authorized, consequently, to provide guidance for applicants and certification/approval authorities to facilitate the use of models in the development and verification processes. The supplement is based on the following key principles:

- Models can represent high-level and/or low-level requirements.
- More than one type of model may be used within a development or verification process."

EUROCAE Document References:

The following text is an excerpt from ED-94C Subsection 5.13:

> "5.13 Rationale for TOOL QUALIFICATION DOCUMENT AND ED-12C/ED-109A SUPPLEMENTS
>
> Supplements were implemented to provide guidelines for technology advances in software engineering. When these technologies are used, it was not always clear how the objectives of the core ED-12C/ED-109A document are mapped to the terminology and approach used by a specific technology. Each Supplement adds, modifies, or deletes the ED-12C/ED-109A objectives to make the guidance more clear."

The following text is an excerpt from ED-94C Paragraph 5.13.2:

> "5.13.2 Rationale for "FORMAL METHODS SUPPLEMENT TO ED-12C and ED-109A"
>
> Formal methods are mathematically based techniques for the specification, development, and verification of computer systems. The use of formal methods is motivated by the fact that performing rigorous mathematical analyses can contribute to establishing the correctness and robustness of software aspects of safety-critical systems. Such techniques are also highly applicable to complex hardware development assurance. The formal logic, discrete mathematics, and computer-readable languages underpinning formal methods, provide a solid and defensible foundation for many of the development and verification activities required for avionics software. Nonetheless, the avionics industry at large has been hesitant to adopt formal methods, despite growing evidence of their benefits.
>
> Since the introduction of formal methods as an alternative method in section 12.3.1 of ED-12B, advances and practical experience have been gained in techniques and tools supporting formal methods, to the extent that they have become sufficiently mature for application on today's avionics products. The Formal Methods Supplement was authorized, consequently, to provide guidance for applicants and

certification/approval authorities to facilitate the use of formal methods. The supplement is based on the following key principles:

- A formal method is the application of a formal analysis to a formal model.
- A formal model must be in a notation with mathematically defined syntax and semantics.
- Formal methods may be used at different verification steps in the software life cycle, for all or part of a step and for all or part of the system being developed.
- A formal method must never produce a result which may not be true (that is, the formal analysis must be sound).
- It is possible to apply the results of formal analysis of Source Code to the corresponding object code by understanding the compilation, link, and load processes in sufficient detail.
- Test is always required to ensure compatibility of the software with target hardware and to fully verify the understanding of the relationship between source and object code."

The following text is an excerpt from ED-94C Paragraph 5.13.3:

> "5.13.3 Rationale for "OBJECT-ORIENTED TECHNOLOGY AND RELATED TECHNIQUES SUPPLEMENT TO ED-12C AND ED-109A"
>
> Object-oriented technologies (OOT) have been widely adopted in non-critical software development projects. The use of these technologies for critical software applications in avionics has increased, but a number of issues need to be considered to ensure the safety and integrity goals are met.
>
> These issues are directly related to language features and to complications encountered with meeting well-established safety objectives. There are a number of additional language features that are part of OOT that need to be considered as well. Clarifying each issue will ease the application of object-oriented technology and related techniques (OOT&RT).
>
> The OOT&RT Supplement was authorized, consequently, to provide guidance for applicants and certification/approval authorities to facilitate the use of OOT in the development process. The supplement addresses both object-oriented technology and related techniques and includes the following key elements:
>
> - Basic concepts of OOT include classes and objects, types and type safety, hierarchical encapsulation, polymorphism, function passing and closures, and method dispatch.

- Related techniques include parametric polymorphism, overloading, type conversion, exception management, dynamic memory management, virtualization, and component-based development.
- Key features include inheritance, parametric polymorphism, overloading, type conversion, software exceptions and exception handling, and dynamic memory management.
- An annex is included to assist in vulnerability analysis for OOT&RT.
- Frequently asked questions are included in an appendix."

The following text is an excerpt from ED-94C Paragraph 5.13.4:

> "5.13.4 Rationale for "MODEL-BASED DEVELOPMENT AND VERIFICATION SUPPLEMENT TO ED-12C AND ED-109A"
>
> Model-based development and verification technology involves methods and techniques to represent requirements in the form of a model, typically a graphical model, to facilitate the development and/or verification of software. The model-based techniques are rarely, if ever, used as the sole means to develop or verify software since model-based techniques may not be the optimum choice for all requirements.
>
> The use of model-based development and verification technology in safety-critical airborne applications pre-dates ED-12B and no special guidance was included in ED-12B to address the use of models. As tools and techniques have evolved with the use of models, auto-code generation, simulation, and test automation, there has not been a consistent understanding and application of how the ED-12B (and hence, ED-109) objectives mapped to the systems and software aspects of model-based requirements and associated verification activity.
>
> The Model-based Development and Verification Supplement was authorized, consequently, to provide guidance for applicants and certification/approval authorities to facilitate the use of models in the development and verification processes. The supplement is based on the following key principles:
>
> - Models can represent high-level and/or low-level requirements.
> - More than one type of model may be used within a development or verification process."