FAS Topic Paper (FTP)

TITLE	REVISION	REVISION DATE
FTP1054 Operating Systems Clarifications	1	03-Dec-2020

ABSTRACT/PURPOSE:

Industry has asked for clarification related to the impacts of DO-178C/ED-12C and DO-278A/ED-109A on the choice of Operating Systems (OS)s used in Unmanned Aircraft Systems (UAS)s.

RELATED DO/ED DOCUMENTS:

_**X**__ DO-178C/ED-12C: SW Airborne Sys & Equip
_**X**__ 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
____ DO-333/ED-216: Formal Methods Supplement
____ Other

For internal use only—This paper is based on internal FAS FTP1054 Revision 7

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

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:

Industry has asked for clarification related to the impacts of DO-178C/ED-12C and DO-278A/ED-109A on the choice of Operating Systems (OS)s used in Unmanned Aircraft Systems (UAS)s.

FTP Discussion:

The UAS community has expressed concerns related to the impacts of DO-178C/ED-12C and DO-278A/ED-109A on the choice of OSs used in both air and ground segments of UASs. Note that this paper uses OS where the content is relevant to both a Real-Time Operating System (RTOS) and non-RTOS.

RTOSs and more generally OSs, by their nature are tightly coupled to the applications executing on them. This implies that with the exception of some secondary functions (e.g., data loading) the opportunity for partitioning and a reduction in DO-178C/ED-12C software level or DO-278A/ED-109A assurance level does not exist. This means an OS needs to be assigned the same or higher software/assurance level as applications that use them.

In addition, there may be system requirements that preclude the use of some OSs or OS capabilities such as more complex scheduling, memory management, and communications.

With due consideration for the constraints discussed above, many OSs can be used in a DO-178C/ED-12C (and/or DO-278A/ED-109A) context at any level if the appropriate requirements capture, verification and assurance are undertaken. This means that the OS is required to satisfy the objectives of DO-178C/ED-12C (and/or DO-278A/ED-109A) as well as any additional OS-specific requirements, such as requirements for deterministic scheduling. Note that other safety-related industry standards such as IEC 61508 and ISO 26262 treat OSs in exactly the same way as DO-178C/ED-12C (and/or DO-278A/ED-109A), and the OS has to comply with the standard, just like any other software. There are commercial organizations that can provide an implementation of an OS together with certification evidence that demonstrates compliance with a standard, including DO-178C/ED-12C (and/or DO-278A/ED-109A). It is possible for the UAS industry to use OSs approved for other safety-critical standards. However the acquisition of an OS with a certification package comes at a price.

DO-178C/ED-12C and DO-278A/ED-109A discusses the use of alternate means of compliance, such as reverse engineering or service history, to gain confidence in any software or any software subset. This is applicable to Commercial-Off-The-Shelf (COTS) and Open Source OSs, while not always possible.

- It is possible to use reverse engineering techniques to provide the required compliance artifacts and assurance. This is discussed in brief in DO-178C/ED-12C and DO-278A/ED-109A Paragraph 12.1.4. With the exception of DO-178C/ED-12C software level D and DO-278A/ED-109A assurance level 5, experience has shown that reverse engineering requires access to any available design data, the OS Source Code, as well as

access to the OS development and/or maintenance organization. DOT/FAA/TC-15/27 provides useful information concerning reverse engineering.

- In some cases it may be possible to construct a Service History argument for an OS. DO-178C/ED-12C Paragraph 12.3.4 provides guidance for use of product Service History in airborne software and DO-278A/ED-109A Paragraph 12.3.4 provides guidance for CNS/ATM non-airborne software (ground and space). In practice Service History arguments are difficult to construct due to the difficulty in retrospectively compiling the necessary evidence and analyses. It may be possible to use a Service History argument combined with other assurance methods, such as additional testing.

If the software is DO-178C/ED-12C software level D or DO-278A/ED-109A assurance level 5, then there is additional latitude in the use of OSs. What is required is to verify the correct operation of the application software against the requirements. Any suitable OS could therefore be used at DO-178C/ED-12C software level D or DO-278A/ED-109A assurance level 5, provided it satisfied the requirements of the applications supported. For example, the OS must ensure that deadlines are met.

For configuration management activities, OS configuration control must be exercised in accordance with DO-178C/ED-12C for software levels A through D and DO-278A/ED-109A assurance levels 1-5. Any changes to the OS, such as OS service pack updates must be analyzed for impact to the software previously accepted. This means changes to OSs cannot be automatically pushed into the fleet until the impact is assessed, re-verification and lifecycle data updates are accomplished and the software is re-approved/re-accepted (see DO-178C/ED-12C and DO-278A/ED-109A Subsection 12.1).

It is important that the chosen COTS OS includes vendor support for identification, analysis, and communication of issues and errata. This errata needs to be reviewed and mitigated during development and integration of the product using the OS, as well as throughout the service life of the product. The rigor the COTS OS vendor exercises in change control is typically undefined, so review and assessment of errata cannot be the sole means of understanding errant or undefined behavior of the OS. Thorough verification of the application integrated with the target OS must be performed including hardware/software integration and verification of robust behavior (see DO-178C/ED-12C Paragraphs 12.1.4 and 12.3.4; as well as DO-278A/ED-109A Paragraphs 12.1.4, 12.3.4, and 12.4). These principles apply to Open Source OSs as well.

For CNS/ATM non-airborne software developed under DO-278A/ED-109A, the OSs are treated similarly to airborne software. However, DO-278A/ED-109A discusses more considerations on the use of COTS software in DO-278A/ED-109A Subsection 12.4, which includes the development of a COTS software integrity assurance case, gap analysis and additional testing. In the end, compliance to DO-278A/ED-109A should be achieved for both the non-COTS software and any OSs that have been used.