Certification Authorities Software Team (CAST)

Position Paper CAST-31

Technical Clarifications Identified for RTCA DO-254 / EUROCAE ED-80

COMPLETED December 2012

(Rev 4)

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, Europe, and Asia. However, it does not constitute official policy or guidance from any of the authorities. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

Technical Clarifications Identified for RTCA DO-254 / EUROCAE ED-80

1.0 Introduction

This CAST paper identifies technical clarifications; including errors, omissions, obsolescence and other required clarifications, needed for RTCA document DO-254 and EUROCAE document ED-80. Examples of obsolescence items include references to Joint Aviation Regulations (JARs). Omissions include topics such as firmware and commercial-off-the-shelf (COTS) intellectual property (IP). EASA has published policy memorandum "Development Assurance of Airborne Electronic Hardware (AEH)", which provides guidance on specific issues that are either not addressed by ED-80 / DO-254 or are in need of some additional discussion and clarification. The EASA AEH policy memorandum provides a list of specific issues related to ED-80 / DO-254 in section 2 of their document.

The development of other documents in support of ED-80 / DO-254 (e.g., advisory circulars, FAA orders, EASA certification memorandum, and other certification policy such as issue papers and certification review items (CRI)), indicates that additional information for the development assurance of airborne electronic hardware is required.

2.0 References and Related Documents: Policy, Guidance and Standards

A. SAE ARP 4754a / EUROCAE ED 79a, Guidelines for Development of Civil Aircraft and Systems
B. AC 20-174, Development of Civil Aircraft and Systems
C. SAE ARP 4761 / EUROCAE ED 135, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
D. RTCA DO-178B / EUROCAE ED 12B, Software Considerations in Airborne Systems and Equipment Certification
E. RTCA DO-178C / EUROCAE ED 12C, Software Considerations in Airborne Systems and Equipment Certification
F. AC 20-115B – Radio Technical Commission for Aeronautic, Inc. Document RTCA/DO-178B
G. AC 21-16G - RTCA Document DO-160 versions D, E and F / EUROCAE ED-14 versions D, E and F, Environmental Conditions and Test Procedures for Airborne Equipment
H. RTCA DO-254 / EUROCAE ED-80, Design Assurance Guidance for AEH
I. Advisory Circular (AC) 20-152 / RTCA DO-254, Design Assurance Guidance for AEH

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, Europe, and Asia. However, <u>it does not constitute official policy or guidance from any of the authorities</u>. This document is provided for educational and informational purposes only and should be discussed with the appropriate certification authority when considering for actual projects.**

J. Order 8110.105 Change 1, Simple and Complex Electronic Hardware Approval Guidance
K. TSO template standard (Requires update to address DO-254 Scope and Applicability)
L. Issue Papers for certain AEH related projects
M. EASA CS-ETSO Amendment 7, Certification Specifications, including Airworthiness Codes and Acceptable Means of Compliance, for European Technical Standard Orders (« CS-ETSO »), July 5, 2012
N. EASA Certification Memorandum, EASA CM - SWCEH - 001 Issue 01, Revision 01 "Development Assurance of Airborne Electronic Hardware" dated March 09, 2012

3.0 Background

DO-254/ED-80 was published on April 19, 2000. The guidance in the document is applicable, but not limited to, the following hardware items:

A. Line Replaceable Units (LRUs)
B. Circuit Board Assemblies
C. Custom micro-coded components, such as Application Specific Integrated Circuits (ASICs) and Programmable Logic Devices (PLDs) including any associated macro functions
D. Integrated technology components, such as hybrids and multi-chip modules
E. Commercial Off-The-Shelf (COTS) components

4.0 Description of Concern

Technical clarifications required for RTCA document DO-254 and EUROCAE document ED-80 include:

A. Errors (Revision to DO-254/ED-80 required)
    1. Inconsistent definitions of "complex". Document should contain one standard definition for complex (refer to Transport Standard Staff (TSS) Issue Paper template Section 9)
    2. Change the term Design Assurance to Development Assurance
    3. Change the term Design Assurance Level to Item Development Assurance Level (IDAL)

B. Omissions
   1. Address COTS intellectual property (IP) (refer to FAA Order 8110.105, Section 4-9 and EASA CM - SWCEH – 001 Section 8.4.4)
   2. Add definition of "Tool" to Glossary
   3. Address modifiable devices (refer to TSS Issue Paper template Section 1, field-loadable hardware components), and modifiable Custom Micro-Coded Components (refer to FAA Order 8110.105, Section 4-2 and EASA CM - SWCEH – 001 Section 8.6.1)
   4. Address additional planning – PHAC (refer to TSS Issue Paper template Section 3 and FAA Order 8110.105, Section 4-3)
   5. Address Configuration Management issues, define Hardware Life Cycle Environment Configuration Index (refer to TSS Issue Paper template Section 7 and FAA Order 8110.105, Section 4-5 and EASA CM - SWCEH – 001 Section 8.4.5)
   6. Address Item Development Assurance Level (IDAL), and Function Design Assurance Level (FDAL) as described in SAE ARP 4754A and EUROCAE ED-79A
   7. Address tool assessment and qualification, tool service history, tool reuse (refer to TSS Issue Paper template Section 8, and FAA Order 8110.105, Section 4-6 and EASA CM - SWCEH – 001 Section 8.6.2) and the following item regarding tool qualification
      a. Should Tool Qualification be allowed for Levels A and B design tools?
      b. Should tools that are used to assess completion of verification testing for Levels A and B be allowed without baseline and problem reporting (box 6) basic tool qualification (box 7) (Figure 11-1)?
      c. Reassess full Figure 11-1 and section on Tool Qualification. Baseline and problem reporting (box 6) should be required for all tools irrespective of whether they are qualified. Or when is tool qualification required, e.g., DO-254 objectives are eliminated, reduced, or automated as DO-178/ED-12B states?
      d. Consider CEH Tool Qualification R&D Report for potential topics, issues, concerns
      e. Review DO-330/ED-215 "Software Tool Qualification Considerations" for implications on DO-254/ED-80
   8. Address Legacy Systems and changes to hardware components, including change impact analysis and regression testing (refer to TSS Issue Paper

template section 10 and FAA Order 8110.105, Section 4-7 and EASA CM - SWCEH – 001 section 12)

9. Address hardware data submittals for simple electronic hardware for verification including; PHAC, HVP, HAS, HCI; and traceability (refer to FAA Order 8110.105, Section 5, 5-1, 5-2, 5-3 and to EASA CM - SWCEH – 001 Section 8.5.1)
10. Address applicability to COTS microprocessors (refer to TSS Issue Paper template, Section 11) and EASA CM 001 Section 9 and 10
11. Address RAM-based FPGAs (refer to TSS Issue Paper template, Section 12)
12. Address single event effects (SEE) analysis and mitigation (refer to EASA CM - SWCEH – 001 Section 6)
13. Address simulation environment versus testing on the actual device
14. Address supplier management (refer to EASA CM - SWCEH – 001 Section 11)
15. Address partition integrity (refer to EASA CM 001 Section 9.3.9)
16. Address circuit board assemblies and equipment (refer to EASA CM - SWCEH – 001 Section 7)
17. Address hardware of varying complexity:
    a. Extremely simple hardware
    b. Simple, complex, highly complex hardware (refer to EASA CM 001 Section 9.3.11, 9.3.12, 9.3.13)
18. Add definitions to Glossary of relevant terms, e.g., IC, Intellectual Property, microcontroller, etc. (refer to EASA CM 001 Section 1.4)
19. Address mitigations for unused functions in FPGA (Refer to EASA CM 001 section 10.3 item f.)
20. Address the COTS Graphical Processors (refer to CAST-29 and EASA CM - SWCEH – 001 Section 10)
21. Address the COTS multi-core processors
22. Address a guideline for simple / complex / highly complex COTS components (refer to EASA CM - SWCEH – 001 Section 9)
23. Address precise criteria when assessing the simplicity / complexity of a device (refer to EASA CM - SWCEH – 001 Section 8.3)
24. Address the validation of all the requirements (refer to EASA CM - SWCEH – 001 Section 8.4.1)
25. Address the Hardware Conformity Review (refer to EASA CM - SWCEH – 001 Section 8.4.6)
26. Address the activities to be performed on the Simple Electronic Hardware (refer to EASA CM - SWCEH – 001 Section 8.5)
27. Address the management of Problem Reports (refer to EASA CM - SWCEH – 001 Section 8.5)

C. Obsolescence Items (Revision to DO-254/ED-80 required)
   1. References exist to Joint Aviation Regulations (JARs) should be revised to include Certification Specifications (CS), Acceptable Means of Compliance (AMC)
   2. References to SAE ARP 4754 / EUROCAE ED-79 should be revised to include new version ARP 4754a / ED79a
   3. References to DO-178B/ED-12B should be revised to include new version DO-178C / ED-12C and any relevant ED-12C / DO-178C supplement if necessary

D. Other required clarifications
   1. Define "independent assessment" for Tool Qualification and define minimum requirements for simulation, hardware testing, random testing, etc.
   2. Add coverage requirements (statement, condition (if/then/else), Finite State Machine (FSM), and others as deemed applicable
   3. Add explicit reference to robustness testing
   4. Clarify "validation" and "verification" (refer to IP, Section 4 and 5)
   5. Clarify Hardware Design Languages (HDL, VHDL) usage (refer to FAA Order 8110.105, Section 6-2a. and RTCA DO-254 Users Group Best Practice VHDL Coding Standards for DO-254 Programs)
   6. Clarify "testing", test reviews and coverage analysis expectations (refer to Order 8110.105, Section 6-2)
   7. Clarify traceability expectations for levels A, B, C and D (refer to IP, Section 6 and FAA Order 8110.105, Section 6.3)
   8. Clarify required product service experience (Refer to EASA CM 001 Section 9.3.7)
   9. Clarify additional verification methods for level A versus level B (DO-254 / ED-80 Appendix B)
   10. Clarify simple versus complex
   11. Consider revising Annex A table to use the same structure and format (e.g. objective number, objective description, objective reference paragraph, applicability by assurance level, output data item, output data item reference paragraph, hardware control category by assurance level) as DO-178C/ED-12C and ARP-4754A/ED-79A
   12. Consider outputs from AVSI AFE#75
   13. Consider inputs from the MCFA (Multi-Core For Avionics) Group
   14. Consider input from DO-254 User's Group

15. Implement consistency with DO-178C / ED-12C and ARP-4754a / ED-79A regarding design and development assurance
16. Review FAA Order 8110.105 for additional topics
17. Review EASA Cert Memo for additional topics
18. Consider whether radiation testing should be specifically identified in AC 21-16G / DO-160. Is radiation testing being required for hardware items in DO-160? If not, should it be identified in DO-254?
19. Consider definition differences for "Independence" between DO-254 / ED-80 and DO-178 / ED12, and determine if they need to be made consistent.
20. Review EASA Cert Memo on AEH for differences between FAA and EASA approaches and topics
21. Review ABV-Elemental Analysis Paper (S. Beland) for topic consideration
22. Clarify that transition criteria are required
23. Address conformity reviews and conformity inspections both for parts and installations
24. Address continued operational issues, (e.g., maintenance requirements and obsolescence issues, in service problems)
25. Define the term "element"
26. Clarify the term "acceptance test criteria"
27. Address management of deferred (open) problem reports (refer to EASA CM 001 Section 13)
28. Clarify the Top-Level-Drawing (refer to CAST-28 and to EASA CM - SWCEH – 001 Section 8.4.5)
29. Clarify whether analog components / items are in the scope of ED80 / DO-254
30. Clarify the verification objectives at design description and implementation levels (refer to EASA CM - SWCEH – 001 Section 8.4.2)
31. Clarify the "note 6" from table A-1 for DAL / IDAL C (refer to EASA CM - SWCEH – 001 Section 8.4.3)

5.0 Summary

This paper identifies technical clarifications; including errors, omissions, additions, obsolescence items, and other required clarifications, needed for RTCA document DO-254 and EUROCAE document ED-80.