Certification Authorities Software Team (CAST)

Position Paper CAST-27

CLARIFICATIONS ON THE USE OF RTCA DOCUMENT DO-254 AND EUROCAE DOCUMENT ED-80, *DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE*

COMPLETED June 2006

(Rev 0)

NOTE: **This position paper has been coordinated among representatives from certification authorities in North and South America, and Europe. 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.**

Clarifications on the use of RTCA Document DO-254 and EUROCAE Document ED-80, Design Assurance Guidance for Airborne Electronic Hardware

1. Purpose

Some civil aviation authorities have recognized RTCA document DO-254 and EUROCAE document ED-80 (hereafter referred to in this paper as DO-254/ED-80), *Design Assurance Guidance for Airborne Electronic Hardware* [Ref. a.], as an acceptable means of compliance for satisfying the relevant regulations for custom micro-coded components or devices (such as, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) and Programmable Logic Devices (PLDs)) contained in airborne systems and equipment installed on civil aircraft. This CAST paper provides clarification on some commonly misunderstood areas of DO-254/ED-80 and provides a vehicle for harmonization among the international certification authorities.

2. Background

a. Custom micro-coded devices are often just as complex as software controlled microprocessor-based systems; hence a structured design approach is needed to satisfy applicable functional and safety-related requirements, and to ensure an appropriate level of design assurance for these devices. DO-254/ED-80 provides such an approach; however, there are some areas that need clarification. The following areas are clarified in this paper:

(1) Modifiable devices (see Section 4 below).
(2) Device level assurance (see Section 5 below).
(3) Certification plan (see Section 6 below).
(4) Validation processes (see Section 7 below).
(5) Verification processes (see Section 8 below).
(6) Traceability (see Section 9 below).
(7) Configuration management (see Section 10 below).
(8) Tool assessment and qualification (see Section 11 below).
(9) Commercial Off-the Shelf (COTS) Intellectual Property (see Section 12 below).

.

3. References

a. RTCA/DO-254 (EUROCAE ED-80), *Design Assurance Guidance For Airborne Electronic Hardware*;

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

b. RTCA/DO-178B (EUROCAE ED-12B), *Software Considerations in Airborne Systems and Equipment Certification*;
c. FAA AC 20-152, *RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance For Airborne Electronic Hardware;*
d. FAA Order 8110.49, *Software Approval Guidelines*;
e. FAA Order 8110.4, *Type Certification*;
f. SAE ARP 4754/EUROCAE ED-79, *Certification Considerations for Highly-Integrated or Complex Aircraft Systems.*

Related References

- RTCA/DO-160E (EUROCAE ED-14), *Environmental Conditions and Test Procedures for Airborne Equipment;*
- SAE ARP 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems*;
- FAA Advisory Circular 23.1309-1, *Equipment, Systems, and Installations in Part 23 Airplanes;*
- FAA Advisory Circular 25.1309-1, *System Design and Analysis;*
- FAA Advisory Circular 27-1, *Certification of Normal Category Rotorcraft;*
- FAA Advisory Circular 29-2, *Certification of Transport Category Rotorcraft;*
- FAA Advisory Circular 33.28-1, *Compliance Criteria for 14 CFR §33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems;*
- FAA Advisory Circular 33.28-2, *Guidance Material for 14 CFR §33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems.*

4. Modifiable Devices

a. DO-254/ED-80 does not explicitly address the modifiable aspects of electronic hardware where a part or the entirety of the embedded logic can be changed at any time from an external source without modification of the device hardware, as it may be the case with custom micro-coded devices. Section 1.2 of DO-254/ED-80 explains that the document does not attempt to define firmware, and that the assumption is made that functions have been allocated either to hardware or to software. The area of field-loadable logic/software and on-board modifiable components (e.g., user modifiable logic/software) are not explicitly addressed in DO-254/ED-80.

b. When logic embedded in custom micro-coded devices is modified in the field, in addition to the DO-254/ED-80 guidance material for the hardware, the applicant should apply the guidance of DO-178B/ED-12B (Sections 2.4 and 2.5) [Ref. b.] concerning user-modifiable software,

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

option-selectable software, and field-loadable software as applicable. Additionally, Chapters 5, 6, and 7 of FAA Order 8110.49, *Software Approval Guidelines*, [Ref. d.] should be considered.

5. Design Assurance at the Device Level

a. In this paper, the use of the term "design assurance" should be considered in the context of the "design process" as defined in DO-254/ED-80. These two terms are defined in DO-254/ED-80 as the following:

> "Design Assurance – All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the hardware satisfies the application certification basis."
>
> "Design Process – The process of creating a hardware item from a set of requirements using the following set of processes: requirements capture, conceptual design, detailed design, implementation and product transition."

b. The definition of "hardware item" in DO-254/ED-80 explains that this can be a Line Replaceable Unit (LRU), a circuit board assembly, or a component. Section 5 of DO-254/ED-80 states that design processes may be applied at any hierarchical level of the hardware item, such as LRU, circuit board assembly, or device level. However, similar to FAA Advisory Circular (AC) 20-152 [ref. c.] this CAST paper specifically addresses custom micro-coded devices, such as ASICs and PLDs, rather than LRUs and circuit board assemblies.

c. Therefore, the objectives and guidelines of DO-254/ED-80, together with the clarification of this CAST paper, will provide the needed guidelines to be satisfied at the device level for those custom micro-coded devices classified in accordance with Table 2-1 of DO-254/ED-80. Additionally, Table 5-1 in DO-254/ED-80 indicates how the processes described in the document translate to activities at the device level.

d. There may be some cases where an acceptable level of design assurance for a custom micro-coded device can be obtained by verification and/or architectural strategies at the system or equipment level; however, such design assurance approaches should be agreed-to with the cognizant

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

certification authority early in the project and should be documented in the system certification plan [Ref. f., Section 4.4.1] or Plan for Hardware Aspects of Certification [Ref. a., Section 10.1.1] for electronic devices and in the same manner as other alternative means of compliance or alternative methods.

6. Certification Plan

DO-254/ED-80 specifies the Plan for Hardware Aspects of Certification (PHAC), which is described in Section 10.1.1 of the document. The PHAC addresses the processes and activities for a particular system containing electronic hardware devices. However, when an aircraft or equipment implements multiple systems with software and hardware components, there is a need for a higher-level certification plan that describes the overall development, integration, and compliance approach. Section 2-3.d of FAA Order 8110.4 [Ref. e], *Type Certification*, states: "All TC applicants are required to submit a certification plan to the FAA and to keep it current throughout the project." ARP 4754 [Ref. f.] Section 4.4 states that the certification plan is part of the minimum certification data to be submitted to the certification authority. The plan should be submitted early in the project and updated as necessary throughout the project. Order 8110.4 and ARP 4754 Section 4.4.1 describe the typical contents of a certification plan. Such a plan is essential to determine the level of certification authority involvement, to reduce risk of misunderstandings, to ensure that the design assurance activities are appropriate and support the system safety assessment, and to agree on any alternative methods proposed by the applicant.

a. The plans for electronic hardware can be packaged in a number of ways, including: (i) each electronic hardware component could have its own stand-alone document (PHAC) to support reuse in multiple systems, (ii) all electronic hardware components of a system could be combined in a stand-alone PHAC to support maintenance and changes to that system's electronic hardware, or (iii) the PHAC content could be combined with other planning data for the aircraft or system (e.g., system certification plan). The system certification plan should address custom micro-coded devices (perhaps by reference to the applicable PHAC(s)), as well as their integration with software and other hardware components of the system. In addition to the specified information for a PHAC listed in DO-254/ED-80 Section 10.1.1, the system certification plan or PHAC for all electronic hardware components should include:

(1) Each custom micro-coded device should be listed, along with its failure condition classification and a description of its function

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

(2) The proposed means of compliance for each device (e.g., DO-254/ED-80 and/or DO-178B/ED-12B) should be stated.
(3) The proposed design assurance level of the device and justification for the level should be provided.
(4) Hardware design standards appropriate to the device should be referenced.
(5) Certification data to be delivered and/or available to the certification authority should be listed.
(6) If alternative methods to those described in DO-254/ED-80 are proposed, the applicant should explain their interpretation of the basic objectives and guidelines, describe the alternative methods, and present to the certification authority early in the project, their justification of compliance to the applicable regulations.
(7) If reverse engineering of a device is proposed, the applicant should present and justify to the certification authority the strategy to be used.

7. Validation Processes

Section 6.1 of DO-254/ED-80 addresses validation. SAE ARP 4754, *Certification Considerations for Highly-Integrated or Complex Aircraft System*, [Ref. f.] addresses both verification and validation of aircraft systems. Aircraft systems should have a consistent combination of validation and verification activities to ensure that the aircraft-level requirements are translated correctly into system requirements, and further down into requirements for the electronic devices. The validation activities should address the specification of the devices, the safety-related requirements, and the derived requirements, as further explained in DO-254/ED-80 Sections 5.1, 6.1 and 6.3, and Appendix A. The following items clarify the DO-254/ED-80 validation activities:

a. The hardware requirements and design specification, safety-related requirements and derived requirements should be identified and validated. Validation of requirements may be satisfied by review, analysis, simulation, testing, or a combination of these methods. Completion of the validation processes should be based on defined criteria.

NOTE: Derived requirements for memory address assignments need to be validated particularly when associated with partitioning and other protection concepts for integrated modular avionics (IMA) architectures.

b. The validation processes should be documented as specified by the hardware design assurance level and control category as defined in DO-254/ED-80 Appendix A.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

c. For Levels A and B, the validation processes should be satisfied with independence, independence being defined in Appendix C and further discussed in Appendix A and Table A-1 of DO-254/ED-80.

8. Verification Processes

DO-254/ED-80 Section 6.2 addresses verification, and Section 6.3 addresses in more detail the verification methods. There are a number of specific device-level verification areas clarified below:

a. Hardware Description Language (HDL) Clarification: HDLs, as defined in DO-254/ED-80 Appendix C, have attributes similar to software programming languages. DO-254/ED-80 does not explicitly address these aspects. Therefore, clarification is needed to ensure that potential unsafe aspects of HDLs will not lead to unsafe features of the devices. If an HDL is used, then coding standards for this language consistent with the system safety objectives should be defined, and conformance to those standards should be established by HDL code reviews. These reviews should also include assessment of the HDL (detailed design) with respect to the requirements for completeness, correctness, consistency, verifiability and traceability.

NOTE: For Levels C and D, only the traceability data from requirements to test is needed (see Note 6 of Table A-1 of DO-254/ED-80).

b. Testing Clarification: Testing is described in DO-254/ED-80 Section 6.3.1 as a method that confirms that the hardware item correctly responds to a stimulus or series of stimuli. Robustness testing is not explicitly addressed in DO-254/ED-80; however, the note in Section 5.1.2(4) calls for safety-related derived requirements to address abnormal (worst case) and boundary conditions with respect to input data range, state machines, power-supply and electrical signals. Therefore, to be consistent with derived requirement capture process activities and verification process activities mentioned in Sections 5.1.2(4) and 6.2.2(4) of DO-254/ED-80, both normal and abnormal operating conditions should be captured as derived requirements and addressed in the tests. That is, to demonstrate robustness, requirements-based testing should be defined to cover normal and abnormal operating conditions. Where necessary and appropriate, additional verification activities, such as analysis and review, may have to be performed to address robustness aspects.

c. Test Case and Procedure Review Clarification: Test cases and procedures should be reviewed to confirm they are appropriate for the

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

requirements to which they trace (see Section 6.2.2(4b) of DO-254/ED-80).

d. Verification Completion Criteria Clarification: Consistent with verification Objectives 1 and 2 in DO-254/ED-80 Section 6.2.1, Section 6.2.2 (4) specifies a verification coverage analysis to determine that the verification process is complete, that is, each requirement has been verified appropriately and discrepancies between expected and actual results are explained, especially with respect to safety-related requirements. DO-254/ED-80 Section 6.3.1 specifies that when testing of the hardware item is not feasible, other verification means should be provided and justified. Therefore, the PHAC and/or hardware verification plan should state and justify the intended level of verification coverage of the requirements achieved by test. The following guidelines should be addressed:

(1) The level of verification coverage of the requirements achieved by test on the device itself should be measured and recorded.
(2) Inability to verify specific requirements by test should be justified, and alternate verification means provided and justified.

In addition to complete verification coverage of the requirements, DO-254/ED-80 Section 2.3.4 also specifies that advanced design assurance strategies described in Appendix B be applied for Levels A and B functions. However, DO-254/ED-80 does not explicitly identify completion criteria for these advanced design assurance activities; Appendix B discusses the use of Elemental Analysis, which may be applied to determine completion criteria. Regardless of the approach, the completion criteria of design assurance methods for Level A and B functions should be documented in the PHAC. In particular, for devices that are Design Assurance Levels A or B the following guidelines should be addressed:

(3) A target level of verification coverage of the internal structure of the design implementation using verification procedures that achieve the verification objectives of DO-254/ED-80 Section 6.2 should be defined and justified.
(4) Inability to generate correct and acceptable assurance data showing complete coverage of the internal structure of the design implementation should be justified, and additional advanced design assurance methods should be used to provide mitigation of potential hardware failures and anomalous behaviors.
(5) Verification processes should be satisfied with independence as discussed in DO-254/ED-80 Appendix A and Table A-1.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

e. Partitioning (separation or isolation of functions or circuits) within the device may not be assumed. Partition integrity should be demonstrated, verified, and documented, if partitioning is used to justify a combination of different design assurance levels within a device.

9. Traceability

Multiple sections in DO-254/ED-80 address traceability (e.g., 5.1.1, 5.1.2, 6.1, 6.1.2, 6.3.2, 6.3.3, and 10.4.1). Two areas need clarification for Levels A and B:

a. Traceability between the system requirements, the conceptual design (e.g., high level architecture and detailed functional description), the detailed design (e.g., HDL), and the implementation (e.g., functional elements appropriate for design assurance level), should be ensured.

b. Traceability between the requirements and design items of 9.a above, and the corresponding verification and validation activities, should be ensured.

NOTE: For Levels C and D, only the traceability data from requirements to test is needed (see Note 6 of Table A-1 of DO-254/ED-80).

10. Configuration Management

a. DO-254/ED-80 Section 7.0 provides guidance on configuration management and problem reporting. For complex electronic devices, documented change control and problem reporting should be implemented early in the project when the process of configuration identification as defined in DO-254/ED-80 commences. Implementation of change control and problem reporting may need to precede the baseline from which certification credit is claimed.

b. Although DO-254/ED-80 does not explicitly specify a hardware configuration index (HCI), other documented design assurance guidance such as ARP 4754 Section 4.4.2, and DO-178B Sections 9.3 and 11.16 specify either a system or software configuration index to be submitted to the certification authorities. DO-254/ED-80 Section 10.3.2.2.1 does specify submission to the certification authorities a top-level drawing that uniquely identifies the hardware item and relevant documentation that defines the hardware item; however, it is not clear if a top-level drawing will include configuration information to completely identify the configuration of the hardware and the embedded logic for a specific custom micro-coded device. Therefore, appropriate configuration

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

documentation either in the top-level drawing or a HCI should be submitted to the certification authorities to completely identify the configuration of the hardware and the embedded logic.

c. Furthermore, a hardware life cycle environment configuration index (HECI), which identifies the configuration of the hardware life cycle environment for the hardware and embedded logic, should be available for review by the certification authorities. Similar to the software life cycle environment configuration index as described in DO-178B Section 11.15, the HECI is written to aid reproduction of the hardware and embedded logic life cycle environment, embedded logic regeneration, reverification, or embedded logic modification.

11. Tool Assessment and Qualification

a. Section 11.4 of DO-254/ED-80 provides guidance on tool assessment and qualification. Figure 11.1 is sometimes incorrectly interpreted to indicate that if there is relevant tool service history (Box 5), no further qualification activities are needed. However, DO-254/ED-80 Section 11.4.1(5) explains that data should be available to substantiate the relevance and credibility of the tool's service history. That is, it should be shown that the service history proves that the tool produces acceptable results and the previous tool usage is relevant to the proposed tool usage.

b. A claim for credit of relevant tool history, as discussed in DO-254/ED-80 Section 11.4.1(5), should be justified to the certification authority early in the project and documented in the appropriate certification plan/PHAC.

12. Commercial Off-the Shelf (COTS) Intellectual Property (IP)

Although some civil aviation authorities have recognized DO-254/ED-80 as an acceptable means for design assurance of custom micro-coded components, they have not recognized DO-254/ED-80 as an acceptable means for Commercial Off-the Shelf (COTS) components. Per DO-254/ED80, a COTS component is defined as the following with the corresponding note:

> "Component, integrated circuit or subsystem developed by a supplier for multiple customers, whose design and configuration is controlled by the supplier's or industry specification.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**

> ***Note:*** *Examples of COTS components include resistors, capacitors, microprocessors, unprogrammed Field Programmable Gate Array (FPGA) and Erasable Programmable Logic Devices (EPLD, PLD), other integrated circuit types and their implementable models, printed wiring assemblies and complete LRUs which are typically available as a catalogue item.*"

In this paper, COTS components are limited to COTS Intellectual Property (IP). A COTS IP is defined as commercially available functional logic blocks used to design and implement part or complete custom micro-coded components such as PLDs, FPGAs, or similar programmable devices. A COTS IP may be provided with or without the custom micro-coded component device.

a. Since the use of a COTS IP can greatly impact the performance and functionality of a custom micro-coded component, the rigor of the development processes for a COTS IP implemented in a custom micro-coded device for use in airborne systems or equipment should be commensurate with its intended use and should satisfy applicable functional and safety-related requirements.

b. Moreover, the guidance in section 11.2 of DO-254/ED-80 may not be sufficient for design assurance of a COTS IP implemented in a custom micro-coded device that support safety critical applications such as Level A or B aircraft functions. As a result, life cycle data (i.e., verification, testing, and analysis) of a COTS IP may need to be developed or augmented to demonstrate its intended function, satisfy applicable regulations, and meet airworthiness requirements.

13. Certification Authorities Software Team (CAST) Position

The applicant and certification authority should ensure that the clarifications to the objectives and guidelines of RTCA/DO-254 (EUROCAE/ED-80) provided in this paper are addressed when custom micro-coded devices are implemented in systems and equipment installed on civil aircraft. CAST recognizes the need to continue clarifying and addressing other and emerging technical issues when using DO-254/ED-80. The intent is to provide future CAST papers to address other issues with design assurance of airborne electronic hardware as needed.

NOTE: **This position paper has been coordinated among representatives of certification authorities from North and South America, and Europe. 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.**