FAA Order 8110.105

“Simple And Complex Electronic Hardware Approval Guidance”

Presented to: FAA Software and Airborne Electronic Hardware Conference, Denver

By: Gregg Bartley
FAA, ANM-111/AIR-120

Date: August 20/21, 2008
Why is this Order necessary?

- To assist FAA personnel in their determination of how much the FAA should be involved in any specific project involving compliance to DO-254.
- To cover specific details of the approval of ASIC’s, PLD’s and FPGA’s not covered or not covered in great detail in RTCA DO-254.
- To harmonize with non-U.S. certification authorities, specifically EASA.
- To cover approval of:
  - Simple Electronic Hardware devices.
  - Devices programmed with COTS Intellectual Properties.
What this Order does/does not do.

• This order DOES:
  – Provide guidance on projects when the method of compliance for airborne electronic hardware is agreed to be RTCA/DO-254.
  • Can be thought of as a companion to AC 20-152.
  – Show FAA personnel where attention to detail is required.

• This order DOES NOT mandate:
  – RTCA/DO-254 be used as the sole method of compliance.
  – The specific methodology contained in the order in order to show compliance to DO-254, including Simple Electronic Hardware devices.

• Other acceptable methods may be negotiated (e.g., issue papers) between FAA ACO and applicant.
Is Order 8110.105 a complete surprise?

• It should not be.
  – Much of the basic information contained in this Order contained in Chapters 4, 5 and 6 has been used in project specific Issue Papers being generated from the Transport Airplane Directorate for a number of years.
    • Boeing 787
    • Embraer E-170/190
    • Gulfstream G450/G550
    • Hawker 4000
    • Cessna Citation 560
    • Dassault Falcon 900/2000 EASy
    • Etc.
  – The other FAA Directorates have also been using various versions of this Issue Paper for their projects.
Order 8110.105 Table of Contents

• Chapter 1: Introduction
• Chapter 2: SEH/CEH Review Process
• Chapter 3: Determining FAA Involvement
• Chapter 4: Clarification of Topics Applicable to both SEH and CEH
• Chapter 5: Clarification of Topics Applicable only to SEH
• Chapter 6: Clarification of Topics Applicable only to CEH
• Appendix A: Administrative Information
• Appendix B: Acronyms
Chapter 1: Introduction/Purpose of Order

• Explains how FAA certification staff can use and apply RTCA, Inc. document RTCA/DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, when working on certification projects.

• Gives guidance for approving both *simple* and *complex* custom micro-coded components.
Chapter 1: Introduction/Purpose of Order

- Order 8110.105 *accepts* and *supplements* DO-254 as the means by which an applicant seeks FAA approval for both simple and complex custom micro-coded components.

- If an applicant proposes a means other than DO-254, we may need to develop more guidance (e.g. Issue Papers) on a project-by-project basis.
Chapter 1: Introduction/Key Terms

• A Hardware Item can be a Line Replaceable Units (LRU), a circuit board assembly, or a component.

• DO-254, section 5, states that design processes may be applied at any hierarchical level of the LRU, circuit board assembly, or component.

• Components include commercial off the shelf (COTS) components, integrated technology components like hybrid and multi-chip modules, and custom micro-coded components.

-- Source: RTCA/DO-254
Chapter 1: Introduction/Key Terms

• **Simple Hardware Item**: Item with a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level that ensures correct functional performance under all foreseeable operating conditions, with no anomalous behavior.

  --Source: RTCA/DO-254, paragraph 1.6

• **Complex Hardware Item**: All items that are not simple are considered to be complex.

  --Source: RTCA/DO-254, Appendix C
Chapter 1: Introduction/Key Terms

• Custom micro-coded component: A component that includes application specific integrated circuits (ASIC), programmable logic devices (PLD), field programmable gate arrays (FPGA) and other similar electronic components used in the design of aircraft systems and equipment.

-- Source: AC 20-152
Chapter 1: Introduction/Topics Covered

• In the Order, we call custom micro-coded components either simple electronic hardware (SEH) or complex electronic hardware (CEH).
  – Collectively referred to as Airborne Electronic Hardware (AEH). This order does not use this term, but it is how these items will be referred to as a group (e.g., “Conducting AEH Reviews Job Aid”).

• Order applies only to SEH and CEH, not the broader scope of hardware items defined in DO-254.
  – i.e., not printed circuit boards, modules or LRU’s.

• Lists Topics of Order Chapters.
Chapter 2: SEH/CEH Review Process

• Applying DO-254 to reviews
  – Objectives of reviews
  – Based on Order 8110.49 “Software Approval Guidelines”, Chapter 2

• Four Types of Hardware Reviews
  1. Planning (SOI #1)
  2. Design (SOI #2)
  3. Validation and Verification (SOI #3)
  4. Final (SOI #4)
Chapter 2: SEH/CEH Review Process

• For each review type:
  – Goals
  – Criteria (type and availability of data, and type of transition criteria)
  – Evaluation criteria (measures)

• Preparing and conducting the review
Chapter 3: Determining FAA Involvement

• Criteria for Involvement
  1. Hardware Level (A,B,C,D)
  2. Other Relevant Criteria -> Score (0-207)
  3. Combination of Hardware Level and Score -> Level of Involvement Determination (High, Medium, Low)

• Circumstances that may change Involvement
  – Designee support
  – Project risk
  – FAA workload and resources
  – Hardware type (Simple or Complex)
Chapter 4: Clarification of Topics Applicable to both SEH and CEH

• Modifiable Custom Micro-coded Components
  – When embedded logic is able to be modified by the user, both DO-254 and Sections 2.4 and 2.5 of DO-178B concerning user-modifiable software, option-selectable software, and field-loadable programming are applicable.
  – Order 8110.49, Chapters 5, 6, and 7, which address modification of hardware and software after approval provide additional insight.
Chapter 4: Clarification of Topics Applicable to both SEH and CEH

- Plan for Hardware Aspects of Certification (PHAC)
  - Packaging
    - Each component can have its own stand-alone PHAC.
    - All electronic hardware components of a system can be combined in one PHAC.
    - PHAC content can be combined with other planning data for aircraft or system, e.g. Project Specific Certification Plan (PSCP)
  - Included information:
    - List of each SEH and CEH, with failure condition classifications, and functional description of each component.
    - Proposed means of compliance for each component.
    - Proposed design assurance level and justification.
    - References to appropriate hardware plans and standards.
    - List of certification data to be delivered/or to be made available to the FAA.
    - Description and justification for alternative methods to those in DO-254.
    - Justification for reverse engineering a component.
    - Approach for verification of SEH.
Chapter 4: Clarification of Topics Applicable to both SEH and CEH

• Validation Processes
  – Validate derived requirements per DO-254 Section 6.1.

• Configuration Management
  – Configuration management and problem processes need to be in place prior to any review.
  – Hardware configuration index (HCI) or equivalent
    • Identifies hardware configuration and embedded logic.
  – Hardware environment configuration index (HECI) or equivalent
    • Identifies configuration of the hardware life cycle environment for the hardware and embedded logic.
    • Helps reproduce the hardware and embedded logic life cycle environment, regenerate embedded logic, and re-verify/modify embedded logic.
Chapter 4: Clarification of Topics Applicable to both SEH and CEH

- **Tool Assessment and Qualification**
  - Data must exist to support relevance and credibility of a tool’s service history.

- **Hardware Changes in Legacy Systems**
  - Definitions
    - Previously developed hardware (PDH): SEH or CEH that was approved prior to publishing AC 20-152.
    - Legacy systems: Systems approved prior to publishing AC 20-152.
  - Assess reuse of PDH against DO-254 Section 11.1 and subordinate paragraphs.
Chapter 4: Clarification of Topics Applicable to both SEH and CEH

• Compliance to DO-254 for TSO’s that don’t reference DO-254.
  – If the TSO applicant complies with DO-254, TSOA letter should reference such compliance.
  – FAA should encourage compliance to DO-254 for all TSO application:
    • Newly certified aircraft, engines and airborne systems require compliance to DO-254 (or other acceptable means).
    • Difficult to show compliance at time of installation.
Chapter 4: Clarification of Topics Applicable to both SEH and CEH

- **COTS Intellectual Property**
  - Order 8110.105 is limited to COTS Intellectual Property (IP).
  - DO-254, Section 11.2 is targeted at COTS hardware, not IP.
  - Definition:
    - IP: Commercially available functional logic blocks used to design/implement part or complete custom micro-coded components. May be provided with or without the custom micro-coded component.
  - COTS IP should satisfy applicable functional and safety-related requirements.
  - Methods to establish compliance include:
    - Reverse engineering.
    - Extensive COTS IP testing and analysis.
    - Architectural mitigations at the device, board, LRU, or system level.
    - Product service experience.
Chapter 5: Clarification of Topics Applicable only to SEH

• Verification Processes
  – Varying Rigor of Testing:
    • “Comprehensive combination of deterministic testing and analysis” based on Design Assurance Level (DAL).
      – Similar to software assurance guidance.
    • DAL A and B
      – Correct operation under all unique permutations and concurrence of conditions at the gate or node level.
    • DAL C
      – Correct operation under all unique permutations of conditions at the pin level of the device.
    • DAL D
      – Component level testing not required; test at board, LRU, or other unit level.
Chapter 5: Clarification of Topics
Applicable only to SEH

- Verification Processes (cont)
  - Documentation
    - Plan for Hardware Aspects of Certification (PHAC)
    - Hardware Verification Plan (HVP)
    - Hardware configuration index (HCI) or similar
    - Hardware Accomplishment Summary (HAS)
  - Documentation may be combined with other documentation.
  - Test procedures, test cases, test results and test coverage analyses should be documented and retained as life cycle data.
Chapter 5: Clarification of Topics
Applicable only to SEH

• Traceability
  – In absence of system requirements allocated to hardware, requirements may be identified and addressed as derived requirements.
  
  – If requirements do exist, then traceability should be ensured as for CEH but with less documentation.
Chapter 6: Clarification of Topics
Applicable only to CEH

Verification Processes

– Hardware Description Languages (HDL)
  • Attributes similar to software languages.
  • Coding standards should be defined and followed to prevent unsafe features.

– Testing
  • Note in DO-254 Section 5.1.2(4) calls for safety-related derived requirements to address abnormal conditions (comparable to robustness testing).
  • Abnormal operating conditions should be captured as derived requirements and addressed in requirements-based tests.
Chapter 6: Clarification of Topics
Applicable only to CEH

• Verification Processes (cont.)
  – Test Case Procedure Review
    • Per DO-254 Section 6.2.2(4b), review test cases and procedures to confirm they are appropriate for the requirements.
  – Partitioning Integrity
    • If partitioning is used to justify combining different design assurance levels within a component, then partitioning integrity should be demonstrated, verified, and documented.
Chapter 6: Clarification of Topics
Applicable only to CEH

• Verification Processes (cont.)
  – Completion Criteria
    • PHAC and/or hardware verification plan should state and justify level of verification coverage achieved by test.
      – Measurement of requirements verification coverage achieved by test on the component itself in its operational environment.
      – Proposal and justification of alternate verification means for not verifying specific requirements by test.
Chapter 6: Clarification of Topics Applicable only to CEH

• Verification Processes (cont.)
  – Advanced design assurance strategies (in DO-254 Appendix B) for levels A and B functions
    • PHAC documentation of completion criteria of design assurance methods for level A and B functions.
      – Definition and justification of target level verification coverage of design implementation to achieve verification objectives of DO-254 Section 6.2.
      – Justification of inability to generate correct and acceptable assurance data showing complete coverage of design implementation and using more advanced design assurance methods to mitigate against potential hardware failures and anomalous behaviors.
    • Satisfaction of verification processes with independence.
Chapter 6: Clarification of Topics
Applicable only to CEH

• Traceability
  – For levels A and B,
    • Traceability should be ensured between hardware requirements, conceptual design, detailed design, and implementation.
    • Traceability should be ensured both the between the requirements and design data and corresponding verification and validation results.
  – For levels C and D,
    • Only traceability data from requirements to test is needed (see DO-254, Table A-1, Note 6 ).
Summary

• Order 8110.105
  • Explains how FAA certification staff can use RTCA/DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, on certification projects.
  • Gives guidance for approving both simple and complex custom micro-coded components.
Thank you for your attention.

Any questions?