CHANGE

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

ORDER
8110.105
CHG 1

Effective Date:
9/23/08

National Policy

SUBJ: SIMPLE AND COMPLEX ELECTRONIC HARDWARE APPROVAL GUIDANCE

1. **Purpose.** This purpose of this change is to correct an editorial error that separated the definition of Simple Hardware Item from its applicable Note.

2. **Who this change affects.** Managers and staff of the FAA Aircraft Certification Service, including any persons designated by the administrator, and organizations associated with the certification process required by Title 14 of the Code of Federal Regulations (14 CFR).

3. Disposition of Transmittal Paragraph. Retain this transmittal sheet until this directive is cancelled by a new directive.

PAGE CHANGE CONTROL CHART

Remove Pages	Dated	Insert Pages	Dated
1 and 2	**7/16/08**	**1 and 2**	**9/23/08**

4. **Administrative Information.** You can find this order on the FAA Regulatory and Guidance Library (RGL) website at http://rgl.faa.gov.

Name Susan J.M. Cabler
Title Acting Manager, Aircraft Engineering Division, Aircraft Certification Service
Organization AIR-100

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

National Policy

ORDER 8110.105

Effective Date:
July 16, 2008

SUBJ: Simple And Complex Electronic Hardware Approval Guidance

1. This 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. In this order you'll find a great deal of discussion and FAA interpretation of RTCA/DO 254 sections. Because it's impractical to cover all situations or conditions, supplement these instructions with good judgment when handling problems.

2. Report any deficiencies, need for clarification, or suggested improvements to this order to the Aircraft Certification Service, Automated Systems Branch, AIR-530, Attention: Directives Management Officer. Use FAA Form 1320-19, Directive Feedback Information. If you urgently need an interpretation, contact the Aircraft Engineering Division, Software Specialist, AIR-120, for guidance. Use Form 1320-19 as a follow-up to verbal conversation.

Susan J.M. Cabler
Acting Manager, Aircraft Engineering Division
Aircraft Certification Service

Distribution: A-W(IR/FS/EE)-3; A-X (CD/FS)-3; A-FFS-0(ALL); I
A-FAC-0(ALL); AMA-220 (25 copies); AFS-600 (3 copies); AEU-100;
A-FDR-2

Initiated By: AIR-100

Table of Contents

Paragraph *Page*

Chapter 1. Introduction

1-1. Purpose of this Order.

a. We've written this order to supplement RTCA/DO-254, and give you guidance for approving both simple and complex custom micro-coded components. This guidance applies to airborne systems and equipment, and the airborne electronic hardware of those systems when you work in a certification project (type, supplemental, amended, and amended supplemental) or technical standard order authorization. This order accepts RTCA/DO-254 as the means by which an applicant can seek FAA approval. If an applicant proposes another means, including achieving acceptable design assurance for these components by using verification and/or architectural strategies at the system or equipment level, we may need to develop more guidance (such as issue papers) on a project-by-project basis.

b. If an applicant follows RTCA/DO-254 for level D components, we don't need to review the life cycle data. However, we will review it if the applicant chooses to use their existing design assurance practices, as allowed by Advisory Circular (AC) 20-152, *RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance For Airborne Electronic Hardware*, Paragraph 1.b. Refer to FAA part- specific policy for exceptions.

1-2. Audience. Managers and staff of the FAA Aircraft Certification Service, including any persons designated by the administrator, and organizations associated with the certification process required by Title 14 of the Code of Federal Regulations (14 CFR).

1-3. Where to Find this Order. You can find this order on the FAA Regulatory and Guidance Library (RGL) website at http://rgl.faa.gov.

1-4. Some Useful Definitions.

- 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*

> **Note:** We use the definition above from the body of RTCA/DO-254, *not* the definition in Appendix C that leaves out the words "appropriate to the design assurance level."

- 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.
-- S*ource: AC 20-152*

> **Note:** A custom micro-coded component is normally packaged as a single integrated circuit based device for mounting on a circuit board, or a higher level assembly. "Component" doesn't mean surface mounted

resistors, capacitors or other individual electronic components. "Component" also doesn't mean circuit board assemblies, line replaceable units (LRUs) and other higher-level items.

- Complex hardware item – All items that are not simple are considered to be complex. See definition of simple hardware item.
-- S*ource: RTCA/DO-254, Appendix C*

- Design Assurance – All of these 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.
--Source: RTCA/DO-254, Appendix C

- Design Process –Creating a hardware item from a set of requirements using the following processes: requirements capture, conceptual design, detailed design, implementation and production transition.
--Source: RTCA/DO-254, Appendix C

1-5. Simple and Complex Hardware Topics Covered.

a. AC 20-152 explains to applicants that if they follow RTCA/DO-254, they'll demonstrate compliance to regulations and gain FAA approval for *complex* custom micro-coded components of airborne systems and equipment. The AC, however, doesn't recognize RTCA/DO-254 as a way to demonstrate compliance to regulations for *simple* custom micro-coded components.

b. RTCA/DO-254 explains that a hardware item can be an LRU, a circuit board assembly, or a component. Further, 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. From here on, we call custom micro-coded components either *simple* electronic hardware (SEH) or *complex* electronic hardware (CEH). This order applies only to SEH and CEH, not the broader scope of hardware items defined in RTCA/DO-254.

c. In this order we supplement RTCA/DO-254, explaining---

- How to review SEH and CEH (chapter 2), and

- How much FAA involvement we should apply to hardware projects (chapter 3).

d. In the latter part of this order, we clarify RTCA/DO-254 for both SEH and CEH on the following:

- Modifiable components (paragraph 4-2).

- Certification plan (paragraph 4-3).

- Validation processes (paragraph 4-4).
- Configuration management (paragraph 4-5).
- Assessing and qualifying tools (paragraph 4-6).
- Approving hardware changes in legacy systems using RTCA/DO-254 (paragraph 4-7).
- Acknowledging compliance to RTCA/DO-254 for TSO approvals that don't reference RTCA/DO-254 (paragraph 4-8).
- Commercial-off-the-shelf (COTS) intellectual property (paragraph 4-9).
- Verification processes (paragraph 5-2 for SEH and paragraph 6-2 for CEH), and
- Traceability (paragraph 5-3 for SEH and paragraph 6-3 for CEH).

Chapter 2. SEH/CEH Review Process

2-1. Applying RTCA/DO 254 to Reviews.

a. RTCA/DO-254, Section 9 describes the certification liaison process. This process sets up communication and understanding between the certification authority (which is us at the FAA) and an applicant. Section 9.2 says that the authority may review the hardware design life cycle processes and data to assess compliance to RTCA/DO-254. In this chapter, we clarify how you'll apply RTCA/DO-254.

b. We may use both on-site and desk reviews to review SEH and CEH. Additionally, we can delegate both on-site and desk reviews to designees. In this chapter, we focus on on-site reviews since they give you better access to hardware personnel, to all automation, and to test setup. When preparing for an on-site review, FAA staff should do the following with the applicant and/or hardware developer:

(1) Agree on the type of review(s): planning, design, validation and verification, or final review.

(2) Agree on review date(s) and location(s).

(3) Identify the staff involved.

(4) Identify any designees involved.

(5) Develop the agenda(s) and expectations.

(6) List the hardware data to be made available (both before and at the review(s)).

(7) Clarify how the review will be conducted.

(8) Identify any additional required resources, and

(9) Specify when and how you'll communicate your review results, which may include corrective actions and other post-review activities.

2-2. Objectives of Your Review.

a. As the FAA certifying authority, you review the hardware design life cycle processes and related data to gain assurance that the SEH and CEH comply with the certification basis and objectives of RTCA/DO-254. Hardware review helps both you and the applicant determine if a particular project will meet the certification basis and RTCA/DO-254 objectives by providing:

(1) Timely technical explanation of the certification basis, RTCA/DO-254 objectives, FAA policy, issue papers, and other certification requirements.

(2) Visibility into how the applicant implemented their processes and generated the resulting data.

(3) Objective evidence that SEH and CEH adhere to approved hardware plans and procedures.

(4) The opportunity to monitor designee activities, if applicable.

b. We must determine the level of FAA involvement in a SEH or CEH project, and document it, as soon as possible in the project life cycle. The type and number of reviews will depend on the project's hardware level, applicant (or hardware developer) experience and history, service difficulty history, designee support and other factors. See chapter 3 (this order) to determine FAA involvement.

2-3. Four Types of Hardware Life Cycle Review.

a. The review should begin early in the hardware life cycle. Early involvement reduces the risk that the system, hardware, and planning decisions will not satisfy RTCA/DO-254 objectives. Early involvement requires timely communication between us and the applicant about planning decisions that may affect hardware product and processes. Typically, developing hardware for an aircraft or engine product, or a TSO appliance, takes several months or years. Since RTCA/DO-254 is process-oriented guidance, reviews should be integrated throughout the hardware life cycle. This means there should be regular contact between us and the applicant, system supplier and/or hardware developer. Regular contact increases confidence among participants in the hardware life cycle processes, and in the product. The four types of reviews are:

(1) Stage of involvement (SOI) #1, a hardware planning review, when most of the plans and standards are complete and reviewed.

(2) SOI#2, a hardware design review, typically conducted when at least 50 percent of the hardware design data (requirements, design, and implementation) is complete and reviewed.

(3) SOI#3, a hardware validation and verification review, when typically at least 50 percent of the hardware validation and verification data is complete and reviewed.

(4) SOI#4, a final review, after the final hardware build and verification are complete, a hardware conformity review is done, and the application(s) is ready for formal system approval.

> **Note:** Though we describe four hardware reviews, it doesn't mean we'll require four reviews on every project. Some projects may combine reviews, and others may need more than four.

b. Availability of hardware life cycle data doesn't imply that the data are always complete. The data, however, should be mature enough so we can conduct a reasonable review. Similarly, all transition criteria may not necessarily be complete for that time in the project, but sufficient transition criteria evidence should exist to ensure they are being applied to the project.

c. The following paragraphs define the *goals* of each of the four types of hardware reviews, *criteria* for each type of review (type and availability of data, and type of transition criteria) and the *evaluation* criteria. Paragraph 2-8, this chapter, covers more considerations that may affect review type and timing.

2-4. SOI #1, Hardware Planning Review.

a. Hardware planning is the first process in the hardware life cycle for any hardware project. The planning process establishes the various plans, standards, procedures, activities, methods, and tools to develop, verify, control, assure, and produce the hardware life cycle data. The goal of the hardware planning review is to determine if the applicant's plans and standards satisfy the objectives of RTCA/DO-254. This review can also reduce the risk of a hardware developer producing a hardware product that doesn't meet RTCA/DO-254 objectives or other certification criteria.

b. The hardware planning review is typically scheduled when the hardware planning process is complete. Although the hardware planning process may continue to be refined throughout the hardware life cycle with plans and standards changing as the project progresses, it's generally considered complete when the associated initial transition criteria are satisfied. These are some examples of initial transition criteria:

(1) Hardware plans and standards have been internally reviewed based on company specified criteria and deficiencies resolved.

(2) Hardware plans and standards have been evaluated by hardware process assurance organization or other organization that oversees the process assurance and deficiencies resolved.

(3) Hardware plans and standards have been approved and placed under configuration control.

(4) Objectives of hardware life cycle data applicable to a SOI#1 review in RTCA/DO-254, Appendix A, Table A-1 have been satisfied.

c. Data required. Ask the applicant to make available the hardware plans and standards shown in the availability table 2-1 below. Supporting hardware data should be under configuration control as appropriate for the hardware level.

Table 2-1. Data Availability for Hardware Planning Review

Hardware Data	RTCA/DO-254 Section
Plan for hardware aspects of certification	10.1.1
*Hardware design plan	10.1.2
*Hardware validation plan	10.1.3
Hardware verification plan	10.1.4
Hardware configuration management plan	10.1.5
*Hardware process assurance plan	10.1.6
*Hardware process assurance records (as applied to the planning activities)	10.8

Hardware Data	RTCA/DO-254 Section
*Hardware requirements, design, validation & verification, and archive standards	10.2.1, 10.2.2, 10.2.3, 10.2.4
Tool qualification assessment and data, if applicable	11.4

*Per RTCA/DO-254, Appendix A, Table A-1, some hardware life cycle data may not apply to certain hardware design assurance levels.

d. Evaluation Criteria. Evaluate the plans and standards to ensure that, when they are followed, all applicable RTCA/DO-254 objectives will be satisfied. Assess the applicant's system safety assessment, proposed failure condition classifications, and hardware level(s). Finally, compare the hardware plans and standards to the assigned hardware level.

Note: Given hardware with design assurance A and B, we should evaluate plans and standards applying to RTCA/DO-254 Appendix B, Design Assurance Considerations for Levels A and B Functions. Some of these techniques and methods are new, novel and not well understood by those involved in the project.

2-5. SOI #2, Hardware Design Review.

a. Hardware design includes processes for hardware requirements capture, design, hardware description language (HDL) coding, implementation, and product transition. These are supported by hardware validation, verification, configuration management, process assurance, and certification liaison processes. The goal of your hardware design review is to assess the implementation of the applicant's plans and standards by examining the hardware life cycle data, particularly its hardware design and integral data. During this review, you may agree with the applicant on changes or deviations from plans and standards discovered, and document them. Before you start this review, the hardware design data should be sufficiently complete and mature. To determine completeness and maturity, use the following criteria:

(1) Hardware requirements are identified, documented, unambiguous, traceable to system requirements, verifiable and conform to the requirements standard.

(2) Conceptual hardware design data (specifications, documents and drawings that define the hardware item) are documented, complete, reviewed, under configuration control, conform to standards, and traceable to system requirements.

(3) Hardware architecture is defined, and reviews and analyses are completed.

(4) Detailed design data are documented, reviewed, and traceable to conceptual hardware design data (if applicable) and/or to the system requirements.

(5) Hardware implementation is traceable to the detailed design data, and was reviewed.

(6) Data to develop acceptance test criteria has been determined.

(7) Objectives of hardware life cycle data applicable to a SOI#2 review in RTCA/DO-254, Appendix A, Table A-1 are satisfied.

b. Data required. Ask the applicant to show hardware data in table 2-2 below. The supporting hardware data should be under configuration control appropriate for the hardware level. You should also have on hand the data in table 2-1.

Table 2-2. Data Availability for Hardware Design Review

Hardware Data	RTCA/DO-254 Section
*Hardware requirements, design (including HDL), V &V, and archive, standards	10.2
*Hardware design data	10.3
HDL or hardware design schematics	10.3.2.2
*Hardware review and analysis procedures	10.4.2
Hardware review and analysis results	10.4.3
Hardware life cycle environment configuration index	See paragraph 4-5.b, this order
Problem reports	10.6
Hardware configuration management records	10.7, plus paragraph 4-5.a, this order
*Hardware process assurance records	10.8

*Per RTCA/DO-254, Appendix A, Table A-1, some hardware life cycle data may not apply to certain hardware design assurance levels.

c. Evaluation criteria. Evaluate the hardware life cycle data to determine how effectively the applicant implemented the plans and standards in the development process.

2-6. SOI #3, Hardware Validation and Verification Review.

a. Per RTCA/DO-254, this order limits the discussion of requirements validation to *derived requirements* only. Derived requirements may not be directly traceable to higher level requirements, such as system level requirements. (Validation of system level requirements should be done as part of the system development process, and is not covered in this order.) Validation of derived requirements is intended to ensure the derived requirements are correct and complete with respect to the system requirements allocated to the hardware item. If the derived requirements cannot be traced to a higher level requirement, then they should be validated against the design decision(s) from which they are derived. The validation review will:

(1) Ensure that derived requirements are identified, documented and are complete and correct.

(2) Ensure that system safety assessment process evaluated the derived requirements for the hardware component, to ensure that those derived requirements don't conflict with the system level safety assessment or with any assumptions on which the system safety assessment is based.

b. Hardware verification typically combines inspections, demonstrations, reviews, analyses, tests, and coverage analysis. As with the other reviews, hardware configuration management and process assurance continue during this verification. Verification confirms that the product specified is the product built. The goal of hardware verification is to ensure that the processes will confirm this, and result in objective evidence that the product was sufficiently tested and is the intended product. The hardware verification review will:

(1) Assess the effectiveness and implementation of the applicant's verification plans and procedures; ensure the completion of all associated hardware configuration management and process assurance tasks, and

(2) Ensure that hardware requirements, design, implementation, and integration were verified.

c. Before you start a hardware verification review, the process should be complete and sufficiently mature. To determine completeness and maturity, use the following criteria:

(1) Development data (requirements, design, drawings, hardware/software interface data) are complete, were reviewed, and are under configuration control.

(2) Test cases or procedures (including objective criteria with pass/fail results) are documented, reviewed, and placed under configuration control.

(3) Test cases or procedures have been executed (either formally or informally).

(4) Completed test results are documented, as agreed to in the plans.

(5) Hardware testing environment is documented and controlled.

d. Data required. Ask the applicant to make available the hardware data shown in the availability table 2-3 below. The supporting hardware data should be under configuration control appropriate for the hardware level. You should also have on hand the data in tables 2-1 and 2-2.

Table 2-3. Data Availability for Hardware Validation and Verification Review

Hardware Data	**RTCA/DO-254 Section**
Hardware requirements data	10.3.1
*Hardware design representation data	10.3.2 and subordinate sections
HDL or hardware design schematics	10.3.2.2
Hardware validation and verification procedures	10.4.1, 10.4.2, 10.4.3, 10.4.4
*Hardware validation and verification (review, analysis and test) results	10.4.3, 10.4.5
Hardware life cycle environment configuration index (including the test environment)	See paragraph 4-5.b, this order
Hardware configuration index (test baseline)	See paragraph 4-5.a, this order
Problem reports	10.6
Hardware configuration management records	10.7, plus paragraph 4-5, this order

Hardware Data	RTCA/DO-254 Section
*Hardware process assurance records	10.8
Hardware tool qualification data (if applicable)	11.4.2

*Per RTCA/DO-254, Appendix A, Table A-1, some hardware life cycle data may not apply to certain hardware design assurance levels.

e. Evaluation criteria. Use the objectives applying to validation and verification in RTCA/DO-254 Sections 6.1 and 6.2 (and subordinate sections), respectively.

2-7. SOI #4, Final Review.

a. The final hardware build establishes the hardware component's configuration. At this point, an applicant considers that they have complied with all objectives of RTCA/DO-254. This is the version of the hardware they intend to use in the certified system or equipment. The goal of our review is to:

(1) Determine compliance of the final hardware product with RTCA/DO-254 and this order;

(2) Ensure that all hardware design, validation and verification, process assurance, configuration management, and certification liaison activities are complete;

(3) Ensure a hardware conformity review was done; and

(4) Review the final hardware configuration index (HCI) or other appropriate hardware documentation that establishes the final hardware configuration, and the hardware accomplishment summary (HAS).

b. We do this review when the hardware project is completed and satisfies the following criteria:

(1) Hardware conformity review was performed and any deficiencies resolved.

(2) HAS and HCI (or other configuration data) were completed and reviewed.

(3) All hardware life cycle data are completed, approved, and placed under configuration control.

c. Data required. You or a designee will require all hardware life cycle data of RTCA/DO-254. However, only the data in table 2-4 are of special interest for this review. Supporting hardware data should be under configuration control appropriate for the hardware level.

Table 2-4. Data Availability for Final Review

Hardware Data	RTCA/DO-254 Section
Hardware validation and verification (review, analysis and test) results	10.4.3, 10.4.5
Hardware life cycle environment configuration	See paragraph 4-5.b, this order

Hardware Data	RTCA/DO-254 Section
index	
Hardware configuration index	See paragraph 4-5.a, this order
Problem reports	10.6
Hardware configuration management records	10.7, plus paragraph 4-5, this order
*Hardware process assurance records (including hardware conformity review report)	10.8
Hardware accomplishment summary	10.9
Final tool assessment and qualification data	11.4.1, 11.4.2

*Per RTCA/DO-254, Appendix A, Table A-1, some hardware life cycle data may not apply to certain hardware design assurance levels.

d. Evaluation criteria. Ensure that the applicant addresses all hardware-related problem reports, action items, certification issues, and so on before certification, authorization, or approval. Additionally, applicants have to demonstrate that the end item hardware component is properly configured and identified per the appropriate hardware drawings/documents, including correctly programming a component like an FPGA.

2.8. Additional Considerations for Hardware Review. Although this chapter proposed four types of hardware reviews, the type, number, and extent of those reviews may not suit every certification project and applicant. You may have to consider other approaches. Think about the following when deciding.

a. Hardware level(s), as determined by a system safety assessment.

b. System and hardware component attributes, such as size, complexity, system function or novelty, and hardware design.

c. Use of new technologies or unusual design features.

d. Proposals for novel hardware methods or life cycle model(s).

e. Knowledge and previous success of the applicant (or hardware developer) in developing hardware that complies with RTCA/DO-254.

f. Availability, experience, and authorization of hardware designees.

g. Issues with RTCA/DO-254, Section 11. These include (but are not limited to) reusing previously developed hardware, the presence of COTS intellectual properties (IP) cores used to program hardware components, and using reverse engineering as a primary development model, and

h. Issue papers for hardware-specific aspects of the certification project.

Note: See chapter 3, this order, for more criteria to determine FAA involvement in hardware projects.

2-9. Preparing and Conducting the Hardware Review.

a. The review team typically consists of at least one person knowledgeable in hardware engineering, configuration management, and process assurance, plus one person familiar with the system safety assessment and system requirements. The review team leader contacts the applicant and hardware developer several weeks in advance, proposing an agenda. To optimize team efficiency, ask the applicant to send each review team member the hardware plans identified in RTCA/DO-254, Section 10.1 so each team member has time to review before arriving at the applicant's facility.

b. Prepare an entry briefing to introduce team members, state the review's purpose, and provide an agenda. Ask the applicant or hardware developer to brief the availability of facilities and life cycle data, personnel schedule constraints, system overview, system interaction with other systems. They should cover system architecture, hardware architecture, hardware life cycle model including tools and methods, progress against previous action items or issue papers if appropriate, current status of the development including status accounting report or similar data, summary of self-assessment result (if performed); and additional considerations per RTCA/DO-254, Section 11 and Appendix B, if applicable.

> **Note:** We might appoint a designee as review team leader. How they plan the review and notify the applicant may vary, since the designee may work directly with, or for, the hardware developer.

c. The review team leader should notify the applicant and/or hardware developer (as appropriate) in writing before the review about FAA expectations in the hardware review. Include in the notification letter:

(1) Purpose and type of review (planning, development, verification, or final).

(2) Date and duration.

(3) List of review participants with contact information.

(4) Request that the hardware plans identified in RTCA/DO-254, Section 10.1, be sent to each review participant.

(5) Request the life cycle data at time of review.

(6) Indicate which RTCA/DO-254 objectives will be assessed.

(7) Suggest the applicant and/or hardware developer do a self-assessment before the review, and

(8) Request the responsible managers, developers, verification, configuration management, and process assurance personnel be available to answer questions.

d. Your typical on-site review includes:

(1) An FAA entry briefing. See paragraph 2-9.b, this order.

(2) Applicant or hardware developer briefing. See paragraph 2-9.b, this order.

(3) Your review of applicant and/or hardware developer processes and product.

(4) Your recording of results. Include as a minimum:

(a) Each life cycle data item, including document name, control identity, version and date, requirement identification (where applicable), HDL or hardware design schematic (where applicable), paragraph number (where applicable), and review results

(b) The approach you took to establish the finding or observation. A *finding* is non-compliance to a specific RTCA/DO-254 objective, process or artifact that can be documented. An *observation* is a process improvement, but doesn't have to be addressed for the process to comply

(c) Explanation of the findings or observations, related to RTCA/DO-254 objectives (documented with detailed notes). For each unsatisfied objective, summarize what was done and discuss why the objective was not satisfied. Include examples when necessary. This will ensure the approach and findings can be understood and reconstructed at some future date, if needed

(d) Any necessary actions for us, the applicant and/or hardware developer, and

(e) List of all current or potential issue papers.

(5) Delivery of your exit briefing to the applicant and/or hardware developer, summarizing findings, observations and required corrective actions. Relate the findings and observations to RTCA/DO-254 objectives, certification basis, policy, guidance, or other certification documentation. Give the applicant and/or hardware developer the opportunity to respond. Their response doesn't have to be immediate (it could be several days later), since it typically takes some time to process the review findings and observations.

2-10. After the Review.

a. Prepare a review report, summarizing all findings, observations, and required corrective actions. Coordinate the report with the applicant and/or hardware developer, and send them a copy quickly.

b. Identify and prepare issue papers as soon as possible after discovering an issue. Issue papers document technical and certification issues that must be resolved before certification, creating necessary communication between us and applicants. Coordinate any issue papers with FAA headquarters (AIR-120), the appropriate directorate, and FAA chief scientific and technical advisor (CSTA). Preparing, executing and reporting desk reviews is similar to onsite reviews but may be less formal.

Chapter 3. Determining FAA Involvement in Hardware Projects

3-1. When and Where. These paragraphs consider in more depth when, to what extent, and the areas in which the FAA should be involved when determining the hardware aspects of compliance for a certification program.

a. *When* means that time during the hardware life cycle when we can determine that the project is progressing toward approved plans and procedures (such as planning, design, validation and verification, or final hardware approval).

b. *The extent* means how much and how often the FAA gets involved in the project--how many on-site reviews you conduct; how much oversight you delegate to designees; and how much and what type of applicant data you review, submit, recommend for approval, and approve.

c. *The areas* mean the parts of the hardware processes you will focus on to ensure satisfying RTCA/DO-254 objectives, such as plans, design, standards, requirements, or final hardware implementation (for example, HDL and hardware design schematics).

3-2. Criteria for Involvement. Ideally, we should carry out and document an assessment at the start of each hardware development project. This enables the FAA, applicant and hardware developer to plan and address the project details as early as possible. The assessment outcome will result in *high, medium* or *low* FAA involvement in hardware reviews. There are both hardware level criteria that can provide a rough indicator of involvement, and other criteria that can help fine-tune it.

a. Hardware level criteria: this is the first criterion for determining involvement in the hardware aspects of a project. To start, apply the hardware level criteria as shown in table 3-1. A level D component initially points to *low* involvement, but a level A component might lead to *medium* or *high* involvement.

Table 3-1. Hardware Level Criteria

RTCA/DO-254 Hardware Level	FAA Involvement Level
A	MEDIUM or HIGH
B	MEDIUM or HIGH
C	LOW or MEDIUM
D	LOW

b. Other relevant criteria: table 3-1 shows two values for hardware levels A, B, and C. Therefore, you have to look at other relevant criteria when determining the level of involvement. Those are summarized in figure 3-2. See paragraph 3-3 below for how to use table 3-1 and figure 3-2.

Figure 3-2. Other Relevant Criteria

	CRITERIA	Scale	MIN	to	MAX	Score
1.	Applicant/Developer Hardware Certification Experience					
1.1	Experience with civil aircraft or engine certification	Scale: # projects:	0 0	5 3-5	10 6+	
1.2	Experience with RTCA/DO 254	Scale: # projects:	0 0	5 2-4	10 5+	
1.3	Experience with other process assurance standards (other than RTCA/DO-254)	Scale: # projects:	0 0	2 4-6	4 7+	
2.	Applicant/Developer Demonstrated Hardware Development Capability					
2.1	Ability to consistently produce RTCA/DO-254 hardware items	Scale: Ability:	0 Low	5 Med	10 High	
2.2	Cooperation, openness, and resource commitments	Scale: Ability:	0 Low	5 Med	10 High	
2.3	Ability to manage hardware development and sub-contractors	Scale: Ability:	0 Low	5 Med	10 High	
2.4	Capability assessments	Scale: Ability:	0 Low	2 Med	4 High	
2.5	Development team average based on relevant hardware development experience	Scale: Experience	0 < 2 yrs	5 2-4 yrs	10 > 4 yrs	
3.	Applicant/Developer Hardware Service History					
3.1	Incidents of hardware-related problems (as a percentage of affected hardware items)	Scale: Incidents:	0 > 25%	5 > 10%	10 None	
3.2	Company management's support of designees	Scale: Quality:	0 Weak	5 Med	10 Strong	
3.3	Company hardware process assurance organization and configuration management process	Scale: Quality:	0 Low	5 Med	10 High	
3.4	Company stability and commitment to safety.	Scale: Stability:	0 Weak	3 Med	6 Strong	
3.5	Success of past company certification efforts	Scale: Success:	0 None	3 > 50%	6 All	
4.	The Current System and Hardware Application					
4.1	Complexity of system architecture, functions, and interfaces	Scale: Complex:	0 High	5 Med	10 Low	
4.2	Complexity and size of the hardware and safety features.	Scale: Complex:	0 High	5 Med	10 Low	
4.3	Novelty of design and use of new technology	Scale: Newness:	0 Much	5 Some	10 None	
4.4	Hardware development and verification environment	Scale: Environ:	0 None	3 Old	6 Modern	
4.5	Use of alternative methods or additional considerations	Scale: Standard:	0 Many	3 Few	6 None	

	CRITERIA	Scale	MIN	to	MAX	Score
5.	Designee Capabilities					
5.1	Experience of designees with RTCA/DO-254	Scale: Projects:	0 < 5	5 5-10	10 > 10	
5.2	Designee authority, autonomy, and independence	Scale: Autonomy:	0 Little	5 Some	10 Full	
5.3	Designee cooperation, openness, and issue resolution effectiveness	Scale: Effectiveness:	0 Non-Responsive	5 Responsive	10 Cooperative	
5.4	Relevance of assigned designee experience	Scale: Related:	0 None	5 Somewhat	10 Exact	
5.5	Designee current workload	Scale: Workload:	0 High	5 Medium	10 Low	
5.6	Experience of designees with other process assurance standards (other than RTCA/DO-254)	Scale: Projects:	0 < 5	3 5-10	5 > 10	

Total Score Result (TSR): _____

c. If a hardware component has new technology, new design methods, unusual tools or other issues that may require new FAA policy, our level of involvement may be higher. Typically, if there's a policy issue for level A and B systems, our involvement is *high*. Level C and D systems with a policy issue typically call for *medium* involvement.

3-3. Using Table 3-1 and Figure 3-2.

a. At the start of a project with hardware, the FAA, designee (if applicable), and applicant should work together to assess the project's needs and the level of involvement. Hardware level is typically determined by the systems safety assessment process early in the life cycle and gives an idea of the project's safety needs. Table 3-1 shows the typical relationship between hardware level and our involvement.

> **Note:** See discussion of TSO projects, paragraph 3-4a, for special considerations when overseeing those projects.

b. If table 3-1 assessment indicates more than one level of involvement (for a level A, B, or C hardware components), use figure 3-2 for further assessment. The scale for scoring criteria in figure 3-2 has weighted minimum and maximum values. You can select any value within the scaled range to score the applicant or hardware developer. For example, criteria 1.2, "Experience with RTCA/DO-254," is more critical (it's weighted higher) than criteria 1.3, "Experience with other process assurance standards." You can score the applicant or developer with any value from 0 (zero projects using RTCA/DO-254) to 10 (5 or more completed projects with RTCA/DO-254), as compared to criteria 1.3, where the range of values is only 0 to 4.

c. Use the criteria in figure 3-2 to calculate a TSR for the project. You can use several means, either alone or combined.

(1) The FAA review team member most familiar with the applicant or hardware developer should do the assessment.

(2) Research the applicant's or hardware developer's performance based on previous project successes and problems, past reviews and audits, in-service problems, and other FAA experiences.

(3) A designee assigned to the project may assess the project and hardware developer.

> **Note:** The hardware developer is the *company*, not necessarily the *applicant*, where the hardware development will occur.

d. For most projects, you could do a combined assessment of applicant and hardware developer, but it may be necessary to assess them separately. If your assessment for the applicant and hardware developer is different, then use the higher determination (that is, more involvement).

e. To determine involvement for a specific hardware project, score the applicant and/or hardware developer for each criteria according to the scale provided. Put the score in the score column in figure 3-2. Next, add them up to determine the TSR at the bottom right. Then apply the TSR to figure 3-3.

Figure 3-3. Level of Involvement Determination

TSR (from table 3-1)	Level A	Level B	Level C	Level D
Less than 80	HIGH	HIGH	MEDIUM	LOW
Between 80 and 130	HIGH	MEDIUM	MEDIUM	LOW
More than 130	MEDIUM	MEDIUM	LOW	LOW

> **Note 1:** If the TSR is close to a boundary (to 80 or 130), use the hardware level and your engineering judgment to determine involvement.

> **Note 2:** If any criterion in figure 3-2 doesn't apply, use the average value or adjust the figure 3-3 boundaries.

f. Figure 3-4 shows examples of *high*, *medium* and *low* FAA involvement, and typical actions those levels will necessitate.

Figure 3-4. Sample Program Decisions Based on Level of Involvement Outcome

Level of FAA Involvement:	Typical Program Decisions:
High	• Minimal delegation to designees. Designee can recommend data approval. • FAA chief scientific and technical advisor (CSTA), directorate staff, or headquarters staff involvement (when specific guidance not available). • FAA involvement throughout hardware life cycle: mentoring, on-site reviews, desk reviews (no fewer than 2 on-sites). • Applicant submits all hardware plans. • Applicant submits hardware accomplishment summary (HAS), hardware configuration index (HCI) or other configuration data, and verification results. • Recommend that applicant submit RTCA/DO-254 objectives compliance matrix, traceability data and processes to RTCA/DO-254 objectives. Can be included in HAS.
Medium	• Moderate delegation. Designee can recommend approval of plan for hardware aspects of certification (PHAC) and HAS. Designee may approve HCI. May approve other plans and data. • Moderate FAA involvement initially (planning, regulation and policy interpretation, and some mentoring) and toward the end of the project (final approval). • FAA CSTA, technical specialist, directorate staff, or headquarters staff involvement may be needed. • Conduct at least 1 on-site review but mostly desk reviews. • Submittal of PHAC, HCI or other configuration data, HAS. • Potential submittal of hardware verification plan, hardware process assurance plan, hardware configuration management plan and hardware development plan.
Low	• Maximum delegation to designees. Designee may recommend approval of PHAC. Designee may approve all other data/documents. • Minimal FAA involvement (no on-site reviews, few or no desk reviews). • Rarely need FAA CSTA, technical specialist, directorate staff or headquarters staff involvement. **Note:** We don't need to review the life cycle data if applicant chooses to follow RTCA/DO-254 for level D components. We will review it if applicant uses their existing design assurance practices allowed by AC 20-152, Paragraph 1.b. See FAA part-specific policy for exceptions.

3-4. Things that Could Change our Involvement Level.

a. Computing TSR without Designees. Even though FAA policy allows using designees in the hardware aspects of TSO authorizations (see AIR-100 Policy Memorandum *AIR-140 CEH Memo*, appendix 1 of this order), many TSO manufacturers don't do it. Figure 3-2, criteria 5.1 through 5.6 may not seem to apply. But you can still apply the criteria if your applicant or the hardware developer has at least one individual with qualifications similar to a hardware designee (experience with RTCA/DO-254 and in hardware development). They will provide an independent view of the project and ensure that RTCA/DO-254 objectives are satisfied. For TSO projects, apply the process in paragraph 2-3, but replace the "designee" in figure 3-2 with "applicant personnel responsible for hardware oversight."

b. If the applicant or hardware developer lack such qualified personnel involved in their TSO projects, enter zero ("0") scores for criteria 5.1 through 5.6. See paragraph 5-6, this order, for compliance to RTCA/DO-254 for TSO projects.

> **Note:** Some TSO applicants don't tell us of their project activities until they submit their data package, and this leads to problems for us and them. Both the FAA and applicants should make every effort to address hardware issues early in a program. This typically causes fewer problems and more rapid approval when the data are submitted.

c. Mid-Project Adjustments. We base level of involvement criteria mostly on assessments and determinations early in the certification program. During the certification program and hardware development, we still must monitor both the applicant and hardware developer. If unforeseen problems arise, we may have to re-evaluate the involvement determination and adjust our level. Likewise, some applicants may add experienced designees, or switch from novel to proven technology, reducing the level of involvement.

d. Project Risk. Risks, like schedule slides or reduced or deferred functionality, can occur. We may have to evaluate the applicant's and/or hardware developer's risk management strategy and adjust our level of involvement.

e. FAA Workload. FAA staff working multiple projects should base their decisions to get involved in a particular project on the sum of *all* their projects, plus other job activities. Committing to multiple *high* involvement hardware components, especially if they require visits to remote sites, may not be practical. Generally, hardware level and system novelty are the crucial determinants for which projects get more involvement, and which get fewer on-site reviews for level A components, and desk reviews, or none, for level C components. Report your excessive workload to management to determine the best course of action and identify additional staffing needs. The FAA may have to use staff from the headquarters, directorates, and other ACOs to meet project needs.

> **Note:** We must consider these same workload considerations when designees are involved in the project.

f. FAA Resources. In addition to workload, consider other resources like travel funds. If an FAA aviation safety engineer (ASE) has many high-involvement projects, there may not be enough funding to support all the planned activities. If we have direct oversight responsibilities instead of a designee, the ASE could use that responsibility to justify additional resources, or to ask for help from other FAA offices.

g. Applicability to SEH. Review emphasis for SEH should be on data items generated to demonstrate comprehensive testing and/or analysis—that is, documentation and test results.

Chapter 4. Clarifying RTCA/DO-254 Topics Applicable to Both SEH and CEH

4-1. What to Tell Applicants. In this chapter we clarify and expand on selected RTCA/DO-254 guidance applicable to both SEH and CEH so you'll be able to tell applicants what they need to do to gain approvals.

4-2. Modifiable Custom Micro-Coded Components.

a. RTCA/DO-254 doesn't explicitly cover the possibility that certain aspects of SEH/CEH could be modified by someone other than the component developer, after it was designed and manufactured. We must advise applicants that when logic embedded in SEH or CEH is modified this way, in addition to RTCA-DO-254, they must either follow RTCA/DO-178B, *Software Considerations in Airborne Systems and Equipment Certification,* Sections 2.4 and 2.5 concerning user-modifiable software, option-selectable software and field-loadable software as applicable. Or, they can demonstrate an equivalent level of safety.

b. We also should be familiar with Order 8110.49, *Software Approval Guidelines*, Chapters 5, 6, and 7,which cover hardware and software that can be modified by the user after the hardware or software has been approved.

> **Note:** There can be safety problems with technology-specific implementations of SEH/CEH devices, like static random access memory-based (SRAM) devices. Require applicants to address safety concerns in the project-specific plan.

4-3. Planning for Hardware Aspects of Certification.

a. RTCA/DO-254 Section 10.1.1 discusses the plan for hardware aspects of certification (PHAC). However, when aircraft or engine systems use multiple pieces of equipment with multiple software and hardware components, we may need a higher-level certification plan to describe the overall development, integration, and compliance approach. A plan is essential to determine our level of FAA involvement, reduce the risk of misunderstandings, ensure the design assurance activities are appropriate and support the system safety assessment, and agree on any alternative methods the applicant or their hardware developer proposes.

b. We can permit applicants to package the plans for electronic hardware in different ways, including:

(1) Each electronic hardware component could have its own stand-alone document (PHAC) to support reuse in multiple systems,

(2) 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

(3) Combining the PHAC content with other planning data for the aircraft or system (a project specific certification plan (PSCP). The plan should cover custom micro-coded components, and their integration with software and other system hardware components.

c. In addition to the information for a PHAC in RTCA/DO-254 Section 10.1.1, the system certification plan or PHAC for all electronic hardware components should include:

(1) List of each SEH and CEH, with failure condition classifications, and functional description of each component.

(2) Proposed means of compliance for each component (for example, RTCA/DO-254 or RTCA/DO-178B).

(3) Proposed design assurance level, and justification.

(4) References to appropriate hardware plans and standards.

(5) List of certification data to be delivered and/or to be made available to the FAA.

(6) If proposing alternative methods to those in RTCA/DO-254, the applicant has to explain how they interpret the basic objectives and guidelines, describe the alternative methods, and present their compliance justification early in the project.

(7) If proposing to reverse engineer a component, applicants must justify the proposal.

(8) For SEH, it's important that we understand the applicant's approach for "simple" devices during certification planning. See paragraph 5-2, this order, for detailed guidance.

4-4. Validation Processes. Make sure that applicants validate *derived* requirements. RTCA/DO-254, Section 6.1 covers validation.

a. Expect applicants to identify and validate hardware derived requirements. Review, analysis, simulation, testing, or a combination of these may satisfy the validation of derived requirements against the system requirements allocated to the hardware. Applicants should base the completion of the validation processes on defined criteria as further explained in RTCA/DO-254 Section 6.1.2.

b. Expect applicants to comply with RTCA/DO-254 Appendix A, documenting the validation processes as specified by the hardware design assurance level and control category. See paragraph 5-2.d(5), this order, for required SEH documentation.

4-5. Configuration Management. RTCA/DO-254, Section 7.0 talks about configuration management and problem reporting. Ensure that applicants start documenting change control and reporting problems early in the project when configuration identification (defined in RTCA/DO-254) begins. Ensure that applicants identify a baseline for the hardware before any of the reviews discussed in chapter 2 of this order occur. Configuration management and problem processes also need to be in place before any review. For changes to a previously approved design, applicants should implement change control and report problems from the baseline from which they're claiming certification credit.

a. Although RTCA/DO-254 doesn't clearly require a hardware configuration index (HCI), both SAE International's Aerospace Recommended Practice (ARP) 4754, *Certification Considerations for Highly Integrated or Complex Aircraft Systems*, Section 4.4.2 and RTCA/DO-178B Sections 9.3 and 11.16 say that applicants should submit either a system or software configuration index to their certification authorities. RTCA/DO-254 Section 10.3.2.2.1 describes a top-level drawing that uniquely identifies the hardware item and defining documentation. However, it's not clear if a top-level drawing will include enough information to identify the hardware configuration and the embedded logic for a specific SEH or CEH. Have applicants submit appropriate configuration documentation, either in the top-level drawing or an HCI, to identify completely both the hardware configuration and the embedded logic.

b. You also need to make sure that the applicant has a hardware life cycle environment configuration index (HECI) or equivalent that identifies the configuration of the hardware life cycle environment for the hardware and embedded logic and is available for review. Similar to the software life cycle environment configuration index described in RTCA/DO-178B Section 11.15, the HECI helps an applicant reproduce the hardware and embedded logic life cycle environment, regenerate the embedded logic and re-verify or modify the embedded logic.

4-6. Tool Assessment and Qualification.

a. Sometimes applicants misinterpret RTCA/DO-254, Section 11.4 and Figure 11.1, deciding that if there is relevant tool service history (Box 5 in Figure 11.1), they don't need any further qualification activities. But RTCA/DO-254 Section 11.4.1 bullet 5 explains there should be data to support the relevance and credibility of the tool's service history. Applicants should show that the tool history proves the tool produces acceptable results, and previous tool use is relevant to the applicant's proposed tool use.

b. If applicants do claim for credit of relevant tool history, we should expect them to justify it early in the project, and document it in the certification plan or PHAC.

4-7. Approving Hardware Changes in Legacy Systems Using RTCA/DO-254.

a. Before RTCA/DO-254 was published (April 2000), we approved many airborne systems, including the simple and complex electronic hardware in them. We may have also approved these systems by a TSO authorization (TSOA), whose minimum performance standards (MPS) didn't require compliance to RTCA/DO-254. Applicants may have used a design assurance process for the SEH/CEH in some of these systems. For example, they may have adapted RTCA/DO-178B (or a previous version) to hardware design assurance. In other systems, applicants may not have used any specific standard, and we approved the design assurance aspects of any SEH/CEH in those systems at the system level. After RTCA/DO-254 was published, but before we published AC 20-152 (June 2005), some applicants may have used RTCA/DO-254 to gain approval of some systems.

b. We will call SEH/CEH, approved (or plans for which were approved) before AC 20-152, previously developed hardware, or PDH. We will call systems approved (or plans for which were approved) before AC 20-152 "legacy" systems.

c. In today's programs, some applicants and/or hardware developers intend to reuse PDH components from legacy systems in newly-designed or updated airborne electronic systems. In even more ambitious programs, applicants may want to install the entire airborne system or equipment, originally certified on a particular aircraft or engine, into a different or updated aircraft or engine.

d. We have established that we need to use RTCA/DO-254 Section 11.1 and subordinate paragraphs when an applicant and/or hardware developer proposes to reuse PDH. We require applicants to submit the assessments and analysis of Section 11.1.

e. The intent of these assessments and analysis is to ensure that using the PDH is valid, and the compliance shown by the previous aircraft or engine type certificate or TSOA wasn't compromised by a :

(1) Modification to the PDH for the new application.

(2) Change to the function, use or failure condition classification of the PDH in the new application, or

(3) Change to the design environment of the PDH

f. *Any* of these can invalidate the original design assurance of the PDH. Therefore, we must assess these changes using the RTCA/DO-254 Section 11.1 and subordinate paragraphs.

4-8. Acknowledging Compliance to RTCA/DO-254 for TSOs That Don't Reference It.

a. We allow TSO applicants for any electronic equipment or system with electronic components, including SEH or CEH, to use RTCA/DO-254, even though the TSO MPS don't require compliance to RTCA/DO-254. If the TSO applicant complies with RTCA/DO-254 by AC 20-152, we should write in the TSO authorization (TSOA) letter that the TSOA includes compliance to RTCA/DO-254. This is true for both newly design electronic components in addition to modified PDH.

b. Most TSO MPS don't require compliance to RTCA/DO-254, because RTCA/DO-254 didn't exist when the TSOs were published. However, all newly certified aircraft, engines and airborne systems require compliance to RTCA/DO-254 (or some other acceptable means of compliance) as part of their current installation requirements for electronic systems. Trying to show compliance to RTCA/DO-254 for a component with TSOA at the time of installation may be very difficult, because the design and verification of the component is already complete. However, if the TSOA letter for that article plainly states that the component complies with RTCA/DO-254, then that aspect of the installation becomes easier. Because of this, we must strongly encourage applicants for all TSO applications to include compliance to RTCA/DO-254 by AC 20-152 as part of their data package.

4-9. COTS Intellectual Property (IP).

a. COTS Components Limited to IP. Though AC 20-152 recognized RTCA/DO-254 as an acceptable means to gain FAA approval of complex custom micro-coded components, the AC doesn't recognize RTCA/DO-254 as an acceptable means to gain design assurance for COTS components.

(1) RTCA/DO-254, Appendix C, defines a COTS component this way:

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

(2) In this order, we limit the discussion of COTS components to COTS IP. COTS IP means commercially available functional logic blocks (including libraries) used to design and implement part or complete custom micro-coded components such as PLDs, FPGAs, or similar programmable components. COTS IP may be provided with or without the custom micro-coded component.

b. Using COTS IP in Airborne Systems. While RTCA/DO-254, Section 11.2 covers using COTS components, the information is targeted at the actual COTS hardware, and not the IP that can be used to program other COTS hardware—like an FPGA. Therefore, although Section 11.2 is valuable, it doesn't say enough about issues with using COTS IP in airborne systems or equipment.

(1) COTS components, including IP, are developed by a company other than the applicant and hardware developer. Intended to provide specific functions or abilities in many different applications, COTS components may or may not have been developed using a rigorous design assurance method (such as RTCA/DO-254). Given this, we must ensure that the applicant and hardware developer show that using COTS IP complies with the applicable airworthiness requirements, regulations, policy and guidance for that project.

(2) Availability of COTS IP doesn't automatically guarantee that it can be used in a manner that complies with airworthiness requirements, regulations, policy and guidance. Depending on the complexity of the COTS IP and the availability of IP documentation, applicants and/or hardware developers may have significant work to show compliance for the system or equipment.

> **Note:** COTS IP cores that come as a netlist only and COTS processor cores (soft or hard) may not have the available documentation to show compliance.

(3) Using a COTS IP in a SEH/CEH that's installed in airborne systems or equipment should satisfy applicable functional and safety-related requirements. RTCA/DO-254 Section 11.2 may not be sufficient for design assurance of a COTS IP implemented in a SEH/CEH that supports level A and B aircraft, and other safety critical, functions. As a result, applicants may need to develop or augment system architectural mitigation, component verification, testing, analysis and other life cycle data of a COTS IP. All this is needed to demonstrate its intended function, show it is free from anomalous behavior, satisfies applicable regulations, and meets airworthiness requirements.

(4) Applicants can use methods to help establish compliance to the airworthiness requirements, regulations, policy and guidance for an airborne system or equipment that use COTS IP. Some methods include (but aren't limited to):

(a) Reverse engineering the required life cycle data from known information about the COTS IP functionality and design.

(b) Extensive COTS IP testing and analysis, so the applicant and system developer gain detailed information about the functionality, plus how it operates during boundary and failure conditions. This should include testing and analysis of any functionality from the COTS IP that will not be used or activated in the specific application. Refer applicants to RTCA/DO-254, Appendix B for advance methods and techniques.

(c) Architectural mitigations at the device, board, LRU, or system level that will detect and/or mitigate unforeseen or undesirable CEH/SEH operation in which the COTS IP is installed. This includes mitigating any functionality from the COTS IP that will not be used or activated in the specific application. Applicants have to design architectural mitigations, if required for compliance, to the appropriate design assurance level to satisfy the system safety assessment.

(d) Product service experience, per RTCA/DO-254, Section 11.3 and subordinate paragraphs. Applicants should use documented evidence to support any argument for using product service experience to gain certification credit. We will not accept unsubstantiated statements of compliance.

Chapter 5. Clarifying RTCA/DO-254 Topics Applicable Only to SEH

5-1. How Applicants Gain Approval. In this chapter we'll clarify and expand on selected RTCA/DO-254 guidance applicable only to SEH so you'll be able to tell applicants what they need to do to gain approvals.

5-2. Verification Processes. While we earlier acknowledged that RTCA/DO-254 is an acceptable means of compliance for simple electronic hardware components, RTCA/DO-254 doesn't clearly show readers how they can achieve comprehensive testing and/or analysis of simple hardware items. This paragraph clarifies what we should tell applicants about SEH verification.

a. Varying Levels of Testing.

(1) Given RTCA/DO-254's definition for a simple hardware item (reproduced in paragraph 4 of this order), many applicants have been confused about what is a "comprehensive combination of deterministic tests and analyses," and more specifically, the word "comprehensive" when applied to a simple hardware item. RTCA/DO-254 Section 1.6 offers no extra guidance on how to choose which specific deterministic tests and analyses are appropriate for a level A simple hardware item, as opposed to a level D item. But if we vary the rigor of verification coverage based on the assigned design assurance level of a simple hardware item, this is consistent with RTCA/DO-254 guidance for complex hardware items of different design assurance levels.

(2) See RTCA/DO-254, Appendix A, Modulation of Hardware Life Cycle Data Based on Hardware Design Assurance Level, and Appendix B, Design Assurance Considerations for Levels A and B Functions, to see the different requirements for the different levels of airborne hardware. This difference of rigor between the various assurance levels is similar to the guidance for software design assurance. For example, there are different structural coverage criteria for software levels A, B, C and D based on the potential failure conditions that the software could cause or contribute to, as determined by a system safety assessment.

b. Two Design Assurance Approaches in RTCA/DO-254.

(1) RTCA/DO-254 offers two different ways to show compliance:

(a) Rely on a comprehensive combination of deterministic testing and analysis for simple hardware items.

(b) Rely on a disciplined hardware design assurance process--that is, satisfy the objectives of RTCA/DO-254, Sections 2 through 9.

(2) Testing custom micro-coded components or programmed electronic hardware components often can't show that the component has no design defects and errors. The component is too complex for comprehensive and deterministic test and analysis to remain a practical approach. So RTCA/DO-254 specifies a disciplined, structured design assurance approach for complex hardware items. However, simple hardware items can be comprehensively tested and/or analyzed appropriate

to the design assurance level. This testing and analysis can comprehensively demonstrate that the component performs its intended function, has no design errors, and shows no anomalous behavior. In other words, if applicants don't use a *structured* design assurance approach, they must rely on a comprehensive combination of testing and analysis to ensure correct function without design errors or unexpected behavior.

(3) Hidden in the two approaches for design assurance listed above, and in RTCA/DO-254, is a risk for certification programs: the decision whether to treat a component as simple or complex has to be both correct *and* be made early in the program. Early on, an applicant could classify a component as simple, even though they might not be sure that they can demonstrate correct functional performance with no anomalous behavior through testing and analysis alone. If, later in the program, the applicant finds that indeed, it isn't possible or practical (or within the program schedule), then they have to reclassify the component as complex.

(4) Reclassifying the component after starting the project can cause many problems, as the design assurance process of DO-254 may not have been used at the beginning of the program. Reclassification will likely require that applicants repeat the development activities for the device to produce the necessary life cycle data, demonstrating that they followed a disciplined and structured design assurance approach required by RTCA/DO-254 for complex hardware items. So, if an applicant classifies a component as simple, *you* must ensure that they can demonstrate the feasibility of the required verification coverage in the hardware plans. Discuss the applicant's proposed approach with them. Ensure that they understand the potential risks to the certification program.

c. Clarifying RTCA/DO-254 for SEH.

(1) Although it's generally accepted that most modern custom micro-coded components like PLDs, FPGAs (with thousands of configurable logic cells supporting many functions at the airborne system level) and ASICs are complex electronic components, some applicants have proposed their FPGAs as SEH. RTCA/DO-254 says little about how to demonstrate that simple hardware items comply with the applicable certification requirements. The following clarification on SEH will give you a more standardized approach to assess compliance when an applicant implements SEH in airborne systems.

(2) More than once in the next paragraphs we'll use the phrase "comprehensive combination of deterministic testing and analysis." The meaning of "comprehensive" depends on the assessed design assurance level (DAL) for SEH. Because the need for correct operation increases as a component's hazard classification increases, you have to be more thorough and rigorous when testing a DAL A or B device than a DAL C or D. This direct proportion is like the increasingly rigorous design assurance processes in RTCA/DO-178B for airborne software and in RTCA/DO-254 for complex hardware items.

5-2. d. Things Applicants Proposing SEH Should Address.

(1) DAL A and B: SEH with functions whose failure or malfunction could cause a *catastrophic*, or *hazardous/severe-major* failure condition as determined by the system safety assessment process, should have the following:

(a) A comprehensive combination of deterministic tests and analysis that demonstrates correct operation under all possible combinations, permutations, and concurrence of conditions across all primary inputs, internal elements, nodes, registers, latches, logic components, and gates within the component, with no anomalous behavior. Comprehensive testing and analysis for SEH should also consider a dynamic view of the component and include input parameters/characteristics like input set-up and hold time. If the inputs of some specific gates, nodes, and so forth can't be sufficiently controlled using external component inputs to create all required transitions, applicants should augment the testing with techniques for acceptable component stimulation. If the outputs of some specific gates and nodes can't be sufficiently observed using external device outputs to detect correct operation, applicants should augment the testing with more observation techniques.

(b) A coverage analysis that ensures the testing and analyses satisfy the specified criteria and are complete. Test coverage analysis should confirm that all logical gate/nodes within the component, plus the interconnections between these gates/nodes, have indeed been exercised to demonstrate proper operation of the elements within the component. For example, applicants should test an "OR" gate to show that it truly operates as an "OR" gate. Plus, applicants should test all possible states of a sequential state machine and if applicable, all combinations of possible states of multiple state machines. If concurrency is present in the component, then all possible concurrency conditions should be tested. Concurrency will be present any time a component has multiple independent data streams that interact together in some way through shared resources, arbiters, and multiple interacting state machines.

(c) Timing analysis that covers best-case and worst-case timing conditions, potential clock drift, and other timing issues that may prevent a component's correct operation. Tell applicants they should consider adverse environmental conditions, like temperature, in this timing analysis.

(2) DAL C: SEH with functions whose failure or malfunction could cause a *major* failure condition as determined by the system safety assessment should have a comprehensive combination of deterministic testing and analysis that demonstrates correct operation under all possible combinations and permutations of conditions of the inputs at the pins of the component--those inputs available outside the component packaging. Applicants must test all possible states of any sequential state machines. We should ensure that, when they comprehensively test and analyze SEH, applicants also take a dynamic view of the component and include input parameters/characteristics, like input set-up time and input hold time.

(3) DAL D: we don't require specific component level testing of level D SEH. But if applicants don't perform component level testing, they should test at the board, LRU, or other unit level to show that level D SEH satisfies the component level requirements.

(4) Testing Environment: when testing SEH in its operational environment isn't feasible, applicants have to offer, and justify, other verification means.

(5) Documentation: see paragraph 1.b, this order, for Level D components. To clarify and support requirements for SEH documentation in RTCA/DO-254 Section 1.6, advise applicants to submit the following:

(a) Plan for hardware aspects of certification (PHAC) (RTCA/DO-254, Section 10.1.1).

(b) Hardware verification plan (RTCA/DO-254, Section 10.1.4).

(c) Hardware configuration index (paragraph 4-5.a, this order), and

(d) Hardware accomplishment summary (RTCA/DO-254, Section 10.9).

(6) Combine the Documentation: tell applicants that they can combine the SEH documentation with other documentation when using RTCA/DO-254. For example, they can submit a single PHAC for both SEH and CEH to you. Also, they should document test cases or procedures, test, results and test coverage analyses for SEH and retain it all as life cycle data, which is subject to your review.

5-3. Traceability. RTCA/DO-254 Sections 5.1.1, 5.1.2, 6.1, 6.1.2, 6.2.1, 6.2.2, 6.3.2, 6.3.3, and 10.4.1 talk about traceability. Though RTCA/DO-254 requires that the verification process be performed and documented for a simple hardware item, it doesn't require extensive documentation. In this paragraph we clarify traceability for SEH:

a. In the absence of system requirements allocated to hardware, applicants may identify all requirements as derived. Clarifications in paragraph 4-4 of this order apply.

b. If hardware requirements do exist, then clarifications in paragraph 6-3 (this order) apply. See paragraph 5-2.d for required SEH documentation.

Chapter 6. Clarifying RTCA/DO-254 Topics Applicable Only to CEH

6-1. Expanding on CEH Guidance. In this chapter we'll clarify and expand on selected RTCA/DO-254 guidance applicable only to CEH so you'll be able to tell applicants what they need to do to gain approvals.

6-2. Verification Processes. RTCA/DO-254 Section 6.2 talks about verification. Section 6.3 covers verification methods in more detail. Here are some particular clarifications.

a. Hardware description language (HDL). HDLs, defined in RTCA/DO-254 Appendix C, have attributes similar to software programming languages. RTCA/DO-254 doesn't explicitly address these attributes. To prevent potentially unsafe attributes of HDLs from leading to unsafe features of the components, we must expect that, if they use an HDL, applicants define the coding standards for this language consistent with the system safety objectives, and establish conformance to those standards by HDL code reviews. Reviews should also include assessing the HDL (detailed design) with respect to the requirement for completeness, correctness, consistency, verifiability and traceability.

> **Note:** For levels C and D, the applicant need show only the traceability data from requirements to test (see RTCA/DO-254, Table A-1, Note 6.).

b. Testing.

(1) RTCA/DO-254 Section 6.3.1 says testing confirms the hardware item correctly responds to a stimulus or series of stimuli. RTCA/DO-254 doesn't explicitly address robustness testing, but the note in Section 5.1.2(4) calls for safety-related derived requirements to address abnormal (worst case) and boundary conditions on input data range, state machines, power-supply and electrical signals.

(2) To make sure that applicants consistently capture and verify derived requirements per Section 5.1.2(4), we expect them to capture abnormal operating conditions as derived requirements, and address them in the tests. In addition to normal range testing and to demonstrate robustness, applicants should define requirements-based testing to cover normal and abnormal operating conditions. And where necessary and appropriate, applicants may have to do more verification (like analysis and review) to address robustness.

c. Test case and procedure review: emphasize to applicants that, according to RTCA/DO-254 Section 6.2.2(4b), they have to review test cases or procedures to confirm they are appropriate for the requirements to which they trace and are intended to verify.

d. Verification completion criteria: RTCA/DO-254 Section 6.2.2 (4) requires applicants to analyze the verification coverage and determine that the verification process is complete. This is consistent with verification objectives 1 and 2 in Section 6.2.1. It means that applicants have to verify each requirement and explain discrepancies between expected and actual results, especially safety-related requirements. RTCA/DO-254 Section 6.3.1 says that when testing the hardware item in its intended operational environment is not feasible, applicants have to offer, and justify, other verification means. So we should expect their PHAC and/or hardware verification plan to state and

justify the level of verification coverage of the requirements achieved by test. We support RTCA/DO-254 when we require applicants to:

(1) Measure and record the verification coverage of the requirements achieved by test on the component itself in its operational environment, and

(2) Propose and justify an alternate verification means if we accept applicant's justification for not verifying specific requirements by test.

e. In addition to complete verification coverage of the requirements, RTCA/DO-254 Section 2.3.4 also requires that applicants apply advanced design assurance strategies (in RTCA/DO-254 Appendix B) for levels A and B functions. According to the description for item 4 in Figure 2-3, a single Appendix B approach may not be sufficient to ensure complete mitigation of potential failures and anomalous behavior for level A functional failure paths. But RTCA/DO-254 doesn't explicitly identify completion criteria for these advanced design assurance activities. Appendix B discusses using elemental analysis, which may be applied to determine completion criteria. Appendix B also covers other advanced verification methods, like safety-specific analysis and formal methods.

f. Regardless of the approach methods and approaches they propose, applicants should document the completion criteria of design assurance methods for level A and B functions in the PHAC. In particular, for components with design assurance levels A or B, applicants should adhere to RTCA/DO-254 guidelines:

(1) Define and justify a target level of verification coverage of the internal structure of the design implementation using verification procedures that achieve the verification objectives of RTCA/DO-254 Section 6.2.

(2) Justify an inability to generate correct and acceptable assurance data showing complete coverage of the internal structure of the design implementation. Applicants should use more advanced design assurance methods to mitigate against potential hardware failures and anomalous behaviors.

(3) Satisfy verification processes with independence (refer applicants to RTCA/DO-254 Appendix A and Table A-1).

> **Note:** Branch and decision coverage is an example of an additional advanced design assurance strategy for level A.

f. Finally, we can't assume partitioning (separating or isolating functions or circuits) within the hardware component. If they use partitioning to justify combining different design assurance levels within a component, applicants should demonstrate, verify, and document partition integrity.

6-3. Traceability. Many RTCA/DO-254 sections talk about traceability, including Sections 5.1.1, 5.1.2, 6.1, 6.1.2, 6.2.1, 6.2.2, 6.3.2, 6.3.3, and 10.4.1. In this paragraph we clarify two areas for levels A and B:

a. Applicants should ensure traceability between the hardware requirements, the conceptual design, the detailed design, and the implementation.

b. Applicants should ensure both the traceability between the requirements and design data covered in paragraph 6-3a above and the corresponding verification and validation results.

c. For levels C and D, applicants need to ensure only the traceability from requirements to test (see RTCA/DO-254, Table A-1, Note 6).

Appendix A. Administrative Information

101. Distribution. Distribute this order to the branch level in Washington headquarters Aircraft Certification Service, section level in all aircraft certification directorates, all chief scientific and technical advisors (CSTA), all aircraft certification offices (ACO), all manufacturing inspection offices (MIO), all manufacturing inspection district or satellite offices (MIDO/MISO), and all flight standards district offices (FSDO) and the FAA Academy.

102. Forms and Reports. Find the Directives Comment Form 1320.19 at http://feds.faa.gov/. Select "Browse" and limit the range of forms presented to 1300-1329.

103. Related Publications.

a. Code of Federal Regulations. Title 14 of the Code of Federal Regulations (14 CFR) part 21, *Certification Procedures for Products and Parts*.

b. FAA Orders and Advisory Circulars (AC). View and download the following orders and ACs from the FAA website at http://rgl.faa.gov.

- Order 8100.15, *Organization Designation Authorization Procedures*
- Order 8110.42, *Parts Manufacturer Approval Procedures*
- Order 8110.49, *Software Approval Guidelines*
- AC 20-152, *RTCA, Inc. Document RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware*

c. Other FAA Policy Documents. These documents are available from the FAA website at http://rgl.faa.gov/.

- AIR-100 Policy Memorandum #2001-01, *Use of Designated Engineering Representatives in the Technical Standard Order Authorization Process*, dated April 16, 2001
- AIR-100 Policy Memorandum *AIR-140 CEH Memo, Designated Engineering Representative (DER) Authority for Complex Electronic Hardware Approval and Special Delegation for TSO Complex Electronic Hardware*, dated December 20, 2007
- PS-ACE100-2005-50001, *Design Assurance Guidance for Airborne Electronic Hardware*, dated January 31, 2007

d. RTCA, Inc. Documents. Order copies of RTCA documents from RTCA, Inc., 1828 L Street, NW, Suite 805, Washington, D.C. 20036. You can also order copies online at http://www.rtca.org. RTCA documents referenced in this order are:

- RTCA/DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*

- RTCA/DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*

e. SAE International Documents. Order SAE documents from SAE International, 400 Commonwealth Drive, Warrendale, Pennsylvania, 15096. You can also order copies online at http://www.sae.org/servlets/index. The SAE document referenced in this order is SAE ARP 4754, *Certification Considerations for Highly Integrated or Complex Aircraft Systems.*

Appendix B. Acronyms

AC	advisory circular
ACO	aircraft certification office
AIR	Aircraft Certification Service
ASE	aviation safety engineer
ASIC	application specific integrated circuit
CEH	complex electronic hardware
CFR	Code of Federal Regulations
COTS	commercial off the shelf
CSTA	chief scientific and technical advisor
DER	designated engineering representative
DAL	design assurance level
FAA	Federal Aviation Administration
FPGA	field programmable gate array
FSDO	flight standards district office
HAS	hardware accomplishment summary
HCI	hardware configuration index
HDL	hardware description language
HECI	hardware life cycle environment configuration index
IP	intellectual property
LRU	line replaceable unit
MIDO	manufacturing inspection district office
MIO	manufacturing inspection office
MISO	manufacturing inspection satellite office
MPS	minimum performance standards
PHAC	plan for hardware aspects of certification
PLD	programmable logic device
PSCP	project specific certification plan
RGL	Regulatory and Guidance Library
SEH	simple electronic hardware
SOI	stage of involvement
SRAM	static random access memory-based
TSO	technical standard order
TSOA	technical standard order authorization
TSR	total score result
V&V	validation and verification