WP332 (v1.0) January 26, 2009

Meeting DO-254 and ED-80 Guidelines When Using Xilinx FPGAs

By: Joël Le Mauff and Jeff Elliott

RTCA DO-254 [Ref 1] and its counterpart in Europe, EUROCAE ED-80 [Ref 2], are guidelines for the design of complex electronic hardware (CEH) for use in avionics systems. FAA advisory circular AC 20-152, dated June 30, 2005, made DO-254 an official requirement for suppliers of civil aviation avionics systems. DO-254 is a collection of best industry practices for design assurance of airborne electronic hardware. These guidelines advocate a top-down approach for design and verification of safety critical electronics and other avionics systems and represent the consensus of the aviation community. This white paper addresses how Xilinx can support customers in meeting these design assurance requirements with regards to Xilinx® silicon, design software, internal configuration management, and internal validation processes.

DO-254 Overview

DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, published by RTCA, Inc., provides guidance for design assurance in airborne electronic hardware to ensure its safe operation. Rather than specify how to implement the requirements or which test should be completed, DO-254 specifies the process of design assurance and certification. According to the document, design assurance is:

> *All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the hardware satisfies the application certification basis.*

While this paper addresses DO-254 design assurance for Xilinx FPGAs, it is the hardware system and not the individual components that achieves DO-254 certification — an integrated circuit (IC) cannot be DO-254 certified. Each system, including any FPGAs *and* their associated bitstreams, must be tested and validated.

Related Standards and Documents

EUROCAE ED-80

EUROCAE ED-80 is the European counterpart to DO-254. These documents are considered identical in intent and application.

FAA AC No: 20-152

The FAA Advisory Circular 20-152 [Ref 3] makes DO-254 mandatory for new designs involving complex custom micro-coded components including:

> *… application specific integrated circuits (ASIC), programmable logic devices (PLD), field programmable gate arrays (FPGA), or similar electronic components used in the design of aircraft systems and equipment.*

This circular mandates the use of DO-254 for hardware design assurance levels A to C (DO-254 is optional for level D). Level D hardware development can continue to use existing design assurance practices (see "System Failure Levels").

FAA Order 8110.105

FAA Order 8110.105, Simple And Complex Electronic Hardware Approval Guidance [Ref 4], explains how FAA certification staff can use and apply RTCA DO-254 when working on certification projects, and providing guidance on understanding complex versus simple electronic hardware issues.

RTCA DO-160E

RTCA DO-160E, Environmental Conditions and Test Procedures for Airborne Equipment, specifies standard procedures and environmental test criteria for testing airborne equipment for the entire spectrum of aircraft. This standard is also known as ISO-7137.

RTCA DO-178B

RTCA DO-178B, Software Considerations in Airborne Systems and Equipment Certification, was developed by the commercial avionics industry to establish software guidelines for avionics software developers. DO-178 is analogous to DO-254 for software.

RTCA DO-297

RTCA DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations covers design assurance as it relates to integrated modular avionics (IMA) — flexible, reusable, and interoperable hardware and software that form a platform allowing multiple applications to be run on the same hardware (in contrast to fixed-purpose line-replaceable units (LRUs)).

Hardware Classification

According to DO-254, hardware is classified as either simple or complex. This classification determines the rigorousness of the design assurance process. Simple electronic hardware is defined as systems/components that can be rigorously tested over all operating conditions, covering all possible fault mechanisms.

Complex electronic hardware and components are those that cannot be rigorously tested over all operating conditions and must rely on a disciplined hardware design assurance process for verification (DO-254 applies). Systems containing FPGAs and PLDs are classified as complex electronic hardware (CEH).

Note: See [Ref 5] for a detailed discussion on simple versus complex electronic hardware and whether FPGAs can ever be designated as simple.

System Failure Levels

The FAA defines a number of hardware design assurance levels with respect to the safety and criticality of an avionic system (Table 1). For example, engineers designing to level A or B face a much more rigorous test, verification, and documentation process than for levels C, D, or E. All flight hardware needs to be classified as having one of these failure levels.

Table 1: **DO-254 Flight System Failure Levels**

Level	Impact of a Failure	Failure Condition	Probability	
			Level	Per Flight Hour
A	Catastrophic	Failure that would prevent continued safe flight and landing.	Extremely Improbable	$<10^{-9}$
B	Hazardous/ Severe-Major	Large reduction in safety margins or functional capabilities, physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.	Extremely Remote	$<10^{-7}$
C	Major	Significant reduction in safety margins or functional capabilities, a significant increase in flight crew workload or in conditions impairing flight crew efficiency, or discomfort to the occupants, possibly including injuries.	Remote	$<10^{-5}$
D	Minor	Slight reduction in safety margins or functional capabilities, a slight increase in flight crew workload, such as routine flight plan changes, or some inconvenience to the occupants.	Probable	$<10^{-3}$
E	No Effect	Failure conditions that do not affect the operational capability of the aircraft or increase the flight crew workload.	–	–

Hardware Life Cycle

DO-254 introduces the concepts of the hardware life cycle. The DO-254 life cycle describes the general phases a project moves through, from initial planning to certification (Figure 1). The life cycle is assumed to be iterative, reacting to modifications and feedback.

While the requirements do not dictate how the life cycle should be managed nor what tools and methods should be used, they do require that the procedures, methods, and tools be documented, along with the criterion used to determine when a project can move to the next phase.

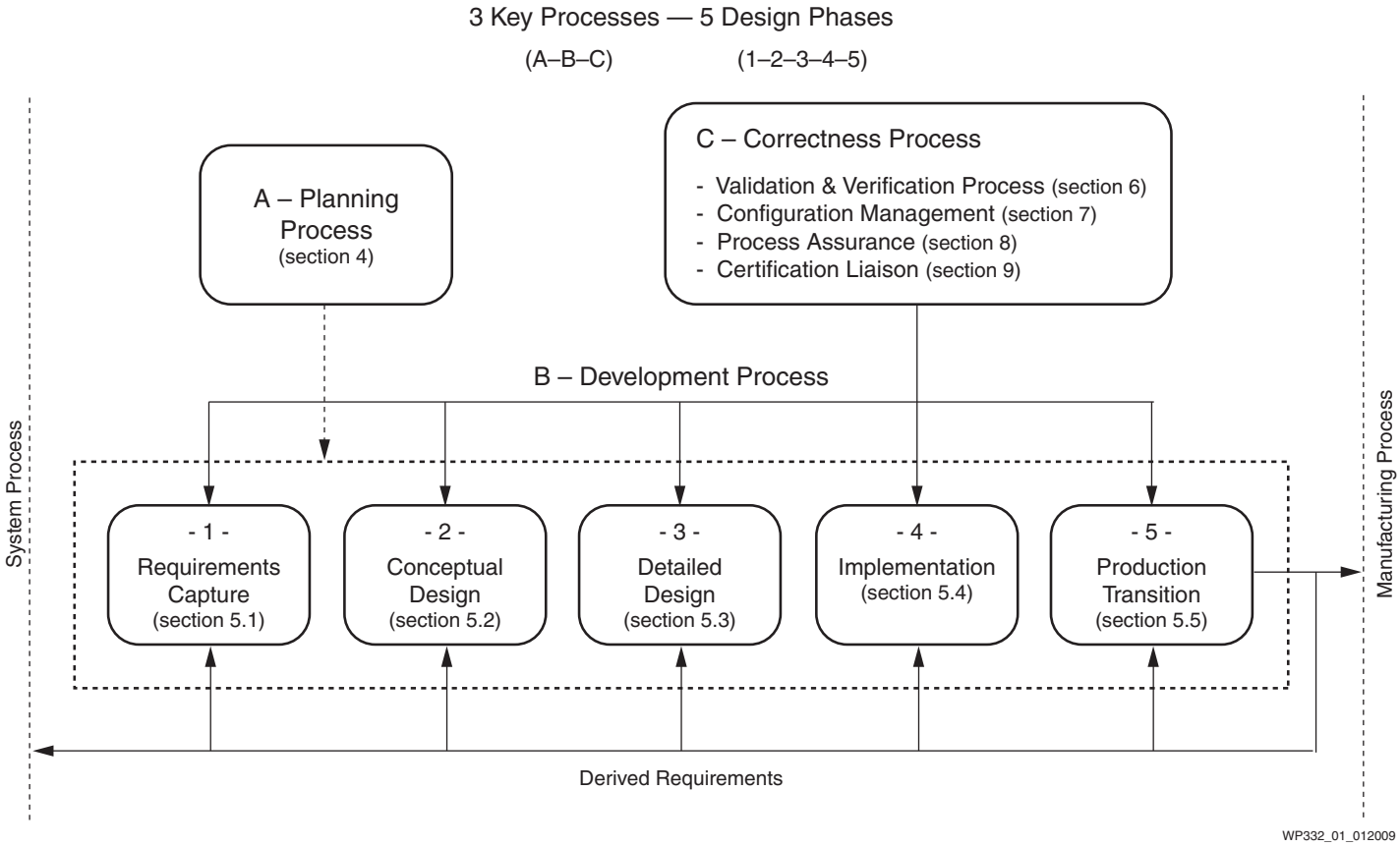

Figure 1: **Hardware Life Cycle**

DO-254 Processes

The requirements segregate activities during the hardware life cycle into one of three processes:

- Planning (including traceability)
- Design
- Correctness

Planning

In the planning stage, the exact methods, strategies, and toolsets expected to be used for tracing hardware requirements to functionality must be documented, along with the hardware development environment. Basically, the plan for achieving DO-254 certification must be documented for review by the certification authority (see "Certification Authority").

Design

The primary focus of the requirements is to assure the design process. The requirements break the design process into five parts:

- Requirements capture

  All system-level requirements along with the architecture of the system must be documented, including items such as test structures and interfaces. In addition, the mechanism for incorporating derived requirements (in other words, detailed requirements stemming from the system-level requirements).

- Conceptual design

  A block-level description of the design consistent with the requirements documents, detailing all of the major components and potential sources must be written. Any derived requirements from this process are fed back to the requirements document. In addition, any errors or omissions detected in the requirements document must be fed back through the appropriate process.

- Detail design

  At this stage, detailed design work can begin, for example, creation of the HDL for major components as well as the definition of test features and design failure mitigation. Again, any errors or omissions detected in the earlier steps must be fed back to the appropriate process.

- Implementation

  During this phase, the actual system is implemented. In the case of programmable logic, the design is synthesized, place-and-route completed, and bitstreams are generated. This phase also includes procurement, test design, and assembly procedure definition. Again, any errors or omission detected in the earlier steps must be fed back through the appropriate process.

- Production transition

  In the last phase, the system is released to manufacturing. A baseline is established to ensure consistent system production. In addition, acceptance testing and a manufacturing process regarding safety are documented. As with earlier steps, any errors or omissions detected in the earlier steps must be fed back through the appropriate process.

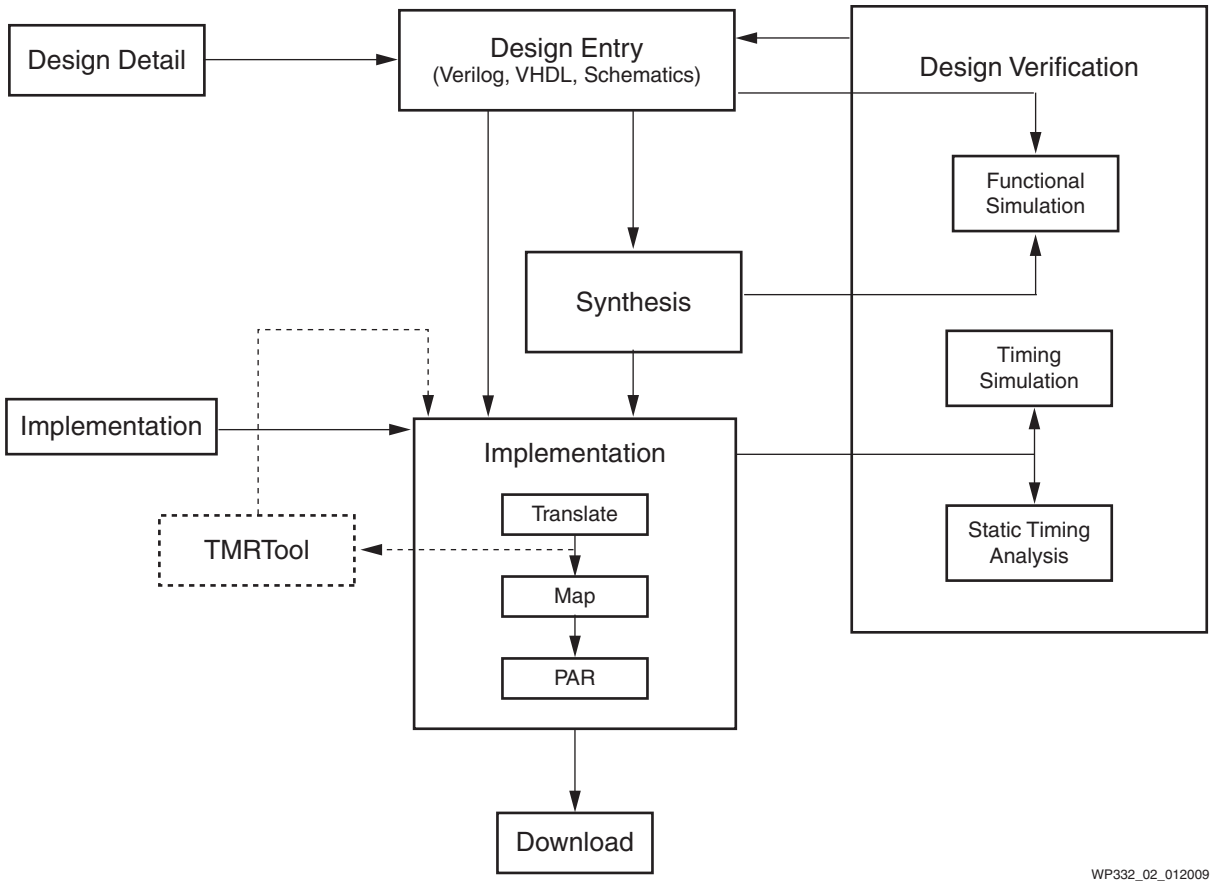

Figure 2: **DO-254 Design Process**

Correctness Processes

The requirements define a set of processes parallel to the planning and design processes.

- Validation and verification processes

  Validation assures that derived requirements (especially those relating to safety) are correct and complete with respect to system requirements. Verification assures that the hardware implementation meets all of the hardware requirements, including derived requirements. From a verification standpoint, level A and B hardware carry additional requirements.

- Configuration management

  This process archives all data needed for certification, allowing any system configuration to be restored if needed. The type of data that must be tracked depends on the assurance level of the system.

- Process assurance

  Process assurance ensures that hardware life cycle data and processes comply with the planning documents.

- Certification liaison

  This process defines the communication between the system developer and the certification authority, covering how data is approved, joint reviews, and when and how the certifying authority witnesses compliance testing.

DO-254 Deliverable Documentation

As with any certification process, documentation is key. The requirements specify four documents that must be delivered to the certification authority.

Plan for Hardware Aspects of Certification

The plan for hardware aspects of certification (PHAC) is the prime deliverable document required for achieving DO-254 certification, summarizing system functionality, its architecture, hardware and validation process, and for levels A to C, verify fail-safe operation of the system using different redundancy strategies. The PHAC includes information about development environment, system testing, and the different phases of system hardware development. With the approval of the PHAC by the certification authority, the development, testing, and implementation of the system can begin.

Hardware Verification Plan

The hardware verification plan describes the procedures, methods, and standards to be applied, and the processes and activities to be conducted to achieve verification of the Xilinx FPGA device(s) included in the system. The plan can be included in the PHAC.

Top-Level Drawing

The top-level drawing identifies all assemblies, subassemblies, and components that define the hardware.

Hardware Accomplishment Summary

The hardware accomplishment summary (HAS) is the conclusion of the development process. It identifies differences between the approved PHAC and the final design. The HAS should include change history and status of the hardware along with system and hardware overview, hardware life cycle data, alternative methods used for certification, and any previously developed hardware.

Certification Authority

For the FAA, designated engineering representatives (DERs) act on behalf of the FAA as the certification authority. The DER is an appointed engineering resource who has the authority to pass judgment on aviation-related design and development. The DER can either be an employee of the system developer or an independent consultant.

It is incumbent upon the application developer to designate a DER with care, selecting one who is approved by the FAA, has a verifiable track record, and is committed to seeing the project through to conclusion.

DO-254-Compliant FPGA Design

The FPGA design flow for DO-254 resembles the typical RTL design flow except more emphasis is placed on the validation, verification, and documentation of the design. The user has the flexibility to choose the desired design flow, but this flow must be reviewed and approved during the planning stage.

For FPGA design certification, the user has to demonstrate design assurance of both the design *and* the design process.

Design Reliability

Design reliability can be broken down in to two different aspects: design-specific and device-specific issues. Design-specific issues are controlled by the user, and device-specific issues are the domain of the device vendor.

Design-Specific Issues

Design-specific issues include the actual logic used to implement the design. The application developer must demonstrate the correctness of the design's functions, its safety aspects, fault tolerance/mitigation, and testing. The application developer must focus on *how* the design was determined to be correct as well as the thoroughness of the fault analysis. For design assurance levels A and B, these analyses must be completed at the gate level. For level C, pin level is sufficient.

Standard design validation and verification tools/techniques are applicable here. In addition, the history of successful use of all or part of a design in previous applications eases the certification task.

Depending upon the design assurance level, the application developer can employ several fault mitigation schemes when implementing the design into an FPGA (in descending order of *strength*):

- Triple-FPGA redundancy with external voting circuits
- Dual-FPGA redundancy
- Triple-module redundancy (TMR) with voting circuits implemented in the FPGA
- Circuit redundancy with arbitration inside a single FPGA
- Bitstream scrubbing with error correction
- Periodic FPGA reconfiguration

Note: For a discussion of FPGA configuration memory upsets and TMR mitigation techniques, see [Ref 6].

Device-Specific Issues

Device-specific issues include the design of the device's circuitry, the manufacturing process, quality assurance, and device testing and screening. The application developer must rely on the device vendor to provide supporting documentation and details. In addition, it is the application developer's responsibility to select the appropriate device screening and temperature range for the application.

Design Flow Reliability

Assuring design flow reliability requires the application developer to work with the various tool vendors to obtain the necessary data required for certification — information on how the software was verified and tested as well as the tool experience base.

In addition, the application developer must generate a plan for configuration management of the design flow tools, working with vendors to ensure the required support.

How Xilinx Can Help

While Xilinx cannot deliver DO-254 certified devices or tool flows, the company can assist the application developer with certification in many areas.

Devices

Xilinx offers devices supporting a wide range of operating temperatures and processing levels, from commercial specification to radiation tolerance. In addition, the company can provide the application developer with detailed reliability and qualification data as well as details on the manufacturing process controls and quality systems used in producing the devices.

Design Tools

In addition to the robust ISE® Design Suite and the Xilinx Triple Module Redundancy (XTMR) tools delivered and supported by Xilinx, specialized tools that support the DO-254 design effort such as requirements traceability and advanced verification are available from our partners, such as Mentor Graphics (see www.xilinx.com/esp/aerospace.htm).

Conclusion

DO-254 is now required for assuring the reliability of commercial aircraft electronics. Rather than specify the details, the requirements define procedures and policies, allowing application developers the freedom to define the exact methodology while in consultation with their DER. While DO-254 certified devices do not exist, Xilinx can assist application developers with documentation, tools, design methodologies, and high-reliability FPGAs in achieving DO-254 certification.

References

1. *RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware (AEH)* www.rtca.org/
2. *EUROCAE ED-80: Design Assurance Guidance for Airborne Electronic Hardware* www.eurocae.eu/
3. *FAA AC 20-152: RTCA, INC., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware*, June 2005.
4. *FAA Order 8110.105: Simple And Complex Electronic Hardware Approval Guidance*
5. *Certification Authorities Software Team (CAST) Position Paper, CAST-30: Simple Electronic Hardware and RTCA Document DO-254 and EUROCAE Document ED-80, Design Assurance Guidance for Airborne Electronic Hardware*, August 2007
6. XAPP987, *Single-Event Upset Mitigation Selection Guide*

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
01/26/09	1.0	Initial Xilinx release.

Notice of Disclaimer

The information disclosed to you hereunder (the "Information") is provided "AS-IS" with no warranty of any kind, express or implied. Xilinx does not assume any liability arising from your use of the Information. You are responsible for obtaining any rights you may require for your use of this Information. Xilinx reserves the right to make changes, at any time, to the Information without notice and at its sole discretion. Xilinx assumes no obligation to correct any errors contained in the Information or to advise you of any corrections or updates. Xilinx expressly disclaims any liability in connection with technical support or assistance that may be provided to you in connection with the Information. XILINX MAKES NO OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, REGARDING THE INFORMATION, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT OF THIRD-PARTY RIGHTS.