White Paper

DO-254 Support for FPGA Design Flows

Introduction

For most defense engineers, the first time they hear about the DO-254 Design Assurance Standard is in a request from their customer beginning with the words "Thou shalt comply with…" This leaves many engineers and engineering managers unsure on how to get started on the DO-254 process. Because DO-254 is a high-level, process-oriented standard, responsibility for design assurance necessarily requires a team approach among designers and suppliers. As such, defense organizations should seek out team solutions and partnerships with suppliers in order to best meet the needs of their customers.

HighRely, a Phoenix, Arizona-based process and education consultancy on DO-254 design assurance, introduces DO-254 in the following way:

"For decades, military organizations have developed hardware and software using a variety of specialized, defense-oriented standards including 2167A, 498, and 882. As military organizations, they were highly motivated to use hardware and software standards that differed from the commercial sector since it was perceived that military applications were 'different.' The military's utmost concern was primarily 'the mission.' Today however, there is an accelerating momentum towards military and commercial avionics convergence: adopting DO-178B and DO-254 worldwide."

History

As more software and embedded code saw use in safety-critical and avionics applications, an industry standard group developed the RTCA/DO-178B: Software Considerations in Airborne Systems and Equipment Certification. With the increasing use of high-density circuits and programmable logic in safety-critical and avionics equipment, the DO-254 body was formed to offer the same hardware design guidelines and certifications for hardware engineering that are now being implemented for software.

DO-254 Overview

The design assurance guidelines (shown in Table 1) of DO-254 break down the safety-assurance requirements of each design element of a military or avionics system based on its impact on aircraft mission and survivability in the case of failure.

Table 1. DO-254 and DO-178 Design-Assurance Levels

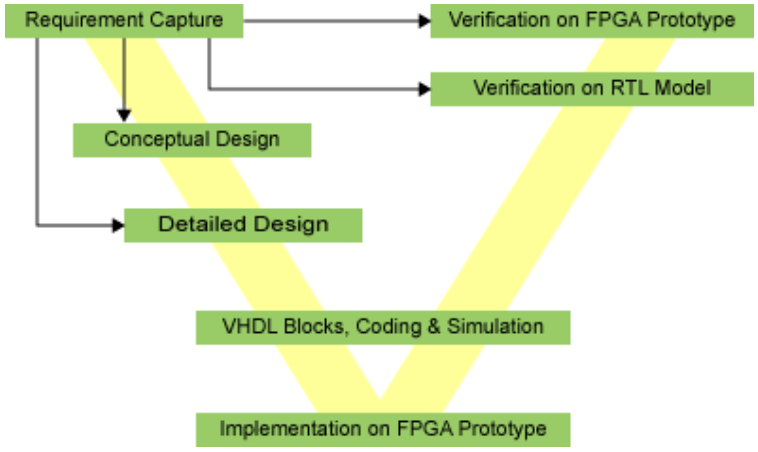
Level	Description	Affected Area	Altera Solution
A	Failure will cause or contribute to a catastrophic failure of the aircraft	Display unit, switch systems, airborne computing	FPGA or HardCopy® ASIC with cyclic redundancy check (CRC) feature
B	Failure will cause or contribute to a hazardous/severe failure condition	Backup power, heads-up display	FPGA or HardCopy ASIC with CRC feature
C	Failure will cause or contribute to a major failure condition	Any	FPGA with or without CRC feature
D	Failure will cause or contribute to a minor failure condition	Any	FPGA with or without CRC feature
E	Failure will have no effect on the aircraft or on pilot workload	Any	FPGA with or without CRC feature

The requirement terminology is important in the DO-254 process, and helps identify where documentation and verification effort is required, versus where precedent and experience may be sufficient. For example:

- *Certified:* An entire system is certified and components may have different certification levels
- *Certifiable:* System component achieving its highest certification status prior to certifying it within the system
- *Qualified:* Certification of a tool that does not have safety requirements

DO-254 guidance and consultation offers several different approaches to a DO-254 design flow for military and avionics hardware. In certifying a version of the Altera® Nios® II embedded processor for use in avionics (described later), a "V-Cycle" design flow (shown in Figure 1) was used. This is a design approach that uses a simple diagram to identify relationships between different steps in the requirements, design, verification, and documentation of a sub-system.

Figure 1. Common "V-Cycle" Design Flow Process



Cost Risks in DO-254 Certification

There are many managerial concerns about the impact of DO-254 certification on the cost efficiency of design organizations, and on the end equipment price of avionics and military equipment subject to certification. This results in cost risk and uncertainty in development schedules, inefficiency where DO-254 documentation practices are not yet in place, and inability to scope projects where certification procedures are not clear. Experienced partners and consultants are the best bulwark against this cost and efficiency risk.

The DO-254 Partnership

The Altera partner network for the DO-254 standard provides design assurance and guidance from conception through initial certification, as well as through post-certification product improvements. With partners Aldec, Mentor Graphics, Geensys, HighRely, and HCELL Engineering, Altera is committed to delivering specialty solutions and services that enable Altera FPGA and HardCopy ASIC solutions to be quickly approved and implemented in avionics and military applications, with a focus on DO-254 level-A, -B, -C, and -D compliance.

Partner Roles in Certification

Each of the partners in a DO-254 certification network has a different role in the success of the DO-254 certification requirements.

Verification Tools

Several vendors offer compliance tool sets for simulation, in-hardware verification, and, in some cases, tool certification for military and avionics hardware design. Aldec provides test and verification of FPGA designs in the target Altera device, while Mentor Graphics provides requirements tracking, verification, development flows, management reporting, and documentation of Altera designs.

Education and Process Support

An important part of controlling the cost risks in DO-254 certification is the education of engineering and quality assurance staff, and in identifying best practices in DO-254 certification. Geensys (Europe) and HighRely (North America) offer consulting, documentation, and training.

Independent IP Suppliers

Independent suppliers of FPGA intellectual property (IP) may be part of a certification network where they offer previously certified IP blocks, with sample certification and documentation. They may offer IP testbenches for DO-254 verification procedures, as well. Table 2 shows an example set of IP of interest to developers of avionics and military hardware.

Table 2. Avionic- and Military-Related Certifiable IP and Providers

IP Core and Function	Provider
NIOSII_SC 32-bit microprocessor	HCELL Engineering or Altera
Avalon® system interconnect	HCELL Engineering or Altera
UART, timer, compact flash	HCELL Engineering or Altera
Graphics IP	IMAGEM
AFDX end-system switch	MorethanIP
Time-triggered protocol	TTTech
10/100 and 10/100/1000 Ethernet	MorethanIP
1553 bus controller/remote terminal	Arion
ARINC 429 bus controller	Arion
32-/66-MHz PCI	PLDA
PCI Express Gen1	PLDA

Certification Services

HCELL Engineering is an example of an engineering services group that can perform some of the documentation and test-bench development services required for a DO-254 certification. A typical example of a certification service operation would be preparation of a single piece of stand-alone IP for FPGA design, or a soft embedded processor.

Programmable Logic and IP Supplier

Altera offers IP integration expertise to help with the DO-254 requirements and delivery process for military customer projects. In addition, Altera has participated in a DO-254 Users Group since 2005 to discuss best practices, successful implementation results, and other issues with aerospace companies. Most importantly, Altera's Cyclone®, Stratix®, and Arria® FPGA families, along with HardCopy ASICs, are equipped with features suited for military and airborne applications:

- Anti-tampering design security
- End-of-life protection
- Military temperature support
- Quality and reliability levels for rugged environments

Altera has several key customer engagements going through the DO-254 certification process, in both programmable logic and HardCopy ASIC. These certifications are occurring at the Federal Aviation Administration, as well as at several European agencies (to include a recent successful "CRI F9" audit).

The newest additions to Altera's portfolio, the 40-nm Stratix IV FPGAs and HardCopy IV ASICs, also deliver the advantages of the market's smallest technology node. Both device families, available with and without transceivers, were manufactured on longtime partner Taiwan Semiconductor Manufacturing Company's (TSMC's) 40-nm process. Together, the two companies engaged in a rigorous multi-stage test chip program to ensure device performance and reliability.

Stratix IV FPGAs are based on a proven architecture utilized in previous-generation devices, delivering the highest density, highest performance, and the lowest power. The transceiver-based Stratix IV GX variant provides unprecedented system bandwidth and superior signal integrity, with up to 48 high-speed transceivers supporting data rates up to 8.5 Gbps. HardCopy IV ASICs offer the benefits of both FPGAs and ASICs, with an equivalent

transceiver block and package- and pin-compatibility to Stratix IV FPGAs that supports a seamless prototype-to-production path. An Altera DO-254 design flow can apply towards certification with a final system implemented either in FPGA or HardCopy ASIC.

Secure Soft Processor Core

The Nios II embedded processor is the first DO-254-certified solution (DAL Level A) in the embedded processor space. To ensure safety of airborne equipment, HCELL Engineering offers the NIOSII_SC, a soft IP package providing a general-purpose RISC processor that can be reused in different airborne electronic hardware. Among its design assurance considerations are:

- Architecture mitigation at the IP and user levels
- Monitoring of errors such as an invalid instruction's operation code, division by zero, and division overflow
- Single event upset (SEU) mitigation through SEU immunity of the NIOSII_SC embedded memory

The tool versions used in this verification include Quartus® II software version 6.1 (VHDL synthesis, FPGA place and route, and programming), ModelSim SE version 6.1 (HDL simulation and VHDL coverage analysis). The Reqtify tool is used for requirements traceability. Verification of the Nios II embedded processor core has been 100% verified and documented using four different procedures:

- RTL simulation
- Post-layout simulation
- Analysis
- Physical testing

Conclusion

Engineers and engineering managers faced with new DO-254 certification requirements should know they are not alone. The objective of DO-254 is to create a reasonable, cost-effective, and repeatable process to ensure safe operations of mission critical equipment, and is intended to help engineers develop electronics with a high assurance product mind-set. Through Altera's team of education, consulting, IP providers, documentation providers, and solution providers, DO-254 is a manageable cost risk for defense programs.

Further Information

- Simplify the DO-254 Process with Altera Partner Solutions:
  www.altera.com/end-markets/military-aerospace/do-254/mil-do-254.html
- Altera's Military Risk and Productivity Management:
  www.altera.com/products/devices/stratix-fpgas/stratix-iv/end-markets-applications/stxiv-military.html
- *Military Benefits of the Managed Risk Process at 40 nm*:
  www.altera.com/literature/wp/wp-01063-military-benefits-managed-risk-process-40nm.pdf
- Altera's Enhanced COTS Initiative:
  www.altera.com/end-markets/military-aerospace/overview/mil-overview.html
- Altera's 40-nm Portfolio:
  www.altera.com/b/40-nm-devices.html
- Nios II Embedded Processor:
  www.altera.com/products/ip/processors/nios2/ni2-index.html
- Aldec:
  www.aldec.com
- Mentor Graphics:
  www.mentor.com
- Geensys:
  www.geensys.com
- HighRely:
  www.highrely.com
- HCELL Engineering:
  www.hcell-engineering.com

Acknowledgements

- J. Ryan Kenny, Technical Marketing Manager, Military and Aerospace Business Unit, Altera Corporation
- Karl-Heinz Gatterer, Military and Aerospace Marketing Manager Europe, Altera Corporation

101 Innovation Drive
San Jose, CA 95134
www.altera.com