Demystifying DO-254

Tom Dewey, Technical Marketing Engineer
Design Creation and Synthesis Division
Mentor Graphics Corporation
March 2008
INTRODUCTION
Interest in DO-254 first occurred in Europe and has since spread to the US commercial aircraft industry. If you are being asked about your company’s DO-254 direction and compliance, but have been overwhelmed with information on the subject, then this article is for you. This article presents DO-254 for the novice, boiling down the standard, reducing it to its essential points so that you will be ready to respond with confidence, as well as understand its potential impact on your products or services.

WHAT IS DO-254?
DO-254 provides guidance for design assurance in airborne electronic hardware to ensure safe function. It provides a framework of considerations for certification across the entire engineering lifecycle — but does not specify how to implement the standard. Thus, a cottage industry has formed to provide training and consulting, complicating the novice’s task of getting smart quickly.

A few years back, the FAA issued AC 20-152 that stated DO-254 must be used for programmable hardware (they included FPGAs as well as ASICs as programmable. At that point, the US commercial aircraft industry took serious notice. Europe has been involved in DO-254 even longer and their regulatory agencies apply a more rigorous treatment of the standard.

When you first take a look at the standard document you may be shocked to find how thin it is. After all, this standard is supposed to ensure that no aircraft drops out of the sky due to electronic hardware failure. Rather than provide detail, the standard covers a lot of ground but at high, conceptual levels. For example, the standard states “establish and document your hardware design process.” Many books have been written on this topic alone and companies have spent years defining and perfecting this process.

DO-254 does not sit in isolation; it complements a whole host of other standards and processes, such as safety and environmental impact assessments that provide complete guidance. But the focus of DO-254 is solely on electronic hardware. As far as the standard is concerned, there only exists hardware and software (to which DO-178 applies). There is no middle ground (for example firmware). If the hardware is going into anything that flies commercially, DO-254 likely applies.

Figure 1 shows the high-level process for selecting a design assurance strategy.
The criticality or failure condition is determined using a system safety assessment process described by the standard. This process assigns a Level A to E to describe the severity of a failure:

A. **Catastrophic**: failure prevents the safe flight and landing of the aircraft, resulting in many fatalities including the crew. A Level A failure might occur 1 in 1 billion flights.

B. **Hazardous**: failure significantly reduces flight safety margins and the capability of the aircraft to fly, possibly resulting in fatal injuries but not to the crew. A Level B failure might occur 1 in 10 million flights.

C. **Major**: failure reduces flight safety margins and the capability of the aircraft to the point where potential injuries could occur. A Level C failure should might 1 in 100,000 flights.

D. **Minor**: failure does not significantly reduce aircraft safety, resulting in potential discomfort to passengers or crew. A level D failure might occur 1 in 100,000 flights.

E. **No Effect**: failure does not affect the operation of the aircraft.

While a major failure rate of 1 in 100,000 flights might sound scary, assuming an aircraft makes 4 flights a day, 365 days a year, it would translate to only one failure in over 68 years of flight.

It is important to assign the correct level to a potential failure, as it is very expensive to design and certify hardware at a higher level. However, proper classification of a potential error is not always obvious. For example, flight entertainment systems may not be viewed as flight critical or even as a potential source for fatalities, but in reality, a failure in such a system has brought down an aircraft. The Swissair 111 crash on September 2, 1998 was traced to the in-flight entertainment system that caused arcing across wires, setting fire to the cockpit ceiling (which was lined with flammable material). It is unlikely that the entertainment system would have been classified as a Level-A system.

The standard also differentiates the rigor of the processes based on whether the hardware is simple or complex:

- **Simple**: a set of comprehensive tests can be created to exhaustively determine correct functionality under all operating conditions.

- **Complex**: if the hardware is not simple, it is complex.

Thus, the majority of FPGA and ASIC systems are typically complex. A complex, Level-A system means that you must follow the maximum guidance from DO-254.

The certification process for the standard adds costs to the development process. If the process is efficiently followed, the added cost should be 25% to 50% higher than for the development of a non-compliant system. However, industry averages approach 100% in additional cost — DO-254 compliance is a significant investment.

Developing the assurance strategy for Levels A or B means applying one or more of the methods described by the standard, including their associated analysis techniques. This task (along with the documentation that goes with it) comprises the bulk of the standard.

For all levels, a design assurance approach document is required for certification. This document is called the Plan for Hardware Aspects of Certification.
(PHAC) and fundamentally documents the assurance strategy. In addition, for Levels A to C, the fail-safe aspects of the system must be documented.

**THE HARDWARE LIFECYCLE**

DO-254 fits the assurance process into a hardware lifecycle (Figure 2). While the specification covers this lifecycle in broad-stroke concepts, it does not mandate the actual process.

![Figure 2: The Hardware Lifecycle](image)

There are several key points about the hardware lifecycle:

- The planning process is completed before any development on the design is performed.
- There are five key planning documents required for certification that can all be included in the PHAC: design, validation, verification, configuration management, and process assurance plans.
- Support processes are in place to monitor correctness for the project, including the PHAC.
- Transition criteria must be in place in order to move from one key process to another.
- The lifecycle process can be iterative based on modification and feedback between each of the three major processes.

**THE PLANNING PROCESS**

The planning process is captured in one or more documents that are reviewed for certification. This process defines how the hardware requirements trace to functionality and the process for proving assurance. The objectives of the planning process are:

- Define the lifecycle process used for hardware design.
- Select and document any standards used in the project and any expected deviations.
  - Define and document the hardware development and verification environment, including the tools used.
  - Define and document the hardware design assurance strategy.

DO-254 provides high-level guidance for the activities that should used to meet the objectives of the planning process. This process and schedules are documented in the PHAC. Typically, a designated engineering representative (DER) can provide examples and help on the PHAC. The DER will typically audit this document along with the other planning documents in the first phase of certification to determine compliance with DO-254.

**THE DESIGN PROCESS**

As expected, the majority of the standard applies to the hardware design process (Figure 3).

The standard briefly discusses the system processes, but those are covered in more detail by other standards. For example, manufacturing processes are outside of the standard. Interactions between the processes are iterative (if necessary).

**REQUIREMENTS CAPTURE**

Requirements capture and tracing are key to DO-254. The documents and processes used for requirements are closely audited for certification. Many companies use tools to identify, record, and manage this process.
DO-254 addresses hierarchical, high-level and derived requirements. A derived requirement is an additional requirement inferred from the hardware development process. For example:

- **High-level requirement**: the airspeed shall be written to the flight recorder every 5 seconds.
- **Derived requirement**: the WZX channel of the airspeed indicator shall be written to address 163 of the flight recorder RAM every 5 seconds.

The standard provides guidance for requirements capture activities:

- All system requirements implemented in hardware should be documented. For example, architecture, test structures, interfaces, and power characteristics.
- Any safety requirements related to the hardware should be documented. For example, requirements for loss of function or damage.
- Design constraints should be identified. For example, standards and technology processes.
- Deriving requirements.
- Design tolerances
- Feeding back and monitoring requirement changes and additions.

**CONCEPTUAL DESIGN**

The conceptual design process provides a high-level look at the hardware so that reviewers can determine if the resulting implementation will meet the requirements. These high-level descriptions could be block diagrams, flowcharts, finite state machine bubble diagrams, or spreadsheets. The standard provides guidance for conceptual design activities:

- Creation of the high-level description of the hardware.
- Major component identification and whether or not any functions of those components will not be used. If IP from a third party is used, extra work is required to establish assurance.
- Identification of reliability, test features, and maintenance.

**DETAILED DESIGN**

Using the requirements and the conceptual design, the next step is the detailed design process. The standard provides guidance for detailed design activities:

- Writing of the HDL code for the design.
- Implementing any architecture design techniques.
- Designing in any necessary test features.
- Assessing the impact on safety of any unused functionality.
- Identification of constraints or installation of the hardware that if not met, could affect safety.

**IMPLEMENTATION**

Using the detailed design data, the hardware device is produced during the implementation process. Thus, the device implementation, assembly, and installation
processes are complete. The standard provides guidance for implementation:

• Procurement of parts
• Building the device
• Programming the device
• Assembly
• Inspection and test

PRODUCT TRANSITION
The production transition process takes the completed hardware implementation and the verification processes into production/manufacturing. This establishes a baseline such that the hardware can be consistently replicated. The standard provides guidance for product transition:

• Preparing manufacturing data from the configured design data.
• Checking manufacturing data for completeness.
• Defining any manufacturing requirements related to safety.
• Acceptance testing.

Acceptance testing ensures that the manufactured product is in compliance with key requirements. It is up to the team to choose which key requirements should be tested. The standard does provide guidance on acceptance test criteria.

THE SUPPORT PROCESSES
The standard provides guidance on a set processes that support the planning and design processes. These support processes include:

• Validation
• Verification
• Configuration Management
• Process Assurance
• Certification Liaison

VALIDATION PROCESS
In terms of DO-254, the validation process ensures that the derived hardware requirements are correct (rather than validation of system requirements). Not all derived requirements have to be validated. Special attention is paid to those derived requirements relating to safety. The standard provides guidance for the validation process:

• Identify all derived requirements needing validation.
• Validate each requirement by review, analysis, or testing.
• Emphasis of the review, analysis, or testing should be on safety.
• Document differences between expected and actual results for pre-defined results. Otherwise, ensure the results are consistent with the requirement.
• Evaluate derived requirements for completeness in the context of the associated system requirements.
• Test requirements for ambiguity.
• Trace derived requirements to the validation activity and results.

VERIFICATION PROCESS
The verification process ensures that the hardware implementation matches the requirements. It is applied to any level of the design hierarchy. The standard provides guidance for the verification process:

• Identify requirements that require verification.
• Verify each requirement by testing, simulation, analyses, and reviews.
• Perform verification coverage analysis. Essentially, this means ensuring each requirement is verified by one of the verification techniques.
• Trace requirements to implementation and to the verification activity and results.
• Document the results.
For both the validation and verification processes, the standard provides guidance for testing and analysis tasks. In addition, the standard provides guidance for requirements and design reviews.

**CONFIGURATION MANAGEMENT PROCESS**
The configuration management process provides the ability to replicate data or to restore data if necessary. This process also provides a controlled method for managing changes and for archiving data. In the hardware world, this process is typically accomplished with the combination of enterprise systems, problem tracking, and version management software. The data under configuration management is typically anything required for DO-254 certification. The types of objects and the level of configuration management required depend on the criticality level of the design.

**PROCESS ASSURANCE**
Process assurance ensures that the hardware lifecycle data and processes comply with the planning documents (such as the PHAC). Typical activities include:

- Reviewing and tracking compliance with plans.
- Identifying and documenting deviations from plans.
- Determining if transition criteria have been met between lifecycle stages.

**CERTIFICATION LIAISON PROCESS**
The certification liaison process provides for communication between the company creating the design and the certification representatives. This process is documented in the PHAC. The process typically includes:

- The inputs and outputs of the planning process.
- Negotiation points on compliance.
- Design approach approval.
- How data is to be approved.
- Joint review points.

- The witnessing of tests by the certification representatives.

**THE DATA**
Data (or artifacts) are created throughout the design process. DO-254 auditors link this data to requirements and plans in order to certify the system. The standard specifies general characteristics for all data. The data should be:

- Unambiguous: a single interpretation.
- Complete: all necessary requirements are present along with the associated data.
- Verifiable: there exists a means to determine if the data is correct.
- Consistent: no conflicting data exists.
- Modifiable: data exists in a standard structure so that changes can be made consistently without a structure change.
- Traceable: the origin of the data can be determined.

Arrangement, packaging, and storing the data are up to the user, but the process must be documented in the PHAC. Figure 4 presents the artifacts for DO-254. Some of the plans can be embedded within the PHAC (as Figure 4 indicates), or separate documents can be created for them. The hardware accomplishment summary is the method of presenting compliance to the PHAC to the certification representatives. The standard outlines the information that should be contained in this summary. It is good practice to work with the certification contact to determine a template, examples, and what is expected in the summary. The key component of this document is a summary statement as to compliance.

**EDA TOOLS**
EDA tools are essential to hardware design and can play a big role in helping to automate the DO-254 methodology. When a human step of the standard is
replaced by a tool, that tool needs to by qualified using the process provided for by DO-254. Tools that generate code have more rigorous qualification steps than tools that verify results.

Can an EDA tool be labeled as certified for DO-254 similar to a Good Housekeeping™ seal? No, there is no such thing as a DO-254-certified EDA tool. Each version of a tool needs to be qualified in the context of a particular project if required by the standard. Tool qualification is a complex subject best addressed in a more focused paper. However, the ramifications of using any EDA tool in the DO-254 development process should be considered.

**LEARNING MORE**

As this paper is intended as an overview of the standard, more information about the standard can be found at [www.do254.com](http://www.do254.com). Or the standard can be ordered at [www.rtca.org](http://www.rtca.org). An alternative is to talk to expert customers that have been living the standard for a few years. They can offer amazing insight into the

---

**Artifacts for DO-254**

<table>
<thead>
<tr>
<th>Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHAC</td>
</tr>
<tr>
<td>Design Plan</td>
</tr>
<tr>
<td>Validation Plan</td>
</tr>
<tr>
<td>Verification Plan</td>
</tr>
<tr>
<td>Configuration Mgt Plan</td>
</tr>
<tr>
<td>Process Assurance Plan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
</tr>
<tr>
<td>Design</td>
</tr>
<tr>
<td>Validation/Verification</td>
</tr>
<tr>
<td>Archive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
</tr>
<tr>
<td>Design Presentation</td>
</tr>
<tr>
<td>Conceptual Design</td>
</tr>
<tr>
<td>Detailed Design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Validation/Verification Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
</tr>
<tr>
<td>Review &amp; Analysis Procedures</td>
</tr>
<tr>
<td>Test Procedures</td>
</tr>
<tr>
<td>Review &amp; Analysis Results</td>
</tr>
<tr>
<td>Test Results</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptance Test Criteria</td>
</tr>
<tr>
<td>Configuration Mgt.Records</td>
</tr>
<tr>
<td>Problem Reports</td>
</tr>
<tr>
<td>Accomplishment Summary</td>
</tr>
</tbody>
</table>

Figure 4: The artifacts of DO-254
vagaries of compliance. Finally, stay tuned for more papers on various interesting DO-254 topics from an EDA perspective by Mentor Graphics.

CONCLUSION
DO-254 provides a flexible framework for assuring hardware design, but actual implementation of the high-level concepts can be daunting. With an understanding of the basics, you probably realize that your company has many of the equivalent concepts already in practice. Many of your current assurance processes may already relate to the standard. In addition, many of your partners and customers may already be working with the standard, or just starting out. Whatever the situation, together with your partners and tool vendors, you can seek advice, investigate tools to help the process, and get on the road to being part of the DO-254 community.