cadence®

DO-254 Explained

By Cadence

This white paper, the first in a series of DO-254-related white papers, will explore the high-level concepts and activities within the DO-254 Design Assurance Guidance for Airborne Electronic Hardware specification, why they exist, and what they mean. In this paper, we will explore the safety-related concepts of requirements traceability, design assurance levels, the overall DO-254-compliant flow as documented in the spec, and several other aspects that might not be well documented but are critical to project approval.

Contents

Introduction

If you're reading this paper, you are likely struggling to understand the DO-254 specification[1], what this standard means, what it takes to comply, and how much more time and cost you should allocate to meet this standard. This white paper, the first in a series of white papers, will attempt to explain the standard, the concepts and reasoning behind the standard, and the basic steps and components necessary to successfully complete the project and achieve DO-254 approval.

According to several industry sources, a project meeting DO-254 can cost 1.5X to 4X more than the same project without DO-254. Why the extra expense? Usually the "4X" cost increases come from a lack of DO-254 experience, further compounded when current methodologies and processes are significantly lacking compared to a structured flow conforming to DO-254. In addition, a lack of adequate project planning and evidence that the overall process was followed can lead to audit failures—causing design and verification re-work and additional justification headaches.

However, there are ways to create a DO-254-approved project without breaking your schedule or budget. A well planned and executed DO-254 project will almost certainly take more time and money than a non-DO-254 project, but there are ways to reduce these costs to manageable levels. The first step in the process is becoming better educated in the underlying concepts and components of DO-254.

What Is DO-254?

Simply stated, DO-254 is a requirements-driven process-oriented safety standard used on commercial electronics that go into aircraft. (Conceptually speaking, this standard applies to all electronics in anything that flies or could crash and pose a hazard to the public.)

[1]The DO-254 spec is available on the RTCA website: http://www.rtca.org/store_product.asp?prodid=752

Based on their safety criticality, different parts of the aircraft are designated different Design Assurance Levels, or DALs for short (Figure 1). A system that is highly critical will receive a higher DAL, with DAL A reserved for the most critical systems. This criticality is determined by a safety assessment of the aircraft and interacting systems to determine the required target failure rate. For DO-254, the difference between meeting DAL A and DAL B is minimal, so they are frequently referred to as "DAL A/B" in various writings, including aspects of this whitepaper.

Design Assurance Level (DAL)	Description	Target System Failure Rate	Example System
Level A (Catastrophic)	Failure causes crash, deaths	<1 x 10-9 chance of failure/flight-hr	Flight controls
Level B (Hazardous)	Failure may cause crash, deaths	<1 x 10-7 chance of failure/flight-hr	Braking systems
Level C (Major)	Failure may cause stress, injuries	<1 x 10-5 chance of failure/flight-hr	Backup systems
Level D (Minor)	Failure may cause inconvenience	No safety metric	Ground navigation systems
Level E (No effect)	No safety effect on passengers/crew	No safety metric	Passenger entertainment

Figure 1: Design Assurance Levels (DALs)

Because DO-254 is a process-oriented standard, it's important to understand the overall flow, shown in Figure 2 (and in Figure 5-1 of the DO-254 specification), expected by a DO-254 certification official.

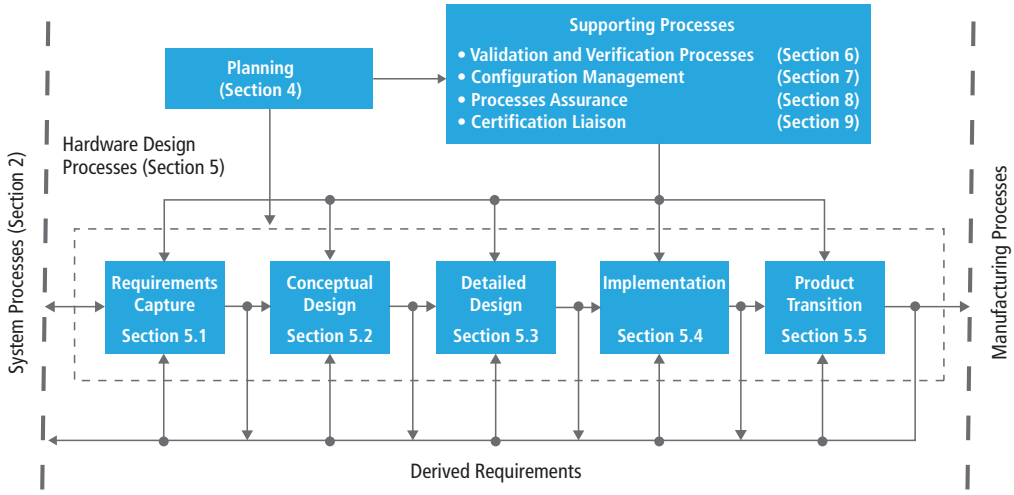

Figure 2: DO-254 flow

Let's walk through this process to briefly explain each component of this flow.

Planning

Planning is a critical piece of the DO-254 certification. It's important to document your project flow up-front and approach your certification official to gain their approval early in the project. Typically the high-level plans are documented in the Plan for Hardware Aspects of Certification (PHAC—commonly pronounced as "pea-hack"). This plan should include all aspects of your project and how you will meet the DO-254 requirements.

Requirements Capture and Validation

The DO-254 specification utilizes a requirements-based design and verification approach. This means that the entire hardware project revolves around a formal set of high-level requirements. Before any RTL is written, each of these requirements must be written down, given a unique reference name, and reviewed for a variety of criteria including understandability, testability, verifiability, etc.

Conceptual Design

At the conceptual design stage, a larger design is broken down into smaller, more manageable components. This might be thought of as a high-level block diagram. (Note: For a sufficiently simple system, the conceptual design step may be skipped or merged with the Detailed Design step.)

Detailed Design

This step is where the real design work takes place. For each component detailed in the conceptual design, the RTL hardware design should implement each and every requirement for that component. Each high-level requirement should be "traced" to the top-level RTL module implementing that requirement. This traceability can happen in a variety of ways, and it is up to the implementation team to determine the desired approach.

Separately, the verification team should create verification tests to verify that each requirement has been met by the RTL, including a message to the log file showing the expected result, the actual result seen in the simulation, and the result (pass/fail). Each test must also be linked to the high-level requirement, including the pass/fail criteria (all must pass, obviously). Constrained random testing can also be used for more complex designs; however, special care must be used to create additional verification coverage components tied to all the requirements. If you are using an advanced verification tool such as the Cadence® vManager™ Metric-Driven Signoff Platform, then the additional traceability automation needed is built into the tool.

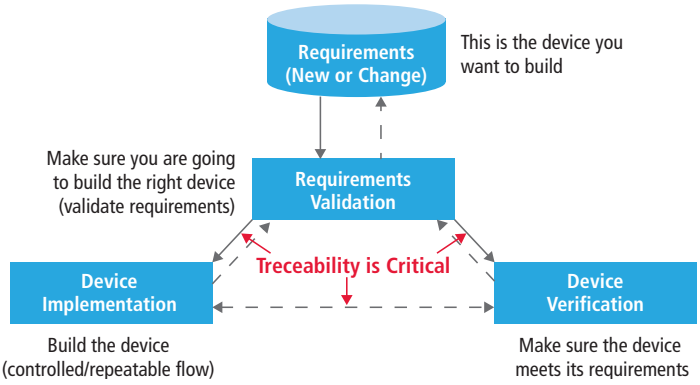

Figure 3: Requirements-driven flow, including traceability

Implementation

The implementation process is obviously technology specific. For an RTL-based design (such as an FPGA or ASIC), the implementation step includes the synthesis process of converting RTL into actual technology-specific gates. For an FPGA, this also includes creating the programming file to load into the FPGA. For an ASIC, this step includes the backend design/verification steps. Here, the main point is to follow the process detailed in your PHAC document up-front. The DO-254 specification typically allows you to remain somewhat high level while documenting your activities during implementation (especially during ASIC implementation). This is due to the fact that there will be significant testing performed on the final design.

Production Transition

This is the final stage, when you are transferring your design over to manufacturing. Typically, this ensures such aspects as:

- How can you be sure you're using the correct version of the programming file during the manufacturing process? (FPGA)

- How can you be sure you're using the correct part? (ASIC and FPGA)
- Have you properly handled any errata for the device?
- Etc.

This portion of the process can be quite complex, and can involve several systems flowing back into the requirements process tools (such as IBM DOORS), and is critically important to ensure the final system receives the results of all processes.

Process Assurance

Along with your DO-254-compliant plan, you should also document how you will ensure you will meet this plan, typically documented in a Process Assurance or Quality Assurance plan. This plan documents who will be designated as the process assurance person or organization to double check that your PHAC and other plans are followed, and how this checking will be performed.

It's important to realize that you must be able to prove that this checking happened, typically by creating a paper trail of internal meetings, reviews, internal audits, etc. Typically, a DO-254 certification official wants this process assurance performed by a separate qualified person or organization (for example, someone knowledgeable about design/verification, but not someone on this design or verification team). This person/organization must also be given the authority to carry out this process, and be provided access to the engineers and design environment.

Configuration Management

In addition to the Process Assurance plan, you should also create a Configuration Management (CM) plan. In this plan, you will document how you will ensure the development process and artifact generation process is repeatable. This typically includes a revision control and bug tracking systems for all design/verification files, as well as all documentation and artifact documents.

The DO-254 specification refers to the importance of tracking all design artifacts throughout the design process. Certification officials understand that design and verification files will go through many iterations. However, once they are stable, you are expected to "baseline" the design. In typical commercial electronics, this is analogous to a design freeze—a point in a schedule when subsequent changes are closely controlled and documented, as shown in Figure 4.

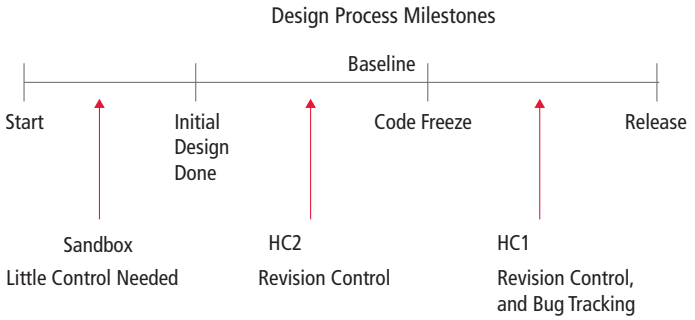

Figure 4: Design process and baselines

Certification Liaison

Typically, a single person is selected as the main communication point for the certification officials. This single point of contact enables clean communication, and ensures that the certification official obtains a clear view of the overall design process. Typically, this certification liaison has previous DO-254 experience, with the skill to communicate the details in a way that the certification official can understand.

In-Target Testing

Although not shown in the diagram in Figure 2, in-target testing is a critical component of the DO-254 specification, and is a required part of the overall flow. From a DO-254 perspective, all verification done in a simulator was performed on a model of the design. There is no guarantee that the model used in simulation

matches the actual device as it sits on the target board that will be installed in the aircraft. In addition, that simulation is typically limited and does not include the actual hardware physics such as voltage and temperature variations, as will as signal degradation, ringing, pin capacitance loading, etc.

To ensure the final device performs as expected, you must somehow demonstrate that the final device sitting on the target system that will go into the aircraft meets its requirements. In an ideal world, the certification official would like to see ALL requirements tested on the final part. However, realistically, this is frequently impossible as internal controllability and observe-ability would be required. As a result, you can decide up-front how you will address this final testing procedure against your requirements in your PHAC document, and discuss this thoroughly with your certification official to reach agreement.

Certification Officials

So, who are the "certification officials" referred to throughout this paper? There are several people that you might interact with throughout your project.

Designated Engineering Representatives (DERs) and Authorized Representatives (ARs) have FAA permission to "approve" a design. (The DER will also "find compliance" when the overall project is done and everything is in place.) DERs are typically an independent consultant or may be an employee of a company. The AR is a somewhat newer role, and is typically an employee of a larger company. Typically, during DO-254 approval audits, you will interact with a DER or AR. It's up to you to hire one if you will be handling the certification approval, but it's best to hire this person early during the planning process.

The FAA also has Aircraft Certification Officers (ACOs) to provide guidance on aircraft-certification-related activities. ACOs assist with:

- Design approval and certificate management
- US production approvals
- Engineering and analysis questions
- Investigating and reporting aircraft accidents, incidents, and service difficulties
- DER oversight

"I Still Don't Get It..."

Understanding the DO-254 specification and how to achieve DO-254 approval is, unfortunately, not as simple as downloading and thoroughly reading the document. The DO-254 specification itself is only part of the story. There are additional supplemental papers that clarify, restrict, and limit how the DO-254 specification is applied. In addition, there are follow-on papers created by other bodies such as the international Commercial Aviation Safety Team (CAST) and the European Aviation Safety Association (EASA), as well as additional regulations set by air framers such as Airbus and Boeing. There are also a variety of commonly accepted industry practices expected by certification officials. A minimal understanding of these documents and their organization is important, as these papers limit the scope, and clarify details necessary to successfully complete a DO-254 project.

The DO-254 specification was created by an RTCA committee back in the 1990s, and was written to apply to all levels of hardware, including circuit boards, resistors, and capacitors—as well as chips such as FPGAs and ASICs. So, if you simply go to the RTCA website and download and read the DO-254 specification, you'd be left with the impression that the document applies to a significant amount of electronic components in your system.

However, when the FAA enacted the DO-254 specification as policy in 2005, it chose to limit the scope to "complex custom micro-coded components"—PALs, PLDs, FPGAs, and ASICs. For example, this means an ASIC or FPGA on your board needs to meet the specification, but the board itself does not. This is described in an FAA Advisory Circular paper[2] entitled "AC 20-152." To make things more confusing, the FAA later released Order 8110.105[3] that attempted to clarify DO-254 ambiguities and firmly close several perceived loopholes.

[2]AC 20-152 is available on the FAA website: http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-152.pdf

[3]FAA Order 8110-105 is available on the FAA website: http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/73625

There are also other related documents such as the "AEH Job Aid"[4], a collection of instructions and questionnaires to help FAA-authorized auditors audit your Airborne Electronic Hardware project.

There are more documents and certification bodies that play a part, but those described above are typically the most critical papers to understand the DO-254 "big picture." In addition, the DO-254 specification is not a prescription—it only says WHAT must be accomplished, it does not try to stipulate HOW to do it.

Other Design Considerations

Although it's not explicitly detailed in the DO-254 specification, certification officials will be expecting you to design your system to adequately handle a variety of nefarious conditions, such as single event upsets on state machines, memory corruption protection (such as ECCs), block or subsystem redundancy when deemed necessary to achieve a sufficiently low failure rate, electrical isolation of different DAL circuits so a lower DAL does not disrupt a higher DAL circuit, and many other aspects required by high-reliability environments. This topic is well beyond the scope of this whitepaper, but the concept is introduced here to avoid the misconception that the DO-254 specification is strictly process oriented like the ISO 90001 specification. In your plans, you should articulate any high-level design and verification aspects you're adding to accommodate the needs of a safety-critical design, especially if the design is DAL A/B.

Don't be surprised if the certification official finds additional concerns that you hadn't previously considered, and obviously, expect to adjust your plans and methodology accordingly. If this is your first DO-254 design and you have concerns, you can also hire another DER as a consultant to help you create your initial plans and methodology. Doing so can help avoid surprises and expensive project kickoff delays.

Conclusion

Meeting DO-254 can be a laborious and expensive process, but proper up-front education and planning can significantly ease the process of achieving DO-254 approval. This whitepaper conveys the high-level concepts required by the DO-254 specification and what they mean, as well as an understanding of the various aspects and players in the DO-254 certification process. The next step in this process is learning more about automating various aspects of the DO-254 specification in the companion whitepaper "Accelerating DO-254 Approval with Cadence Tools."

For Further Information

Learn more about DO-254 and Cadence DO-254 tool offerings at https://www.cadence.com/content/cadence-www/global/en_US/home/solutions/aerospace-and-defense.html.

[4]AEH Job Aid is available on the FAA website: https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/CEH-JobAidRev022808.pdf