DO-254 Compliance: Pitfalls, Challenges and Solutions

This paper presents supplemental information to the presentation of the same title presented by Michelle Lange at MAPLD 2008.

DO-254 Background

In 2005, the Federal Aviation Administration (FAA), the European Aviation Safety Agency (EASA), and other worldwide aviation safety agencies began enforcing a new design assurance standard for hardware. This standard is RTCA/DO-254 (often referred to as ED-80 in Europe), and the official title is "Design Assurance of Airborne Electronic Hardware." The intent of this standard is to ensure safety of in-flight hardware.

DO-254 was derived from a very similar standard which applies to software, which has been applied for software design assurance for over 20 years. This other standard is called DO-178B.

DO-254 was originally written to apply to all levels of electronic design. However, the industry saw it as a very costly standard, if it had to be followed at all levels of hardware development. So the document was finished in 2000 but not officially enforced until 2005, when the FAA issued Advisory Circular 20-152. This document, known as AC20-152, stated: "This AC recognizes the guidance in RTCA/DO-254 applies specifically to complex custom micro-coded components with hardware design assurance levels of A, B, and C, such as ASICs, PLDs, and FPGAs." So today, all PLD, FPGA, or ASIC designs that will be part of any airborne system must follow the guidance given in DO-254.

While the standard currently applies to only the component level of design, it is still a costly proposition: companies can see cost increases of 25–400 percent. So DO-254 compliance is a big business concern. However, with the proper knowledge and preparation, much of this additional cost can be minimized. The intent of this paper is to highlight some of the costly issues that companies commonly stumble upon, get them out in the open, and present practical advice for addressing or avoiding them.

What DO-254 Is…and Isn't

Pretend for a moment that you are required to drive from New York to Los Angeles. You've traveled before, but never driven across the continent. You have a certain amount of money and time, and, naturally, you have to get to your destination in one piece and in good health. You are given only a map, but all the decisions about how you go about your mission are yours.

Now the map gives you a lot of flexibility. You can take freeways (but watch out for traffic jams and accidents), main roads (but watch out for construction), scenic routes (but don't take too much time sight-seeing), back roads (but watch out for wildlife, road closures, etc.). This is great! You get to choose. So what do you do?

Metaphorically, DO-254 is both your mission and the map. DO-254 provides guidance in terms of the objectives you must meet in the certification process. How you comply with

DO-254 and meet those objectives is up to you. Some people expect DO-254 to give them step-by-step process guidance. It does not. Knowing this is an important first step in the journey. You will need to do some research (read up on DO-254), talk to people who've made the same trip (those from your or other companies), maybe even talk to an expert and learn from them (a certification authority perhaps?).

DO-254 and the Aircraft Certification Process

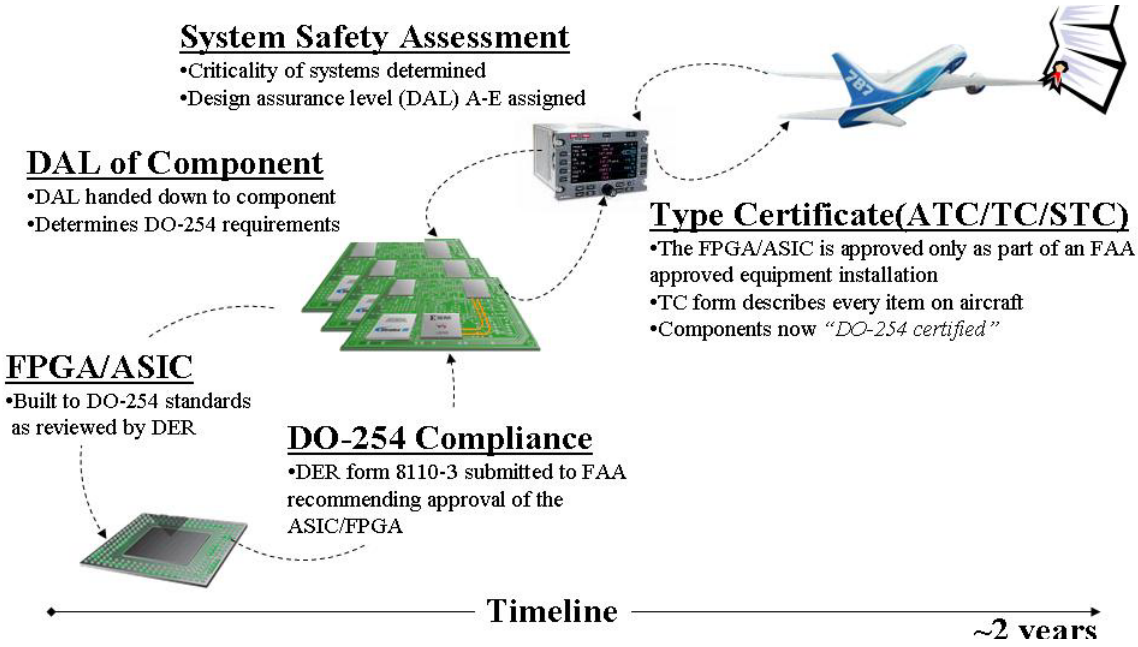
Sometimes it's good to look up from your area of focus to get a bigger view. In the case of DO-254, the engineer designing to the standard does not need to know how compliance fits into the aircraft certification process, but knowing this provides clear insight into how critical compliance is within the larger context.

This broader context encompasses an aircraft, numerous electronic systems in this aircraft, numerous boards that go into these systems, and numerous components that go into the boards. Each system in the aircraft goes through a thorough "system safety assessment" (SSA). This process establishes the criticality level of each system—in other words, the SSA determines the safety implications of each system and the consequences if that system fails.

A system is assigned a design assurance level (DAL) of A through E. Level A systems have catastrophic safety effects given a failure, while level E systems have no safety effect given a failure. These DALs are applied down to the component level. This is where the designation of DO-254 level A/B designs comes from. Thus, at the component level, the DAL has implications in terms of what needs to be followed for the DO-254 process.

The FPGA or ASIC designer works with a designated engineering representative (DER) of the FAA (in the US) to achieve compliance to the appropriate standard level. The final stage of demonstrating compliance involves testing the hardware item in the end system (usually at the board level). Once this has been done, the DER submits a recommendation for approval, called form 8110-3, to the FAA. The FAA then responds with a letter stating whether the component is DO-254 compliant.

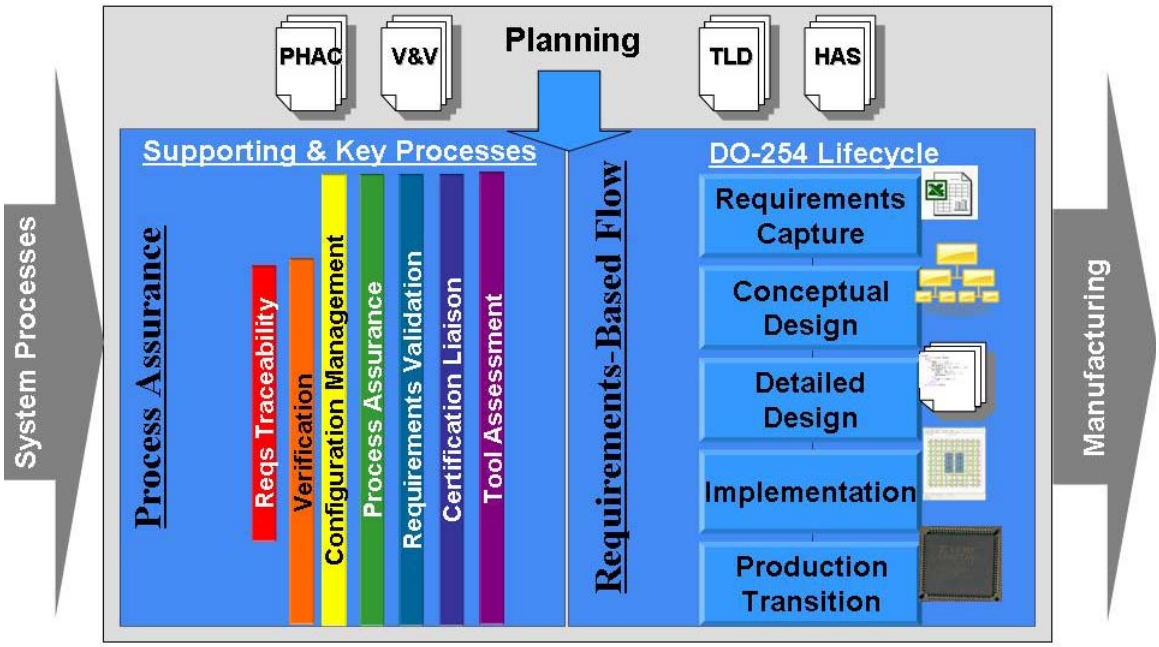
The aircraft, meanwhile, is going through extensive certification processes itself. The aircraft integrator seeks a *type certificate*, such as an ATC, TC, or STC, that says the aircraft is certified. The type certificate identifies every system, board, and component on the aircraft specifically, including the DO-254 compliant components. Once the aircraft has received its type certificate and is fully certified, the DO-254 compliant component is now DO-254 certified—but keep in mind, it is only certified in the context of this specific system and this specific aircraft. Also, this whole process (depicted in the following figure) can take upwards of two or more years to complete.



A Look inside DO-254

Now that you have the proper expectations and understand the broader context, what exactly is DO-254? Simply put, DO-254 is a requirements-based design flow with strict process assurance. In other words, the DO-254 process ensures that your end design will meet the specified requirements and you have proof that it does.

The DO-254 specification describes the Hardware Design Lifecycle, which depicts the scope and design flow of DO-254. The following figure is derived from that information.



The DO-254 process applies to everything within the outer grey box, but this process links tightly with both the system and manufacturing processes. In DO-254 terminology, the design flow is called the "DO-254 Lifecycle" and it is surrounded by "supporting processes." The design flow focuses on designing to the requirements (which are handed down from the system), and the supporting processes ensure that you did this, you can prove it, and you can repeat it.

The DO-254 process starts with an extensive planning phase. The plans produced from this phase guide all of the activities and processes that will be part of the DO-254 project.

The design flow (or DO-254 Lifecycle) itself consists of five phases:

1. The first stage is *requirements capture*, where the project requirements are captured within documents or a requirement management system, such as IBM's DOORs product.
2. The second stage in the process is *conceptual design*, where the basic architecture of the project is established, and, perhaps, a conceptual model is created and evaluated.
3. The third stage is *detailed design*. This stage covers almost the entire FPGA or ASIC design flow, starting with RTL design all the way through synthesis.
4. The fourth stage is *implementation*, where the detailed design model is implemented in silicon—however, the actual manufacturing process itself is beyond the scope of DO-254.
5. The final phase is *production transition*, where a snapshot is taken of all the data necessary to exactly reproduce the hardware item.

The DO-254 standard also mandates that *supporting processes* be followed for certification.
These processes include:

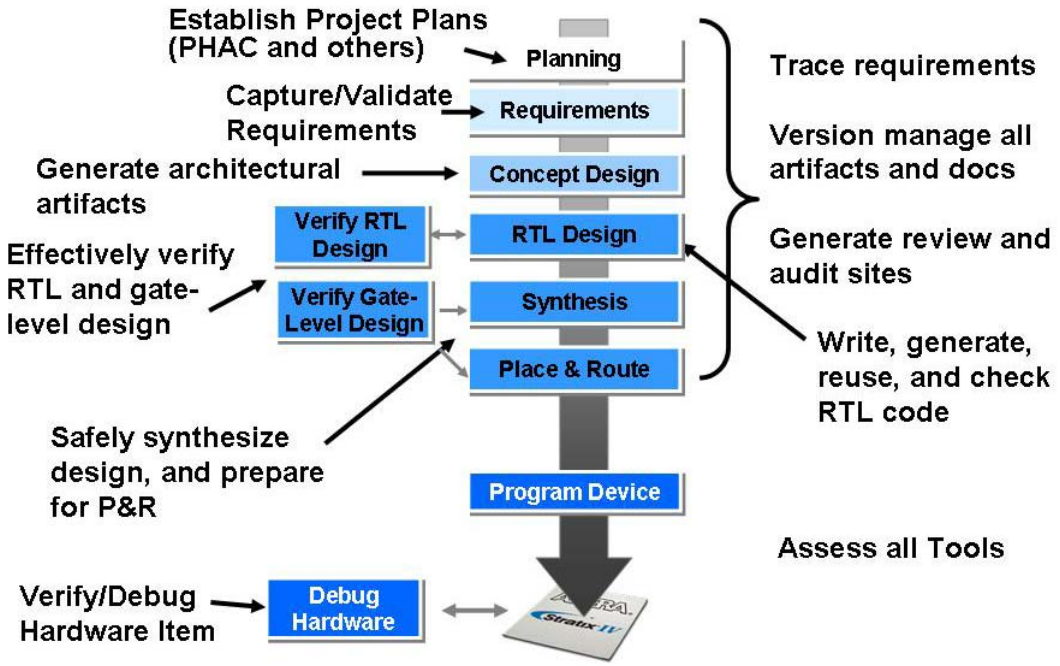
- *Requirements validation*, which means a team of people review the requirements to ensure they're correct
- *Process assurance*, where a QA person monitors the activities to ensure they are as specified in the plans.
- *Certification liaison*, where the designer works with a certification authority throughout the process and conducts audits, as well.
- *Configuration management*, which ensures all the information, design data, and documents are kept under strict version control.
- V*erification*, which checks that the design actually does meet the requirements.

Two other very important processes that are described in DO-254, but not explicitly called out as supporting processes, include:

- *Tool assessment*, which ensures that the tool or tools used in these processes are appropriate and accurate.
- *Requirements traceability*, which ensures that the design and test data all map to the requirements, and vice versa.

A DO-254 Compliant Design Flow

Now, how do you take all of this information and apply it to your FPGA design flow? The following figure shows much of what must be incorporated into a typical FPGA flow in order to achieve DO-254 compliance.



These items are summarized in the following list:

- *Establishing project plans* involves a lot of upfront investment to determine the best way to meet the DO-254 objectives using a high-quality and efficient design flow. All of your decisions will be documented in the planning documents. The main plan is called the "Plan for Hardware Aspects of Certification" (PHAC).
- *Requirements management* is a crucial element woven into the DO-254 design flow. You must have a mechanism to capture requirements and processes to validate them.
- *Conceptual design* involves planning the architecture of the device to meet the specified requirements and capturing the artifacts that represent this architecture.
- *RTL design* involves either writing code or safely reusing code and checking the quality of this code against a set of defined standards.
- *Effective verification* is essential to producing a high-quality design. Verification should be done upfront as much as possible on the RTL and gate-level design, as well as on the physical hardware product itself.
- *Synthesis* is a part of every design flow, but steps should be taken to ensure that the process is done with safety in mind.
- *Requirements traceability, configuration management* (of the design and process artifacts), and *reviews/audits* are all done throughout all of these design stages.
- *Tool assessment* must be performed on all tools that automate manual work.

Common Pitfalls and Recommended Solutions

Many folks stumble on very similar issues when they begin their journey towards creating and executing DO-254 compliant design projects. The good news is that each of these issues has solutions. Some of these common pitfalls, along with advice for addressing them (based on learnings from successful DO-254 programs), are described here.

Companies are engaging in DO-254 programs without proper preparation.
This situation leads to many missteps and rework, failed audits, and costs escalating potentially up to 400 percent. In order to address this, invest in training and/or consulting. DO-254 is an ambiguous document and trying to figure out how to comply without the help of experts will result in much wasted effort. First, invest in training for the key team members (and ensure you're taking training from a reputable company—check around). Next, start working with your DER early on. Don't wait until you are through planning and are ready for your first design audit before you have a conversation with your DER. This is bound to lead to much rework and frustration. Finally, while in the early stages of planning, do some assessments of your current methodologies. A DER can do a *gap analysis* of your existing process to show you how far off you are from compliance and can provide advice and/or a plan to get you on track. Likewise, other experts can help you analyze your design flows for efficiencies by doing *methodology assessments* to improve your methods and resource productivity. Seek all the help you can get—before you get started.

Companies think they can "get around" DO-254.
Getting around DO-254 means your hardware component won't be allowed for use in airborne systems. It's very simple. If your company wants to sell into this market, it must comply. Don't waste time trying to find ways around DO-254. Use your time and resources wisely to build expertise and become a credible supplier to this market.

Requirements traceability is a reactive process.
This is one of the leading causes of failed audits, resulting in much rework and increased expense. Requirements traceability must be a proactive, well thought out effort. It should not be an after-thought, left to an intern or junior employee to try to create a paper trail of what was already done. Requirements management and traceability is a very important aspect of DO-254 flows, you should be proactive in terms of defining the process that you will use and how it will be integrated into the design flow. You can also seek help from some new tools on the market that automate these traceability requirements.

Groups within a company don't talk and share information.
This is a common practice that leads to wasted resources, as each group has to reinvent the wheel. Instead, share information. Find others in your company who are experts. Share your expertise with the industry. Join the DO-254 User's Group. Write papers on your successes and what you've learned.

Companies don't consider reuse or future uses of current design.
This can lock a design out of reuse in a future project and/or can cost the company a lot of money in re-certification costs. If your component may be reused in future systems, design to the highest level of compliance to open doors for inexpensive reuse.

Companies struggle with verification.
This is probably the single greatest challenge of today's design flows. If you don't have an effective, high-quality verification methodology, your company cannot assure a high-quality product and risks damaging its reputation, or you might lose bids or avoid complex projects altogether. To address this issue, ensure your verification methodology can handle the complexity of your designs. Verification methodologies have evolved rapidly over the past decade, keeping pace with the needs of complex designs. Ensure you're up to speed by reading up on state-of-the-art methodologies and tools. Seek expertise in terms of evaluating your process by getting a verification methodology assessment. Bring in consultants who can revamp your methods and train your team.

Tool qualification is difficult.
Many companies end up making this task harder than it has to be, spending too much time on it. First, you should understand the intent of tool assessment and qualification, along with its process and options. Much information is published on this. You have several options for getting through the flow. Understand the best option for your situation. Generally, "independent output assessment" is the best approach because instead of performing a "quality assurance" role on a vendor tool, you're building process assurance into your flow, which is really the intent of DO-254 in the first place. Also, while the task of tool assessment really falls on the hardware application, don't be afraid to ask your tool-vendors for help. Those who take this market seriously will provide advice, assistance, or even compliance kits. If your tool vendor doesn't know what DO-254 is, find a tool vendor that does.

Conclusion

DO-254 is a new hardware design standard for airborne electronics. While this standard can increase costs due to the added design assurance it requires, this cost can be minimized by understanding DO-254, gaining experience using it, and working with partners who are knowledgeable and who care about the needs of this market. This paper provided an overview of the standard, talked about some of the challenges and pitfalls, and provided advice on how to build expertise and develop DO-254 products as cost-effectively as possible.

About the Author

***Michelle Lange**, the DO-254 program manager at Mentor Graphics Corporation, has held various technical and business-oriented roles in the field of electronic design automation (EDA) for over 18 years. Michelle has a BSEE from the University of Portland and an MBA from University of Phoenix.*

About Mentor Graphics

Mentor Graphics® is a technology leader in electronic design automation (EDA), providing software and hardware design solutions that enable companies to develop better electronic products faster and more cost-effectively. The company offers innovative products and solutions that help engineers overcome the design challenges they face in the increasingly complex worlds of board and chip design. Mentor Graphics has the broadest industry portfolio of best-in-class products and is the only EDA company with an embedded software solution. Mentor's worldwide web site is www.mentor.com and DO-254 specific solution information and publications can be found at www.mentor.com/go/do-254.