cadence®

Accelerating DO-254 Approval with Cadence Tools

By David Landoll, Cadence

This white paper, the second in a series of DO-254-related white papers, will explore software tools as they relate to meeting the DO-254 Design Assurance Guidance for Airborne Electronic Hardware specifications, and what steps must be performed in order to use your typical design automation tools such as simulation, synthesis, etc. In this paper, we will explore how DO-254 views tools, learn which tools receive the highest scrutiny and why, and how to manage the tool assessment/qualification process.

Contents

Introduction

In the previous "DO-254 Explained" whitepaper, the core concepts of DO-254 were introduced and explained. In this paper, we'll explore more practical applications of tools and methods that accelerate DO-254 design completion while still conforming to DO-254 goals and objectives. As a reminder, DO-254 is a process-oriented methodology based on meeting high-level requirements, and demonstrating process conformity through Process Assurance records and artifacts. (If this doesn't make sense to you, please go back and re-read the first white paper).

The overall DO-254 flow can be summarized with the diagram shown in Figure 1. On the left are the standard industry names for the various steps in the flow, followed by the steps as they are named in the DO-254 spec, followed by the "supporting processes" of verification, validation, requirements management, and traceability, etc. A new concept, the stage of involvement, is introduced here with the "SOI Reviews". These reviews are the audits performed by the FAA authorized representative (DER or AR). Typically, there are four audits, but this is only a guideline. In reality, two or more of the audits can be combined into a single audit. The diagram shows the most typical places these audits occur, but they frequently happen at other points in the project, and sometimes can even occur well after the program has been completed. It's important to have the first audit as early as possible, in order to obtain plan alignment with the FAA/DER/AR official auditing the remainder of the project. The SOI-1 audit might simply consist of submitting electronic copies of the planning documents to the designated official.

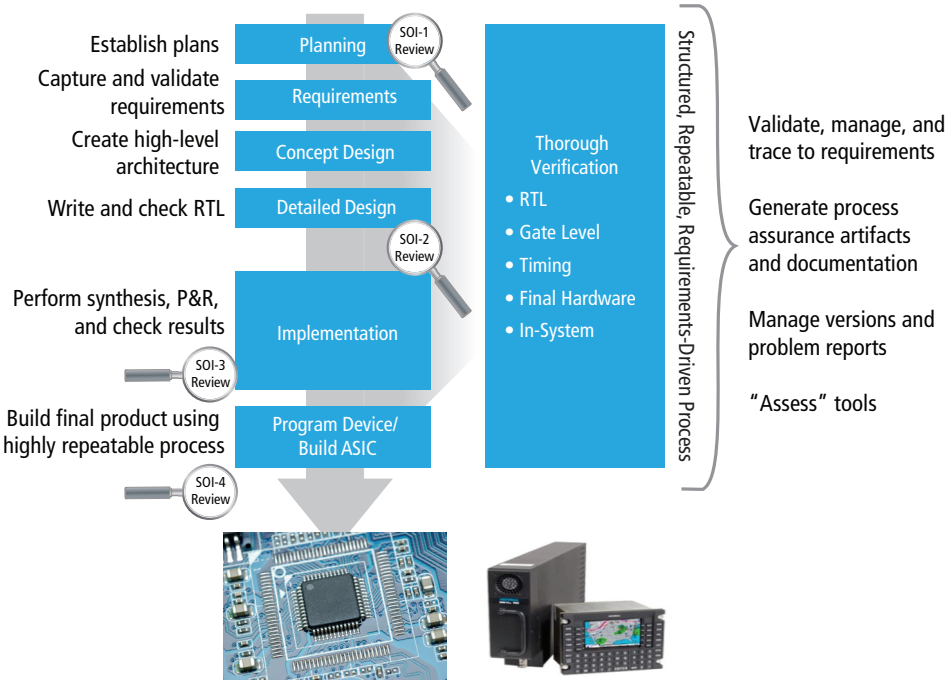

Figure 1: Overall DO-254 flow

So, now that we've reviewed the overall flow through DO-254, how can we accelerate the design, verification, and requirements management process while still meeting DO-254?

Which EDA Tools Can Be Used for DO-254?

A commonly asked question is, "Which of my typical design and verification tools can I use on my DO-254 project?" The answer? All of them! DO-254 does not place ANY restrictions on what tools you can or can't use on a safety-critical project. Instead, DO-254 places various processes in place to check that the tools are operating correctly during the design and verification process.

The general DO-254 philosophy is that tools that can introduce an error are more suspect than tools that are simply checking the design. So, for example, a tool generating RTL will receive more scrutiny than a tool that is simulating RTL.

Manual work is generally considered the gold standard, where one person will perform a task, and a second person will review that task. Any time a tool reduces or eliminates a manual task, that tool must go through a "tool assessment" process to ensure the tool is operating correctly. Realistically, this process includes all commonly used design automation tools (simulation, synthesis, etc.), but it doesn't have to be as daunting as many people think.

Tool Assessment vs. Tool Qualification

Many people incorrectly think that to use a tool on a DO-254 project, it must go through "tool qualification". Tool qualification is a fairly rigorous and time-consuming process where you essentially prove the tool at hand is operating correctly within the project environment. For a simulation tool, this might include testcases designed to demonstrate that the simulator is operating correctly, and failing with adequate error messages when the input is erroneous. Needless to say, this could be an onerous task with today's highly complex EDA tools. However, the original authors of DO-254 never intended people to actually go through the tool qualification process except in extraordinary cases.

All tools have to go through the "tool assessment" process, however, as Figure 2 shows, only certain tools require further scrutiny. If you're doing a DAL A/B/C project (highest 3 DAL levels), then your design tool assessment needs to go through the rest of the flow diagram. For verification tools, you only need to proceed through the rest of the assessment diagram if you're verifying a DAL A/B project (very highest safety levels).

"Tool assessment" includes several possible activities: independent output assessment, relevant tool history, or tool qualification . We'll discuss each of these in turn. Figure 2 shows the tool assessment flow.

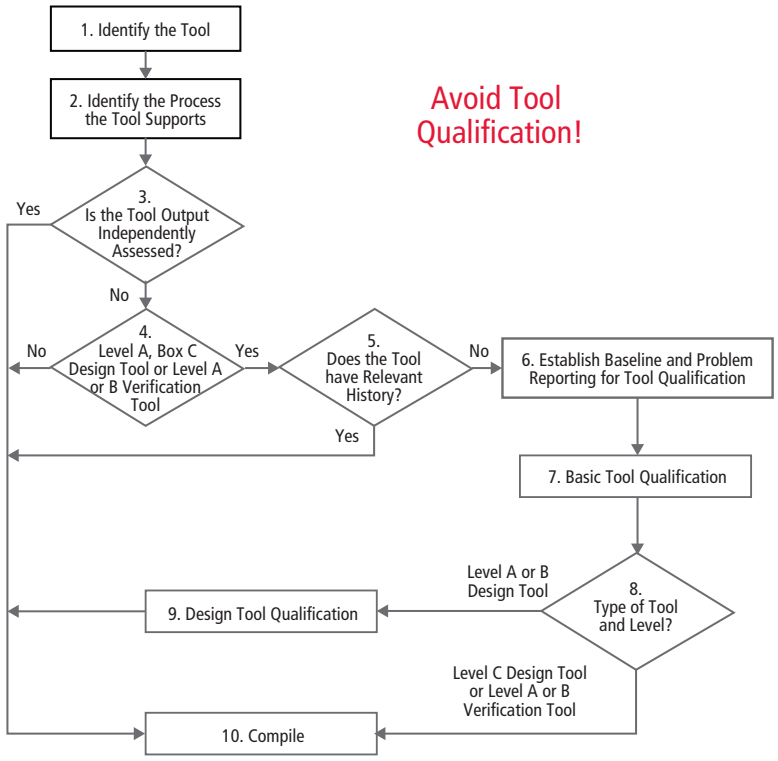

Figure 2: Tool assessment flow

Tool Assessment—Independent Output Assessment

As the diagram shows with my slight additions, independent output assessment is the most common method of performing tool assessment. This simply means that a human reviewed the output of the tool to ensure the tool is operating correctly, or the output of the tool was somehow double-checked by another tool. Ideally, you should utilize a "layered approach," where you have multiple levels of tools double-checking each other. However, this is likely already being accomplished by the tool flow you have in place now. For example, to perform the tool assessment on a synthesis tool, you can perform simulation on the RTL netlist (the input to synthesis) versus simulation of the gate-level netlist (the output of the synthesis tool). If you use the same simulation test (the same simulation vectors), and the simulation at RTL level and gate level both pass, then that's a measure of "independent output assessment" of the synthesis tool (see Figure 3). Likewise, to perform tool assessment on a simulation tool, you can argue that the RTL- and gate-level simulations matching is a measure of independent output assessment of the simulator. That the simulator can be demonstrated to work on two logically equivalent but different netlists is an indication that the simulator is installed and working correctly. Leveraging emulation results that also match, and actual lab testing on the final part with similar input stimulus generating the same result, can strengthen this argument. There are many other ways to achieve independent output assessment, but hopefully this will provide you with some details to get you started with the thought process.

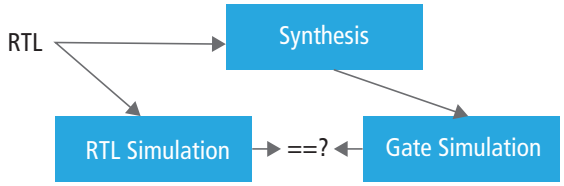

Figure 3: Synthesis tool assessment example

Tool Assessment—Relevant Tool History

If you can't or don't want to perform independent output assessment, then the next point in the diagram is "relevant tool history". One might think this should be straightforward, especially if you've been using a particular tool for a long time on previous projects, and it's heavily used in the industry. However, in reality, few DO-254 applicants find this approach successful. The tool in question must be the exact same version of the tool, used on a similar design that has history. Even updating to a later version of the tool can negate this argument. Relevant history can, however, create a useful argument to further strengthen other tool assessment activities. For example, you can claim a certain amount of independent output assessment activity, and further argue that the tool in question also has a tremendous amount of history in your group on relatively similar projects and in the industry as a whole. This kind of layered approach is generally a good idea, as it provides multiple layers of analysis arguments. Even if your FAA/DER/AR official isn't happy with some portion of your tool assessment argument, you'll likely still have additional layers supporting your tool assessment analysis that remain intact.

Tool Qualification

As the diagram shows, tool qualification is your final and last option. The authors of DO-254 did everything in their power to help the applicant avoid tool qualification if at all possible, due to the pain typically involved in performing tool qualification. There are rare cases when you will have to proceed with tool qualification for various reasons. However, if you do find yourself thinking you need to perform tool qualification, you'd be wise to go back just one more time and double-check whether or not you can find a creative way to utilize independent output assessment, as it's typically simpler, easier, less time consuming, and less resource intensive. Your schedule and budget will thank you for it.

To perform tool qualification, you'll need to somehow create testcases for the tool, and then demonstrate that the tool operates correctly with these testcases (both positive and negative testcases, demonstrating that the tool generates correct output, and generates some kind of error message or operates correctly even in the presence of incorrect input stimulus). You'll need to be able to argue to a certification official that these testcases cover the aspects of the tool used by your project. You do not typically have to cover aspects of the tool that you will not be using, however you may be required to somehow show that the other aspects of the tool do not interfere in any way with your expected tool usage. For example, if a synthesis tool is capable of performing register retiming, but you do not plan to use this feature, you likely do not need to create testcases demonstrating that this aspect of the tool operates correctly. However, you might need to demonstrate that this feature is turned off by default, and somehow test that this option is actually not operational during your synthesis process.

Cadence Tools in the DO-254 Flow

Cadence has tools and solutions covering all front-end and back-end procedures. Figure 4 shows a common tool flow for a typical project, and Figure 5 shows the same flow leveraging Cadence® design and verification solutions.

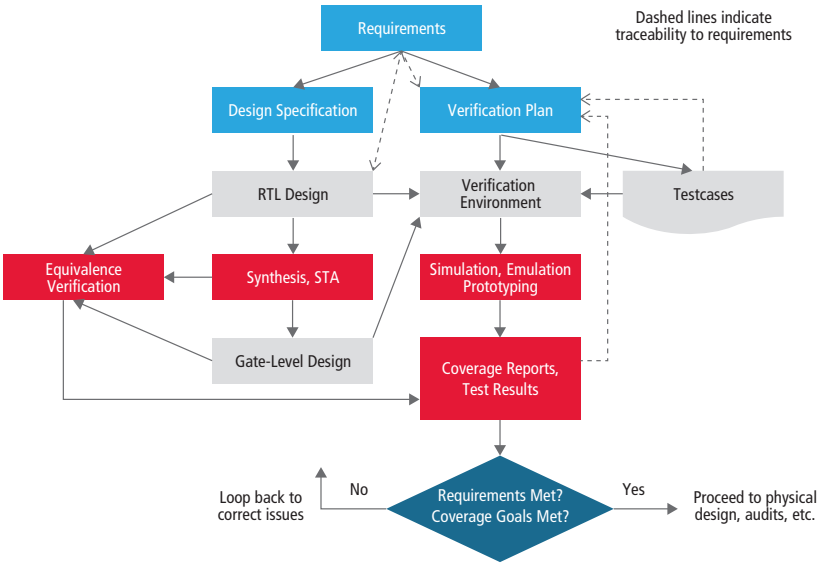

Figure 4: Common generic tool flow diagram

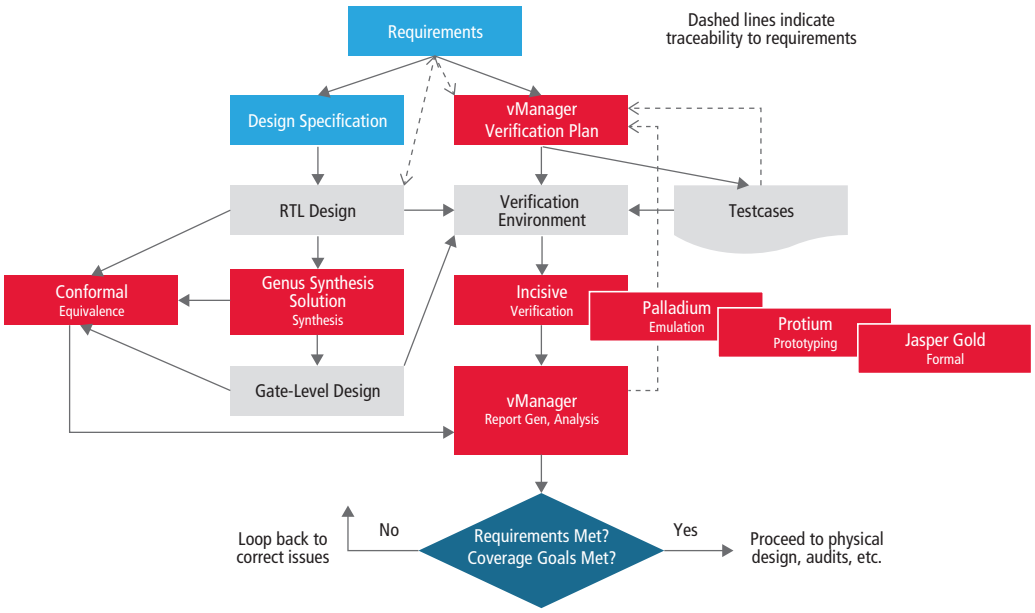

Figure 5: Tool flow diagram leveraging Cadence tools

Figure 6 describes the Cadence tools at a high level, including a brief description of functionality, as well as their inputs and outputs. (For more information on each solution, click on the links provided.)

Tool	Name	Function	Inputs	Outputs
Verification planning/ management	vManager™ Metric-Driven Signoff Platform	Provides verification planning and management; Links verification plan, tests, and tools; manages regression and status	Verification plan plan to test mapping	Reporting for DO-254 SOI reviews, simulation data for live or offline debug
HDL simulation	Incisive® Enterprise Simulator	HDL simulation tool that executes testbench and computes design response	HDL design, HDL testbench, debugging and configuration files	Simulation response data, error, and status messages
HDL emulation/ICE	Palladium® Z1 Enterprise Emulation System	HDL emulation hardware platform that executes testbench and computes design response, also capable of in-circuit emulation	HDL design, HDL testbench, debugging and configuration files	Emulation response data, error, and status messages
FPGA prototyping	Protium™ Rapid Prototyping Platform	HDL emulation hardware platform that executes testbench and computes design response, also capable of in-circuit emulation	HDL design, HDL testbench, debugging and configuration files	Emulation response data, error, and status messages
Formal verification	JasperGold® Apps	Mathematically formal methods for property proofs; including deadlock, reachability, cross clock domain checks, and unknown propagation	HDL design, properties, configu-ration files	Property check outcome reports, error messages
RTL synthesis	Genus™ Synthesis Solution	RTL/gate-level synthesis tool produces a constraint-optimized gate-level netlist	Constraints, HDL design, target technology library	Optimized HDL design, error messages, timing, area, power reports
Equivalence	Conformal® Equivalence Checker	Performs formal equivalence check between two HDL descriptions (RTL or gate level)	Two HDL design descriptions, technology library(s)	Report in mismatches, error messages

Figure 6: Cadence tools typically utilized in a DO-254 flow

Summary

Hopefully you now better understand DO-254, what it is, and how it views your design and verification tools, as well as how Cadence tools and solutions support this avionics standard. Using the tool assessment guidance provided within this whitepaper, your standard tool flow will likely provide a good starting point for your tool assessment plan, and you will likely just need to leverage this flow and activities into your DO-254 planning documents, and collect evidence that you performed these steps.

Cadence has a full suite of tools and solutions that are readily usable toward DO-254 projects of all DAL levels. Cadence tools and solutions can accelerate your design and verification process, while still fully conforming to DO-254 regulations.

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