SIEMENS
Ingenuity for life

Siemens Digital Industries Software

How Do You Qualify Tools for DO-254 Programs?

Executive summary

This paper describes the terminology and requirements related to tool qualification specific to the safety-critical programs governed by DO-254 compliance. It also provides some practical examples of tool qualification processes and strategies for commonly used tools.

Michelle Lange and Tammy Reeve, Patmos Engineering Services
Jacob Wiltgen, Siemens EDA

Introduction

Tools used in the design and verification of electronics have played a huge role in the dramatic evolution of these devices over the past few decades. Afterall, there is a limit to the amount of work and detail that even a good aerospace engineer can handle, but add the use of tools, and the sky (pun intended) is the limit.

While the use of state-of-the art development tools has led to ever increasing design complexity, the use of modern verification tools has at the same time made these complex designs more reliable. In addition, lifecycle management tools have facilitated management of both the development process and data. All these types of tools have been essential in modern avionics development.

While tools make amazing designs possible, what happens when you need to "Qualify" these tools? What does that even mean? How much work is it? Is it worth it? These are common questions asked by tool users subject to RTCA/DO-254 compliance. Companies, like Siemens, who provide tools that are of great benefit to the goal of safety (such as in the aerospace domain), must understand and support their tools in the context of these programs. This paper describes the terminology and requirements related to tool qualification specific to the safety-critical programs governed by DO-254 compliance. It also provides some practical examples of tool qualification processes and strategies for commonly used tools.

Policy

Complying with DO-254 provides a means for avionics designers to demonstrate that their designs meet the rigorous design and safety requirements for airborne electronics mandated by the FAA, EASA and other worldwide certification agencies. (To purchase the DO-254 document from the RTCA organization, click here. For a short, complementary overview of DO-254, click here.)

So what does DO-254 say about tools? First, as part of project planning, you must identify the tools you plan to use in the context of the hardware design life cycle processes and how you intend to use them. This is summarized in the Plan for Hardware Aspects of Certification (PHAC) and then typically elaborated on in the specific document focusing on each part of the development process; for example, the Hardware Design Document may describe the detailed process for using development tools such as code generators and the Hardware Verification & Validation Processes Document may describe the detailed process for using verification tools, such as simulators. See DO-254 Section 4 for more information on the documentation requirement of tools within the planning process. Second, tools must be part of the configuration management processes of DO-254. See DO-254 Section 7 for more information on the configuration management requirements for tools. Third, you must adhere to the requirements of "Tool Assessment and Qualification," which is the real focus of this paper.

DO-254 Section 11.4 is entitled "Tool Assessment and Qualification." To understand this content, it helps to understand the terminology used. Tool assessment means examining the role of the tool in the design process and determining if it needs to be qualified. All tools must be assessed. Tool qualification means demonstrating that the tool produces the expected outputs. Not all tools must be qualified. All too often these two terms are equated, and tool users may end up performing more work than required as a result.

Next, to understand the point of all this, it helps to be reminded that DO-254 is a design assurance standard. Design assurance requires multiple layers of review and verification within the development process to ensure safe operation of the design being produced. This means when an engineer is doing design work, his/her work is always being reviewed and verified, usually in numerous ways – depending on the safety criticality as indicated by the design assurance level, or DAL. When tools automate processes that an engineer would normally perform, then these tools need some checks and balances as well. This is where tool assessment, and in some cases, qualification, fits in. To quote from DO-254, "The purpose of tool assessment and qualification is to ensure that the tool is capable of performing the particular design or verification activity to an acceptable level of confidence for which the tool will be used."

DO-254 11.4 presents a flowchart of the "Tool Assessment and Qualification" process. In truth, it's not as straightforward as it could be. In short, it means project teams have to do the following.

- Identify all the tools used in your development process.
- Describe how they are being used, including identifying if they automate design work or verification work. (Note that design and verification are key designations of tools and depending upon which category a tool falls in, the assessment and qualification process may be different.)

- Look at the output of the tool and see if some other aspect of the process verifies the tool output – note: this is a very key step.
  - o If so, document this and you're done.
  - o If not, continue evaluating if qualification is needed.
- Determine if qualification is needed as follows
  - o If the tool is NOT a DAL A/B/C design tool or DAL A/B verification tool, then you're done.
  - o If it is, continue evaluating.
- If the tool has "Relevant History" (explained further below), then document it and you're done.
- Otherwise, you need to perform the following:
  - o Set up a baseline and problem reporting for the tool(s).
  - o Perform a basic qualification (explained further below) for verification tools used in DAL A or B projects and design tools for DAL C projects.
  - o Perform a design tool qualification (explained further below) for design tools used in DAL A or B projects.

It is important to note that the steps above attempt to simplify the concepts presented in the DO-254 flow chart, which is re-created in Figure 1.

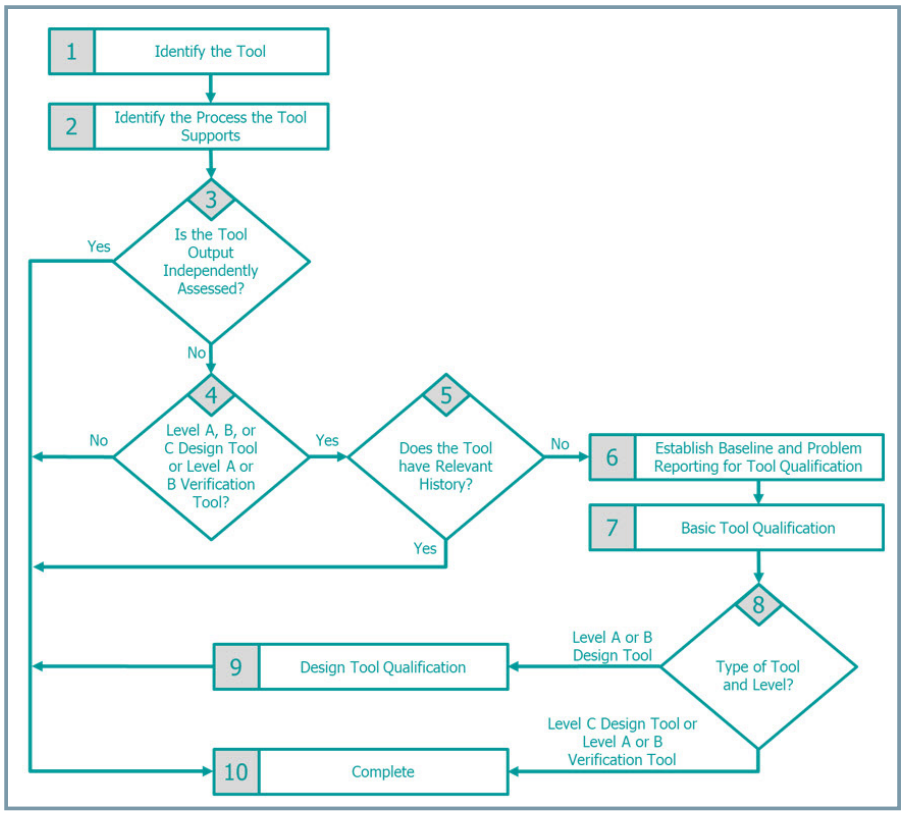

Figure 1: DO-254 Tool Assessment and Qualification Flow Chart

Nuances of Tool Assessment & Qualification

The flowchart and text of DO-254 are important to understand and acknowledge, but they do not tell the whole story. To fully understand DO-254 tool assessment and qualification, you must understand some of the related terminology and nuances.

Assessment Methods to Avoid Qualification

In examining the description and flow chart, its clear that tool qualification isn't always a requirement. Independent assessment and relevant history are often presented instead of qualification. DO-254 describes independent assessment as a method that "verifies the correctness of the tool output using an independent means." DO-254 describes relevant history as demonstrating that a tool has been "previously used and has been found to produce acceptable results."

Both of these terms have little further description, and clever project teams (i.e., applicants) have, throughout the years, cited these as reasons why tool qualification is unnecessary – often without sufficient evidence. As a result, the new policy document (published by EASA, and harmonized and soon to be published by the FAA), AMC 20-152A, which must be used alongside DO-254, adds some clarity and additional objectives to these aspects of tool assessment. These additional objectives, which apply to "Complex Designs" only (and thus the "CD" prefix) are included here verbatim.

Objective CD-10

When the applicant intends to independently assess a tool output, the applicant should propose an independent assessment that verifies the tool output is correct. The independent assessment should justify that there is sufficient coverage of the tool output. The completeness of the tool assessment should be based on the design/implementation and/or verification objectives that the tool is used to satisfy.

Objective CD-11

When the applicant intends to claim credit for the relevant history of a tool, sufficient data should be provided as a part of the tool assessment to demonstrate that there is a relevant and credible tool history to

justify that the tool will produce correct results for its proposed use.

AMC 20-152A also clarifies (or possibly adds more confusion) to relevant tool history stating that it alone may be insufficient to avoid tool qualification and should only be used compensate for gaps in other approaches.

Basic Versus Design Tool Qualification

If you are not able to demonstrate independent output assessment and/or relevant history, you must qualify the tool. Depending on the tool type and DAL, its either a basic qualification (DAL C design tool or DAL A/B verification tool) or design tool qualification (DAL A/B design tool). Project teams looking for guidance may be disappointed since DO-254 does not say much about either of these.

For Basic Tool Qualification DO-254 says "Establish and execute a plan to confirm that the tool produces correct outputs for its intended application using analysis or testing." In common practice this means defining the tool functions as "Requirements" and testing these requirements to prove the tool works. For Design Tool Qualification, DO-254 points the user to "the strategies described in Appendix B of this document, the tool qualification guidance of RTCA DO-178B / EUROCAE ED-12B for software development tools or other means acceptable to the certification authority." In other words, the applicant/tool user is left to figure this out on their own, perhaps looking at either the somewhat obscure methods presented in Appendix B or what's now in DO-330 (a supplement to the newer version of document DO-178C for software, focusing exclusively on Tool Qualification). Whatever method proposed is subject to the scrutiny of the authorities, who are notoriously stringent about the efforts for Design Tool Qualification. (Hint: Don't despair! Keep reading to learn how to avoid Design Tool Qualification).

Tool Features

Additionally, ED-80/DO-254 states "It is only necessary to assess those functions of the tool used for a specific hardware life cycle activity, not the entire tool." In other words, you only need to assess what you use. As an example, a functional simulator today has a suite of features supporting multiple languages, debug and visualization, digital and mixed-signal designs. In the event the design is entirely digital, the features enabling simulation of analog circuits coded in SV RNM, Verilog-A, etc. would not be utilized and therefore would not be assessed. In addition, if a tool has both design and verification features, DO-254 allows you to separate those features, which may provide some advantage.

Leveraging Tool Flows

DO-254 states "The tool assessment and qualification process may be applied to either a single tool or a collection of tools." A tool flow, sometimes referred to as a toolchain, is comprised of a set of independent tools deployed together to perform a complex task. As it pertains to DO-254, this set of tools forms a toolchain, which takes project teams through planning, requirements, design modeling, design creation, verification and validation, and through backend processes such as RTL Synthesis and Place and Route. Commonly, the outputs of one tool or set of tools form the inputs to the next tool in the chain. Below is a graphic of a traditional FPGA development flow. At each stage, one or more development tools will be deployed to accomplish the objective.

As shown in Figure 2, the development lifecycle consists of a tool chain and often has multiple, overlapping stages of verification to ensure the design does what it's supposed to. As an example, project teams frequently want to take credit for requirements-based testing at an RTL level of design abstraction. Fortunately, this can be done, but you are required to demonstrate that the testing results at the RTL level are valid. To accomplish this, you run at least a sufficient subset of the tests in a gate level simulation environment and/or execute those tests on hardware. Figure 2 shows this concept, and these multiple layers of verification on the verification results (which is the tool output) mean that the tool

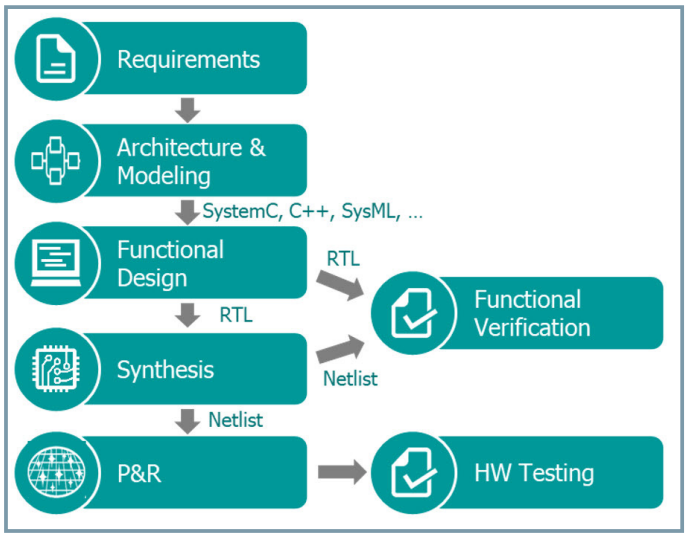

Figure 2: Sample Tool Flow

output is "independently assessed" and therefore qualification is not needed. The trick is to ensure proper evidence, which usually requires tracing verification results (from multiple verification methods/stages) to/from requirements, comparing results from the various verification processes, and documenting all this.

Legitimate Strategies to Avoid Design Tool Qualification
First and foremost, design tool qualification in DO-254 programs can nearly always. All you need to do is ensure that somewhere in your downstream process, you have one or more steps in your development process that verifies the results delivered from such a tool. DO-254 itself even suggests this, stating "Using such a design tool without independent assessment of the tool's output or establishing relevant history is discouraged..." For example, if you are using a code generator on a DAL A/B design, you would have to both review the output from the tool (since code must be reviewed in a DO-254 process) and verify the generated code (through simulation or other means, along with target hardware testing – which should already be processes in your development flow). Performing these activities would provide independent assessment of the code generator's tool output and thus allow you to avoid design tool qualification.

Qualification for Synthesis, Compilers, and Place-and-Route Tools
Synthesis, Compiler, and P&R tools migrate a design from one level of maturity to the next. A synthesis tool consumes a design model commonly described in one of the RTL languages (Verilog, System Verilog, VHDL), and synthesizes the design into a gate level netlist. DO-254 requires verification as the design matures from RTL to gates and all the way until the function is loaded on the airborne target. Given this, it is accepted across the industry that the testing performed throughout this process is inherently ensuring the design function is still behaving per the requirements, and therefore, tool qualification of Synthesis, Compilers, and Place and Route tools is not required.

Qualification for Tools that Verify Coverage
There is a special category of verification tools whose purpose is to verify coverage. DO-254 states that tools "used to assess the completion of verification testing" do not require qualification. AMC 20-152A further clarifies and confirms the "exclusion of tool assessment/qualification activities for code coverage tools only when they are used to assess whether the code has been exercised by requirements-based testing/simulations (elemental analysis)."

Basic Guidelines and Siemens Examples

Below are a few examples of Siemens verification tools in a toolchain utilized within DO-254 development lifecycle.

Figure-3 shows the Questa simulator and the Veloce prototyping system as two methods of verifying a design's function by two distinct methods at two distinct levels of the design flow. Some project teams believe that they must qualify their simulator, but this is rarely the case given multiple verification and test activities required throughout the flow, as explained earlier. A functional simulator is independently assessed by comparing the results of a single test executed on different design models (RTL, Gates, Bitfile, etc.). The primary means of verifying the results of previous simulations should be physical testing -- as much as reasonable. The example above highlights how the Siemens Questa Simulator is independently assessed when comparing the results of Veloce prototyping test. It would also or alternately be assessed against the results of the same test executed in hardware on the primary device (target hardware).

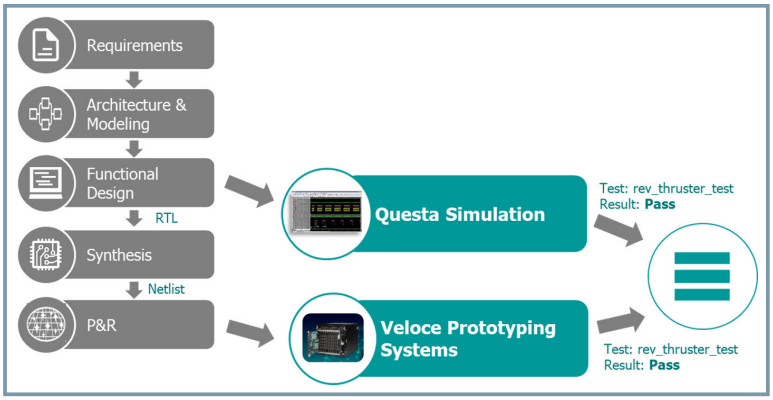

Figure 3: Independent Assessment of a Simulator

Another example highlights how to leverage formal equivalence checking to assess design transformations made during synthesis and P&R tools. The example in Figure 4 demonstrates how OneSpin EC-FPGA performs equivalence checking between different stages of the FPGA development flow. If there was any question as to a tools' abilities to appropriately transform the design from one format to another (e.g., from RTL to netlist via synthesis) as a matter of safety, this method is an excellent independent assessment of that tool function.

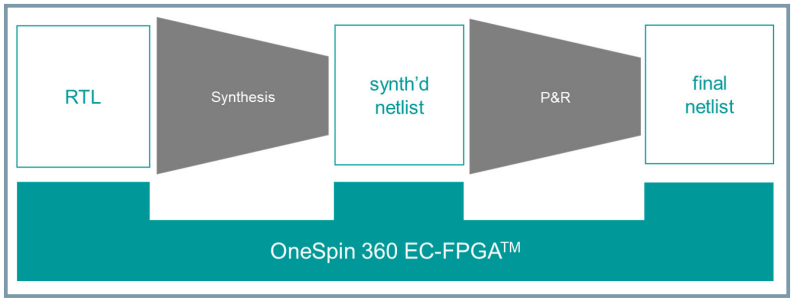

Figure 4: Equivalence Checking across Levels of Design Maturity

A final example is the Siemens EDA Questa Lint solution. DO-254 Section 10.2 specifically states "Tools may be used to enforce standards." Questa Lint is a special type of verification tool with a built-in code checker and incorporates the DO-254 User's Group recommended HDL coding rule set (or design standards employed for RTL type design). In this situation, the design flow typically will not offer an independent assessment of this capability. Therefore, you must devise a strategy for basic tool qualification. The easiest way to do this is to define each "standard" or HDL coding rule being checked as a "requirement" and then create a series of tests to demonstrate the tool is catching compliance (both positive and negative) to the standard.

Siemens Tool Flows

Figure-5 provides an overview of the Siemens EDA DO-254 Platform and toolchain. This overview, while not exhaustive, summarizes the stack of software solutions and services available to project teams at each phase of the development lifecycle.

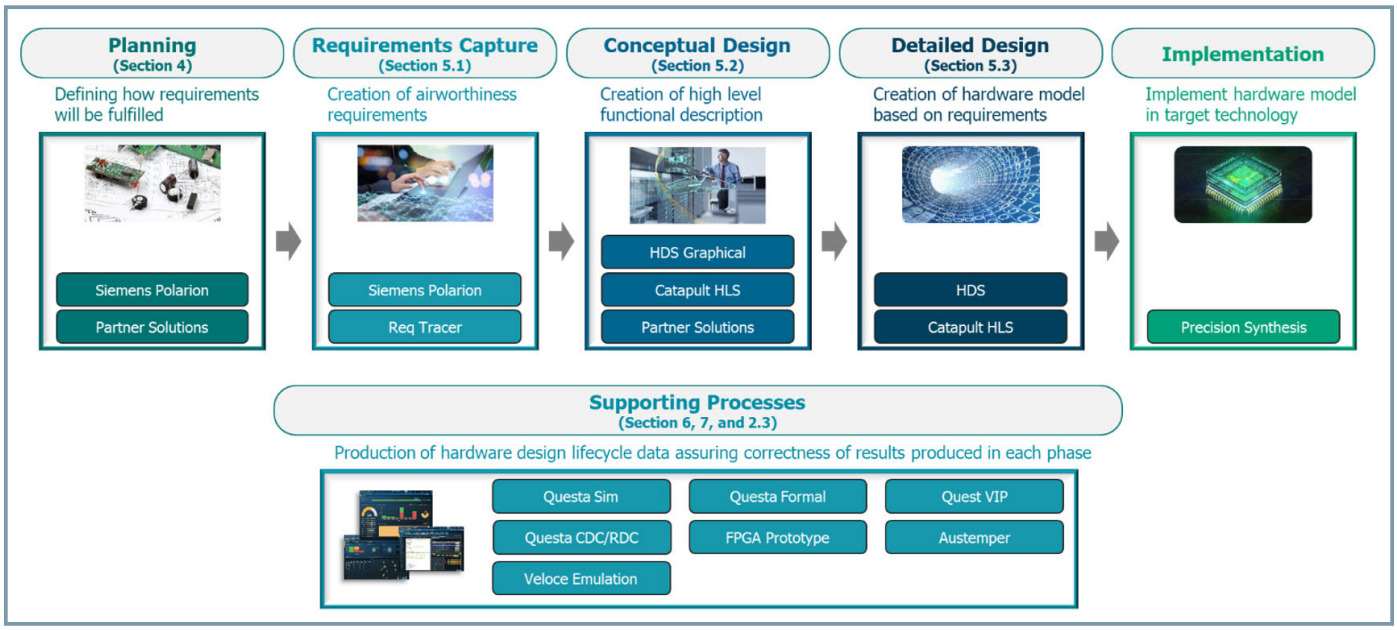

Figure 5: Siemens DO-254 Toolchain

About Patmos Engineering Services

Patmos Engineering Services is an independent engineering consulting company founded and incorporated by Jeff Reeve and Tammy Reeve in January 2000. Patmos has been certified by the Washington State Office of Minority and Women's Business Enterprises (OMWBE) as a Women's Business Enterprise in Engineering Consulting Services, NAICS Code 541330. Patmos offers a unique skillset for digital design (FPGA, ASIC, board level) as well as FAA DER review and approval authority for programmable devices and software. Specifically, Patmos offers:

- DO-254 and DO-178C compliance auditing for FAA, EASA and FAA-EASA coordination
- DO-254 (TR-101), DO-178C (TR-102) and ARP 4754A (TR-103) training
- Process evaluation ("gap analysis") and advising
- Support for commercial and military compliance
- Support for unmanned aerial systems (UAS) i.e., drones
- Support for certifiable IP
- Support for TSO and STC application

In the aerospace domain, the Patmos team supports both commercial and military avionics design and certification programs and is DDTC registered with the United States Department of State Bureau of Military affairs. Outside of the aerospace domain, Patmos has developed a diversity of designs for fields including medical, commercial, and consumer products. The Patmos team has a combined experience in digital hardware design and certification of over 40 years. The goal of Patmos is to provide integrity and honesty in engineering practices and activities. Patmos is a partner with Siemens EDA in support of DO-254 and DO-178C programs.

Patmos Engineering Services:
https://www.patmos-eng.com/about-us/

Siemens Digital Industries Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

About Siemens Digital Industries Software

Siemens Digital Industries Software is driving transformation to enable a digital enterprise where engineering, manufacturing and electronics design meet tomorrow. Xcelerator, the comprehensive and integrated portfolio of software and services from Siemens Digital Industries Software, helps companies of all sizes create and leverage a comprehensive digital twin that provides organizations with new insights, opportunities and levels of automation to drive innovation. For more information on Siemens Digital Industries Software products and services, visit siemens.com/software or follow us on LinkedIn, Twitter, Facebook and Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

siemens.com/eda

84250-C1 11/21 TGB