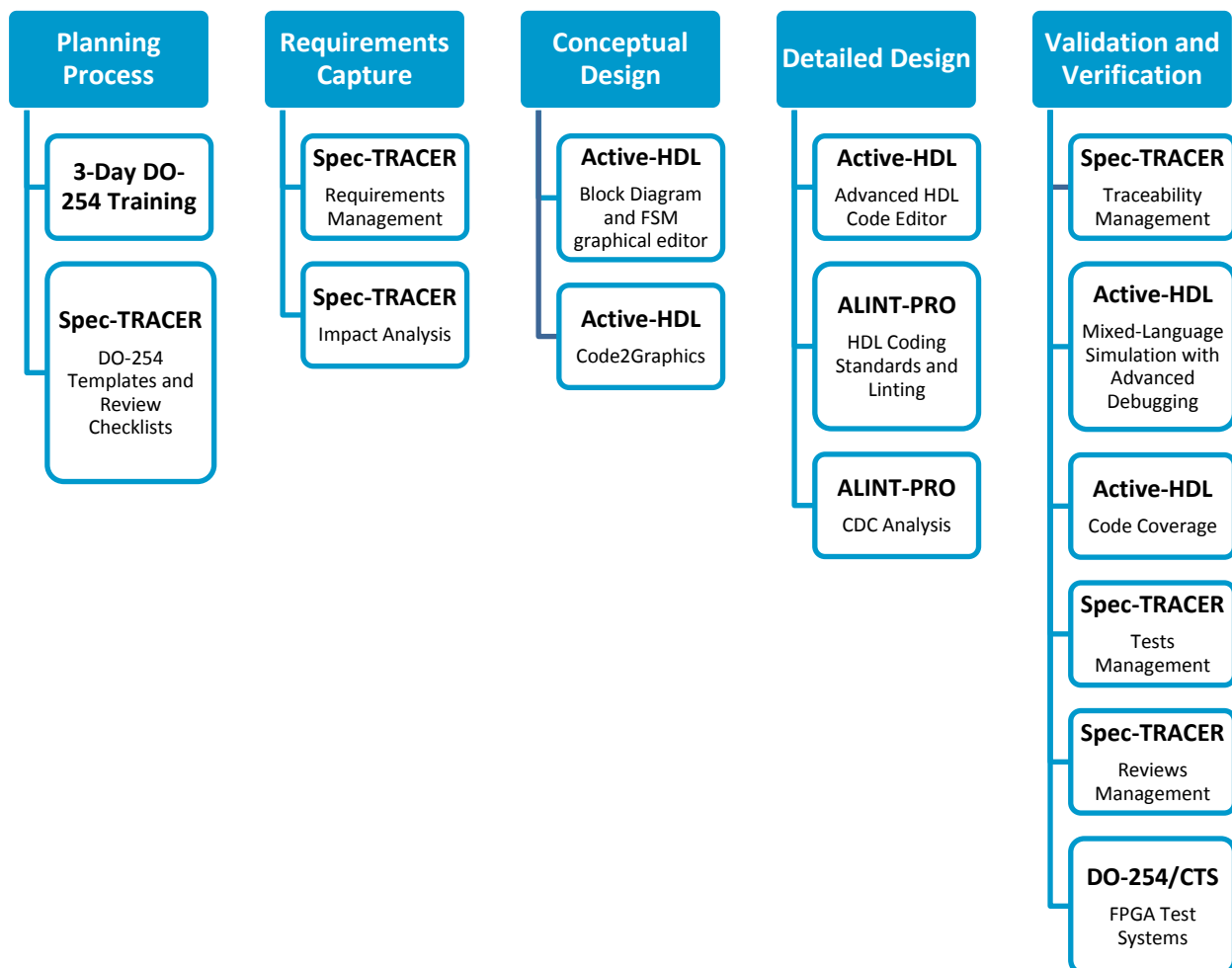




DO-254 Solutions

The Federal Aviation Administration (FAA) recognizes the use of commonly used tools for FPGA design and verification such as RTL Simulator, Synthesis, Place & Route and Static Timing Analysis. For DAL A and B FPGAs, the FAA also recognizes other tools that improve design, verification, traceability and project management including Requirements Management, Traceability, Tests Management, Design Rule Checker, Clock Domain Crossings (CDC) Analysis, Code Coverage and FPGA Physical Test Systems. The following section provides an overview of Aldec's specialized tools for design and verification of FPGAs for boosting productivity and DO-254 compliance such as **Spec-TRACER**, **ALINT-PRO**, **Active-HDL** and **DO-254/CTS**.



Planning Process

3-day DO-254 Training

Aldec conducts a 3-day DO-254 training annually in Las Vegas, NV. The instructors include FAA Consultant Designated Engineering Representative (DER), Randall Fulton and DO-254 Specialist, Roy Vandermolen. The course is designed to provide a comprehensive understanding of DO-254 specification, objectives and requirements for airborne electronic hardware development, and teach efficient, well-proven and compliant methods to enable a faster, easier and more cost-effective path to DO-254 compliance.

DO-254 Templates and Review Checklists

Developing FPGAs for DO-254 compliance entails that applicants submit extensive professional documents and artifacts to the DER. It is the applicant's responsibility to author and create the documents and review them with the highest scrutiny against a high-quality checklist.

Organizations new to DO-254 may find it difficult to start a new DO-254 project without a baseline of the required documents and review checklists. Organizations experienced in DO-254 may want to improve their existing baseline and review checklists due to lessons learned from previous projects. Nonetheless, Aldec has DO-254 Templates/Checklist data package that provides significant value to both new and experienced DO-254 practitioners because it has been developed by an FAA Consultant DER through many years of auditing several DO-254 programs with design assurance level (DAL) A, B, C and D FPGAs. This data package includes DO-254 templates and review checklists which can be easily adopted by applicants as a starting baseline for generating their own documents and artifacts.

Requirements Capture

Spec-TRACER™ Requirements Management

With the growing complexity and size of today's FPGA designs, requirements have also grown exponentially, and methodologies to effectively manage and track requirements have never been more crucial to produce high-quality, reliable and safe products on time and within budget. FPGAs seeking DO-254 compliance face greater challenges with a strict requirements-based design and verification process that must be followed to ensure that the product built functions as intended based on the requirements.

Aldec's Spec-TRACER streamlines the requirements engineering process from capture to traceability, analysis to reporting and design to test results management. FPGA requirements are automatically traced down to HDL design and testbench sources ensuring that each requirement has been fully implemented, covered and verified. Requirements coverage gaps and as well as unused HDL functions are easily exposed and reported using multi-directional traceability.

Spec-TRACER™ Impact Analysis

Requirements changes are a part of the development cycle. If they are not properly controlled, they can make the project more complicated, delay delivery schedules and put pressure to the development team affecting their morale. In FPGA development, a requirement change can impact any of the following areas:

- Lower level requirements

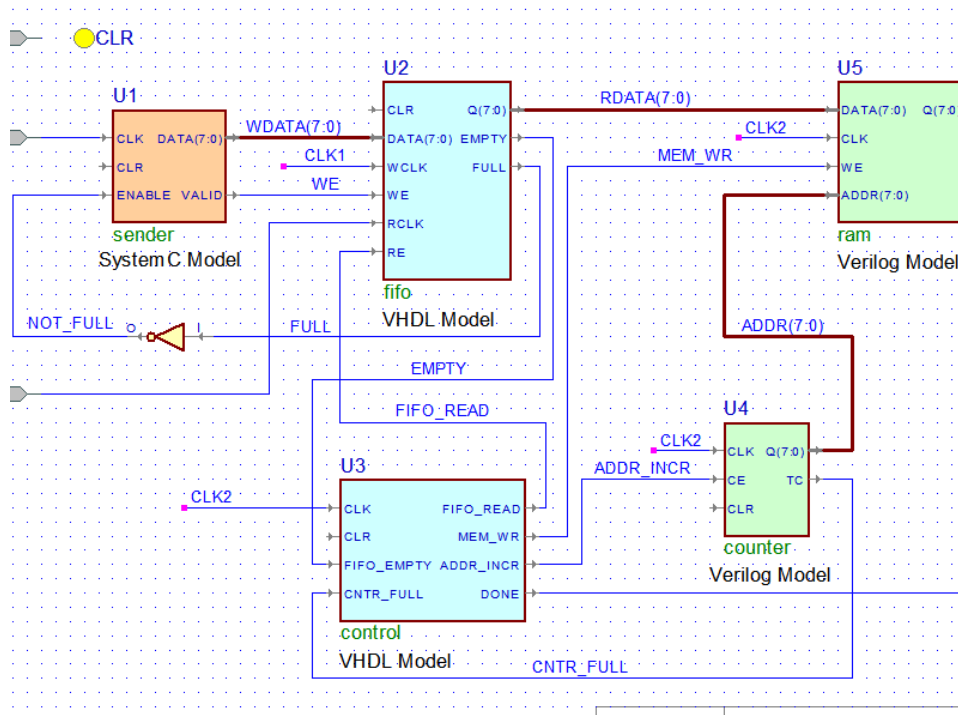
- Lines of code in the HDL design files (top level or sub blocks)
- Requirements-based test cases
- Lines of code in the testbench files and components of the verification environment
- Simulation runs, Code Coverage analysis and reports, waveforms and log files
- Synthesis, Timing or Placement constraints
- Review activities
- Team member(s) responsible for the affected element
- Delivery schedules

Spec-TRACER is equipped with several features and built-in reporting for Impact Analysis. Spec-TRACER Impact Analysis is key in determining the magnitude of the impact before change requests are approved and implemented. It helps teams make well-informed decisions that align with business objectives and project goals. With the growing complexity and size of today's FPGA/ASIC in which an average design consists of hundreds of requirements and thousands of related elements, running Impact Analysis as part of the change control process has never been more crucial to a project's success.

Conceptual Design

Active-HDL™ Block Diagram, Finite State Machine (FSM) Editors and Code2Graphics

The Block Diagram Editor and Finite State Machine Editor are tools for graphical entry of VHDL, Verilog and EDIF designs. The Code2Graphics converter is a tool designed for automatic translation of VHDL, Verilog/SystemVerilog and EDIF netlist into Active-HDL block diagrams and state diagrams. It analyzes VHDL, Verilog, or EDIF files and generates one or more schematic and state diagram files depending on the number of design entities, modules, or cells found in the analyzed file. The resulting schematics and state diagrams files can be automatically attached to a design or saved in a separate location.



During DO-254 Concept Design Process, the combination of these three tools can be used for conceptualizing the architecture, functional diagram, major functions and dataflow of the FPGA design.

Detailed Design

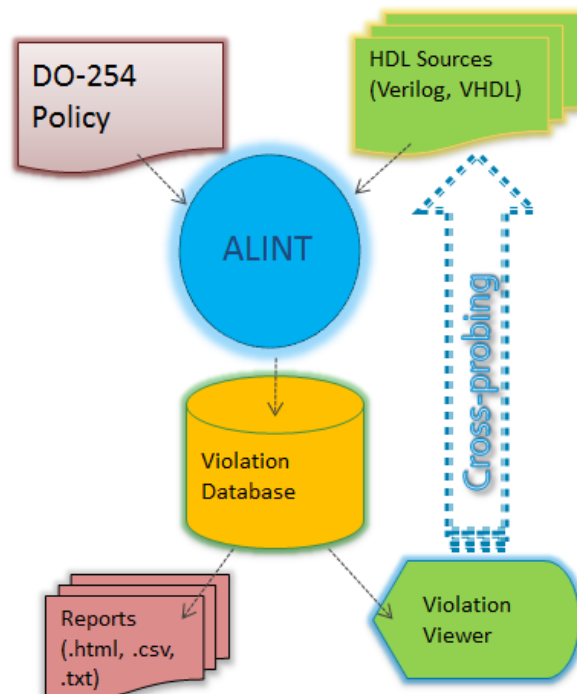
Active-HDL™ HDL Code Editor

The HDL Editor is a text editor designed for editing HDL source code. It is tightly integrated with the compiler and simulator to enable debugging capabilities. Some of the major features of HDL text editor are Keyword highlighting (VHDL, Verilog/SystemVerilog, C/C++, SystemC, OVA, and PSL), Support for code groups and code structure, Auto-complete and Auto-format, Bookmarks and named bookmarks for easy navigation through source code, Breakpoints and Columns Selection.

ALINT-PRO™ HDL Coding Standards and Linting

In order to prevent potentially unsafe attributes of HDL code from leading to unsafe design issues, the use of HDL coding standards is recommended by the FAA as described in the *FAA Order 8110-105 6-2.a*. The HDL coding standards must be defined, reviewed and documented which entails a tedious and lengthy manual review of the HDL source code.

ALINT is a fully automated design rule checker equipped with industry-proven VHDL/Verilog standards and provides an automated code review. The built-in DO-254 best-practice HDL coding standards include essential areas in HDL coding such as coding style, readability, simulation, clock/reset management, design reuse, coding for safe synthesis and implementation, clock domain crossings (CDC) and design for test (DFT). ALINT also provides robust documentation features beneficial to reporting, audits and reviews. ALINT features a Violation Viewer for detected violations and Exclusion Management mechanism that allows associating “irrelevant” violations with the appropriate justification comments. Being tightly integrated with the coding standard violation analysis and reporting interfaces, these features enable push-button reporting and facilitate the desirable practice of creating quality design artifacts essential to obtaining compliance.



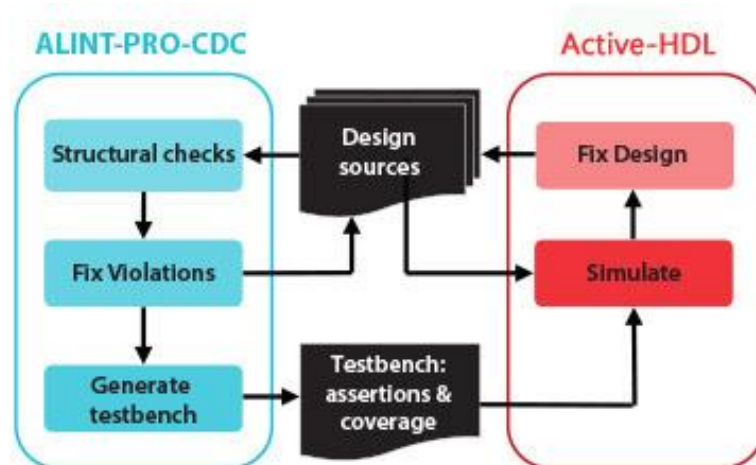
ALINT-PRO™ CDC Analysis

With state-of-the-art FPGAs adding more clock domains and more logic capability, clock domain crossings (CDCs) are almost a certainty in new projects. Complex designs contain the potential for large numbers of CDCs, leaving the door wide open for anomalous behavior in safety-critical environments. Even if teams have the knowledge to manually review designs for CDC issues, the costs of time and documentation loom large. For teams seeking DO-254 compliance, the stakes are even higher.

Inevitably, CDCs appear in large FPGA designs. When logic spans a boundary between two separately clocked asynchronous domains, the result can be unpredictable. If clocks happen to align properly, all is

well. When they misalign for even a brief moment, two probabilistic effects become major concerns: metastability and data incoherence.

ALINT-PRO is equipped with a full-scale CDC verification solution capable of complex clock domain crossings analysis and handling of metastability issues in modern multi-clock designs. The verification strategy in ALINT-PRO is comprised from three key elements: static structural verification, design constraints setup, and dynamic functional verification. The first two steps are executed in ALINT-PRO, while dynamic checks are implemented via integration with simulators with Active-HDL based on the automatically generated testbench. This approach reveals potential CDC problems during RTL simulation, which otherwise would require lab tests to be detected.



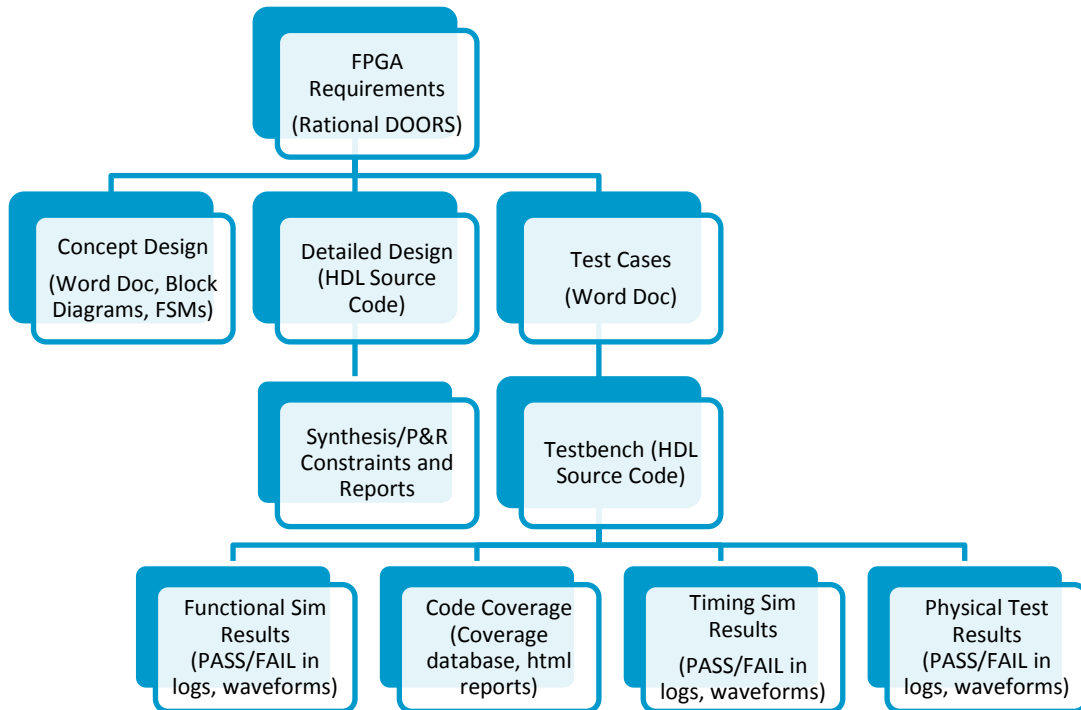
Validation and Verification

Active-HDL™ Mixed-Language Simulation and Advanced Debugging

Active-HDL is equipped with a powerful common kernel mixed language simulator that supports VHDL, Verilog, SystemVerilog(Design) and SystemC. Active-HDL supports VHDL IEEE 1076-2008 language standard. VHDL-2008 adds important language enhancements for verification and design engineers and delivers many benefits from numerous added functionalities, including: PSL incorporation (properties and assertions support), IP protection (encrypted files compilation), VHPI, fixed and floating point packages, generics packages, new types (integer_vector and boolean_vector, etc.), process for combinatorial logic, simplified conditional and case statements, extended assignments, new and enhanced operators, extended bit string literals, enhanced port maps, context declarations and clauses. VHDL IEEE 1076-2008 is the biggest VHDL language standard change since the VHDL IEEE 1076-1993.

Spec-TRACER™ Traceability Management

Traceability is a verification activity that maps all of the design and verification elements back to requirements to ensure that what is being designed and tested is based on the requirements. *RTCA/DO-254 Section 10.4.1* and *FAA Order 8110.105 6-3* both define traceability as the correlation between circuit board requirements, FPGA requirements, conceptual design, HDL design, post-layout design, verification test cases, testbench and test results. Spec-TRACER offers several traceability flows that can be easily adopted. A common traceability flow is shown in the figure below where the FPGA requirements reside in IBM® Rational® DOORS®, HDL source code in Notepad++ and Test Cases in Word Doc. Spec-TRACER is able to connect and maintain traceability from various sources as shown below.



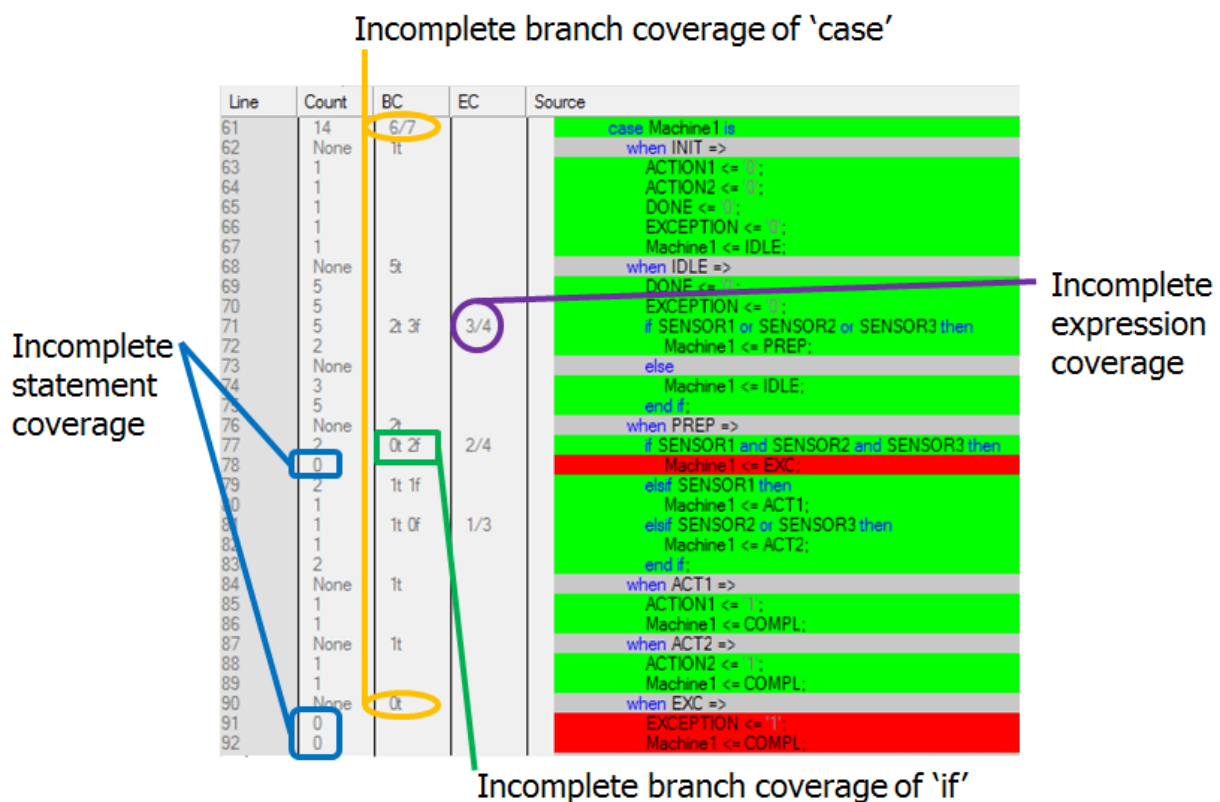
Spec-TRACER™ Tests Management – Tests Management is an important and integral part of verification. A tremendous amount of development cycle is usually spent on verification, so managing tests in a systematic way helps decrease and ease the verification cycle significantly. Common questions such as *Do we have a test for each requirement? Which tests should we prioritize? Have we executed all of the tests? What is the status of the tests? Am I done with verification?* - can be answered easily with efficient tests management. Spec-TRACER offers robust tests management features providing Verification Engineers and Project Managers real-time visibility to verification activities, tests status and test results. Spec-TRACER provides the following:

- Creation and management of test plans and test cases
- Environment for review of test plans, test cases and test results against a checklist, and report generation of the review activities
- Creation and assignment of test attributes
- Parses log files based on regular expressions and stores test results in the Spec-TRACER database
- Reads coverage database (*.ucis*, *.acdb*, *.ucdb*) and stores coverage results in the Spec-TRACER database
- Automatically creates traceability from test case to test results (log files, waveforms, code coverage and functional coverage)
- Results analysis

Active-HDL™ Code Coverage – For DAL and B, the FAA recommends the use of code coverage to satisfy Elemental Analysis, an advanced verification method described in *RTCA/DO-254 Appendix B 3.3.1*. Code coverage is generated automatically from design source code. This verification metrics does not indicate correctness of the design – but measures how code is exercised by the requirements-based testbench. If coverage is missing, it usually indicates either unused code or incomplete tests. Unused code must be

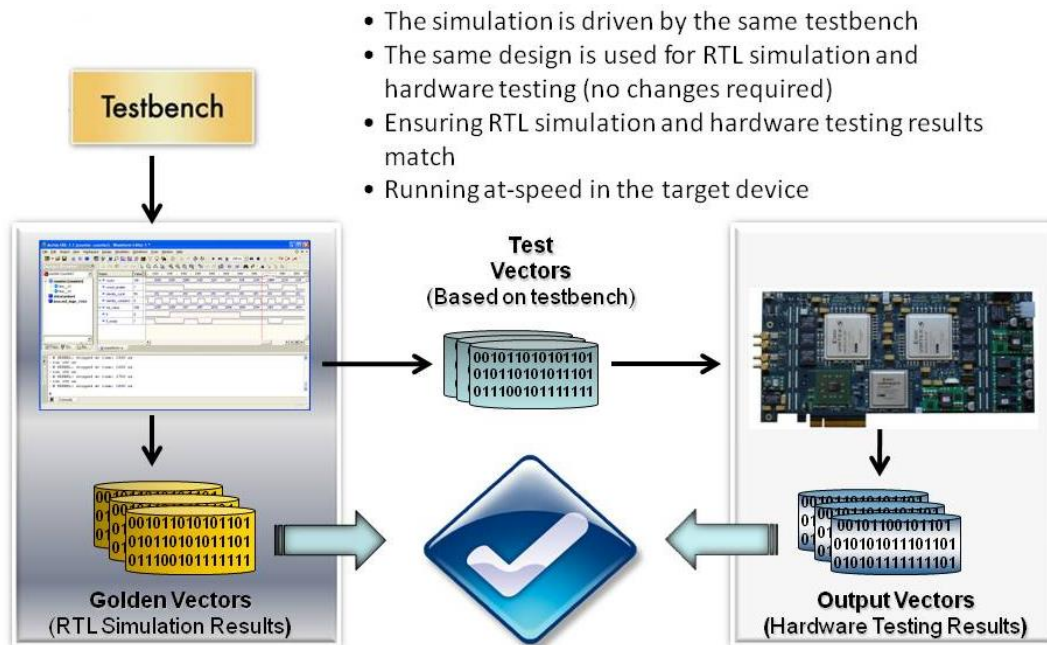
properly scrutinized since they may impact the safe flight of the FPGA. The following types of code coverage are available from Active-HDL:

- *Statement coverage* – examines each executable statement and counts the number of times it has been executed.
- *Branch coverage* – examines branches of each conditional statement and counts true or false conditions that have been met by a branch during simulation.
- *Path coverage* – examines the order of conditional statements execution and indicates whether all possible execution sequences have been verified by a testbench.
- *Expression coverage* – monitors logical expressions and indicates whether all possible states of a logical expression were exercised.
- *Toggle coverage* – monitors signals logic value changes and indicates signals that were not exercised properly by a testbench.



DO-254/CTS™ FPGA Test System – For DAL A and B, verification of the FPGA requirements by physical test is required as described in *FAA Order 8110.105 6-2.b*. Verification by simulations are insufficient because they are based on models and do not represent the intended environment of the FPGA. The FAA and the avionics industry have recognized the benefits of FPGA tests systems such as DO-254/CTS. DO-254/CTS is a fully customized hardware and software platform that augments target board testing to increase verification coverage by test and satisfy the verification objectives of DO-254. The target design runs at-speed in the target device mounted on the custom daughter board. The simulation testbench is used as test vectors to enable requirements-based testing with 100% FPGA pin-level controllability and visibility necessary to implement normal range and abnormal range tests. The FPGA testing results are

captured at-speed and displayed using a simulator waveform viewer for advanced analysis and documentation.



The following are the main capabilities of DO-254/CTS:

- *Physical Testing and At-Speed Testing* - The custom hardware contains the specific part number of the FPGA device from vendors such as Altera, Microsemi and Xilinx. Allows streaming of test vectors through the FPGA inputs at the required operational speed using real clocks in excess of 250 MHz. If the required test time is 500ms, then hardware testing completes within 500ms. Additional features to vary the frequency and voltage to +/-10% can also be used for robustness.
- *Automatic Generation of Test Vectors for Hardware Testing* - Development of test vectors for hardware testing for an average DAL A/B design normally takes 6-12 months manual engineering time. This tool is equipped with a utility that converts the testbench within minutes into test vectors to be used for hardware testing. This ensures the same requirements that are verified by simulation are verified again by physical tests. No changes to the testbench are necessary.
- *Single-Environment to Verify all FPGA Level Requirements* - Traditionally, multiple sets of testing environment must be created to verify groups of FPGA requirements, and this usually entails manual connections/bypasses of wires and cables which are prone to errors and bugs. One of the primary goals of this tool is to prevent such cases. This tool consists of custom hardware (PCIe interface) and software providing a single-environment to test all FPGA level requirements.
- *Automated Physical Testing* - This tool is a "push-button" automated in-hardware testing environment to test all FPGA level requirements. It is equipped with a utility to automatically compare RTL simulation results with hardware testing results. The utility displays either a PASS or FAIL message in which results can be further investigated using a standard waveform viewer.
- *Physical Testing Results Visualization with Waveform Viewer* - The capabilities for capturing/recording and visualization of hardware testing results using Logic Analyzers and Digital Oscilloscopes are limited. This tool allows capturing and visualization of results using the

simulator's standard waveform viewer, providing storage for waveform files of up to 16TB and capturing of results immediately after simulation. Comparison between RTL simulation and hardware testing results is also possible.

- *Integration with 3rd Party HDL Simulator, Synthesis and P&R Tools* - This tool can be used with any 3rd party RTL Simulator, Synthesis and P&R tools.

Tool Assessment and Qualification

Aldec has done the due diligence to rigorously test its tools according to the stringent process defined in RTCA/DO-254 Section 11.4 Tool Assessment and Qualification Process. Whenever feasible, Aldec recommends manual review of the verification results in order to claim independent assessment. If manual review is not feasible, then Aldec provides specific Tool Qualification Data Packages for specific Aldec DO-254 tools.

For more information about Aldec's data packages for Tool Qualification, go to

https://www.aldec.com/en/solutions/do_254_compliance/tool_assessment_qualification_process

DO-254 White Papers and Webinars

Aldec has authored several white papers and conducted several webinars to educate the industry with DO-254 best practices and recommendations. The following is a list of literature that can be downloaded from Aldec's website.

[White Papers](#)

[Introduction to DO-254](#)

[DO-254 Requirements Traceability](#)

[Q & A with FAA DO-254 DER Randall Fulton](#)

[Managing Validation and Verification Activities for DO-254](#)

[DO-254: Increasing Verification Coverage by Test](#)

[DO-254 Tool Qualification Process Guidance for Active-HDL Code Coverage](#)

[Tool Assessment and Qualification with the Aldec DO-254 Compliance Tool Set](#)

[Finding CDC Issues Before They Find You: Advanced CDC Verification for DO-254 Compliance](#)

[Recorded Webinars](#)

[DO-254: How to Formulate an Efficient PHAC](#)

[Q & A with FAA DO-254 DER Randall Fulton \(US\)](#)

[DO-254: Requirements Optimization for Verification](#)

[DO-254 Requirements Traceability](#)

[Best Practices for DO-254 Requirements Traceability](#)

[Elemental Analysis: DO-254 Additional Verification for Levels A and B](#)

[Validation and Verification Process for DO-254](#)

[DO-254 Verification Strategies](#)

[Physical Testing for DO-254](#)

[Managing Requirements-Based Verification for Safety-Critical FPGAs and SoCs](#)

[Eliminating Clock Domain Crossing \(CDC\) Issues Early in the Design Cycle](#)

References

- RTCA/DO-254 “Design Assurance Guidance for Airborne Electronic Hardware”, 2000
- FAA Order 8110-105, “Subject: Simple and Complex Electronic Hardware Approval Guidance”, 2008
- FAA AC 20-115C “Advisory Circular: Airborne Software Assurance”, 2013
- FAA AC 20-152 “Advisory Circular: RTCA, INC., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware”, 2005
- FAA “Conducting Airborne Electronic Hardware Reviews Job Aid”, 2008
- SAE ARP4754A “Guidelines for Development of Civil Aircraft and Systems”, 2010
- “Airborne Electronic Hardware Design Assurance”, Randall Fulton and Roy Vandermolen, 2015

About Aldec, Inc.

Established in 1984, Aldec Inc. is an industry leader in Electronic Design Verification and offers a patented technology tool suite including: RTL Design, RTL Simulators, Hardware-Assisted Verification, Design Rule Checking, IP Cores, Requirements Management and Traceability, DO-254 Functional Verification and Military/Aerospace solutions. Continuous innovation, superior product quality and total commitment to customer service comprise the foundation of Aldec’s corporate mission. For more information, visit www.aldec.com.