As airborne systems increase in complexity to take advantage of the benefits that the latest technology can offer, the arduous task of validating the design for assurance per specifications set forth by governing bodies becomes monumental. Software tools offer limited features and do not always offer a solution that meets the required specification. A hardware solution in combination with software offers a more complete solution and helps to speed up the verification and validation process.

Today, in the era of multimillion gate designs, reusable IP, and Systems-on-Chip (SoCs), verification is considered the largest bottleneck in the design assurance process. Simultaneously, time to market continues to shrink as avionics designs have the same timing pressures as commercial applications. The avionics industry faces a test/cost problem where verification and testing represent a large part of the development expenses. In order to address the lack of complete verification, the hardware design life cycle should include new technologies that can help accelerate the design assurance process.

Three methodologies – hardware emulators, hardware accelerators, and FPGA prototypes – have emerged to the forefront to provide the highest performance of complete verification methodologies in the industry. As the level of design assurance increases to accommodate new industry guidelines, design verification approaches require special methods and tools. COTS hardware-software platforms directly address these challenges.

**Hardware design assurance**

More and more frequently, industry guidelines drive how systems are designed and verified. In the avionics industry, for example, the DO-254 document provides design assurance guidance for the development of “safe” airborne electronic hardware. The process involves multiple steps. First, system functions must be allocated to different hardware blocks at the system level. These blocks are then assigned corresponding system development assurance levels.

Figure 1 illustrates the relationships and interactions between three processes – hardware, software, and safety assessments – as a system requirement may result in the design assurance of multiple complex processes. For example, a hardware function that contains safety requirements involves both the safety assessment and the hardware design life-cycle processes.

It is important to note that the hardware design assurance level is associated with the five levels of safety criticality: Levels A through E (see sidebar, page 28). The DO-254 document notes that the hardware design assurance process and safety assess-
The results of each simulation stage are stored, compared, and verified. The resulting data then establishes functional completeness and correctness of the hardware design. The verification process is complete if all simulation stages confirm the same data. If this occurs, the verification process and data can be included in the DO-254 certification documents such as the Hardware Verification Plan and Hardware Verification Data.

**RTL simulation**

At the RTL simulation level, an extensive test suite that consists of different test benches is developed to support all aspects of the design specification. In many cases, the same test bench can be used with different input data to simulate design functionality. Test benches can be based on traditional HDL languages, such as Verilog or VHDL, and assertion checkers need to be included. All simulation activity must be performed within the logic simulator environment. One means of design checking involves the use of simulation results as a waveform file. Subsequently, the waveform file can be utilized to compare results from other levels of design verification. After successful verification, design sources can be synthesized to receive the post-synthesis netlist.

**Gate-level simulation**

To achieve gate-level simulation, the aforementioned test bench suite can be used again. As before, all verification activity is done using a software simulator. All gate-level, nontiming simulation results are compared against the RTL simulation using waveform files. Since automatic waveform comparison is not applicable for timing simulation, special checkpoints are put in place to compare corresponding simulation results.

The Aldec-Actel solution offers three stages of design verification support: RTL simulation to verify design functionality, gate-level simulation to check timing and catch errors introduced during synthesis and place and route, and verification of the design in hardware. For all three simulation runs, designers can utilize the same test bench or a set of golden vectors as shown in Figure 2.
Hardware-level simulation

Hardware simulation is used to accomplish two major goals. The first is the achievement of functional design verification in real hardware. Because simulation performance is an order of magnitude faster in hardware than in software, the second goal is validation of the design by running more test cases.

Using Hardware Embedded Simulation (HES) technology, the designer can start design verification in the actual hardware immediately following initial RTL validation. HES is a hybrid software-hardware simulation platform that is driven by software that functions as a design test bench executed by a logic simulator. HES technology is designed to implement the Design Under Test (DUT) in a reconfigurable hardware device, such as an FPGA, and then verify that the design functions in actual hardware.

The FPGA communicates on an event basis with the remaining sections of the test bench resident in the logic simulator. The HES technology then utilizes the same set of test benches and generates a signal waveform file that will need to match the one from RTL simulation.

Another advantage of HES simulation is that the DUT interface signal data can be stored and used later as simulation input vectors. Recording both the input and output interface data allows not only DUT testing but also comparison of the output with the set of golden vectors.

Design prototyping

The design prototyping phase proves the logic operates as close to or equal to the application’s target speed. As it is one of the final stages of the design verification, this phase requires the most resources to set up and execute.

FPGAs are ideal for this design phase and offer the benefits of programmability that can accommodate design changes with little impact to the design verification phase. Two types of challenges can be encountered at this stage. The first challenge is the process of setting up the design in the hardware target, such as reprogrammable flash-based FPGAs. These single-chip solutions offer several advantages that make them ideal for design assurance. Unlike an SRAM FPGA with an external boot ROM, flash-based FPGAs are highly secure and immune to neutrons. Alternatively, SRAM FPGAs are very susceptible to neutrons and cause configuration upsets – not well-matched for stringent DO-254 requirements. Configuration upsets in SRAM FPGAs can cause the functionality of the FPGA to change. This demonstrates poor design assurance, but more importantly, these changes can result in low safety assessments and grave consequences, particularly in the avionics industry.

The design is first targeted to a high-density FPGA for initial prototyping. If a smaller size device is used, the design may have to be partitioned across multiple FPGAs using commercially available software, adding a layer of complexity to the design assurance process. Initial testing of the prototype FPGA can be accomplished using the test vectors generated during HES simulation as inputs. Special input/output interface logic has to be designed into the FPGA to ensure the synchronization of the hardware with the generated output from the software application. FIFO memory blocks on board the FPGA can be used as the input/output interface using two interrupt lines. A request is then made to the software application to fill the input buffer or to empty an output buffer. The output vectors generated are converted into a standard waveform format and used to compare the results with the outputs from earlier verification stages. To achieve further testing after debugging the FPGA under test, the design can be exercised further with different test vectors or real-time data.

DO-254 verification made easier

Along with traditional design verification methodologies, such as RTL and gate-level simulation, HES can be used successfully to test the design in hardware, using a simulator and then later using a real-time high-speed clock. The delta cycle accurate behavior can be validated using off-the-shelf standard tools, such as a waveform viewer or list viewer.

These methods allow the customer to meet the hardware verification plan specified in design assurance guidance for airborne electronic hardware. There are procedures, methods, and standards to be applied to achieve hardware verification compliance with a set of established standards such as DO-254. The Aldec-Actel Design Assurance HES and prototyping methodology for verification and validation of airborne systems provides a complete solution to meet airborne system safety requirements as specified by the DO-254 objectives.

Irene Sysenko has worked as a research engineer at Aldec Inc. since 2005. Prior to that, she spent two years at Aldec, Inc. working as an R&D engineer, designing processor-based simulation systems. Before joining Aldec, Irene worked as a professor at Kharkov National University of Radio-Electronics, Ukraine, teaching digital design testing and diagnostics. She holds a PhD in Computer Engineering from Kharkov National University of Radio-Electronics.

Aldec, Inc.
2260 Corporate Circle
Henderson, NV, 89074
702-990-4400, Ext. 254
irenes@aldec.com
www.aldec.com

Ravi Pragasam is a senior marketing manager in the military and aerospace product marketing team at Actel Corporation. He has worked in the FPGA industry for more than 15 years and has served in a variety of roles including marketing and applications engineering. He has two MS degrees in Electrical and Computer Engineering from Kansas State University and College of Engineering, India.

Actel Corporation
2061 Stierlin Court
Mt. View, CA 94043-4655
650-318-4773
ravi.pragasam@actel.com
www.actel.com