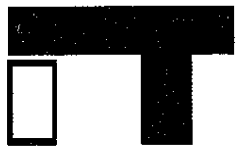
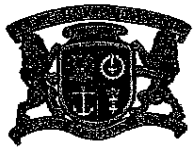
Proceedings of the
2008 1st International Conference on Information Technology

Sponsored by IEEE

19-21 May, 2008, Poland, Gdansk University of Technology,
Faculty of Electronics, Telecommunications and Informatics



Editors
Andrzej Stepnowski
Marek Moszyński
Thaddeus Kochanski
Jacek Dąbrowski



Gdansk University of Technology, 2008

Proceedings of the 2008 1st International Conference on Information Technology, IT 2008
19-21 May 2008, Gdansk, Poland

Safety Assurance for Safety-Critical Embedded Systems: Qualification of Tools for Complex Electronic Hardware

Andrew Kornecki
Dept. of Computer & Software Engineering
Embry-Riddle Aeronautical University
Daytona Beach, FL 32114, USA
kornecka@erau.edu

Janusz Zalewski
Dept. of Computer Science
Florida Gulf Coast University
Ft. Myers, FL 33965, USA
zalewski@fgcu.edu

Abstract

In recent decades, multiple application domains emerged that use computational devices embedded in commercial products that are sensitive to safety concerns. They include not only typical areas, such as nuclear technology and aircraft avionics, but also many medical devices, cars, railway transportation, and others. The essential requirements for this kind of products are so strict that they are regulated by respective government agencies, for example FAA and FDA in the U.S. This paper addresses the most important aspects of using software tools for designing complex electronic hardware for such systems and focuses on special assessment criteria for these tools.

1. Introduction

Computer and software safety is a major issue in safety-critical embedded applications, in various industries, such as aerospace, aircraft, automobile, railways, nuclear, medical, and others. Safety in this context means avoiding harm to the individuals or the society, due to a malfunction of computer equipment or software. The general view of safety assurance is to minimize the risk that may lead to accidents. In this view, not only the computer and software products have to be evaluated for safety, but also the tools used to develop this hardware and software. Our previous work concerned the evaluation of software tools for developing real-time safety-critical systems [1]. The current project concerns the qualification of software tools used in designing Complex Electronic Hardware (CEH) for avionics applications.

The primary devices in this category include equipment based on PLD (Programmable Logic Devices), FPGA (Field Programmable Gate Arrays), ASIC (Application Specific Integrated Circuits), and similar circuits used as components of programmable electronic hardware. Often the circuit includes dedicated processors whose Intellectual Property (IP) is made into the final product silicon.

To identify issues and concerns in CEH tool qualification and certification, one has to start with a broader view of an industry perspective. This paper focuses on a survey of the aviation community conducted to review related practices. The survey was conducted to collect data on the experiences and opinions concerning the use of software tools as applied in the design or verification of complex electronic hardware according to the RTCA DO-254 standard [2]. The objective was to collect feedback, from industry and certification authorities on assessment and qualification of CEH programmable logic tools. The participants included individuals who have experience with developing or using such tools or experience with qualifying such tools.

The paper is structured as follows. First, we present a basis for this research, discussing briefly the relevant industry standard in Section 2. Section 3 includes a brief review of related work, and Section 4 discusses the results obtained via industry survey. The paper ends with conclusion in Section 5.

2. Basis for the Research

Hardware development for safety-critical avionics systems is guided by the RTCA DO-254 standard "Design Assurance Guidance for Airborne Electronic Hardware" [2]. This document provides details on the processes that must be followed in assessment and certification of hardware components. In particular, it provides certification information on project conception, planning, design, implementation, testing,

978-1-4244-2244-9/08/$25.00 ©2008 IEEE

and verification. It also addresses the issue of qualification of the tools used for creation of an airborne system, depending on specific levels of safety assurance, called Design Assurance Levels (DAL), and defined by the categories from A to D, i.e., from the most to the least critical.

RTCA DO-254 was released in 2000 addressing the design assurance for complex electronic hardware. The guidance is applicable to wide range of hardware devices ranging from integrated technology hybrid and multi-chip components, to custom programmable micro-coded components to Circuit Board Assemblies (CBA), to entire Line Replaceable Units (LRU). The guidance addresses also issue of Commercial-Off-The-Shelf (COTS) components.

It provides guidance for objectives to be met and data to be submitted for review. Independence and control data category, based on the assigned assurance level, describes Functional Failure Path Analysis (FFPA) method applicable to hardware with DAL levels A and B, and discusses additional assurance techniques to support and validate the analysis results. The FFPA can be accomplished on five levels: (a) system, (b) hardware, (c) circuit, (d) component, and (e) elemental. There is the same number of objectives to be met and thus there is no difference in the design assurance process for systems level A and B.

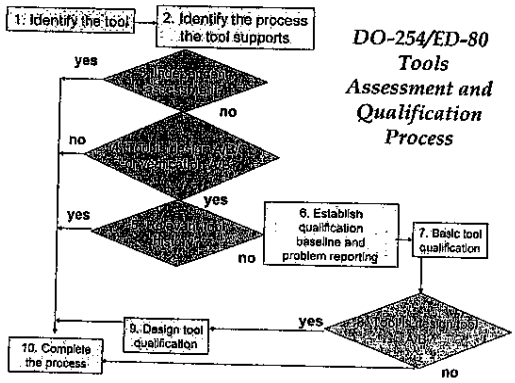


Fig. 1. Tool qualification procedure according to DO-254 [2].

It is widely recognized that in safety critical applications, with millions of gates on a chip, the role of hardware design tools and hardware verification tools becomes increasingly critical. The process of developing CEH for airborne applications is described in the aforementioned standard, so is the tool qualification process. Section 11.4 of DO-254 distinguishes between design and verification tools:

- *When design tools are used to generate the hardware item or the hardware design, an error in the tool could introduce an error in the hardware item;*
- *When verification tools are used to verify the hardware item, an error in the tool may cause the tool to fail to detect an error in the hardware item or hardware design.*

3. Related Work

It is interesting to notice industry practices in tool qualification, as reported in the available literature. Some of these papers deal directly with vendors' views on tool qualification according to DO-254. Mentor Graphics [3] and TNI-Software [4] describe their approach to comply with the requirements of DO-254 for their respective verification tools: *ModelSim* and *Reqtify*, and formal property checker, *improve-HDL*.

Two COTS tools from the GNU package, a configuration management tool, *CVS*, and a problem reporting took, *GNATS*, are recommended in [5]. Four vendors, Xilinx, Altera, TNI-Software and Mentor Graphics, identify their tools and processes in [6], and Aldec and Barco-Siles S.A., outline their processes to comply with DO-254, in [7] and [8-9], respectively. Airbus [10] and DO-254 User Group [11] do it separately, with a list of issues and clarifications regarding compliance.

Several authors present academic and research views on the issue of certification. Lundquist [12] addresses the question of certification of an Actel FPGA chip and concludes that this question "remains unanswered." Hilton and Hill [13] advocate the use of SRPT (Synchronous Receptive Process Theory) to reason about the FPGA as a collection of small processes reacting to signal inputs.

Jacklin et al. [14] argue that complete verification and validation of learning systems should not be viewed as running test cases and comparing expected results to actual results, because such testing can never reveal the absence of errors. Finally, Crum et al. [15] point out that the lack of research investment in certification technologies will have a significant impact on levels of autonomous control approaches that can be properly flight certified, and could lead to limiting capability for future autonomous systems.

4. Industry Survey

The survey was conducted to collect data on the experiences and opinions concerning the use of programmable logic tools as applied to design or

verification of complex electronic hardware. The questionnaire has been distributed, intended for the individuals who have experience with developing or using such tools or experience with qualifying such tools. It was distributed during the 2007 FAA Software & Complex Electronic Hardware Conference, in New Orleans, Louisiana, in July 2007, attended by over 200 participants. A special session dedicated to the CEH was attended by 54 individuals representing industry and government organizations interested in the CEH and the application of DO-254.

In addition to distributing and collecting the paper copies of the questionnaire at the conference, we followed-up with a mailing to over 150 individuals engaged in development of the aviation software and hardware. The questionnaire was also distributed internally in a few companies engaged in the design of programmable logic devices. As a result of these activities we received a sample of over twenty fully filed responses. Even though this is a rather disappointing outcome, the collected results provide several interesting observations.

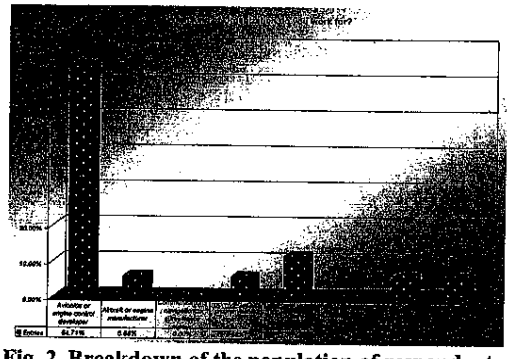


Fig. 2. Breakdown of the population of respondents.

The survey population, by type of the organization, is shown in Figure 2. The majority of respondents work for avionics or engine control developers (~65%). Over 95% of respondents have technical background with ~55% having bachelor and ~45% master degrees and over 72% have educational background in electronics. 97% of respondents have more than three years experience, with 59% having more that 12 years experience.

The most frequent respondents' roles relevant to the CEH tools are shown in Figure 3:

- use of the tools including development or verification of systems (~62%)
- managing and acting as company's engineering representative (~26%)
- development of the tools (~2%)
- development of components (~12%).

The respondents' primary interest was divided between verification (32%), development (27%), hardware (22%) and concept/architecture (18%).

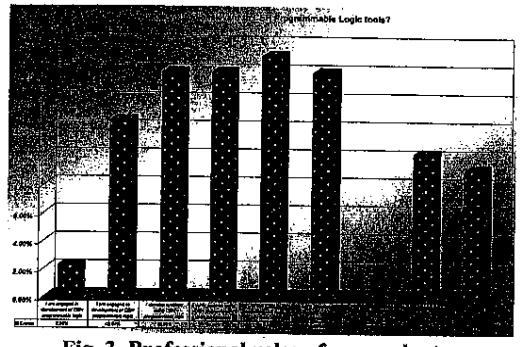


Fig. 3. Professional roles of respondents.

The types of devices used include a wide range of them, with most frequently used being FPGA (~27%) and CPLD (~18%). Other technologies that have been also used include: ASIC (~15%), PAL (~11%), PLA (~9%) and EPLD (~8%),. The most popular hardware device vendors are Actel (~27%) and Xilinx (~24%), Lattice (~13%) and Cypress (~11%) with Quick Logic, Altera and Atmel below 10%.

The most widely used tools are from Mentor Graphics (~27%) and Synplify (~22%), followed by Synopsys (~17%), Aldec (~11%) and Cadence (~8%). About 23% respondents use other tools.

Considering criteria for the selection of tools for use in DO-254 projects (see Figure 4), the most important are: the available documentation, ease of qualification, previous tool use, and host platform, followed by the quality of support, tool functionality, tool vendor reputation, and the previous use on airborne project. Selection of a tool for the project is based either on a limited familiarization with the demo version (50%) or an extensive review and test (40%). The approach to review and test the tool by training the personnel and using trial period on a smaller project seems to be prevailing.

For those who have experienced effort to qualify programmable logic tools (only 14% of respondents), the quality of the guidelines is sufficient or appropriate (62%), so is the ease of finding required information (67%), while the increase of workload was deemed negligible or moderate (80%). An interesting observation concerns the scale of safety improvement: marginal (43%), moderate (21%), noticeable (7%) and significant (29%). Similarly, the question about errors

found in the tools may be a source for concern: no errors (11%), few and minor errors (50%), significant and numerous (17%). Despite all this, the satisfaction level towards programmable logic tools was positive, and more than 96% of the respondents marked their satisfaction level as 4 out of 5.

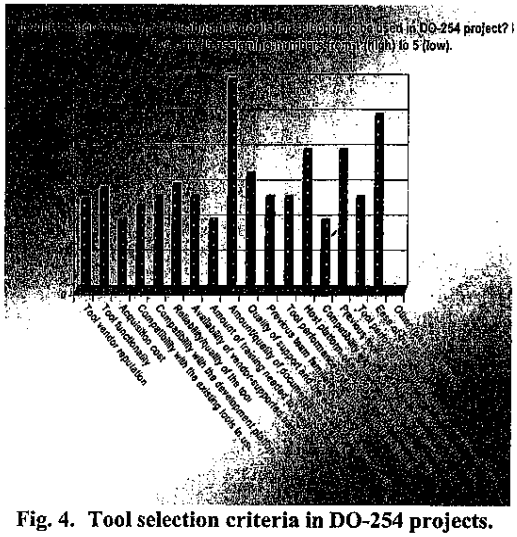


Fig. 4. Tool selection criteria in DO-254 projects.

5. Conclusion

Software tools used in design and verification of complex electronic hardware in safety-critical applications should be scrutinized because of concerns that they may introduce design errors leading to accidents. The tool assessment process must follow the DO-254 guidelines, but the relative vagueness of these guidelines causes significant differences in interpretation by industry.

This project has identified industry practices in the area of tool qualification. The survey indicated that the most important criteria for tool selection are: available documentation, ease of qualification, and previous tool use. Future work in this project will involve conducting experiments with tools to identify their most vulnerable functions that may be a source of subsequent design faults and operational errors.

Acknowledgment

This work has been done under a contract from Federal Aviation Administration DTFACT-07-C-00010.

References

[1] Kornecki A. and J. Zalewski, "Experimental Evaluation of Software Development Tools for Safety-Critical Real-Time Systems", *Innovations in Systems and Software Engineering: a NASA Journal*, Vol. 1, 2005, pp. 176-188.

[2] RTCA Inc., *Design Assurance Guidance for Airborne Electronic Hardware*, DO-254, Washington, DC, 2000

[3] Lange M, *Assessing the ModelSim Tool for Use in DO-254 Projects*, Rev. 1.1, Mentor Graphics Corp., May 2007

[4] Dellacherie S., L. Burgaud and P. di Crescenzo, Improve–HDL: A DO-254 Formal Property Checker Used for Design and Verification of Avionics Protocol, *Proc. DACS'03, 22nd Digital Avionics Systems Conf.*, Indianapolis, Ind., October 12-16, 2003, Vol. 1, pp. 1.A.1-1.1-8

[5] Hilderman V. and T. Baghai, Avionics Hardware Must Now Meet Same FAA Requirements as Airborne Software, *COTS Journal*, September 2003

[6] Burgaud L., The DO-254 Users Group: A Proactive Initiative to Federate Industry Efforts, Presentation at the FAA Software & CEH Conf., New Orleans, LA, July 2007

[7] Aldec, Inc., *DO-254 Hardware Verification: Prototyping with Vectors Mode*, June 26, 2007

[8] Leroy J.-E. and J. Bezamat, *Experience at Barco-Silex in FPGA Design with DAL C (DO254)*, Barco-Siles S.A., Peynier, France, Internal Paper, 2007

[9] Pampagnin P. and J.F. Menis, *DO254-ED80 for High Performance and High Reliable Electronic Components*, Barco-Siles S.A., Peynier, France, Internal Paper, 2007

[10] *A380 Certification Review Item*, Airbus Industries, Toulouse, France, March 2003

[11] Baghai T. and L. Burgaud, DO-254 Package: Process and Checklists Overview and Compliance with RTCA/DO-254 Document, March 2004

[12] Lundquist P., *Certification of Actel Fusion according to RTCA DO-254*. Master Thesis, Report LiTH-ISY-EX-ET-07/0332-SE, Linköping University, Sweden, May 4, 2007

[13] Hilton A. and Jon G. Hill, *On Applying Software Development Best Practices to FPGAs in Safety-Critical Systems*, The Open University, 2000

[14] Jacklin S. et al., Development of Advanced Verification and Validation Procedures and Tools for the Certification of Learning Systems in Aerospace. *Proc. AIAA Infotech@Aerospace 2007 Conference and Exhibit*, Arlington, Virginia, Sept. 26-29, 2005, Paper No. AIAA 2005-6912.

[15] Crum V., D. Homan and R. Bortner, Certification Challenges for Autonomous Flight Control Systems, *Proc. AIAA Guidance, Navigation, and Control Conference and Exhibit*, Providence, R.I., August 16-19, 2004, Paper No. AIAA 2004-5257.