Proceedings of 2015 International Symposium on Embedded Technology
(ISET 2015)
Hotel Inter-Burgo Daegu, Korea, 04-*06 June, 2015.*

Verification Techniques for COTS Dedication of Commercial FPGA Tools

Junbeom Yoo Eui-Sub Kim Sejin Jung

Department of Computer Science and Engineering
Konkuk University, Seoul, Republic of Korea
E-mail: {jbyoo, atang34, jsjj0728}@konkuk.ac.kr

Abstract

FPGA (Field-Programmable Gate Array) has received much attention from nuclear industry as an alternative platform of digital I&C (Instrumentation & Control) in nuclear power plants [1,2]. Commercial FPGA synthesis tools synthesize gate-level designs mechanically from RTL (Register Transistor Logic) designs modeled with HDLs (Hardware Description Languages). Nuclear regulation authorities [3], however, require more considerate demonstration of the correctness of the mechanical logic synthesis (*i.e.*, COTS dedication), even if the FPGA industry have acknowledged them empirically as correct and safe processes and tools. While the synthesis can be formally verified with compiler verification techniques [4] directly, it is hard to apply them to the products of 3rd-party developers. An alternative solution we propose is to do the demonstration indirectly. For a specific input program (*e.g.*, Verilog program), if a synthesis tool produces a program (*e.g.*, Netlist) which shows the same behavior for all possible cases, we can claim that the tool works correctly at least for the program.

We could use various commercial formal verification tools such as '*FormalPro*', '*Encounter Conformal EC*' and '*Formality,*' which can be used as a means of the indirect demonstration. They are, however, too case-sensitive to use naively, as depending on the combination of synthesis and verification tools. For example, we cannot use '*FormalPro*' for '*Actel Libero IDE*' with '*Synopsys Synplify Pro*' synthesizer, which is the combination of the project we are working with. We need to develop a new customized solution for the combination.

We propose a VIS-based correctness verification technique [5] for commercial FPGA logic synthesis. It formally checks the behavioral equivalence between an RTL design (*i.e.* Verilog) and a subsequently synthesized gate-level design (*i.e.*, Netlist) with the support of two transformations making the VIS verification possible. The technique targets the combination of '*Actel Libero IDE*' and '*Synopsys Synplify Pro*' synthesizer, which other commercial verification tools could not deal with. If the formal equivalence checking succeeds, we can assure that the logic synthesis worked correctly. A case study we conducted also showed that the VIS-based correctness verification technique can be used positively as a means of demonstrating the correctness [6] of commercial FPGA synthesis tools of 3rd-party developers.

Keywords: FPGA Logic Synthesis, Formal Equivalence Checking, COTS Dedication, VIS

Acknowledgement
This research was supported, in part, by a grant from the Korea ministry of science, ICT and future planning under the I&C Safety Conformance Assessment Platform. It was also supported, in part, by a grant from the Korea Atomic Energy Research Institute, under the development of the core software technologies of the integrated development environment for FPGA-based controllers.

References

[1] J. Yoo, E.-S. Kim, and J.-S. Lee, “A Behavior-Preserving Translation from FBD Design to C Implementation for Reactor Protection System Software,” Nuclear Engineering and Technology, Vol.45, No.4, pp.489-504, 2013.

[2] J. She, “Investigation on the benefits of safety margin improvement in CANDU nuclear power plant using an FPGA-based shutdown system,” Ph.D. dissertation, The University of Western Ontario, 2012.

[3] Electric Power Research Institute (EPRI), “Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications (EPRI NP-5652),” 2014.

[4] T. Hoare, “The verifying compiler: A grand challenge for computing research,” Journalof the ACM, Vol.50, No.1, pp.63-69, 2003.

[5] E.-S. Kim, J. Yoo and J-Y. Kim, "A VIS-based Correctness Verification Technique for Commercial FPGA Logic Synthesis," Formal Methods in System Design, submitted, 2015.

[6] E.-S. Kim, J. Yoo, J.-G. Choi, Y. J. Lee, and J.-S. Lee, “A Technique for Demonstrating Safety and Correctness of Program Translators: Strategy and Case Study,” in The 2nd International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), pp.210-215, 2014.