Proceedings of 2016 IEMEK Symposium on Embedded Technology
(ISET 2016)
Hotel Inter-Citi Daejeon, Korea, 26-27 May, 2016.

A New Equivalence Checker for Demonstrating Correctness of Synthesis and Generation of Safety-Critical Software

Eui-Sub Kim Junbeom Yoo

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

Abstract

FPGA (Field-Programmable Gate Array) has received much attention from nuclear industry as an alternative platform of PLC-based (Programmable Logic Controller) digital I&C (Instrumentation & Control) in nuclear power plants [1,2]. The FPGA is designed with HDL (Hardware Description Language) such as Verilog and VHDL, and the design is synthesized by commercial FPGA synthesis tools, mechanically. This synthesized gate-level designs is placed & routed for identifying physical position in the circuit and mapping for the FPGA resources. Each process needs specific tools, which are provided by the FPGA vendors. This tools has many advantage such as optimization to achieve completive functionality and performance. Nuclear regulation authorities [3], however, require more considerate demonstration of the correctness of the mechanical tools (*i.e.*, COTS dedication).

While simulation is the most widely used technique to verify the equivalency between two programs, this technique has a problem that the quality of the verification is only as good as the quality of the test vector set and the performance is gradually slowed down as the logic size is grown. On the other hand, equivalence checking [4] can check the functional equivalence of two programs, exhaustively. It does not require test vectors nor manual comparisons of simulation techniques. It will provides reasonable clues for demonstrating the correctness of the synthesis and generation tools.

We proposed a VIS-based correctness verification technique [5,6] 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 VIS verification [7]. The technique can prove the equivalence of two program successively, but there are some problems that its performance depends on VIS verification performance and additional translation needs to use VIS engine.

This paper proposes a new combinational/sequential equivalence checker for intermediate program such as FBD (Function Block Diagram) in safety critical development. The first target is FBD program, which is an alternative design program of HDL in the *NuDE* framework [8]. We can now verify the equivalence of two version of FBD programs (an original FBD vs. a modified version FBD). We developed the equivalence checking engine from the scratch, and this engine can directly verify the FBD program without any translation process and any assistance of other checking engine, as discussed in [5].

We are now planning to extend the tool to be used in the tool can be used in anywhere in *NuDE* as depicted in <Fig.1>. If all verifications succeed, we can say that the final software will operate exactly as we intended, and we also can demonstrate the correctness of the used synthesis and generation tools, in regard to the COTS software dedication.

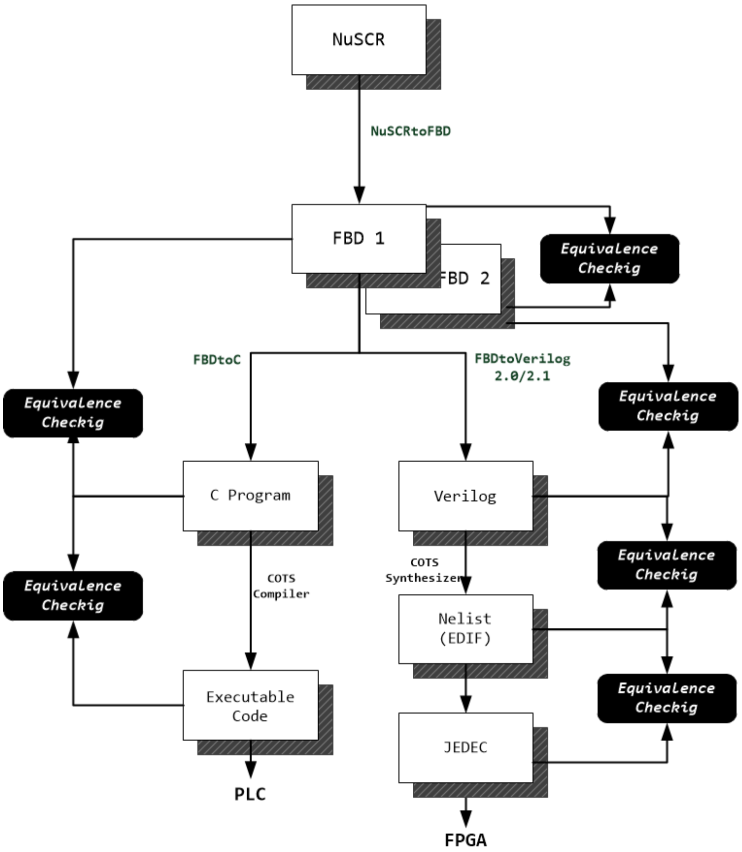

Figure 1. Equivalence Checking processes in compliance with the *NuDE*

Keywords: Function Block Diagram, Combinational Equivalence Checking, Binary Decision Diagram

Acknowledgement

It was also supported by the National Research Foundation of Korea (NRF-2015R1D1A1A02062154).

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] R. E. Bryant. “Graph-Based Algorithms for Boolean Function Manipulation,” IEEE Trans. on Computers, Vol.C-35, No.8, 1986.

[5] E.-S. Kim, J. Yoo and J-Y. Kim, “CVEC: A Customized VIS-based Equivalence Checker for FPGA Logic Synthesis,” Science of Computer Programming, submitted, 2016.

[6] J. Yoo, E.-S. Kim and S. Jung, "Verification Techniques for COTS Dedication of Commercial FPGA Tools," The 10th International Symposium on Embedded Technology (ISET 2015), pp.150-151, 2015.

[7] R.K. Brayton, G.D. Hachtel, A. Sangiovanni-Vincentelli, F. Somenzi, A. Aziz, S.-T. Cheng, S. Edwards, S. Khatri, Y. Kukimoto, A. Pardo, S. Qadeer, R.K. Ranjan, S. Sarwary, T.R. Shiple, G. Swamy, and T. Villa, “VIS: A System for Verification and Synthesis,” Proc. Eighth Int’l Conf. Computer-Aided Verification, 1996.

[8] J. Yoo, E.-S. Kim, D.-A. Lee and J.-G. Choi, “An Integrated Software Development Framework for PLC & FPGA based Digital I&Cs,” International Symposium on Future I&C for Nuclear Power Plants (ISOFIC/ISSNP 2014), 2014.