DATE: 2017/1/10

Department of Electrical and Electronic Information Engineering		ID	M133205
Name	Yoshiki Ishigaki		

Supervisor	Shuichi Ichikawa Naoki Fujieda

Abstract

Title	Hardware implementation and obfuscation of PLC instructions by high level synthesis

An instruction sequence of a programmable logic controller (PLC) is important intellectual property. Techniques for protecting and concealing PLC instruction sequences are required. One of such techniques is implementing PLC instruction sequence by hard-wired logic and obfuscating it. This study achieves it by high level synthesis (HLS) and quantitatively evaluates obtained circuits.

A PLC instruction sequence is converted by a dedicated converter to C, which is further translated into hardware description by an HLS tool. Xilinx Vivado HLS is adopted as an HLS tool. The system was implemented in a Digilent ZedBoard equipped with a Xilinx Zynq-7000 SoC. The PLC instruction sequence was implemented as a coprocessor and driven from software in consideration of hardware/software cooperative design. Opaque pedicates proposed by Collberg et al. is adapted as an obfuscation method.

Vivado HLS can adjust generated circuits by giving directives and options. Ichikawa et al. (2011) proposed several hardware designs of PLC instruction sequences. Tanaka (2016) examined whether these designs can be reproduced by directives and options. This stady further examines and evaluates it using more directives and options on a system considering data transfer with a processor. This has been done in previous studies by Tanaka (2016), but it is inadequate. Therefore, we further study and evaluation. As a result, only Levelized Design (LD) was reproduced, which LD performs parallel execution of the PLC instruction sequence to shorten the execution time. Next, to obtarin a better LD design, several combinations of directives ware examined and compared with the circuit without directive. As a result, the execution time was reduced by 2% at a maximum by the pipeline directive, and the circuit size was reduced by up to 44% by the allocation directive. Differences in execution time among designs were hardly seen because most of the execution time was spent by data transfer. Comparing the previous results with this study, they are comparable in both circuit size and execution time.

Obfuscation was reproduced in a high-level synthesis environment with reference to the framework of opaque predicates implemented by Uyama (2015). This framework uses a strongly connected graph as a branch condition, and adds a false PLC instruction for a fake branch destination. Uyama changed both the type and the operands from the original instruction for a fake instruction, while this study only changes the instruction type. As a result, the additional execution time was less than 1% of the system without obfuscation. The circuit size increased by up to 2.5 times, and increase rate depended on the scale of the original circuit. Although the increase rate of the circuit size is larger than that of Uyama, both of them showed the same characteristics. Therefore, it was found that Opaque Predicates implementation similar to Uyama was also possible by the high level synthesis environment.