Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 25-26, 2012

Fault mode and Optimization Design of FPGA-based Applications for Instrumentation and Control System of NPPs

Joon-Ku Lee[1], Je-Yun Park[1], Yang-Mo Kim[2]
[1]Research Reactor Engineering Division, Korea Atomic Energy Research Institute
[2]Department of Electrical Engineering, Chungnam National University
Mail to: jklee@kaeri.re.kr

1. Introduction

Intuitively Field Programmable Gate Arrays(FPGA) technology is replacing the high level of micro-processor type equipped with various software and hardware which causes acceleration of the aging and obsolescence, and demands for system modernization in I&C system in Nuclear Power Plants. FPGAs are highlighted as an alternative means for obsolete control systems. When the instrumentation and control system of NPPs is designed with FPGAs, it is important to meet the system development life cycles and conduct the verification and validation activities regarding to FPGA-based applications. Because the knowledge of both the software and hardware is needed in a FPGA-based application design, engineer should consider the characteristics of FPGA such as faults mode, and optimization technique. And also these characteristics should be reflected in verification and validation activities.

2. FPGA-based Applications

2.1 Development Life Cycle for FPGA-based Applications

FPGA-based applications have been developed in consideration of the needs described above, and should be developed according to Figure 1 in IEC 61513[1], the system development life cycle complemented in IEC 60880[2] and IEC 62138 for software development, and IEC 60987[3] for the hardware development of a computer based system. The core design requirement of FPGA-based application is based on the IEC 62566[4] standard, which addresses the HPD (Highly-reliable Programmed Devices) in nuclear society. IEC 62566 illustrates in more detail the phases between the specifications of the requirements and validation for the system components.

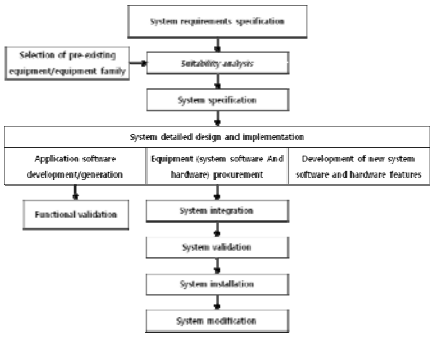


Figure 1 IEC 61513 System Development Life Cycle

2.2 Characteristics of FPGA-based Application Design

The FPGA delivers tremendous advantages of flexibility, productivity, and performance to industry. With these advantages, it can be applied to nuclear power plants. To ensure its application, it is necessary to investigate the characteristics of FPGA-based applications design and inherent potential faults. The FPGA inherently has a glitch problem owing to this time-delay, which can be hazardous or cause potential faults to the instrumentation and control system of nuclear power plants. These features can cause a metastability to occur Therefore, software engineers should be able to identify the timing problems in a design and modify or optimize the design. The design process and verification process should proceed iteratively, and together, until the logic and devices are ensured, such that the required functions are guaranteed and no potential faults are found. Nevertheless, with these limitations, the system designers of nuclear power plants try to use FPGA nowadays.

2.3 Fault mode of a FPGA

Engineers should consider the fault modes of a FPGA in terms of hardware and software faults. The hardware fault mode is usually related to short or open in the circuits of FPGA. The software fault mode is a type of design error caused by humans. Each clock used in FPGA, no matter the rate of the clock, has a low skew. Logic circuits use boolean gates to perform certain functions as a result of certain inputs. An ideal gate has an instantaneous change in state when its inputs change, but in reality there is actually some delay. Engineers need to investigate and collect faults that have occurred during HDL programming. In FPGA, fault modes are mostly timing problems. The setup and hold time violations are mostly caused by asynchronous timing. Engineers should consider the setup and hold time for the design process. A setup and hold time violation may cause metastability, glitch, and other timing problems. And also a time variation such as a setup or hold time violation may be caused by the device heating. Software engineer or logic designer always thinks synthesized hardware, because FPGA is controlled by clock. In the implementation phase, potential faults, mostly timing hazard, are below.

Table. 1 Classification of fault modes

	Fault modes

Clock slack	•Loose state of clock timing, as in Figure 2
Clock skew	•Unintended state of the different arrival times in different flip flops with the same clock, as in Figure 3
Glitch	•Glitch in digital logic is a short-lived fault in the logic system owing to a change at the input. Glitch is the inherent characteristic of logic design caused by asynchronous timing, as in Figure 4
Metastability	•Metastability is an undefined state, when the output of the flip-flop is not 0 or 1, as in Figure 5, and is mostly caused by setup/hold time violation. Asynchronous logic can create a matastability state that can seriously degrade the performance of the design or destroy the functionality.

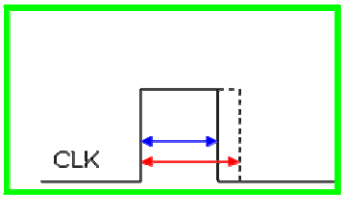


Figure 2 Clock slack

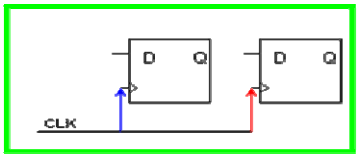
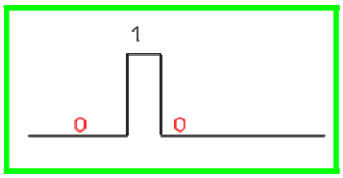


Figure 3 Clock skew



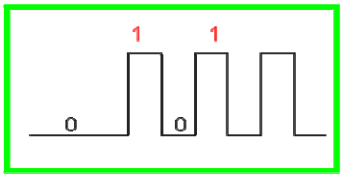


Figure 4 Glitch

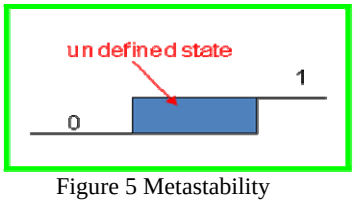


Figure 5 Metastability

2.4 Optimization to reduce the potential faults

Up to now, potential faults have been addressed in the design and implementation phases. To reduce or eliminate the potential faults, it is important to fix the setup and hold time. The optimization techniques are to fix the setup time and the hold time. An optimization technique such as a karnaugh map is also applied to reduce the number of gates and the delay time in a circuit.

Setup time fixing techniques are as below.

1) Reduce the combinational logic delay by minimizing the number of logic levels.
2) Split the complex combinational logics.
3) Use a double synchronizer using flip flops.

Hold time fixing techniques are as below.

1) Add delays on the input ports, if the delay time is needed.
2) Adjust the clock speed.

3. Conclusion

When engineers design the instrumentation and control system of NPPs with FPGA, they generally decompose the function of system into subsystem or blocks, and then implement the function of system into a FPGA chip. At that time, top-down approach will enhance the generic design process. hardware description language provides both the top-down approach and bottom-up approach, and various advantages. It is important to meet the system development life cycles and conduct the verification and validation activities regarding to FPGA-based applications for used in NPPs. This paper presented faults mode in FPGA-based applications that are important to design and implementation phases. Engineers need to investigate and collect faults which have occurred during a HDL programming. And also engineer should consider optimization technique. In the verification and validation processes, a review, test and analysis activities should be properly conducted in the consideration of the characteristics of FPGA, HDL programming, and faults mode.

REFERENCES

[1] IEC 61513, Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems.
[2] IEC 60880, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.
[3] IEC 60987, Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems.
[4] IEC 62566, Selection and use of complex electronic components for systems performing category A functions.
[5] JoonKu LEE, GwangIl JEONG, YongSuk SUH, YangMo Kim, Development of Digital Instrumentation and Control Technology using Field Programmable Gate Array for Nuclear Power Plants, A transaction of the Korean Electronics Engineering Society Autumn Meeting, 2011.
[6] K. Y. Sohn, W. J. Yi, J. K. Lee, I. S. Koo., "PROTECTION AND CONTROL WITH FPGA", The 18th Pacific Basin Nuclear Conference (PBNC 2012), BEXCO, Busan, Korea, March 18 ~ 23, 2012.