Field programmable gate array-based I&C safety system

KIM Hyun Jeong, HWANG In Seok, KIM Young Geul, KWON Jong Soo, CHOI Woong Seock, SOHN Se Do, and BAEK Seung Min

1-7.I&C System Eng. Dep't, KEPCO E&C, Daejeon 305-353, Korea (hjkim[1], narosoo[2], young.g.kim[3], jskwon[4], cwkjc[5], sdsohn[6] , smbaek[7] @kepco-enc.com)

Abstract: The PLC (Programmable Logic Controller)-based I&C safety system used in the operating nuclear power plants has the disadvantages of a CCF (Common Cause Failure), high maintenance costs and quick obsolescence, and then it is necessary to develop the other platform to replace the PLC. The FPGA (Field Programmable Gate Array)-based I&C (Instrumentation & Control) safety system is safer and more economical than the PLC-based I&C safety system. Therefore, the FPGA-based I&C safety system will be able to replace the PLC-based I&C safety system in the operating and new nuclear power plants to benefit from its safety and economic advantage. The FPGA-based I&C safety system is being developed and verified by applying the related requirements to perform the safety function. This paper describes the requirements, implementation, verification, software development tools, and hardware qualification of the FPGA-based I&C safety system in the nuclear power plant.
Keyword: FPGA; I&C safety system; V&V

1 Introduction

Currently, I&C (Instrumentation & Control) safety system is implemented using the PLC (Programmable Logic Controller)-based system. The PLC-based system that consists of various software implemented on microprocessors is inherently prone to the CCF (Common Cause Failure: Multiple failures attributable to a common cause), and has high maintenance costs, quick obsolescence, *etc*. To overcome this disadvantage, it is necessary to develop an alternative platform to the PLC-based system.

The FPGA (Field Programmable Gate Array) is generally used in the IC (Integrated Circuit) development. The structure of FPGA-based system is very simple and a CCF is less likely to occur. Main advantages of using the FPGA are as follows:

1) No runtime operating system
2) High speed parallel processing
3) High safety, reliability and economics

Therefore, the FPGA-based I&C system can replace the PLC-based I&C safety system.

In addition, the difference between PLC and FPGA is described in Table 1.

Table 1 Difference between PLC and FPGA

Characteristic	PLC	FPGA
Implementation	Serial	Parallel
Code & Data	Memory	Gate Cell
Signal Processing	Serial	Parallel
Processing Speed	High	Ultra High
Functional Capacity	No limit	Limit
Peripheral Circuits	Complex	Simple
Language	C, Assembly	VHDL, Verilog
Targeting	Compile, Link	Synthesis, Place & Route

This paper describes the requirements, implementation, verification, software development tools and hardware qualification of the FPGA-based I&C safety system to enhance the safety, reliability and economics compared to the PLC-based I&C safety system.

2 Requirements

To implement I&C system functions using FPGA, many standards and guidelines have been provided as references [1] through [8]. The key requirements

Received date: October 10, 2014
(Revised date: October 28, 2014)

related to design the FPGA-based I&C safety system are CCF prevention, software integrity level, life cycle and cyber security as described in the following sections.

2.1 CCF prevention

To prevent the CCF by software errors or software logic malfunction, the safety system shall be provided with diversity and testability in design. Diversity and testability design shall be sufficient to eliminate a software-based or software logic-based CCF.

Diversity in I&C safety system can be implemented using the following features [2].

1) Design
2) Life cycle (human)
3) Equipment manufacturer
4) Logic processing equipment
5) Logic
6) Function
7) Signal

For testability, a system shall be sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested)[1].

2.2 Software integrity levels

SILs (Software Integrity Levels) are classified by the software complexity, criticality, risk, safety level, and security level (Reference [5]). SIL 1 software element must execute correctly or intended function will not be realized, causing negligible consequences, and SIL 2 software element must execute correctly, or an intended function will not be realized, causing minor consequences. SIL 3 software element must execute correctly, or the intended use (mission) of the system/software will not be realized, causing serious consequences. SIL 4 Software element must execute correctly or grave consequences will occur.

2.3 Life cycle

Figure 1 shows the HPD (HDL(Hardware Description Language)-Programmed Devices) development life-cycle for the HPD project. The approach proposed for development is based on the traditional "V cycle" model and is also recommended in Reference [9].

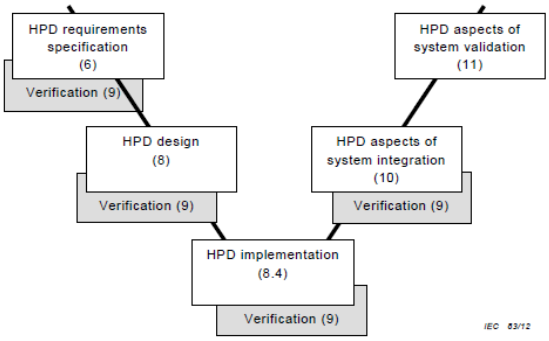

Fig 1. Development life-cycle of HPD[6].

2.4 Cyber security

The objective of cyber security is the protection of computer hardware and/or software from accidental or malicious access, use, modification, destruction, or disclosure. Cyber security also pertains to personnel, data, communications, and the physical protection of computer installations. The protection of information and data shall be provided so that unauthorized persons or systems may not read or modify them and, furthermore, unauthorized persons or systems are denied access to them as described in reference [7].

3 Implementation

The FPGA-based I&C system is being designed to meet the requirements of Section 2 as follows:

3.1 CCF prevention

Diversity and testability methods are adopted in the I&C safety system to prevent the CCF. The diversity with FPGA-based I&C safety system can be implemented using various methods which are described in Table 2. For example, the DPS (Diverse Protection System) is used to meet the diversity for reactor trip and auxiliary feedwater actuation functions of PPS (Plant Protection System) in I&C safety system. The DPS and PPS each use a different designer, equipment manufacturer, logic processing equipment, *etc.*

The FPGA-based I&C safety system software is simplified and segmented functionally such that the 100% testability can be achieved. The

simplified and segmented software eventually results in the simplified test procedure and segmented test scope to perform 100% testability.

Table 2 Methods to implement the diversity

Diversity	Methods
Design	Digital vs. analog, or PLC vs. FPGA
Life cycle (human)	Different development, implementation and test teams
Equipment manufacturer	Different manufacturers (*e.g*., Actel vs. Xilinx)
Logic processing equipment	Different equipment or data flow architectures
Logic	Different algorithms or orders of execution
Function	Different response time scales
Signal	Different process parameters

3.2 Software integrity levels

The software of I&C safety system is classified as the SC (Safety Critical) level (SIL4) or (ITS (Important To Safety) level (SIL3). The safety actuation for reactor protection function, engineered safety feature actuation function and safe shutdown functions in I&C safety system are to be implemented as SC level. The monitoring and test functions for SC level in I&C safety system are to be implemented as a SC or ITS level. Generally, the FPGA-based I&C safety system consists of the FLC (FPGA-based Logic Controller), MTP (Maintenance and Test Panel), and ITP (Interface and Test Processor). According to the SIL requirements, the FLC software is designed as the SC level and MTP/ITP software is designed as the SC or ITS level. The FLC and MTP/ITP software are designed to meet the requirements of the related SC and ITS levels as Table 3.

Table 3 SIL Requirements and applications

SIL Requirements	Classification	
	SC level	ITS level
V&V (Verification & Validation	Strict Independent	Moderate Independent
Safety Analysis	O	O*
Cyber Security	O	O
COTS	O	O
Suitability Analysis	O**	O**

O: Implementation is required.

O*: If not implemented, justification analysis is required for its validity.

O**: Implementation of suitability analysis per detail lifecycle phase is required.

3.3 Life cycle

The FPGA-based I&C safety system is developed as Fig. 1, and the process is described below.

3.3.1 HPD requirement specification

HPD requirement specification is documented such as SysRS (System Requirement Specification) and/or SRS (Software Requirement Specification).

3.3.2 HPD design

HPD design is documented such as SDD (Software Design Description).

3.3.3 HPD implementation

HPD implementation is coded by VHDL or Verilog code, *etc*. The VHDL code certified by IEEE 1076 is more stringent than Verilog code. It is preferred to use VHDL code to meet I&C safety system requirements.

HPD implementation processes the synthesis, and P&R (Place and Route). The synthesis and P&R are implemented using the integrated design environment tools that provide the output waves before and after the synthesis and P&R.

The base attributes which facilitate the predictability of the FPGA internal logic design are as follows: [8]

1) Asynchronous design

   The FPGA-based system is designed as synchronous as much as possible. Asynchronous designs are prone to glitches, bus skews, and other timing issues. Furthermore, the FPGA design tools do not generally support asynchronous timing constraint and analysis. If asynchronous designs are used for 100 % testability or any other reason, appropriate measures need to be taken to make sure that the output glitches and the

bus skews are not affecting the safe operation of the FPGA design.

2) Metastability
   Metastability can occur when an asynchronous input gets clocked within the FPGA, and it is expressed as an undetermined state. The undetermined state resolves itself after the recovery time, which is on the order of several ns to several tens of ns for most of FPGAs.
3) Internal FPGA Reset
   All flip-flops in FPGAs are cleared after the power-up unless specified differently by the designer, in which case a dedicated synchronous/asynchronous reset network controlled by the reset logic inside the FPGA is used. Care is taken to ensure synchronous reset of all flip-flops across the FPGA. This is especially critical when an asynchronous reset signal is used to clear counter or state machines that need to run synchronously.
4) PLL (Phase Locked Loop) Locking Time
   PLL inside FPGA is used to generate synchronous clocks or to fine-control signal delays. They require an additional time to lock after the FPGA power-up.
5) Time Constraints
   Most of FPGA design tools base their timing constraints and analysis on synchronous design. The timing constrains include the period.
6) State Machines
   Behavior of a state machine is defined not only for the used states but also for the unused states. Most synthesis tools ignore unused states and synthesize a state machine that can become stuck in an undefined state after entering it unexpectedly.
7) Multiple Clock Domains
   When designing the interface between clock islands that use different synchronous or asynchronous clock, one uses double register for edge-sensitive transfers to mitigate the occurrence of metastability.
8) Latches
   Even though latches use fewer gates than conventional flip-flops, special care is taken when the use of latches is necessary as the noise occurring at the latch inputs may propagate to the latch outputs.

3.3.4 HPD aspects of system integration

System integration of HPD is implemented by loading the software on the hardware.

3.3.5 HPD aspects of system validation

The system validation is performed by the channel software test using the DCS (Distributed Control System), logic analyzer or I/O simulator after system integration. All FPGA-based I&C safety function including the monitoring function is tested via one channel software test.

3.4 Cyber security

Six (6) methods to meet cyber security requirements are applied as follows:

1) The first method is to use the Antifuse device that is the most secure programmable device available.
2) The second method is to maintain the communication separation between the control function (SIL4) and monitoring function (SIL3) such that the monitoring function failure does not affect the control function.
3) The third method is to use the special device or administrative control during the software change to prevent unintentional change of software by external access.
4) The fourth method is to apply the encryption techniques such as CRC (Cyclic Redundancy Check) or Checksum, during signal transmission.
5) The fifth method is to verify the cyber security function during the software verification and validation.
6) The sixth method is to use the password, manual switch or cabinet lock device for allowing external access.

4 Verification and Validation

The V&V (Verification and Validation) of FPGA-based I&C safety system is performed as Fig. 1 and the detailed process is described below.

4.1 V&V of HPD requirements specification

The V&V of HPD requirements specification is performed using the RTM (Requirements Traceability Matrix).

4.2 V&V of HPD design

The V&V of HPD design is performed by comparing the results between the other unused code (*e.g.*, Verilog) and used code (*e.g.*, VHDL) using the same testbench program. In addition, the code coverage analysis is performed for HPD verification. The code coverage consists of the statement coverage, branch coverage, expression coverage, condition coverage, finite state machine coverage, and toggle coverage. The code coverage analysis can be performed using the integrated design environment tools.

4.3 V&V of HPD implementation

The V&V of HPD implementation is performed by module test. That is, the V&V of HPD is implemented through the comparison with output waves before and after the synthesis and P&R using the HPD module units. In addition, it is possible to verify the HPD using other integrated design environment tools not used. In this case, verification can be performed comparing the output waves between other integrated design environment tool not used and integrated design environment tool used.

The V&V of HPD implementation is achieved using the SDD document. That is, HPD functions are confirmed if the HPD functions implement all SDD functions.

4.4 HPD V&V of system integration

The HPD V&V of system integration is achieved by unit test using the DCS, logic analyzer or I/O simulator. The unit test confirms that the test results for the system integration are same as the module test results for HPD implementation.

4.5 HPD V&V of system validation

The system validation is performed by the channel software test using the DCS, logic analyzer or I/O simulator after system integration. All FPGA-based I&C safety functions including the monitoring function can be tested via channel software test.

5 Software development tools

There are several software tools to develop the HPD code, synthesis and P&R. The software of I&C safety system is verified to meet the safety function requirements. Software development tools for FPGA-based I&C safety system in nuclear plant are not authenticated yet. Therefore, software development tools shall be certified by licensing authority or through the basis on operating experience for the applicability to the FPGA-based I&C safety system.

The safety function using FPGA software in the aircraft or space industry has been developed in accordance with DO-254 requirements[10]. For example, “Questasim”, “Precision” or “Formal pro” software development tool by Mentor graphics meet the DO-254 requirements, and are already certified in aircraft and space industry [11]. These software tools are used for simulation and V&V of HPD code.

These software development tools to implement the safety function in aircraft or space industry can use the design the FPGA-based I&C safety system. In this case, the additional certification is required to apply the safety function in nuclear power plant.

6 Hardware qualification

The Hardware of I&C safety system shall be implemented as Quality Class 1E (Q, Safety Class 3) to perform safety functions and operations during normal, abnormal, and DBE (Design Basis Event) condition in accordance with the Reference [12]. I&C safety system is expected to be mainly installed in a mild environment and therefore, the only DBE of consequence is a seismic event.

The hardware qualification of I&C safety system to meet the Quality Class 1E requirements includes the following:

1) Environmental Qualification
2) Seismic Qualification
3) EMC Qualification

Therefore, the hardware of FPGA-based I&C safety system is qualified via the equipment qualification and operating experience to install in the nuclear power plant, *etc*.

7 Conclusions

The FPGA-based I&C safety system is safer and more economical than the PLC-based I&C safety system. Therefore, it is necessary to develop the FPGA-based I&C safety system.

The FPGA-based I&C safety system is being implemented and verified in accordance with the requirements. The software development tools to implement the FPGA-based I&C safety system will be certified by operating history or licensing authority for nuclear application. In addition, hardware qualification is applied to meet the Quality Class 1E requirements.

Since the FPGA-based I&C safety system has been considered indispensable for the application to the safety functions such as reactor trip and engineered safety features actuation, continued efforts are being employed in the nuclear community for its development at reasonable expenses and in short period of time.

In the future, the FPGA-based I&C safety system will replace the PLC-based I&C safety system in the operating and new nuclear power plants for being benefited from its safer, more reliable and economic advantages.

Acknowledgement

This project has involved heavy efforts and concentration. It would not have been possible without the kind support and help of many individuals and organizations. The authors would like to extend their sincere thanks to all of them.

The authors sincerely appreciate the I&C system engineering group for their guidance and constant supervision.

References

[1] NUREG 0800, SRP BTP 7-19, 2012, “Guidance for Evaluation of Diversity and Defense-In-Depth in digital computer-based instrumentation and control systems”.
[2] NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems”
[3] IEEE Std. 603, 1998, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”
[4] IEEE 7-4.3.2, 2010, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”
[5] IEEE Std. 1012, 2004, “Standard for software verification and validation”.
[6] IEC 62566, 2012, “I&C-Development of HDL programmed integrated circuits for systems performing category a function”.
[7] KINS Regulatory Guide 8.22, “Cyber security”
[8] NUREG/CR-7006, “Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems”
[9] IAEA guide NS-G 1.3 : 2002, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
[10] RTCA/DO-254, “Design Assurance Guidance for Airborne Electronic Hardware”
[11] Mentor Graphics Corporation, “Assessing the ModelSim and Questa Tools for Use in DO-254 Projects”.
[12] IEEE Std. 323, 2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations”