Transactions of the Korean Nuclear Society Spring Meeting
Gwangju, Korea, May 30-31, 2013

FPGA-based dual controllers

wooseok Heo[a*], kwang-young SOHN[a], jun-ku LEE[b], geun-ok PARK[b]
[a]*Nuclear Engineering, Korea Reliability Technology and System (KoRTS)*
[b]*Research Reactor Engineering Division, Korea Atomic Energy Research Institute (KAERI)*
Corresponding author: gopark@kaeri.re.kr

1. Introduction

Field-programmable gate arrays (FPGAs) are gaining increased attention worldwide for application in nuclear plant instrumentation and control (I&C) systems, particularly for safety applications. Use of FPGAs has potential to reduce complexity and the associated burden of gaining regulatory approval and also provide better protection against obsolescence as compared to conventional microprocessor-based systems, which have been the technology of choice over the last two decades. [1] This report addresses the activities and result to develop the FPGA-based dual controller performed by Korea Reliability Technology and System (KoRTS) and Korea Atomic Energy Research Institute (KAERI).

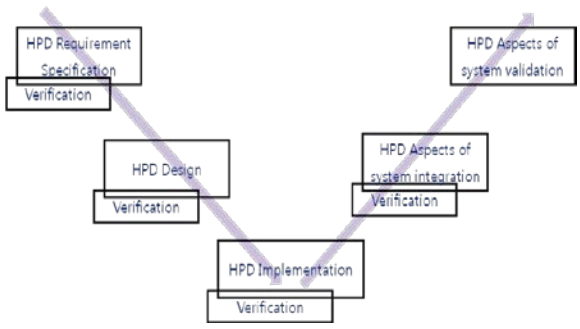
2. FPGA-based dual controller

2.1 planning

As a early phase, project planning, market review and feasibility study for part selection for development. Also firmware verification and validation plan and configuration management plan in order to define the design document list are produced in planning/conceptual phase.

2.2 SDLC development.

According to the IEC 62566, the system firmware requirement is developed.



Software development plan, configuration plan and verification and validation plan is developed, and according to it, design document is prepared for system firmware integrity. Prototype FPGA-based redundant controller is inspected based on NUREG-7006, and verified and validated by IEEE 1012. Also equipment qualification is conducted according to the IEEE Std. 323 and EPRI TR-107330 except destructive testing with an application of Diverse Protection System (DPS) of YongGwang nuclear power plant unit 3 &4. For upgrading the reliability of FPGA-based dual controller, the ELT (Estimated Life Time) of hardware component and Failure Mode and Effect Analysis (FMEA) have been conducted.

The hardware specification is as follows.

3.1 Product Highlights

- FPGA-based controller with redundant Backplane interface
- Proven in-use reliability
- Categorized flexible redundancy management
- Comprehensive on-line diagnostic
- Extremely hard real-time (Non-delay) response time
- Hot-swapping of modules
- High resistance to external impacts
- Usable 15 slot except for two(2) Power Supply Module

Figure 1 FPGA-based redundant controller

3.2 Set of Input Modules

- Analog Input Board(AIB)
  - Enhanced self-diagnostic
  - Enhanced I/O diagnostics
  - 16 independent analog input channels
  - 16-bit A/D conversion
  - Integrity usingCRC-CCITT
  - Hot swappable
- Contact Dry Input Board(CIB)
  - FPGA-based
  - Enhanced self-diagnostic
  - 16 independent input discrete channels (“dry” contact type)
  - Enhanced diagnostics of inputs
  - Hot swappable
- FPGA Process Board(FPB)
  - FPGA-based
  - Dedicated FPGA chip for user

configurable control logic
  - Enhanced self-diagnostics
  - Integrity checks on each communication line(CRS)
  - One-directional dual backplane bus for only failover between FPGA Process Board
  - RS-422 communication line
  - Hot swappable
- Analog Output Board(AOB)
  - FPGA-based
  - Enhanced self-diagnostic
  - 16 independent output channels
  - 14 bit D/A conversion in each digital input channel
  - Enhanced diagnostics of output current channels
  - Integrity checks on each input
  - Hot swappable
- Contact Dry Output Board(COB)
  - FPGA-based
  - Enhanced self-diagnostics
  - Integrity checks on each communication line (CRC)
  - 16 independent digital A-form relay isolated output channels
  - Fuse protected outputs
- CoMmunication Board(CMB)
  - FPGA-based
  - Enhanced self-diagnostics
  - One(1) 100 BASE-FX Ethernet communication line and one(1) RS-422 serial link
  - Integrity checks on each communication line (CRC-CCITT)
  - Hot swappable
- Power Supply Modules (PSM)
  - Overvoltage / Overcurrent protection
- Chassis and Backplanes (Redundant)

3. Failover

The controller is composed of 2 identical FPGA board. According to the status of each board, each controller can acquire the mastership or relinquish the mastership. FPGA-based controller is designed not to exceed the 40 ms of failover time, and automatically synchronized on application termination.

Through the well-defined State Transition diagram for failover, the exclusive ownership is always guaranteed. When each FPGA board is exchanging the heartbeat information, it is recognizable to FPGA generating the heartbeat is master or slave by the help of discriminating the Least Significant Bit (LSB).

4. Diagnostics

FPGA-based dual controller performs the diagnostic function that is necessary for safe operation of major component such as function, processor and memory. The frequency of most diagnosis function is within 10ms. The specific method to diagnose is to monitor the watch-dog timer, every boards including I/O board and communication board, low voltage, and CRC-CCITT for data exchange. Also the main Arithmetic FPGA is monitored by Watchdog FPGA that is also watched by Watchdog Timer conservatively in order to keep highly reliable controller status.

5. Verification and validation

System firmware and application firmware of Diverse Protection System (DPS) is verified and validate according to the IEEE 1012[3] and inspected based in NUREG-7006[2]

6. Equipment Qualification

Except the destructive testing, burn-in test for 352 hours and environment (temperature and humidity) test for 92 hours have been conducted in KIMM according to the IEEE Std. 323[4], EPRI TR-107330[5]. The EQ is successful and reported through Reference [6].

7. Reliability Issues

The component consisting of FPGA board is estimated for life time evaluation. This report shall be revised due to the some of component replacement.

5. Summary

The FPGA-based dual controller development has be completed and it is time to keep upgrade and optimize the hardware platform. The running of DPS on developed platform is successful and stable. Furthermore it is needed to conduct the long time running test for reliability.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012M2A8A4025979)

REFERENCES

[1] EPRI-TR 1019181, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems, 2009
[2] NUREG-7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems
[3] IEEE 1012, software verification and validation
[4] IEEE Std. 323, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
[5] EPRI TR-107330, Generic requirements specification for Qualifying a commercially available PLC safety-related applications in nuclear power plants
[6] KIMMRAC-N0140-120315-00000, Visual Inspection, Burn-in and environment report, KIMM