Qualification of FPGA-Based Safety-Related PRM System

Tadashi Miyazaki, Naotaka Oda, Yasushi Goto, Toshifumi Hayashi

Toshiba Corporation, Yokohama, Japan

Abstract. Toshiba has developed Non-rewritable (NRW) Field Programmable Gate Array (FPGA)-based safety-related Instrumentation and Control (I&C) system. Considering application to safety-related systems, nonvolatile and non-rewritable FPGA which is impossible to be changed after once manufactured has been adopted in Toshiba FPGA-based system. FPGA is a device which consists only of basic logic circuits, and FPGA performs defined processing which is configured by connecting the basic logic circuit inside the FPGA. FPGA-based system solves issues existing both in the conventional systems operated by analog circuits (analog-based system) and the systems operated by central processing unit (CPU-based system). The advantages of applying FPGA are to keep the long-life supply of products, improving testability (verification), and to reduce the drift which may occur in analog-based system. The system which Toshiba developed this time is Power Range Neutron Monitor (PRM). Toshiba is planning to expand application of FPGA-based technology by adopting this development process to the other safety-related systems such as RPS from now on. Toshiba developed a special design process for NRW-FPGA-based safety-related I&C systems. The design process resolves issues for many years regarding testability of the digital system for nuclear safety application. Thus, Toshiba NRW-FPGA-based safety-related I&C systems has much advantage to be a would standard of the digital systems for nuclear safety application.

1. INTRODUCTION

Nuclear Power Plants I&C systems was analog-based in the beginning. In 1980 and 90 computer-based I&C systems have developed. In particular, the system used in Advance Boiling Water Reactor (ABWR) is the world first fully digital I&C system for BWR plants. The computer-based I&C systems have many advantages compared with older analog-based systems. The computer-based I&C systems are free from drift issues that annoyed the maintainer of the analog-based system. The computer-based I&C systems have many advanced features, including some automatic functions, which any analog-based systems cannot provide. These advanced features of computer-based I&C systems have been contributing to safe operations of nuclear plants.

Because the computer-based I&C systems are safety-related, they are required to be subject to V&V in regulations and standards. However, abundant functions and resulting complexity of software make the V&V of computer-based I&C systems time-consuming and expensive. In addition, computer-based systems use micro-processors produced in semiconductor industry, which have shorter product life cycle compared with that in nuclear industry. Most micro-processors may be obsolete within years.

FPGA has been developed in semiconductor industry through 1990. Unlike ordinary semiconductor devices or Application Specific Integrated Circuit (ASIC), circuits in FPGAs can be determined or programmed after they were shipped from semiconductor foundries. Therefore, it is suited for low volume applications, such as those in nuclear industry.

Because, an FPGA is a semiconductor device, and its function is determined by the circuit embedded in the device, FPGAs operate without Operating System (OS) or complex applications that are necessary for computer-based I&C systems. Generally speaking, FPGA-Based I&C systems is simpler than computer-based I&C systems, and that makes V&V efforts simpler and affordable.

In addition, FPGA vendors tend to offer long term support of their products compared with microprocessor vendors.

Considering those benefits, Toshiba chose FPGA as a next generation device for nuclear power plants I&C that could succeed the microprocessors, and has developed FPGA-Based I&C systems. Toshiba employed FPGAs for radiation monitors for non-safety related system, first. The radiation monitors were applied for Japanese nuclear plants, and have been marked excellent operating experiences. And on the experiences, Toshiba has established the FPGA-based safety-related I&C system design process that conforms to the US nuclear regulation. This paper describes the Toshiba FPGA-based safety-related I&C design process, and the qualification result of the FPGA-based PRM System in accordance with the established process.

2. FPGA-BASED PRM SYSTEM

2.1. FPGA

An FPGA is a type of logic chip that can be programmed. The FPGA incorporates thousands of logic cells linked by programmable switches that logically interconnect cells to meet different design requirements. In addition to logic cells, other programmable elements of an FPGA are (1) I/O blocks, which serve as the interface between internal signal lines and the chip's external pins, and (2) interconnects, which route I/O signals of the other elements to appropriate networks. An FPGA can only implement digital logic. For FPGA-based safety-related products, Toshiba selected NRW-FPGA that is one-time programmable devices. FPGA based on the same technology has been applied to satellites, military, aerospace, aircraft, etc., the fields where reliability is of primary importance.

Because the NRW-FPGA is one-time programmable, the devices using the FPGA are free from the issues that programs embedded in the FPGA may change during operation or maintenance inadvertently.

2.2. Functional Elements

A Functional Element (FE) is defined as the minimum logical functional element in an FPGA. Each FE contains a simple logic functions that can be verified through exhaustive or full pattern testing. Full pattern testing is not practical for digital circuits as large as nuclear power plants safety-related I&C systems, because the number of input signal combinations may become so great that testing cannot finish in a practically acceptable time. The size of an FE is limited by the time needed to complete full pattern testing. FPGA is programmed using combinations of verified FE. Fig. 1 illustrates the concept how an FPGA is composed of FE.

To ensure that FPGA is correctly built from FE, the connections between FE must be confirmed. Toshiba surveyed testing techniques used in the semiconductor industries, and determined to use the toggle coverage ratio as a tool to judge if the test cases are sufficient to confirm the connections. In a FPGA test, connections between FE is exercised from logic zero to logic one, and from logic one to logic zero, by test signals. The toggle coverage ratio is obtained by dividing the number of exercised connections by the number operable connections. Note that some connections are directly linked to a ground line, or a power line. These connections are not operable.

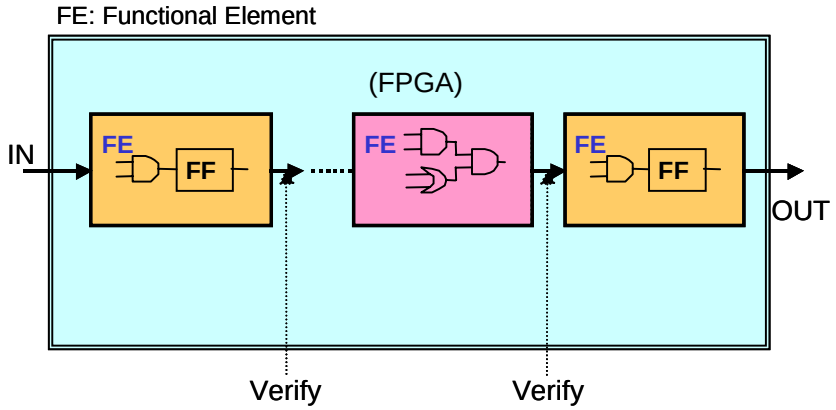

Fig. 1. Toshiba FPGA Structure

2.3. FPGA-Based PRM System

The PRM measures the neutron level in the BWR core from 10 percents through up to 125 percents of its rated power.

Fig. 2 illustrates the PRM system of the BWR. The PRM obtains electrical signals from the neutron detectors distributed in the core, and differential pressure transmitters placed at each recirculation loop. The number of neutron detectors is 172 for typical BWR-5 plants. The PRM consists of units. The unit is a chassis that has front slots and back slots to mount modules. Each unit consists of several modules. There is a vertical middle plane between the front and back slots in each unit. This plane consists of two circuit boards. These circuit boards provide backplanes for the front and rear modules. Modules plug into the backplanes using connectors. Once a module is plugged into the appropriate connector, it exchanges data with other modules in the unit, it connects to other units and any external field equipment, and it is powered.

Each module consists of one or more printed circuit boards and a front panel. The printed circuit boards have some FPGAs for signal processing and for the Human Machine Interface (HMI). The front panel is connected to the HMI FPGA, and allows plant operators or maintenance personnel to set appropriate setpoints.

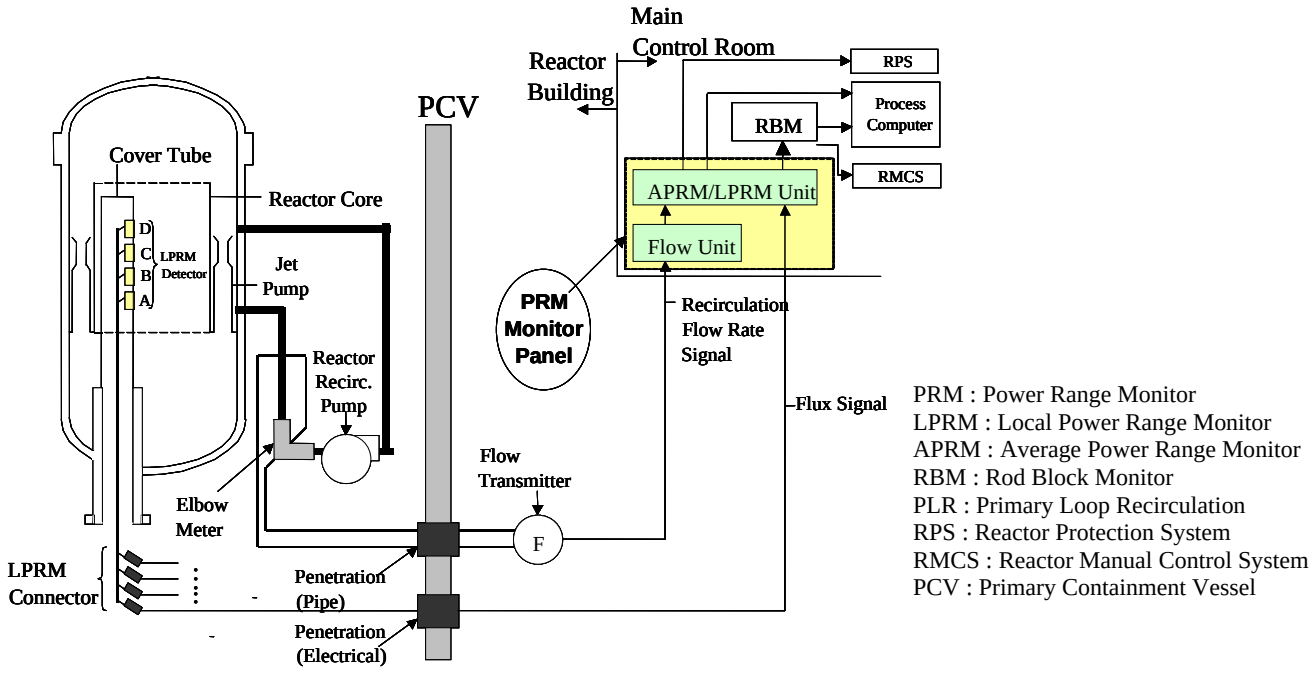

Fig. 2. PRM for BWR Plants

The PRM has the Local Power Range Monitor (LPRM) modules that corresponds to each neutron detector. Fig. 3 shows the configuration of the LPRM module. The LPRM module obtains an electrical signal from the detector, amplifies the signal, and converts the analog electrical signal to the digital signal. The filter FPGA in the LPRM module applies a digital filter to reduce noises caused from commercial power supply.

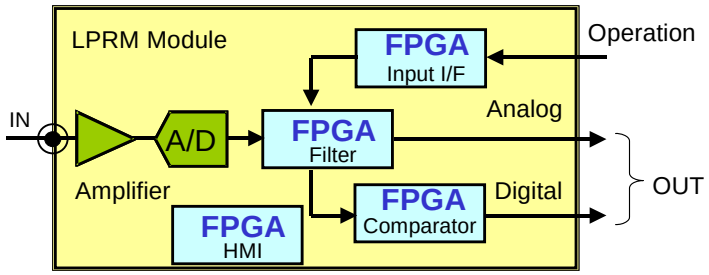

Fig. 3. Module Structure

The LPRM module multiplies a gain value on the filtered signal, and produces the LPRM level, which is transmitted to an Average Power Range Monitor (APRM) module included in the PRM, and to external devices through analog output modules. The LPRM module compares the LPRM level with a pre-determined setpoint, and if the LPRM level exceeds the setpoint, the LPRM module generates an alarm.

In addition, the LPRM module has the Input/Interface and HMI FPGAs, which allow the plant maintenance personnel calibration and setpoint change.

The APRM module has several FPGAs to average up to 22 LPRM levels from the LPRM modules placed in the same PRM, and produces the APRM level that indicates the average reactor power. In addition, the APRM module compares the APRM level with pre-determined setpoints, and if the APRM level exceeds one of the set points, the APRM module generate an alarm or a trip signal. The APRM level High-High is a typical trip signal that initiates a reactor scram.

Fig. 4. is a photograph of the LPRM/APRM unit mounting ten LPRM modules, one APRM module, and one status module from left to right. The status module indicates the result of self-diagnostics on the front panel LEDs.

In addition to the LPRM modules in the LPRM/APRM unit, the APRM module can obtain LPRM levels from twelve LPRM modules, which are mounted in another unit, the LPRM unit. The LPRM unit has similar appearance to the LPRM/APRM unit. The LPRM levels produces in the LPRM modules in the LPRM unit are transmitted to the LPRM/APRM unit over fiber optic cables attached to the unit rear.

The last unit of the PRM system is the FLOW module that converts the differential pressure signal from the flow transmitter to the recirculation flow value, and transmits the value to the APRM module, which uses the flow value to calculate a flow-biased trip setpoint.

In the PRM design, FPGAs are used only for digital processing.

Fig. 4. LPRM/APRM Unit

3. DESIGN PROCESS OF FPGA-BASED SYSTEMS

FPGA is semiconductor devices, and their functions are determined by the circuit programmed in the devices. FPGA themselves is hardware. However, the logic for these FPGA-based components is designed and manufactured by a process which is similar to generating software. The logic to be embedded into an FPGA is written in hardware description language as a code, and a logic synthesis tool and a place and layout tool convert the code into a fuse map that determines the circuit in the FPGA. Specifically, Toshiba uses a hardware description language called Very High Speed Integrated Circuit (VHSIC) Hardware Definition Language (VHDL) to define the function of the circuits on the FPGA.

To implement this process, Toshiba had developed a high quality design and manufacturing process for FPGA-based systems, with a lifecycle process suitable for the design and development of safety-related I&C.

The life cycle consists of the following phases:

(1) The design engineer defines system specification. In the case of the PRM, the system was divided into units, and the system functions were allocated to each unit.
(2) The functional requirements for the components consisting of the system are defined. In the case of the PRM, the requirements for the units and modules were defined.
(3) The design engineers designs logic to be embedded in the FPGA.
(4) The logic is embedded in the FPGA by an FPGA programming tool. FPGA validation testing is performed after the embedding.
(5) The FPGAs are soldered on printed circuit boards and fabricated as modules. In this phase, Unit/Module validation test is performed to validate modules containing the FPGAs, and units containing modules.
(6) The units are integrated into a system, and the system validation test is performed to validate the system.

4. LOGIC QUALIFICATION OF FPGA-BASED SYSTEMS

There was no guideline or standard for design process of FPGA which is applied to safety systems of nuclear power plant. Therefore Toshiba developed FPGA design process.

Because the development process of the FPGA-based system is similar to that of computer software, Toshiba applied IEEE 7-4.3.2-2003 to the process. The IEEE 7.4.3.2-2003 requires the performance of V&V in accordance with IEEE Standard 1012-1998.

IEEE Std 1012-1998 defines a number of V&V tasks and activities for life cycle phases, such as requirements traceability analyses. In the requirements traceability analysis, it is verified that the

requirements from the preceding phases are traced to the following phase, and the functions in the following phases are traced back to the preceding phase.

The hazard analyses analyze potential hazards in the FPGA-based system, and are also performed through the life cycle phases.

The V&V activities and hazard analyses in the FPGA development process covers the expectations of IEEE Std 1012-1998.

5. QUALIFICATION TESTS OF FPGA-BASED PRM SYSTEM

Toshiba designed and manufactured the NRW-FPGA-based PRM units, and conducted logic qualification of FPGA-based PRM system in accordance with the established design process.

The hardware qualification test to demonstrate hardware acceptability of the FPGA-based PRM system for safety-related application was also implemented in accordance with EPRI TR-107330 requirements. Even though the Toshiba systems are not PLC-based, these safety-related systems are typically installed in the Main Control Room. Therefore, EPRI TR-107330 is considered as adequate to be applied for the qualification. The tests specified in the EPRI TR are required in order to comply with the applicable regulatory requirements and industry standards.

Following tests were conducted to demonstrate compliance with requirements specifications, and to demonstrate suitability of equipment while subject to stress conditions.

(1) Environmental Test

The Environmental Test was performed to ensure that the system provides the performance required under the temperature and humidity conditions provided in EPRI TR-107330.

The Test Specimen successfully completed the radiation exposure test with no signs of physical or functional degradation. The Test Specimen successfully completed the temperature and humidity test. The Test Specimen met all applicable performance requirements during and after application of the environmental test conditions. The test results show that the Test Specimen will not experience failures due to abnormal service conditions of temperature and humidity.

(2) Seismic Test

The Seismic Test was performed to ensure that the system continues to operate correctly during the seismic conditions provided in EPRI TR-107330 to the extent achievable at the test facility.

The Test Specimen met all applicable performance requirements during and after application of the seismic test vibration levels. The Test Specimen units successfully completed seismic testing with no signs of physical or functional degradation.

(3) Electromagnetic Interference/Radio-Frequency Interference (EMI/RFI) Test

The EMI/RFI Test was performed to ensure that the system is not susceptible to and does not radiate more than the EMI/RFI levels shown in USNRC RG 1.180 Rev.1.

Results of the susceptibility testing showed that the Test Specimen continued to functin correctly throughout all test exposure levels. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system.

For the emissions tests, the Test Specimen was found to comply with the allowable equipment emissions levels.

(4) Surge Withstand Capability Test

The Surge Withstand Capability test was performed to ensure that the system withstands the surge limits shown in the USNRC RG 1.180 Rev.1.

The Test Specimen continued to operate in accordance with the test acceptance criteria following application of the surge test voltages.

(5) Electrical Fast Transient / Burst (EFT/B) Test

The EFT/B Test was performed to ensure that the system withstands the EFT/B limits shown in USNRC RG 1.180 Rev.1.

Results of the EFT/B testing showed that the Test Specimen continued to operate in accordance with the test acceptance criteria.

(6) Electrostatic Discharge (ESD) Test

The ESD Test was performed to ensure that the system can continue to operate when exposed to the ESD levels provided in EPRI TR-107330. The test was performed in accordance with EPRI TR-102323 Rev.2.

Results of the ESD testing showed that the Test Specimen did not present any temporary degradation or loss of function or performance when the ESD noises were applied to front panels, components on the front panels, and side panels, which can all be touched during normal operation.

(7) Isolation Test

The Isolation Test demonstrated that the system provides suitable electrical and functional isolation. The test levels are provided in EPRI TR-107330 and IEEE Standard 384-1992.

Test level voltages were applied to the test points and the safety-related portion of the Test Specimen operated normally during and after the application.

6. CONCLUSIONS

Toshiba developed a design process for NRW-FPGA-based safety-related I&C systems. The design process resolves issues for many years regarding testability of the digital systems for nuclear safety applications. Thus, Toshiba NRW-FPGA-based safety-related I&C systems have many advantages to be a world standard of the digital systems for nuclear safety applications. Toshiba will apply the systems to not only BWRs but also other types of nuclear power plants and nuclear facilities in the world.

The logic qualification method employs life cycle approach similar to that of computer software, because the development process of FPGA systems are similar to that of computer software. In the qualification, hazard analyses and V&V efforts are performed along with development process. For FPGA-Based systems the logic design is rigorous, simple, deterministic, and verifiable. These are advantages of FPGA-Based systems over computer-based systems. However, there are some issues to be addressed in the qualification of FPGA-Based systems, and Toshiba reported countermeasures to resolve these issues in this paper.

Toshiba applied the logic qualification methods on the PRM system for BWR plants, and attained good results. Toshiba concludes that the logic qualification method that Toshiba developed is applicable to FPGA-Based safety-related I&C systems, and expect that the method will contribute to future FPGA-Based systems.

The hardware qualification test to demonstrate hardware acceptability of the FPGA-based PRM system for safety-related application was implemented in accordance with EPRI TR-107330

requirements, and attained good results. Toshiba concludes that the PRM system achieved the required performance and are considered satisfactory for safety-related application.

REFERENCES

[1] Y. GOTO, et al., “Development of FPGA-based Safety-related I&C Systems,” Proceeding of ANS NPIC &HMIT (2006), Albuquerque US, November 12-16, Vol. 5, pp1028-1031 (2006).

[2] T. Miyazaki, et al., “Qualification of FPGA-based Safety-related PRM System,” Proceeding of NPIC&HMIT (2009), Knoxville US, April 5-9, pp 70 (2009).