Application of FPGA to nuclear power plant I&C systems

HAYASHI Toshifumi[1], KOJIMA Atsushi[2], MIYAZAKI Tadashi[3], ODA Naotaka[4], WAKITA Kiyotaka[5], and FURUSAWA Takayoshi[6]

1. *Toshiba Corporation Power Systems Company, 8, Shinsugita-cho, Isogo-ku, Yokohama, 235-8523 Japan, (toshifumi1.hayashi@glb.toshiba.co.jp)*
2. *Toshiba Corporation Power Systems Company, 8, Shinsugita-cho, Isogo-ku, Yokohama, 235-8523 Japan, (atsushi4.kojima@toshiba.co.jp)*
3. *Toshiba Corporation Power Systems Company, 8, Shinsugita-cho, Isogo-ku, Yokohama, 235-8523 Japan, (tadashi.miyazaki@toshiba.co.jp)*
4. *Toshiba Corporation Power Systems Company, 8, Shinsugita-cho, Isogo-ku, Yokohama, 235-8523 Japan, (naotaka.oda@toshiba.co.jp)*
5. *Toshiba Corporation, Fuchu Complex, 1, Toshiba-cho, Fuchu, Tokyo, 183-8511 Japan, (kiyotaka.wakita@toshiba.co.jp)*
6. *Toshiba Corporation, Fuchu Complex, 1, Toshiba-cho, Fuchu, Tokyo, 183-8511 Japan, (takayoshi.furusawa@toshiba.co.jp)*

Abstract: This paper presents a Field Programmable Gate Array (FPGA) application for nuclear power plants, and introduces Toshiba FPGA-based Instrumentation and Control (I&C) systems as typical examples. An FPGA is a semiconductor device including more than thousands of logic gates which can be connected to constitute application specific circuits. A notable feature of FPGA is its simplicity. Thanks to this feature, several companies including Toshiba have developed FPGA based-systems for nuclear power plants recently. The simplicity of FPGAs is one of the most notable advantages to provide cost-effective options for I&C systems, ensuring reliable and safe operation of nuclear power plants.
Keyword: Instrumentation and control; digital I&C system; FPGA

1 Introduction

The application of digital technology into Instrumentation and Control (I&C) systems for nuclear power plants (NPPs) had began in 1980s, by replacing or by upgrading gradually the conventional I&C systems which use various analog devices. The digital systems in those days have been using microprocessors. At the beginning of digital systems application for NPPs, the digital systems were applied to non-safety systems where reliability or safety was not so strictly required to be compared with the application for safety systems. And then, the application to safety systems had been considered and challenged. The Safety System Logic and Control (SSLC) that Toshiba has developed for Advanced Boiling Water Reactor (ABWR) plants is one typical example of digital applications for safety systems.

Received date: March 13, 2012
(Revised date: April 12, 2012)

One of the merits of Digital I&C systems is that they can provide richer functionality including automatic functions such as self-diagnosis, which are difficult to implement in the case of analog systems. Digital I&C systems are less susceptible to component aging than analog systems, and therefore they need less frequent calibration to retain their accuracy than for analog devices. These features have been considered to improve maintainability, performance and reliability of the I&C systems.

There are two types of digital I&C systems which are applicable to NPPs:

1) microprocessor-based systems, and
2) semiconductor-based systems.

Programmable Logic Controller (PLC) is a typical example of the microprocessor-based systems which basically belong to a type of computer, where various functions of the system are implemented by computer programs. Owing to the development of digital technology, the capacity and capability of the PLCs had grown so sufficient as to be used gradually in NPPs since 1980s. In order to program the PLCs,

special programming languages suited to the application domain have been generically used instead of general purpose programming language such as C.

On the other hand of the microprocessor-based systems, the semiconductor-based systems can be categorized into the following two types; (i) non-programmable type such as Application Specific Integrated Circuit (ASIC), and (ii) programmable type such as Programmable Logic Array (PLA) or Field Programmable Gate Array (FPGA).

ASIC is a semiconductor customized for a specific purpose. An ASIC includes thousands or millions of gates which are to be connected to implement the functions for the purpose. The main difference between ASIC and FPGA is that ASIC needs gate connections made in the semiconductor fabrication plant, while FPGA allows gate connections in the field.

PLA is an early type of programmable logic device, and its capacity and capability was rather limited for wide applications due to the relatively small numbers of the gates included in a semiconductor chip and the slow switching time of the gates. However after the invention of the FPGA in 1992, the limitation of the PLA has been gradually overcome. Although early FPGA had similar limitations of the PLA, advance of the semiconductor technology made the FPGA more capacitive, capable, and cost effective to be used in NPPs.

However, there is a peculiar issue on introducing digital I&C equipments to safety systems of NPPs. It is that nuclear regulators often require intensive verification and validation (V&V) for digital I&C systems to ensure the reliability and safety of those systems. V&V activities are time-consuming and expensive efforts.

In which follows, an overview will be made of FPGA application for NPPs and the introduction of Toshiba FPGA-based I&C systems and their development and qualification processes.

2 Overview of FPGA

2.1 FPGA device

An FPGA includes thousands or millions of logic gates aligned in an array, which is often called “sea of gates.” The interconnections between each gate are allowed to be determined, or programmed in the field.

There is a fundamental difference between FPGA-based systems and microprocessor-based systems, as explained in the report by United States Nuclear Regulatory Commission (USNRC) NUREG/CR-6992[1] Since FPGA is parallel in its nature, the array elements in the FPGA can operate simultaneously, whereas microprocessors can only perform one function at a time. This parallel nature of FPGAs not only contributes to higher performance, but also reduces complexity of microprocessor-based systems by eliminating needs of context switching and memory access.

FPGA-based systems do not need any operating systems, and they are free from the associated reliability limitations caused by context switching times, memory overflow, virus vulnerability, and the bugs generally existed in the operating system.

There are several types of FPGA which are categorized by the methods to interconnect the internal gates. SRAM type FPGA uses static random access memory (SRAM) to interconnect the gates, and provides largest counts of gates. Since SRAM is volatile memory, the SRAM type FPGAs should need configuration data source such as Electrically Erasable Programmable Read-Only Memory (EEPROM). The SRAM type FPGAs are initialized by using the configuration data each time the power is applied. This is a drawback of SRAM type FPGA.

Another shortcoming of SRAM type FPGAs is its vulnerability to single event upsets (SEU). The SEU is a phenomena that the logic values in the semiconductor are affected by radiation exposure[2]. Because the SRAM type FPGA should provide largest counts of gates, appropriate mitigation measure against SEU such as triple modular redundancy could be used for NPP application.

Flash type FPGA uses flash memories to interconnect the gates. Unlike SRAM, flash memories are non-volatile; this type of FPGA does not need configuration data source. Instead, configuration data are embedded into the FPGA chip using special programming tools. Flash type FPGA is less vulnerable to SEU compared with the previous SRAM type FPGAs.

Antifuse type FPGAs use antifuses, *i.e.*, a thin barrier of non-conducting amorphous silicon between the two metal conductors. The antifuses are normally open circuit. When a sufficient high voltage is applied, the amorphous silicon turns into a polycrystalline silicon-metal alloy, which is conductive. Thus, the antifuses form a permanent, passive, low impedance connection when programmed. These interconnections are considered to be hard-wired, and ensure the higher level of confidence on the integrity of the programmed logic. In addition, antifuse type FPGAs are least vulnerable to SEU.

2.2 Development of FPGA

Development process of FPGA is similar to that of software for microprocessor-based systems, so that the logic is described by source code and that the source code is converted to implementation data using software tools. The logic to be programmed into the FPGA is described using hardware design languages. Very High Speed Integrated Circuit Hardware Description Language (VHDL) and Verilog are the commonly used languages for FPGA design.

Engineers produce source code describing the logic by those languages. After the engineers produce source code, a special software tool called a logic synthesizer is used to convert the source code to a gate level representation, and the gate level representation is further converted to the configuration data of the FPGA by using another software tool called a Place and Route tool.

The Place and Route tool determines the places where specific logic elements reside in the FPGA chip, and the route of interconnecting lines among the placed logic elements, counting the signal delays over the interconnecting lines. The places and routes determined by the Place and Route tool are delivered by a configuration data.

For antifuse type FPGA, this configuration data is called fuse map. The programming of FPGA is performed using this data.

3 Application of FPGA in NPP

3.1 General

There are two approaches to apply FPGAs to NPPs. The first approach is to use FPGAs as a replacement of other logic devices. Since FPGAs are programmable outside semiconductor foundry plants, they are more suitable for low-volume products than ASICs. Therefore, FPGAs have been used for logic circuits for which ASICs were used before then. A notable example of this approach is using FPGAs as a replacement of an old discontinued microprocessor. For example, Motorola (Now Freescale Semiconductor) MC6800 is the microprocessor that has been used in Électricité de France (EdF)'s 1300 MW Series NPPs. EdF is developing a MC6800 emulator using FPGAs as a replacement of this old microprocessor [3].

The second approach is to implement nuclear application specific logic circuits into FPGAs directly. There are some examples which take this approach.

The Main Steam and Feedwater Isolation System (MSFIS) of Wolf Creek Nuclear Generating Station in US was updated using the FPGA-based system[4]. The MSFIS provides valve control equipment for main steam and feedwater automatic isolation and manual valve control. The MSFIS enclosure contains one set of the main steam isolation valves and feed water isolation valves control circuitry, which was implemented using the CS Innovation's Advanced Logic System (ALS) based on FPGA technology. The ALS includes a flash type FPGA to implement valve control logic.

A Ukraine-based Research and Production Corporation (RPC) called Radiy has developed an FPGA-based I&C platform[5], and has already implemented the platform in more than 50 NPP applications including:

- Reactor Trip System (RTS),

- Reactor Power Control and Limitation System (RPCLS),
- Engineering Safety Features Actuation System (ESFAS), and
- Automatic Regulation, Monitoring, Control, and Protection System (RMCPS) for Research Reactors.

Toshiba has developed several FPGA-based systems for NPPs, including the Power Range Neutron Monitor (PRNM) and Reactor Trip and Isolation System (RTIS). Those systems will be introduced in Chapter 4.

3.2 Development process and verification and validation efforts

FPGAs were first introduced in non-safety systems in NPPs, where no specific process over general FPGA development process as described in Section 2.2 will be required. However, to use FPGAs for safety systems, more stringent processes will be imposed by nuclear regulators to ensure the reliability and safety of the systems.

Because the development process of FPGA is similar to that of software for microprocessor-based systems, the conventional safety software development process including V&V methods can be applied. The MSFIS of Wolf Creak Nuclear Generating Station, the systems supplied by the RPC Radiy, and the systems of Toshiba were subjected to V&V process to ensure their reliability and safety.

For US commercial NPPs, the US NRC endorses IEEE Standard 7-4.3.2-2003[6] as the methods for high functional reliability and design requirements for computers, whereas IEEE Standard 1012-1998[7] as the methods of V&V.

IEEE Standard 1012-1998 postulates a phased software life cycle, and defines a number of V&V activities to be performed throughout the software life cycle. The V&V activities include the following types of activities:

- Software requirements evaluation,
- Design evaluation,
- Interface analysis,
- Requirements traceability analysis,
- Source code and source code documentation evaluation,
- Validation testing, and
- Hazard analysis.

The first four types of activities can be applied for FPGA-based systems with minimal modification, because they are activities in upstream, and the dependency on the technologies, *i.e.*, microprocessors or FPGAs, are limited.

The last three activities need more modifications, depending on the difference of technologies. For source code evaluation, the activities must be performed considering not only the use of different programming languages but also the parallel nature of FPGAs.

The validation testing needs to be designed based on the implementation method of the FPGA-based systems. For example, the authors of this paper applied the functional element (FE) method[8, 9] for the Toshiba FPGA-based safety I&C systems. In this FE method, the logic is built up from small logic elements called FE. The authors of this paper designed the validation testing according to this FE method as summarized by the following steps: *First, validate the FEs; second, validate the connections between FEs; and last, validate the integrated system.*

The hazard analysis is another issue to be carefully considered. In addition to the architectural analysis, the authors of this paper examined the FPGA for its hardware features as a semiconductor device, and logic implementation methods to identify hazards and to take appropriate countermeasures in the development of the safety systems.

For Japanese NPPs, codes and guidelines published by the Japan Electric Association are used for the software V&V to the digital safety systems[12]. Since they are similar to IEEE standards, Toshiba uses a similar approach as that for US NPPs.

3.3 Equipment Qualification (EQ) and Electromagnetic Compatibility (EMC) qualification

Hardware qualification tests demonstrate hardware

acceptability of the FPGA-based I&C systems for safety applications. There are two types of qualification: equipment qualification (EQ) and electromagnetic compatibility (EMC) qualification. EQ includes environmental and seismic tests.

For US commercial NPPs, the US NRC endorses Electric Power Research Institute (EPRI) TR-107330[10]. EPRI TR-107330 includes generic requirements specification, for EQ and EMC qualification of programmable logic controller (PLC), and the authors of this paper consider that TR-107330 is applicable for qualification of FPGA-based safety I&C systems, because FPGA-based systems are the same as the PLCs in terms of digital devices. EPRI TR-107330 provides a set of extensive requirements as described below;

(1) Environmental Test

The environmental test ensures that the system operate correctly under the temperature and humidity conditions presumed to be possible.

(2) Seismic Test

The seismic test ensures that the system continues to operate correctly during the seismic conditions which are provided in EPRI TR-107330.

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

The EMI/RFI test ensures that the system is not susceptible to and does not radiate more than the specified EMI/RFI levels.

(4) Surge Withstand Capability Test

The surge withstand capability test ensures that the system withstands the specified surge limits.

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

The EFT/B test ensures that the system withstands the specified EFT/B limits.

(6) Electrostatic Discharge (ESD) Test

The ESD test ensures that the system continues operation when exposed to the specified ESD levels.

(7) Class 1E to Non Class 1E Isolation Test

Class 1E to Non Class 1E isolation test demonstrates that the system provides suitable electrical and functional isolation.

3.4 Standards

The International Electrotechnical Commission (IEC) Technical Committee (TC) 45 has been working on a standard for applications of FPGAs and other digital devices in nuclear plants since 2007. The standard was published as IEC 62566[11].

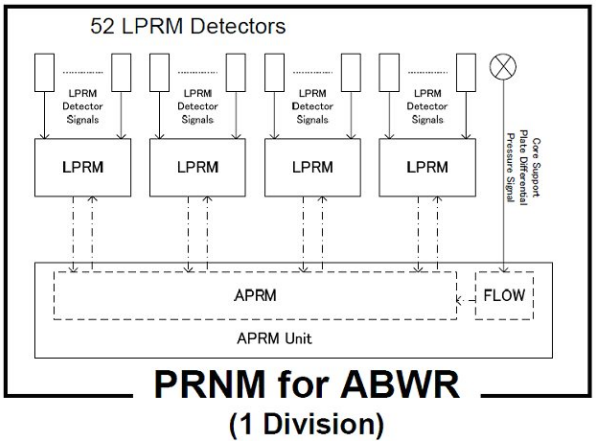

Fig. 1 Configuration of PRNM for ABWR plants

4 Toshiba FPGA-based I&C systems

4.1 System architecture

Toshiba developed several FPGA-based systems[5]. Toshiba designs them as modular, rack-mounted systems. The FPGA-based system is constituted of chassis, called units that accommodate a several number of modules.

A unit has front slots and back slots to which modules are inserted. 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.
Each module consists of one or more printed circuit boards, on which the FPGAs and other circuitry are mounted, and a front panel. Most modules require two printed circuit boards, including a small printed circuit board for the Human Machine Interface (HMI) on each module's front panel.

The following subsections present some examples of the Toshiba FPGA-based I&C systems. From the experiences gained in the development of these systems, the authors of this paper consider that the development process of FPGA-based systems is simpler compared with that of microprocessor-based systems, though the process is similar. The authors of this paper consider that this simplicity is one of the most notable advantages of FPGA-based systems, which provides cost-effective options for I&C systems, ensuring safe and reliable operation of NPPs.

4.2 Power Range Neutron Monitor (PRNM)

The Power Range Neutron Monitor (PRNM) is a subsystem of the Neutron Monitoring System (NMS), to which Toshiba applies FPGAs. The PRNM monitors neutron flux in a Boiling Water Reactor (BWR) core in the power range. The PRNM for the Advanced BWR (ABWR) plants is a safety system consisting of four independent divisions. Toshiba uses antifuse type FPGAs for the PRNM for its safe and reliable operation. Figure 1 illustrates the configuration of one division. The PRNM includes the Local Power Range Monitor (LPRM) and Average Power Range Monitor (APRM).

For a typical ABWR plant, there are 208 LPRM detectors in the core. These LPRM detectors are assigned to four APRM channels corresponding to four divisions; hence each APRM channel receives 52 LPRM detector signals. One division PRNM system includes four LPRM units, each of which accepts 13 LPRM detector signals. Each LPRM unit converts the LPRM detector signal into digital signal, applies digital filters, and sends the digital LPRM signal to the APRM unit. The APRM unit calculates an averaged neutron flux from the LPRM signals, and determines generation of a high neutron flux trip, a thermal power trip signal, or a core flow rapid coastdown trip signal. The signal processing in the LPRM and APRM units are performed by FPGAs. The trip signal is sent to the Reactor Trip and Isolation System (RTIS).

In addition to the PRNM for ABWR plants, Toshiba developed a PRNM for conventional BWRs, and applied for US NRC for safety evaluation.

4.3 RTIS

The RTIS is an important safety system having functions of the Reactor Protection System (RPS) and the main steam isolation system. The RTIS monitors safety-related plant signals to generate a trip signal for reactor scram and for main steam isolation. Toshiba uses antifuse type FPGAs for the RTIS. Figure 2 illustrates the configuration of the RPS function. The main steam isolation function is configured similarly. The RTIS consists of four independent divisions. Each division consists of the Digital Trip Function (DTF) unit, Trip Logic Function (TLF) unit, Output Logic Unit (OLU), Load Driver (LD), and Suppression Pool Temperature Monitoring Calculation (SPTM) unit. The DTF receives safety-related plant signals such as reactor water level, reactor pressure, and drywell (D/W) pressure signals from local sensors. The DTF compares each signal with a predefined set point value and generates a trip signal if the signal exceeds the set point value. In addition, the DTF receives a suppression pool

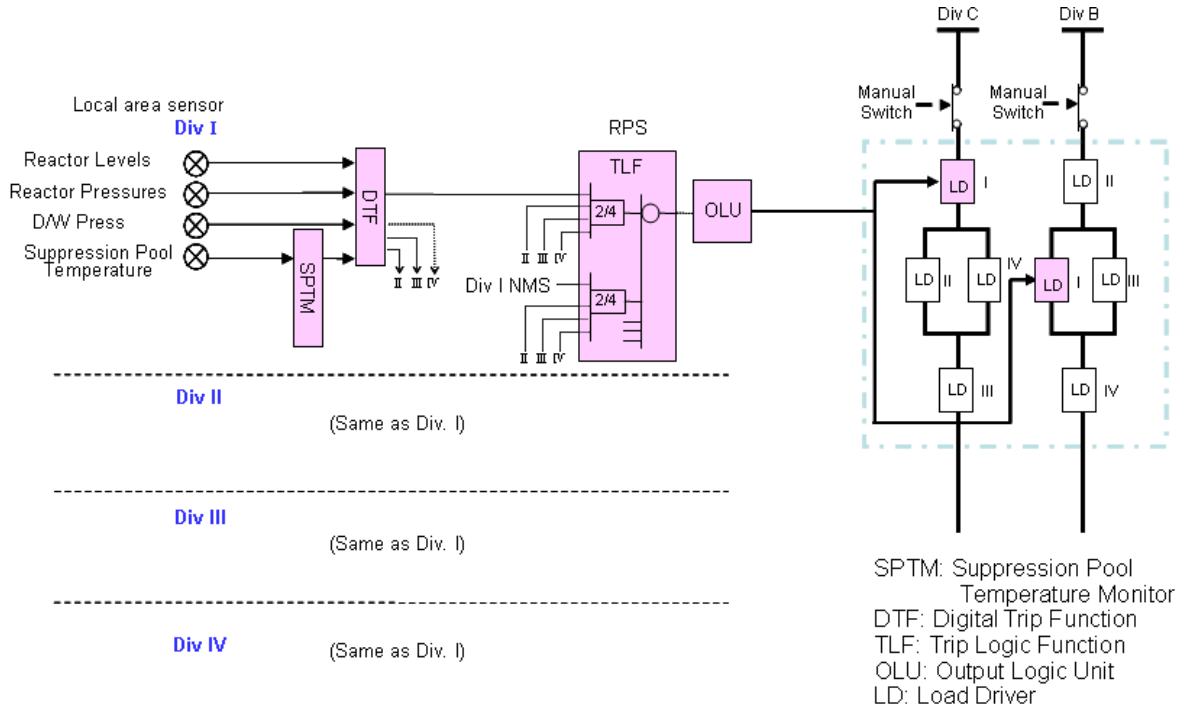

Fig. 2 Configuration of reactor trip and isolation system.

temperature trip signal from the SPTM which calculates the averaged suppression pool temperature and generates a trip signal. The DTF combines the self generated trip signals and the trip signal from the SPTM, and transmits them to the TLFs. The TLF receives the trip signals from the four DTFs and the four NMSs, and performs two-out-of-four voting logic. The OLU receives a trip signal from the TLF and actuates the LD. The four LDs constitute two-out-of-four voting logic for the reactor scram.

4.4 FPGA-based non-safety systems

Toshiba has developed and shipped several FPGA-based non-safety systems for NPPs, including radiation monitors and the traverse in-core probe (TIP) for BWR plants. These non-safety FPGA-based systems have been operating in the plants for years, and have good operating history.

4.5 Advantage of Toshiba FPGA-based I&C systems

Toshiba has been supplying FPGA-Based I&C Systems for many years. With this experience, the authors of this paper have established a design method utilizing FEs as described in Section 3.2. FPGA-based systems are inherently simple, hence more suitable for V&V. This FE method augments this advantage of FPGA by allowing intensive and convincing V&V at affordable cost, which is especially important for safety systems.

5 Conclusions

FPGA is relatively new digital technology in the nuclear industry. A notable feature of FPGAs is its simplicity compared with microprocessor-based systems. FPGA-based systems do not need any operating system, and can implement application logic directly into the FPGA circuits. Although the development process of FPGA-based systems is similar to that of microprocessor-based systems, the simplicity of the FPGAs reduces the necessary efforts for qualification.

Thanks to this simplicity, several companies have succeeded to develop and commercialize FPGA-based safety systems for NPPs. Among them, Toshiba developed the safety systems, *i.e.*, the NMS and RTIS for ABWR plants, and other non-safety systems for NPPs. Toshiba plans to expand use of the FPGAs for other NPP applications.

The authors of this paper consider FPGA-based systems provide cost-effective options for I&C systems, ensuring safe and reliable operation of NPPs.

Acknowledgement

The authors would like to acknowledge engineers of Toshiba who are working for FPGA-based I&C systems.

Nomenclature

ABWR	Advanced Boiling Water Reactor
ALS	Advanced Logic System
APRM	Average Power Range Monitor
ASIC	Application Specific Integrated Circuit
D/W	Drywell
DTF	Digital Trip Function
EdF	Électricité de France
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFT/B	Electrical Fast Transient / Burst
EMC	Electromagnetic Compatibility
EMI/RFI	Electromagnetic Interference / Radio-Frequency Interference
EPRI	Electric Power Research Institute
EQ	Equipment Qualification
ESD	Electrostatic Discharge
ESFAS	Engineering Safety Features Actuation System
FE	Functional element
FPGA	Field Programmable Gate Array
HMI	Human Machine Interface
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
LD	Load Driver
LPRM	Local Power Range Monitor
MSFIS	Main Steam and Feedwater Isolation System
NMS	Neutron Monitoring System
NPP	Nuclear power plant
OLU	Output Logic Unit
PLA	Programmable Logic Array
PLC	Programmable Logic Controller
PRNM	Power Range Neutron Monitor

RMCPS	Automatic Regulation, Monitoring, Control, and Protection System for Research Reactors
RPCLS	Reactor Power Control and Limitation System
RPS	Reactor Protection System
RTIS	Reactor Trip and Isolation System
RTS	Reactor Trip System
SEU	Single event upsets
SPTM	Suppression Pool Temperature Monitoring Calculation
SRAM	Static Random Access Memory
SSLC	Safety System Logic and Control
TC	Technical Committee
TIP	Traverse in-core probe
TLF	Trip Logic Function
USNRC	United States Nuclear Regulatory Commission
V&V	Verification and validation
VHDL	VHSIC (Very High Speed Integrated Circuit) Hardware Description Language

References

[1] NUREG/CR-6992: Instrumentation and Controls in Nuclear Power Plants: An Emerging Technologies Update United States Nuclear Regulatory Commission, October 2009.

[2] BOBREK, M., WOOD, R. T., WARD, C. D., KILLLOUGH, S. M., BOULDIN, D., and WATERMAN, M. E.: Safe FPGA Design Practices for Instrumentation and Control in Nuclear Plants, IAEA First Workshop on the Application of FPGA in Nuclear Power Plants, 2008, Presentation files are available via http://entrac.iaea.org/I-and-C/WS_EDF_CHATOU_2008_10/Start.htm (accessed March 31, 2012).

[3] SALAÜN, P.: Interest in FPGA/ASIC Technology for I&C Systems in NPP, IAEA First Workshop on the Application of FPGA in Nuclear Power Plants, 2008, Presentation files are available via http://entrac.iaea.org/I-and-C/WS_EDF_CHATOU_2008_10/Start.htm (accessed March 31, 2012).

[4] US NRC Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 181 to Renewed Facility Operating License No. FPF-42 Wolf Creek Nuclear Operating Corporation Wolf Creek Generating Station Docket No. 50-482, available via http://www.nrc.gov (accessed March 31, 2012).

[5] ANDRASHOV, A., KHARCHENKO, V., SKLYAR, V., and SIORA, A.: Innovative Approach to Implementation of FPGA-based NPP Instrumentation and Control Systems, Nuclear Safety and Simulation, 2011, 2(4): 364-373.

[6] IEEE Standard 7-4.3.2-2003: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, December 2003.

[7] IEEE Standard 1012-1998: IEEE Standard for Software Verification and Validation, Institute of Electrical and Electronics Engineers, March 1998.

[8] KOJIMA, A., KATO, M., TAHIRA, M., MIYAZAKI, T., ODA, N., GOTO, Y., and HAYASHI, T.: Qualification of Toshiba's FPGA-Based Safety-Related Systems, Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010.

[9] MAEKAWA, T., and HAYASHI, T.: Next Generation Technologies in the Digital I&C Systems for Nuclear Power Plants, Springer, Advances in Light Water Reactor Technologies, 2011: 223-250.

[10] EPRI TR-107330: Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, Electric Power Research Institute, December 1996.

[11] IEC 62566: Nuclear Power Plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A Functions, International Electrotechnical Commission, January 2012.

[12] JEAG 4609-2008: Guidelines for Verification and Validation of Digital Safety Protection Systems of Nuclear Power Plants, The Japan Electric Association, March, 2008 (in Japanese)