Design of an FPGA-based PWR ATWS mitigation system

LU Jun-Jen[1], and CHOU Hwai-Pwu[2]

1. *Department of Engineering and System Science, National TsingHua University, No. 101, Section 2, Kung-Fu Road, Hsinchu City 30013, Taiwan (gerardljr@hotmail.com)*
2. *Department of Engineering and System Science, National TsingHua University, No. 101, Section 2, Kung-Fu Road, Hsinchu City 30013, Taiwan (hpc@ess.nthu.edu.tw)*

Abstract: The present research is to explore the feasibility and conceptual design by using triple-redundant FPGA-based system for Anticipated-Transient-Without-Scram (ATWS) Mitigation System and Actuation Circuit (AMSAC) of a pressurized water reactor (PWR) type nuclear power plant (NPP). The Taipower's (Taiwan Power Company) Maanshan NPP was chosen for demonstration. An engineering simulated interface between AMSAC system and reactor/plant systems of Maanshan NPP was developed to provide an environment to validate the triple-redundant FPGA-based system. The software-free FPGA-based nuclear instrumentation and control (I&C) systems can easily be used for the modernization of the Taipower's nuclear power plant analog systems, thus may reduce the safety risk of undetectable software faults and common cause failures, and also minimize the regulatory licensing efforts and cost.

Keyword: Field Programmable Gate Array (FPGA); Nuclear Reactor Safety; Transient Mitigation; Anticipated-Transient-Without-Scram (ATWS); ATWS Mitigation System and Actuation Circuit (AMSAC).

1 Introduction

Due to the great advanced improvement in semiconductor technology, customized application specific integrated circuits (ASIC) become more complicated in the last two decades. The device suppliers intend to utilize high density and customized semiconductor chips to design their products in order to reduce the size and power consumption of their application circuits. However, high NRE (Non-Recurring Engineering Expense) and long turn-around time of the ASIC design have significant impacts to many designers who want customized functionality for systems in development. The large initial investment in ASIC design is easy to justify for OEM (Original Equipment Manufacturer) shipping thousands of chips per month. For the many designers who just want customized functionality in development, field services, and limited quantities, the FPGA technology becomes their favorite choice.

Basically, an FPGA chip is a functional programmable semiconductor contains millions of logical gates and several specific functional modules, such as memory blocks, bus controllers, UARTs. Similar to the microcontroller, an FPGA chip requires the designer to assign a definition or function for normal operation. Both the microcontroller and the FPGA chip start from zero and require the designer to give them a "Life" or "Intelligence". The designers use some kinds of software tools for coding, compiling, and configuring the chips, then testing and debugging their functions. Both microcontroller and FPGA designs can implement specific and unique applications, as simple as a traffic lights controller, or as complicated as a controller in a nuclear power plant. Both elements should follow the same development guidance. But unlike microcontrollers, the FPGA chip functions as a piece of hardware.

Wolf Creek Generating Station (WCGS, USA) started modernization by using microprocessor and software technology in 2002, but faced to regulatory licensing troubles from fall 2003, and informally rejected by U.S. NRC on spring 2004. WCGS restarted the modernization by using FPGA technology on fall 2004, and got the regulatory license, granted by NRC on March 2009, to retrofit the main steam and feed-water isolation system (MSFIS) [1].

The Research and Production Corporation (RPC, Ukraine) used FPGA systems (called "RADIY") to modernize 6 engineering safety feature actuation systems (ESFAS) for Bulgarian NPPs (Kozloduy-5 and Kozloduy-6) from 2008 to 2011[2]. Toshiba had developed safety-related I&C system (Power Range

Received date: December 15, 2013
(Revised date: December 24, 2013)

Monitor) by using non-rewritable FPGA technology in 2009[3]. An FPGA-based safety-relative shutdown system for CANadian Deuterium Uranium (CANDU) reactor was implemented in 2009[4].

The goal of the present research is to explore the feasibility and conceptual design by using triple-redundant FPGA-based AMSAC system for a PWR type nuclear power plant. The Taipower's Maanshan NPP was chosen for demonstration. The Maanshan NPP, located in the south end of Taiwan, is equipped with two identical 2785MWt nuclear steam supply systems (NSSS) and 951MWe turbine generators. The AMSAC system of the Maanshan NPP was implemented based on microprocessor technology. The Maanshan NPP is in operation more than 25 years and the obsolete issue will soon become a problem for its AMSAC system. In addition, based on the microprocessor and software design technology, undetectable software faults and common cause failures may exist, that will defeat the hardware redundancy and will impact the operation of a NPP. Thus, an alternative digital design approach using software-free FPGA-based technology is worthwhile to study in advance.

2 AMSAC System of Maanshan NPP

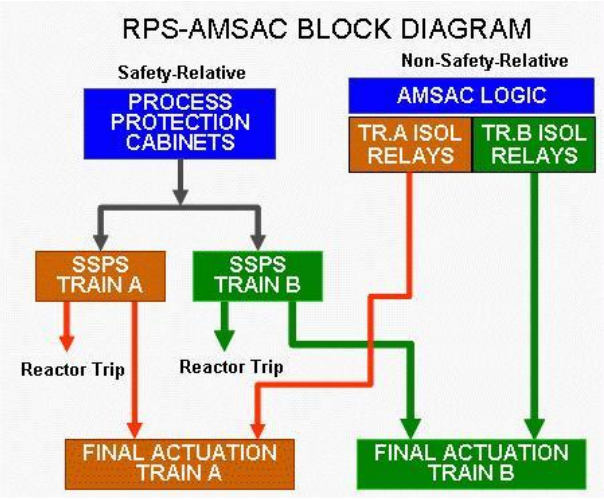

Fig. 1 Relationship between RPS and AMSAC [5].

According to the FSAR (Final Safety Analysis Report) of Maanshan NPP, the AMSAC is a diverse and backup system for Reactor Trip System (RTS) and Engineering Safety Feature Actuation System (ESFAS), as shown in Fig. 1. The Maanshan AMSAC system is designed to mitigate the consequences of a NPP and to prevent primary pressure exceeding 3200psig if an ATWS event occurs. The requirements of AMSAC system are to provide turbine trip, start auxiliary feed water, and isolate stream generators [5-7].

The primary design functions of the AMSAC system is described as following:

(1) AMSAC system senses main feed water pump (MFWP) condition, feed water isolation valve (FIV) position, and main feed water control valve (FCV) position to detect the lose of heat sink for secondary side and decides to trip the turbine, and to start the auxiliary feed water system (Motor/Turbine Driven Auxiliary Feed water System, MDAFS & TDAFS).

(2) Normally, the primary coolant pressure of Maanshan NPP is operated under 2750psig. The AMSAC system prevents the primary coolant pressure to exceed 3200psig when an ATWS event occurs.

(3) The Maanshan AMSAC is a microprocessor and software based system. All the devices relative to AMSAC system are located outside the reactor containment, and are powered by None-Class-1E. Besides the final voting and actuation relays, the AMSAC system is electrically independent and physically separated with RTS and ESFAS systems.

(4) The actuation of AMSAC system is delayed for several seconds, in order to wait for actuations of safety-relative systems first during the plant transience. The delay period depends on the turbine power before the plant transience, the larger turbine power the less delay period, as shown in Fig. 2.

(5) The C-20 (Turbine Power < 36%) signal blocks the actuation of AMSAC. Even when the turbine power is less than 36% and the ATWS event occurs, the primary coolant pressure will never exceed 3200psig.

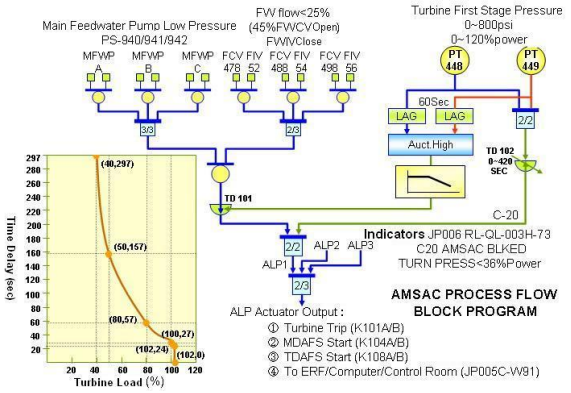

Fig. 2 Control Logic of Maanshan NPP AMSAC [5].

The AMSAC system contains two analog inputs, 6 digital input groups, 3 digital actuation outputs and some indicators connected to AMSAC panels, plant computer and main control room, as shown in Fig. 2. The two analog inputs are the pressures of the turbine first stage (PT-448 and PT-449, 4~20mA, 0~800psig, equal to 0~120% turbine power). The 6 digital input groups are the discrete contact conditions of main feed water pumps (MFWP), positions of feed water isolation valves (FIV) and positions of main feed water control valves (FCV).

(1) TD-101: Power-Time delay, from 24 seconds (102%) to 297seconds (36%).
   (A) Prevents feed water transient to actuate AMSAC.
   (B) Allows RPS actuates first and AMSAC is the backup.
   (C) Allows operators having enough time to manipulate the ATWS event or plant transient.

(2) C-20: Arming-Off delay (fixed at 327seconds). When the turbine power drops under 36% from higher power level, the Arming-Off delay signal will still be Hold-On for 327 seconds to ensure that the AMSAC system will still function properly during the first 327 seconds after the turbine is trip.

The AMSAC system is divided into three identical ALPs (Actuation Logic Processor) and one TMP (Test/Maintenance Processor). The three ALP loops calculate the logic decision of AMSAC design functions. The TMP monitors the operations of the three ALPs and provides indicators to panels, plant computer and main control room. The TMP also provides the interface for AMSAC system checking and maintenance purpose.

3 Conceptual Design of FPGA-based System

Based on the great flexibility and high density of FPGA technology, an FPGA circuit board usually contains only a few digital components to perform various signal processing and bus communication functions. Common components on the proposed AMSAC boards include FPGA chip, voltage regulator, capacitors, resistors, bus-drivers, NVM (Non-Volatile Memory), optical-couplers, connectors, and several passive components to accommodate the need of flexibility as well as safety measures.

By utilizing the FPGA technology to implement the AMSAC functions of Maanshan NPP, this study proceeded by the following stages:

(1) Designed the FPGA-based AMSAC circuits.
(2) Functional End-to-End testing of FPGA-based AMSAC circuits.
(3) Setup an engineering interface to validate the FPGA circuits.
(4) Proposed a verification and validation plan for the modernization of the Maanshan NPP analog systems with an engineering simulator.

3.1 Generic System Platform

Due to the true flash-based technology, 128-bit pass key write-protection security and superior reliability, Actel's FPGAs are widely used in military and space applications. Actel's SmartFusion intelligent mixed signal FPGA was chosen to be the target FPGA platform in the present study.

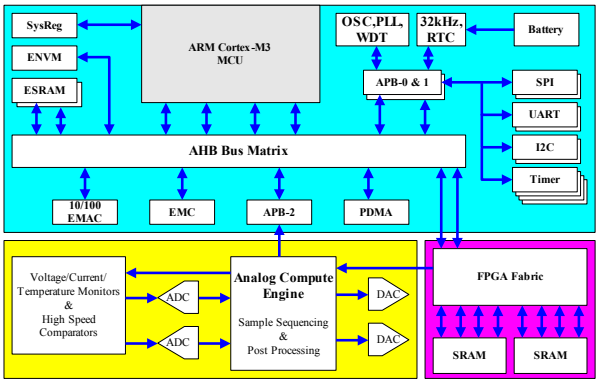

Fig. 3 Functional blocks of the SmartFusion FPGA chip [8].

The functional blocks of SmartFusion FPGA chip are shown in Fig. 3. The SmartFusion FPGA chip integrates flash-based FPGA logical blocks, an ARM Cortex-M3 microcontroller unit (MCU), digital peripherals and programmable analog peripherals. This offers full customization, IP protection and ease-of-use development tools. The SmartFusion intelligent mixed signal FPGA technology is an ideal solution for embedded designs with customized hardware which requires a true system-on-chip (SoC) solution [8].

SmartFusion FPGA Chip = FPGA Fabric +
32-bit ARM Cortex-M3 MCU +
Digital peripherals +
Programmable Analog (ADC + DAC)

The programmable analog peripherals on a SmartFusion FPGA chip include high-speed comparators (up to ten), voltage/current/temperature monitors, 12-bit SAR ADCs (up to 600K sample/sec), Sigma-Delta DACs, analog inputs (up to 32) and 3 analog outputs.

The digital peripherals on a SmartFusion FPGA chip include ARM's AHB Bus matrix, 512KB flash and 64KB SRAM, external memory controller, SPI and I²C interfaces, 32-bit timers, UARTs, 10/100 Ethernet MAC.

3.2 Hardware Design

The SRAM on the proposed FPGA circuits was partitioned into two divisions. All two SRAM divisions were fully Readable/Writeable for the FPGA fabric. One-Directional UART data communication was implemented for the security concerns, so only one of the two SRAM divisions was read-only for the UART to transmit the AMSAC control logic status to provide the interface for real-time monitoring and maintenance purpose of the proposed FPGA-based AMSAC circuit.

In present application, the other digital peripherals and the 100MHz ARM Cortex-M3 based 32-bit MCU are reserved for future functional expansion purpose. In future developments, the ARM MCU integrated with the 10/100 Ethernet MAC can be connected to the Maanshan NPP's plant computer system or the multiplexing network system for non-safety-related processes.

Four FPGA boards were used for the three ALP loops and one TMP, and the proposed triple-redundant FPGA-based AMSAC system consisted of one chassis, three individual patch panels, and dual DC power supplies.

An individual patch panel for each ALP loop was mounted in the back of the chassis. All the inter-connected signals to the other loops were hard-wired to the patch panel. The TMP FPGA board contained an UART port connected to a portable computer for test/maintenance purpose, or connected to the engineering simulator and/or plant computer in the future for real-time monitoring purpose during NPP's modernization.

For security consideration, additional discrete signals were proposed for NPP's modernization, which will be connected to the display panel of the engineering simulator (and/or NPP) to drive indicators if the UART port and/or FPGA download port was connected.

3.3 Software Design

On each FPGA circuit board, any control logic associated with the signal path contained two sets of diverse hardware logic. The two hardware logics were implemented by using two different hardware description language (Verilog and VHDL), and/or one of the two logics was designed by using the graphical schematic capture. Different actuation outputs from the two diverse logics in each FPGA board were indicated to be a failure board. All these design methods are fully supported by the Actel's FPGA development tool "Libero", which is an integrated development environment (IDE) [8].

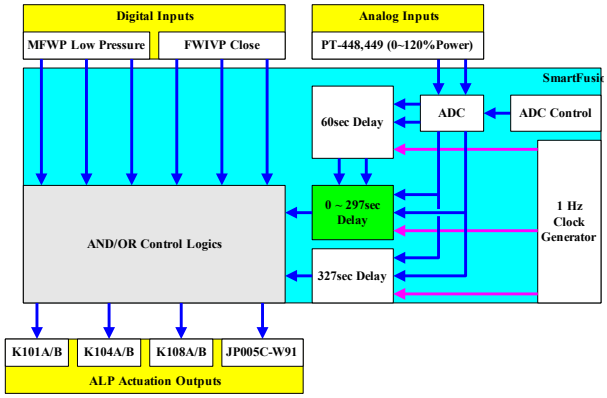

Fig. 4 Functional Blocks for FPGA-based AMSAC.

As shown in Fig. 4, the functions of FPGA-based AMSAC circuit were divided into the following blocks:

(1) **1Hz Clock Generator**: Provides the clock base for time delay of other AMSAC functional blocks.

(2) **ADC & ADC Control Logic**: Provides the control logic to sample the two AMSAC analog inputs, PT-448 and PT-449 (4~20mA, 0~800psig, equal to 0~120% turbine power) of the system.

(3) **60sec Delay Logic**: Provides 60 seconds delay after the sampling of the two AMSAC analog inputs (PT-448 and PT-449), then transfers the two sampling data to next stage, a 0 ~ 297 seconds power dependent delay logic.

(4) **0~297sec Delay Logic**: Depends on the turbine power sampled, provides the following time delay by Look-Up-Table (LUT): (> 102%, 0sec), (102%, 24sec), (100%, 27sec), (80%, 57sec), (50%, 157sec), (36%, 297sec).

(5) **327sec Delay Logic**: When the turbine power drops under 36% from higher power level, the Arming signal (C-20, turbine power < 36%) will still be Hold-On for 327 seconds to ensure that the AMSAC system will still function properly during the first 327 seconds after the turbine is trip.

(6) **Primary AND/OR Control Logics (ALP)**: This is the primary AMSAC actuation control logic, and is used to sense main feed water pump condition, feed water isolation valve position, and main feed water control valve position. When Main Feed water Pump low pressure (3-out-of-3 voting), or Main Feed water Isolation/Control Valves closed (2-out-of-3 voting) signals occur, the control logic delays for several seconds according to TD-101 (depends on turbine power) signal. The three ALP logics send the actuation signals into a 2-out-of-3 voting relay matrix to energize the output relay. The energized output relay actuates the AMSAC system.

4 Verification and Validation

A detailed functional End-to-End testing of the AMSAC circuits were accomplished according to a matrix of all inputs and outputs. As shown in Fig. 5, an engineering interface between the FPGA-based AMSAC system and reactor/plant systems of Maanshan NPP was developed to provide an environment for validating the triple-redundant FPGA-based AMSAC system.

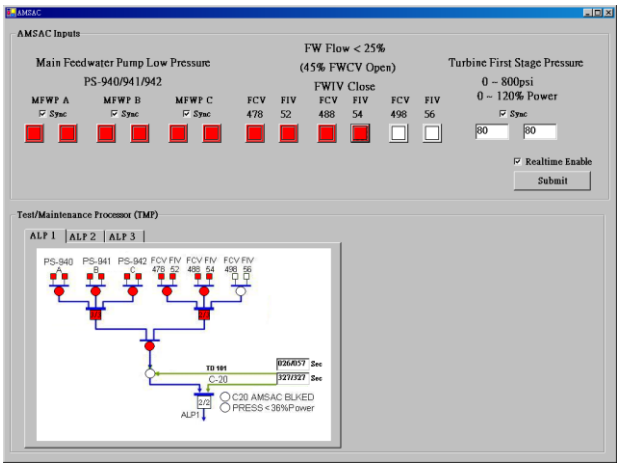

Fig. 5 Validation Interface for FPGA-based AMSAC System.

(1) The 6 discrete contact input groups of the main feed water pumps (MFWP), the positions of feed water isolation valves (FIV) and the positions of main feed water control valves (FCV) could be activated or disabled by clicking the pushbuttons on the interface page. The red pushbuttons indicated the activated discrete contacts.

(2) Two analog signals (PT448, PT449) of the turbine first stage pressure could be modified on the text boxes.

(3) The "Sync" checkboxes enabled the redundant inputs of WFMP, FIV, FCV or turbine pressure could be changed on the same time.

(4) The 6 discrete contact input groups and the two analog signals (PT448, PT449) were connected to the three ALPs individually. Any input of any ALP could be malfunctioned.

(5) All internal logical conditions of the three ALPs collected by the TMP were also displayed on the validation interface.
(6) As shown in Fig. 5, each of the two timers activated the associate logic when the timer counted to zero. (C-20 was a negative logic.)

Due to the short-term, feasibility and conceptual study, the hardware quality assurance verifications (such as Seismic, Temperature/Humidity and EMC/EMI/RFI susceptibility) of the proposed FPGA circuits were not proceeding in the present research, which will be part of the verification and validation for the future NPP modernization. A proposed verification and validation (V&V) plan was provided for the modernization of the Taipower's nuclear power plant analog systems [9-11].

An engineering simulator of the Maanshan NPP was proposed to provide a close-loop, dynamic, integrated and interactive test environment for the verification and validation of the FPGA-based AMSAC functions. Design basis events will be selected from the Maanshan Final Safety Analysis Report (FSAR) Chapter 15. Different accident scenarios and component malfunctions will be inserted into the engineering simulator. A spectrum of responses from the engineering simulator will be used to stimulate the FPGA-based AMSAC. Responses of the FPGA-based AMSAC will be observed and assessed to validate that the FPGA-based AMSAC satisfies all functional and performance requirements. The development process of future NPP modernization and results of the verification and validation will be proceeding and documented following the guidelines [12].

PCTRAN is a Windows-based nuclear power plant simulation platform from Micro Simulation Technology (MST), used to evaluate and analysis the event accidents and operation transients of a nuclear power plant. PCTRAN provides a friendly interface for human operation. Besides the real-time simulation platform, PCTRAN also provides a Faster-Than-Real-Time mechanism to increase the simulation speed for reducing the time needed for accident analysis.

An engineering simulator of Maanshan NPP was setup based on PCTRAN-PWR simulation platform. The engineering simulator will provide a close-loop, dynamic, integrated and interactive test environment for the verification and validation of FPGA-based AMSAC functions during the future modernization of NPP.

In order to setup the engineering simulator to provide a close-loop test environment for the verification and validation of FPGA-based AMSAC functions, some generic DAS (Data Acquisition System) interface shall be design and setup between the FPGA boards and the engineering simulator. The FPGA-based AMSAC validation interface (shown in Fig. 5) can also be integrated into the engineering simulator.

The generic interface includes:
(1) Digital Inputs: Connect the digital outputs of the FPGA boards to the digital inputs of the simulator, such as: actuators, indicators in the simulator.
(2) Analog Inputs: Connect the analog outputs of the FPGA boards to the analog inputs of the simulator. In present study, this interface is reserved for future research, such as: FPGA-based power range neutron flux monitor, FPGA-based feed water controller.
(3) Digital Outputs: Connect the digital outputs of the engineering simulator to the digital inputs of the FPGA boards, such as: panel switches, valve position contacts in the simulator.
(4) Analog Outputs: Connect the analog outputs of the engineering simulator to the analog inputs of the FPGA boards, such as: reactor core power, coolant pressure in the simulator.

The data acquisition system between the FPGA boards and the engineering simulator will be setup by utilizing the generic industrial personal computer (IPC) and extension cards, as shown in Fig. 6. The IPC and extension cards will be under the control of the simulator through generic Ethernet network. Additional control drivers and/or communication software, such as dynamic link library (DLL) for Windows system, will be developed to synchronize and integrate the signals of data acquisition system

with the common share memory of the plant system models in engineering simulator.

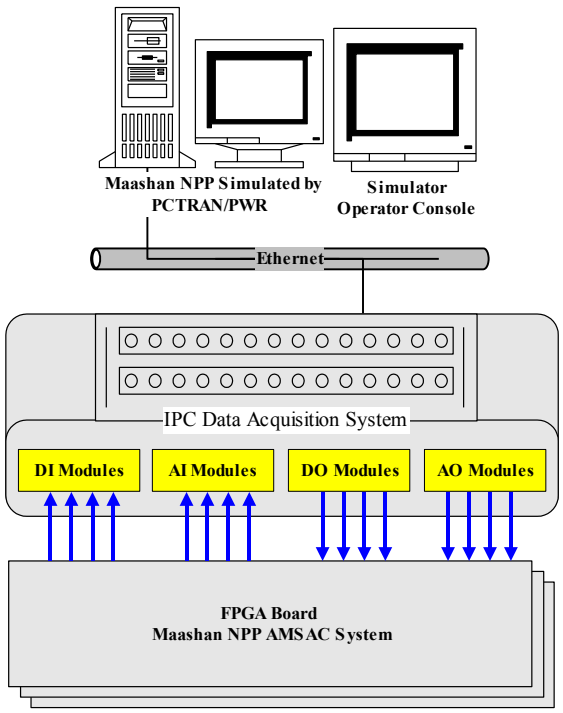

Fig. 6 V&V Architecture of FPGA-based AMSAC.

5 Conclusions

A diverse design was achieved by using two different implementation methods, two different HDL (Verilog and VHDL) languages and/or graphical schematic capture. Detailed functional End-to-End testing of the AMSAC circuits were accomplished according to a matrix of all inputs and outputs. Due to the fast response (less than microsecond) of FPGA logics, the proposed AMSAC circuits meet the response time criterion (seconds).

In the future NPP Modernization, some accident scenarios and abnormal conditions will be inserted into the engineering simulator in order to activate the functions of the FPGA-based AMSAC circuits. Detailed results of the triple-redundant FPGA-based AMSAC system and steady/transient results of the engineering simulator will be presented.

Because AMSAC system is a non-safety-relative function of the Maanshan NPP, more safety-relative FPGA-based I&C systems will be investigated in the future. The FPGA-based safety-relative I&C systems will be integrated into a more accurate full-scope engineering simulator, with the best-estimated reactor core and plant systems. The software-free FPGA-based nuclear I&C systems can easily be used for the modernization of Taipower's nuclear power plant analog systems, that will reduce the safety risk of undetectable software faults and common cause failures, and also will minimize the regulatory licensing efforts and cost.

Nomenclature

ADC - Analog-to-Digital Converter
AEC - Atomic Energy Council
AI - Analog Input
AO - Analog Output
ALP - Actuation Logic Processor
AMSAC - ATWS Mitigation System and Actuation Circuit
ASIC - Application Specific Integrated Circuit
ATWS - Anticipated-Transient-Without-Scram
CANDU - CANadian Deuterium Uranium
DAC - Digital to Analog Converter
DAS - Data Acquisition System
DI - Digital Input
DLL - Dynamic Link Library
DO - Digital Output
EMC - Electro-Magnetic Compatibility
EMI - Electro-Magnetic Interference
ESFAS - Engineering Safety Feature Actuation System
FCV - Feed-water Control Valve
FIV - Feed-water Isolation Valve
FPGA - Field Programmable Gate Array
FSAR - Final Safety Analysis Report
I Ȼ - Inter-Integrated Circuit
I&C - Instrumentation and Control
HDL - Hardware Description Language
IDE - Integrated Development Environment
INER - Institute of Nuclear Energy Research
IPC - Industrial Personal Computer
LUT - Look-Up-Table
MAC - Media Access Control
MCU - Micro-Controller Unit
MDAFS - Motor Driven Auxiliary Feed-water System
MFWP - Main Feed Water Pump
MST - Micro Simulation Technology
NPP - Nuclear Power Plant
NRE - Non-Recurring Engineering Expense
NRC - Nuclear Regulatory Commission

NSC - National Science Council
NSSS - Nuclear Steam Supply System
NVM - Non-Volatile Memory
OEM - Original Equipment Manufacturer
PWR - Pressurized Water Reactor
RFI - Radio Frequency Interference
RPC - Research and Production Corporation
RTS - Reactor Trip System
SAR - Successive Approximation Register
SoC - System-on-Chip
SPI - Serial Peripheral Interface Bus
SRAM - Static Random-Access Memory
TDAFS - Turbine Driven Auxiliary Feed-water System
TMP - Test/Maintenance Processor
Taipower - Taiwan Power Company
UART - Universal Asynchronous Receiver/ Transmitter
V&V - Verification and Validation
WCGS - Wolf Creek Generating Station

Acknowledgement

The work was under the auspices of NSC (National Science Council) and INER (Institute of Nuclear Energy Research) projects. The authors are grateful to all the participants of Taipower, Shian-Shing Shyu and Shi-Yao Luo of INER, Atomic Energy Council (AEC) for their valuable supports and comments.

References

[1] U.S. NRC: Wolf Creek Generating Station – Issuance of Amendment re: Modification of the Main Steam and Feedwater Isolation System Controls (TAC NO. MD4839), U.S. NRC, March 31, 2009, Available at: http://www.cs-innovation.com/docs/WCNOC_MSFIS_SER.pdf

[2] YASTREBENETSKY Mikhail, SKLYAR Volodymyr, ROZEN Yuriy, and VINOGRADSKAYA Svetlana: Safety Assessment of FPGA-based ESFAS. In: NPIC&HMIT 2009, Knoxville, Tennessee, USA, April 5-9, 2009.

[3] MIYAZAKI Tadashi, ODA Naotaka, GOTO Yasushi, and HAYASHI Toshifumi: Qualification of FPGA-Based Safety-Related PRM System. In: NPIC&HMIT 2009, Knoxville, Tennessee, USA, April 5-9, 2009.

[4] SHE Jingke and JIANG Jin: Application of FPGA to Shutdown System No.1 in CANDU. In: NPIC&HMIT 2009, Knoxville, Tennessee, USA, April 5-9, 2009.

[5] Taiwan Power Company: Maanshan Nuclear Power Plant RO23 System Training Material, Feb, 2009.

[6] Westinghouse Electric Corp. Comprehensive Nuclear Training Operations: I&C Integrated Plant Training – Taiwan Power Company Maanshan Units 1 and 2 AMSAC System, 1981.

[7] Westinghouse Electric Corp. Comprehensive Nuclear Training Operations: AMSAC Technical Manual", Vol. 1, 2, and 3.

[8] Actel Corporation: Actel SmartFusion Intelligent Mixed-Signal FPGAs Datasheet, Revision 1, March 2010.

[9] BOBREK Miljko, and WOOD Richard T.: FPGA Design Practices for I&C in Nuclear Power Plants. In: NPIC&HMIT 2009, Knoxville, Tennessee, USA, April 5-9, 2009.

[10] ALVARADO Rossnyev, and HERRELL David: Approach to Designing FPGA-based Digital I&C Systems for Nuclear Applications. In: NPIC&HMIT 2009, Knoxville, Tennessee, USA, April 5-9, 2009.

[11] PATRICK Salaun, FREDERIC Daumas and THUY Nguyen: FPGA/ASIC: A promising technology for future of I&C in power industry. In: NPIC&HMIT 2009, Knoxville, Tennessee, USA, April 5-9, 2009.

[12] U.S. NRC: Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems (NUREG/CR-7006, ORNL/TM-2009/20), U.S. NRC, February 2010, Available at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr7006/