Innovative approach to implementation of FPGA-based NPP instrumentation and control systems

ANDRASHOV Anton[1], KHARCHENKO Vyacheslav[2], SKLYAR Volodymir[3], and SIORA Alexander[4]

1. Research and Production Corporation Radiy, Kirovograd, Geroiv Stalingrada str. 29, 25006, Ukraine, (a.andrashov@radiy.com)
2. Centre for Safety Infrastructure-Oriented Research and Analysis, Kharkov, Astronomicheskaya str. 37, 61085, Ukraine, (v.kharchenko@khai.edu)
3. Research and Production Corporation Radiy, Kirovograd, Geroiv Stalingrada str. 29, 25006, Ukraine, (v.sklyar@radiy.com)
4. Research and Production Corporation Radiy, Kirovograd, Geroiv Stalingrada str. 29, 25006, Ukraine, (marketing@radiy.com)

Abstract: Advantages of application of Field Programmable Gates Arrays (FPGA) technology for implementation of Instrumentation and Control (I&C) systems for Nuclear Power Plants (NPP) are outlined. Specific features of FPGA technology in the context of cyber security threats for NPPs I&C systems are analyzed. Description of FPGA-based platform used for implementation of different safety I&C systems for NPPs is presented. Typical architecture of NPPs safety I&C system based on the platform, as well as approach to implementation of I&C systems using FPGA-based platform are discussed. Data on implementation experience of application of the platform for NPP safety I&C systems modernization projects are finalizing the paper.
Keyword: FPGA; I&C system; nuclear power plant; FPGA-based safety platform

1 Introduction

Assurance of nuclear and radiation safety is the key priority during design, development and operation of NPPs. One of the main tools used to provide safety operation of NPP is I&C system. The criticality of the functions performed by I&C systems are the reason why the requirements for such systems are so high [1-2]. General issues specified by the requirements to I&C systems are the following:
- reliability;
- timing characteristics;
- diversity;
- cyber security, *et al.*

One of the ways to overcome the challenges related with requirements to NPPs I&C systems is application of FPGA technology [3].

Research and Production Corporation (RPC) Radiy has developed an FPGA-based digital I&C platform that uses a basic set of hardware and software components that can be applied to produce I&C systems for NPP or other safety-critical applications (for example, related with aerospace, automotive, oil and gas industries, *et al.*), and has already achieved its successful implementation in more than 50 NPP applications. The general design of the RadICS platform makes innovative use of the FPGAs technology to manage design complexity while providing high functional capability and high performance.

Use of different FPGA chips as programmable components instead of programmable logic controllers (PLC) as well as other diversity attributes is an advantage solution to the decreasing a software source of potential common cause failures (CCF). The high functional capability and high performance of the RadICS platform can support many types of safety I&C systems for different types of existing and future power reactors.

RPC Radiy established the basis for I&C system design, manufacture, assessment, service and maintenance in accordance with requirements of standards, norms and recommendations of the International Atomic Energy Agency (IAEA), as well as the International Electrotechnical Commission (IEC) for application in nuclear safety systems.

The objective of this paper is to present results of an advanced FPGA technology application for

Received date: October 5, 2011
(Revised date: November 9, 2011)

implementation of NPP I&C systems. The paper has the following structure:
- capabilities of FPGA technology for NPP I&C systems;
- RadICS platform;
- implementation of FPGA-based NPP I&C systems based on RadICS platform;
- implementation experience.

2 Capabilities of FPGA technology for NPP I&C systems

FPGA technology goes back to middle of 90s as the alternative to microprocessor technologies and as a sub alternative to programmable logic devices (PLD) and application-specific integrated circuits (ASIC).
Physically FPGA is a semiconductor device that can be programmed or reprogrammed in accordance to customers' requirements.

FPGA is a complex programmable component which includes two entities: 1) FPGA-chip is a part of hardware and that should be qualified against hardware qualification testing requirements; 2) FPGA electronic design is a set of statements in Hardware Description Language (HDL) which is appropriate for implementation in FPGA-chip and that should be verified against functional requirements.

Application of FPGA technology for implementation of NPPs I&C systems provides the following benefits:
- implementation of control logic and other safety-critical functions in the form of FPGA with embedded electronic design. No executable software is needed;
- parallel processing of all process control algorithms within one cycle, thus ensuring high performance of the system;
- proven deterministic temporal characteristics due to parallel operation of control algorithms;
- reduction of volume and complexity of design and verification activities. No black-box or grey-box components in safety systems;
- ability to develop the software-hardware platform in such a way that it becomes a universal interface to create different I&C systems for any type of reactors. Application of the same hardware increases maintainability and availability of I&C systems in operation;
- obsolescence management. FPGA electronic design description is portable to different target devices;
- modification of the I&C systems after commissioning. For example, to conduct control algorithm modification, without any interference in I&C systems' hardware structure.

One of the latest concerns of regulatory bodies and utilities is cyber security. Particularly, after Stuxnet event the attention of the nuclear audience worldwide to cyber security topic increases.

FPGA-based technologies have specific beneficial properties regarding cyber security that are different from those of PLC-based technologies, such as:
- HDL code (usually VHDL or Verilog) without an operating system is used for FPGA programming. At the present there are no known viruses and malware for HDL,
- FPGA-based designs do not rely on operating system and therefore do not have dormant, unused capabilities that can be attacked,
- Some PLDs are not reprogrammable (like ASIC) and program modification requires the physical replacement of the ASIC-based board,
- Some PLDs (like CPLD and FPGA) are reprogrammable. HDL code is located in flash memory (separated chip) without physical access for modification,
- FPGA programming and reprogramming can be done only through a special interface. It is impossible to connect common storage media or communication devices that could infect the control logic code, it was in a case with the Stuxnet,
- FPGA-based devices have simpler designs (compared to conventional PLC-based solutions). It entails more likely possibilities to detect malicious designs through V&V. It also permits to assess COTS-based design.

3 RadICS platform

The digital I&C platform developed by RPC Radiy is composed of multiple modules based on the use of FPGAs as computational engine for each module (see Fig.1). The basic configuration for the platform consists of a rack containing one Logic Module

(LM) and one Diagnostic Module (DM) plus up to 14 other modules of any mix of module types (I/O and optic communication). The basic set of I/O modules comprises analog input (AI), digital input (DI), and digital output (DO) modules. There are also special purpose I/O boards such as RTD, thermocouple, ultra-low voltage AI boards (used for neutronics instrumentation), actuator controller modules, and a fiber-optic communication module that can be used to extend the system to multiple chassis. It is also possible to provide inter-channel communications between 2, 3 or 4 channels via fiber-optic communications directly between logic modules.

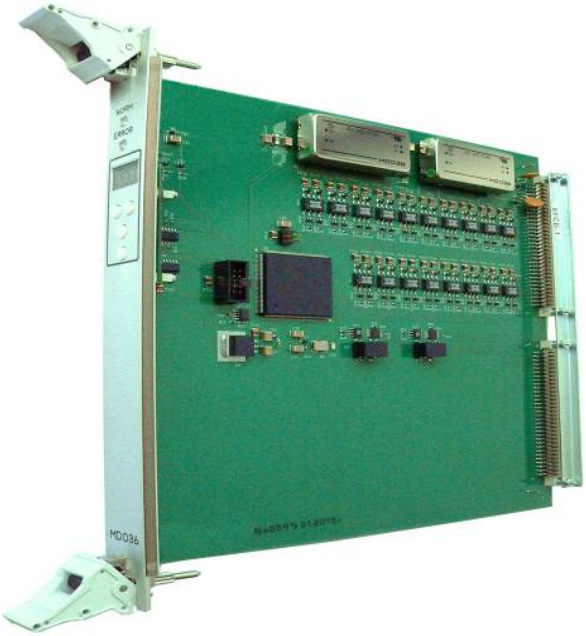

Fig.1 Typical FPGA-based module of RadICS platform.

LMs gather input data from input modules, execute user configured logic, and update the value driving the output modules. DMs gather diagnostic and general health information from all I/O Modules and the Logic Module. The I/O modules provide interfaces with other devices (*e.g.*, sensors, actuators). The functionality of each module is driven by the logic implemented in the onboard FPGA(s).

The backplane for the RadICS platform provides external interfaces to power, process I/O, communications links, and local inputs and indicators. Internal backplane interfaces facilitate connections to the various modules that are installed within the chassis by means of dedicated, isolated, point-to-point low-voltage differential signaling. Basic configuration of RadICS platform is presented on Fig. 2.

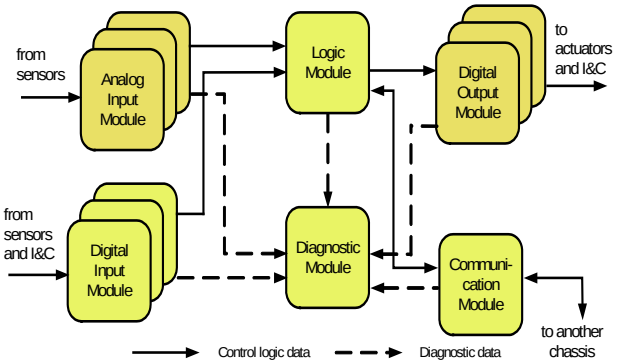

Fig.2 Basic configuration of RadICS platform.

The RadICS platform and the I&C safety systems based on the platform provide extensive on-line self-surveillance and diagnostics at different levels, including:

- Self-diagnostic and defensive coding of electronic design components;
- Self-monitoring of FPGA circuit (control of FPGA power, watchdog timer, CRC calculation, state monitoring, *et al.*);

- Monitoring of FPGA support circuits;
- Input / Output modules;
- Communications units;
- Power supplies, *et al.*

Diagnostic functions are separated from logic functions and are executed independently in a parallel mode. Diagnostic provides a means to put the systems in a safe state depending on the detected fault of the component.

The especial RadICS Platform Configuration Toolset (RPCT) is used to configure NPP applications on the basis of existing platform functional modules, plant input/output signals database, and application control logic. I&C systems' configuration on the basis of RadICS platform includes the following five steps:

1) configuration of input and output signals,
2) configuration of control algorithms,
3) configuration of functional modules, racks, and cabinets set,
4) configuration of internal links (wires and fibre optics),

5) configuration of high level data base for technological and diagnostic information registration, visualization, and archiving.

RadICS platform was applied to the following applications, which perform reactor control and protection functions [4]:
- Reactor Trip System (RTS),
- Reactor Power Control and Limitation System (RPCLS),
- Engineering Safety Features Actuation System (ESFAS),
- Rods Control System (RCS),
- Automatic Regulation, Monitoring, Control, and Protection System for Research Reactors (RMCPS).

The overall architecture for I&C systems designed by RPC Radiy is developed based on customer technical specifications from a standard library of FPGA based electronic modules. Communication methods and protocols between electronic modules, instrument channels and interfacing systems use various proprietary protocols applying appropriate isolation where necessary. Specific installations may differ in certain aspects such as the use of “2 out of 3” or “2 out of 4” logic and to comply with local installation requirements.

Let us consider the example of safety application based on RadICS platform. The RTS design implemented by RPC Radiy consists of two independent and diverse divisions. Safety actuation by either division initiates reactor shutdown and trip functions. Each division is composed of three separate channels (see Fig. 3).

Each channel consists of signal forming cabinets, which receive and process channelized signals from plant instrumentation and provides output signals to voting logic in the cross output cabinet (COC). Logic modules in the signal forming cabinets communicate with operator interface and alarming systems in the main control room (MCR) and the emergency control room (ECR). The diagnostic module in the signal forming cabinets sends diagnostic and status information via one-way link to the engineering workstation.

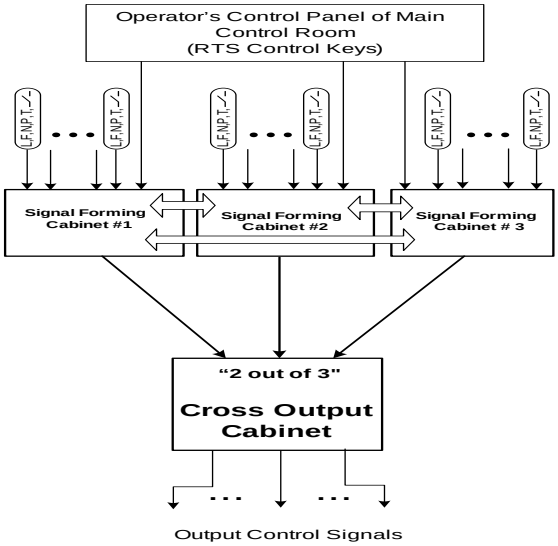

Fig.3 One division of FPGA-based reactor trip system.

4 Development and implementation of FPGA-based NPP I&C systems based on RadICS platform

The RPC Radiy approach to developing a nuclear power plant application using its FPGA-based platform involves establishing system requirements from customer specified requirements, defining a system architecture based on those requirements and the base platform, developing application-specific logic algorithms and hardware configuration parameters, instantiating the logic into hardware and integrating the system, testing the configured system, and installing the final validated system.

The approach of RPC Radiy to implementation of I&C system using RadICS platform is presented on Fig.4.

Design and development processes at RPC Radiy are based on an extremely strong scientific team. Eleven PhDs, one Doctor of Technical Science, one Honour inventor of Ukraine, four members of International Academy of Radio Electronics, and two members of Engineering Academy of Ukraine are currently working for RPC Radiy.

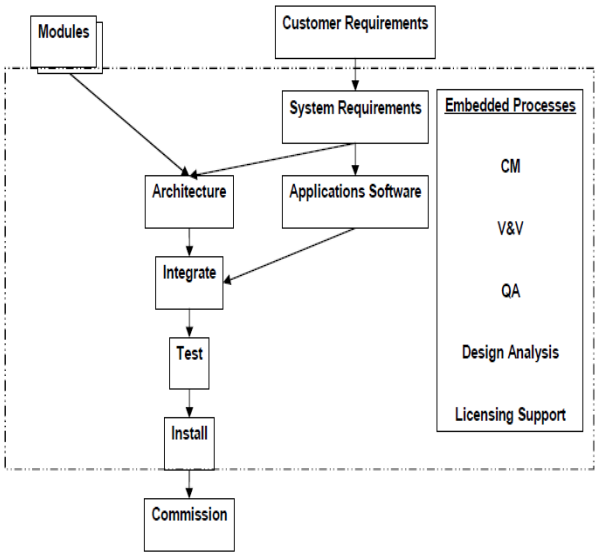

Fig.4 The Approach to implementation of I&C system using RadICS platform.

The structure of RPC Radiy includes the separate Scientific-Technical Centre for Safety Infrastructure-Oriented Research and Analysis (located in Kharkiv). The Centre performs V&V processes with the required degree of technical, managerial, and financial independence from design teams. In particular, Centre's staff carries out independent reviews and implements V&V activities of developments made by the design bureaus of RPC Radiy, as well as researches the technologies of safety systems development and verification. RPC Radiy specialists are active members of international organizations (particularly the IAEA and IEC) specializing in development of regulatory documents and standards, relating to control systems for nuclear facilities.

The FPGA electronic design is accomplished in accordance with RPC Radiy design practices, procedures and policies, as well as with international requirements and includes embedded verification and validation at each stage of the development.

RPC Radiy uses advanced approaches to FPGA development and verification techniques. RPC Radiy anticipates the appearance of new standards that provide requirements applicable to NPP FPGA-based systems. Since 2006, the IEC SC 45A has been developing standard IEC 62566 (Nuclear Power Plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions). RPC Radiy assessed its design practices against the requirements of IEC 62566, and considers it in compliance since 2003.

Application of software tools during V&V activities helps to eliminate human factor errors and faults in design. Also, application of such tools by the independent verification team, that are different from the ones used by the design team, helps to decrease the probability of common cause failures raised by the use of complex software tools [5].

RPC Radiy's development and verification techniques include:
- Preliminary FPGA electronic design development with verification via design review;
- FPGA electronic design development (elaboration & RTL synthesis) with verification via functional simulation;
- FPGA electronic design logic synthesis with verification via gate-level simulation;
- FPGA electronic design place & route with verification via timing simulation and static timing analysis;
- Bitstream generation and FPGA electronic design integration with verification via integration testing.

RPC Radiy design practices are aimed at achieving compliance with the general design and quality assurance activities for I&C systems that have a functional safety role as given in IEC 61508, the specific requirements for nuclear I&C systems as given in IAEA safety standards and IEC standards for nuclear facilities, and the Member State specific regulatory requirements and guidance specified by their customers.

RPC Radiy is an active participant in the nuclear FPGA standard that is under development (IEC 62566) and is considering the guidance of the draft standard as it involved. The development of this standard is also being followed closely by IAEA, Member State regulators, and the Nuclear Energy Agency's Multinational Design Evaluation Program. Therefore, RPC Radiy is fully aware of the emerging consensus on safety application of FPGAs.

The system undergoes equipment qualification testing to demonstrate compatibility and withstand capabilities. Specific qualification tests include:
– Radiation Exposure Withstand Testing;
– Dust Withstand Testing;
– Environmental Testing;
– Mechanical Testing;
– Seismic Testing;
– Power Supply Parameters Changing Testing;
– Electrical Insulation Testing;
– Burn-In Testing;
– X-ray quality control of soldered printed circuits;
– EMC Testing.

5 Implementation experience

The first commissioning of safety I&C system based on RadICS platform was done in 2003 for Ukrainian NPP unit Zaporozhe-1. Between 2003 and 2010, RPC Radiy completed more than 50 “turnkey” projects and provided high quality complex I&C systems of different types for nuclear installations. These systems are commissioned in pressurized water reactor (PWR) units known as “VVER” reactors developed by the former Soviet Union. VVER reactors are used in Armenia, Bulgaria, China, Czech Republic, Finland, Hungary, India, Iran, Russia, Slovakia, and Ukraine. The primary focus was concentrated on modernization projects.

RPC Radiy profile on implementation of NPP’s I&C systems modernization projects is presented on Fig.5. Totally fifty three FPGA-based I&C systems have been supplied to the customers and the maintenance of that systems is ongoing. All the modernization projects have been completed within their schedule and budget. It is important to highlight that modernization projects have different scale and complexity level. For example, one division of 3 channels FPGA-based RTS consists of four cabinets only, while ESFAS comprises more than sixty cabinets (about forty five cabinets include FPGA-based modules).

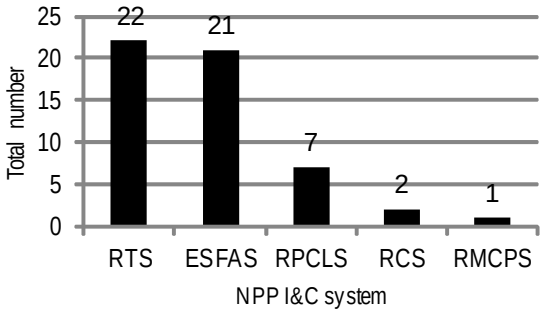

Fig.5 RPC Radiy profile on implementation of NPP’s I&C systems.

One of the complexity issues connected with modernization projects implementation is in necessity of establishing the interfaces between old analog I&C systems and new digital ones. Application of FPGA-based I/O modules of RadICS platform allows implementing such interfaces with less efforts, saving time and recourses.

6 Conclusions

Application of FPGA technology looks like a promising answer on challenges related with high-demand requirements for NPP I&C systems. Many players of nuclear industry worldwide, including vendors, academia and regulatory bodies have already responded to the technology via research programs and product developments. At the moment it is important to support promotion of FPGA technology application in NPP I&C systems.

RPC Radiy is vendor, which designs and produces FPGA-based safety I&C platform, as well as turnkey applications for NPP (safety systems) based on the platform. The RadICS platform has been successfully used for modernization of nuclear installations including PWR units and research reactors. Positive operation and maintenance experience shows that application of RadICS platform can improve NPPs safety.

References

[1] DITTMAN, B.F.: Regulatory experience with a FPGA-based digital I&C review, Presentation given at the 2nd IAEA Workshop on Applications of FPGAs in Nuclear Power Plants, 29 September – 1 October 2009 in Kirovograd, Ukraine, by B.F. Dittman, US Nuclear

Regulatory Commission Office of Nuclear Reactor Regulation. 2009.

[2] KHARCHENKO, V., SKLYAR, V.: FPGA-based NPP I&C systems: development and safety assessment, research and production corporation "Radiy", National aerospace university named after N.E. Zhukovsky "KhAI", State Scientific Technical Centre on Nuclear and Radiation Safety, 2008: 188.

[3] NASER, J., FINK, B., KILLIAN, C., NGUYEN, T., DRUILHE, A.: Guidelines on the use of field programmable gate arrays in nuclear power plant I&C Systems, EPRI, Palo Alto, CA, 2009 1019181.

[4] BAKHMACH, I., KHARCHENKO, V., SIORA, A., SKLYAR, V., TOKAREV, V.: Advanced I&C systems for NPPS based on FPGA technology: European experience. In: Proc. of 17th International Conference on Nuclear Engineering "ICONE 17", Brussels, Belgium, 12-16 July, 2009, on CD-ROM. ISBN: 978-0-7918-3852-5.

[5] ANDRASHOV, A., KHARCHENKO, V., SKLYAR, V., REVA, L., DOVGOPOLYI, V., GOLOVIR, V.: Verification of fpga electronic designs for nuclear reactor trip systems: test- and invariant-based methods. In: Proc. of IEEE East-West Design & Test Symposium, St. Petersburg, Russian Federation, 2010: 92-97.