Research and Production Corporation Radiy activities within Canadian nuclear market

I. Bakhmach, O. Siora, V. Kharchenko, V. Sklyar, A. Andrashov
Research and Production Corporation Radiy, Ukraine

Abstract

This paper presents key results of RPC Radiy activities within Canadian nuclear market. RPC Radiy (located in Kirovograd, Ukraine) is a vendor which designs and produces digital safety I&C platform as well as turnkey applications, based on the platform, for NPPs (safety systems). The main feature of the Radiy Platform is the application of Field Programmable Gates Arrays (FPGA) as programmable components for logic control operations. Since 2009 RPC Radiy started to explore the possibility to conduct the expansion to Canadian nuclear market. The activities performed by RPC Radiy related to this direction are resulted in several joint projects with Canadian companies.

1. Introduction

Rapidly evolving digital technologies led to the necessity of world-wide exchange of nuclear-related technical information and experience. Such exchange may be implemented via establishing of international projects between various organizations within nuclear domain. In this context application of FPGA technology could be a good topic for cooperation.

FPGAs are now widely used for safety-critical applications including systems important to nuclear installations safety. A peculiarity of the FPGA circuits is in using Hardware Design Languages (HDL) for electronic design development [1,2]. Experience of RPC Radiy in the area of FPGA-based I&C platform and systems design, development, installation and operation may be important for international nuclear community, since it provides an example of state-of-the-art technology application. For RPC Radiy, in its turn, such collaboration is a good opportunity to work with power reactors different from Pressurized Water Reactor (PWR) type, for example, Canadian Deuterium-Uranium Reactor (CANDU) as well as to find new markets for Radiy's products and services.

The following points are included in the scope of this paper:

− Radiy Platform peculiarities and advantages for implementation of I&C systems important to safety;

− Experience of the Radiy Platform application for I&C systems modernization;

− On-going projects of RPC Radiy at Canadian nuclear market;

2. Radiy Platform peculiarities and advantages for implementation of I&C systems important to safety

The Digital Safety I&C Radiy Platform comprises both upper and lower levels [3,4]. The upper level has been created on purchased IBM-compatible industrial workstations. The software for the upper level was developed by RPC "Radiy" and loaded into workstations. The functions of the upper level workstations are the following:

– Receipt of process and diagnostic information;

– Creation of man-machine interface in Control Room;

– Displaying of process information for each control algorithm related to control action executed by I&C system components;

– Displaying of diagnostic information concerning failures of I&C system components;

– Registration, archiving and visualization of both process and diagnostic information.

The lower level of the Radiy platform consists of standard cabinets including standard functional modules (blocks). The Radiy platform comprises the following standard cabinets:

– Normalizing Converters Cabinets (NCC) – perform receiving and processing of discrete and analog signals as well as feeding sensors;

– Signal Forming Cabinets (SFC) – perform inputting and processing of discrete and analog signals, processing of control algorithms, and conditioning of output control signals;

– Cross Output Cabinets (COC) – receive signals from three control channels (signal forming cabinets) and form output signals by “two out of three” voting logic ;

– Remote Control Cabinets (RCC) – control 24 actuators on the basis of Control Room signals, automatic adjustment signals and interlocks from signal forming cabinets;

– Signalling Cabinets (SC) – form control signals for process annunciation panel at Control Room;

– Information System Cabinets (CIC);

– Power Supply Cabinets (PSC);

– Unified Current Signal Distribution Cabinets (CDC) and

– Intermediate Clamp Cabinets (ICC) – for signal switching.

The cabinets include functional modules (blocks). The set of cabinets and modules forms the Radiy platform.

The platform includes the following modules:

– Chassis and backplanes;

– Power Supply Modules;

– Analog Input Modules;

– Normalizing Converter Modules, Thermocouples, Resistive Temperature Detector (RTD);

– Discrete Input Modules;

– Discrete Information Input Modules, Pulse;

– Potential Signals Input Modules, High Voltage;

– Logic Modules;

– Analog Output Modules;

– Discrete Output Modules;

– Potential Signal Output Modules;

– Solid-State Output Modules;

– Relay Output Modules;

– Actuator Control Modules;

– Communication Modules;

– Diagnostic Modules.

Application of the Radiy platform with the use of FPGA technology provides the following opportunities:

– To use software only for diagnostics, archiving, signal processing, data reception and transfer between the components of I&C system. Man-machine interface is provided. Failures of those functions do not affect execution of basic control functions of I&C system; operating system is not applied at lower levels of I&C system;

– To reduce verification process of software;

– To process all the control algorithms in a parallel way within single cycle to ensure both high performance of the system and proven determined time characteristics;

– To develop software-hardware platform in such way that it becomes a universal interface for creation of I&C systems for any type of reactor;

– To assure high reliability and availability due to the application of industrial components as well as using the principles of redundancy, independency, single failure criterion, and diversity;

– To resist failures and external impacts;

– To modify the I&C system after commissioning in a quite simple manner, including algorithm alterations, without any interference in I&C systems' hardware structure;

– To monitor and to control circuits of any kind of actuators (gates, engines, pumps, valves, etc.) in industries where very high action speed and reliability are required;

– To reduce by more than 10 times the number of contact and terminal connections which cause many operational failures of equipment due to wide use of integrated solutions and fibre optic communication lines;

– To deepen diagnostics of I&C systems equipment permitting quick and unambiguous detection of place, time, character of a failure and hazard degree of equipment operability violation.

3. Experience of the Radiy Platform application for I&C systems modernization

Radiy Platform has been applied to the following systems which perform reactor control and protection functions:

– Reactor Trip System (RTS);

– Reactor Power Control and Limitation System;

– Engineering Safety Features Actuation System (ESFAS);

– Control Rods Actuation System;

– Automatic Regulation, Monitoring, Control, and Protection System for Research Reactors.

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. Table 1 presents a reference list of applications modernized in Ukraine and Bulgaria [5] on the basis of Radiy platform.

Table 1. I&C systems modernization projects performed by RPC Radiy

NPP	Unit #	Modernized I&C system	Year of project implementation
Zaporozhe NPP (6 VVER units * 1000 MW)	1	RTS (Main)	2004
		RTS (Diverse)	2005
		RPCLS	2008
	2	RTS (Main)	2009
		RTS (Diverse)	2009
	3	RTS (Main)	2006
		RTS (Diverse)	2004
Rovno NPP (2 VVER units * 440 MW and 2 VVER units * 1000 MW)	1	RTS (Main)	2007
		RTS (Diverse)	2007
		ESFAS-1	2007
		ESFAS-2	2008
		ESFAS-3	2009
	2	RTS (Main)	2007
		RTS (Diverse)	2007
		ESFAS-1	2007
		ESFAS-2	2009
		ESFAS-3	2010
	3	RTS (Main)	2005
		RTS (Diverse)	2007

NPP	Unit #	Modernized I&C system	Year of project implementation
		RPCLS	2007
	4	RTS (Main)	2004
		RTS (Diverse)	2004
		RPCLS	2004
South Ukraine NPP (3 units * 1000 MW)	1	RTS (Main)	2005
		RTS (Diverse)	2005
		RPCLS	2005
		ESFAS-1	2007
		ESFAS-2	2006
		ESFAS-3	2005
	2	RTS (Main)	2007
		RTS (Diverse)	2007
		RPCLS	2007
		ESFAS-1	2010
		ESFAS-2	2007
		ESFAS-3	2008
Khmelnitsky NPP (2 units * 1000 MW)	1	RTS (Main)	2007
		RTS (Diverse)	2007
		RPCLS	2008
	2	RTS (Main)	2004
		RTS (Diverse)	2004
		RPCLS	2004
Kozloduy NPP (2 units * 1000 MW)	5	ESFAS-1	2010
		ESFAS-2	2009
		ESFAS-3	2010
		Power Supply of Control Rod System	2008
	6	ESFAS-1	2009
		ESFAS-2	2008
		ESFAS-3	2009
		Power Supply of Control Rod System	2007
Research reactor VVR-M of Ukrainian Nuclear Research Institute	–	Automatic Regulation, Monitoring, Control, and Protection System	2005

4. On-going projects of RPC Radiy at Canadian nuclear market

Since 2009 RPC Radiy started to explore the possibility to conduct the expansion to Canadian nuclear market. The efforts were distributed inside two main directions:

- certification of Radiy Platform in accordance with IEC 61508 SIL3 requirements;

- identification of potential customers and their needs.

The activities implemented by RPC Radiy related to these directions are resulted in several joint projects with Canadian companies, including the following:

- IEC 61508 certification with Exida;

- CANDU Shutdown System 1 (SDS 1) test specimen based on Radiy Platform for Atomic Energy of Canada Limited (AECL).

The following chapters will provide some details on each of the projects mentioned above.

4.1 IEC 61508 certification with Exida

The main goal of this project is to certify «the core part» of Radiy Platform in accordance with requirements of IEC 61508:2010 ed. 2. The idea of SIL certification is quite clear – this is a mandatory requirement of Canadian nuclear industry. Beside that IEC 61508 is approved and recognized by the most part of nuclear community worldwide.

Product conception has been developed to define a market niche and SIL number for the product. The product is a basic set of FPGA-based functional modules (I/O modules, logic module, diagnostic module, communication module) which permit to configure safety application using appropriate configuration tool which also is a part of the product. The idea is to certify separate modules (single channel configuration, see fig. 1) in accordance with SIL2 (it means that average probability of failure on demand (PFD) per hour is $10E\text{-}7 \leq PFDavg < 10E\text{-}6$) and applications with redundant configuration 1oo2, 2oo3 or 2oo4 (see fig. 2) in accordance with SIL3 (it means that $10E\text{-}8 \leq PFDavg < 10E\text{-}7$).

It is important to highlight that this certification project is rather unique because it is the first application of new edition of IEC 61508 for FPGA-based product of such scale and complexity.

In general the project’s plan consists of the following items:

- Selection of consulting company;

- Gap analysis of RPC Radiy on compliance with the requirements of IEC 61508;

- Identification and implementation of corrective actions concerning fulfilment of identified gaps;

- Conduction of independent assessment (certification audit).

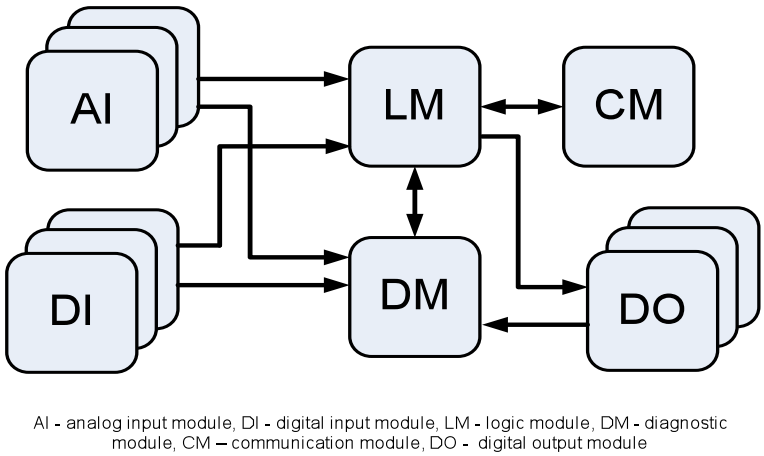

Figure 1 Single channel configuration of the product

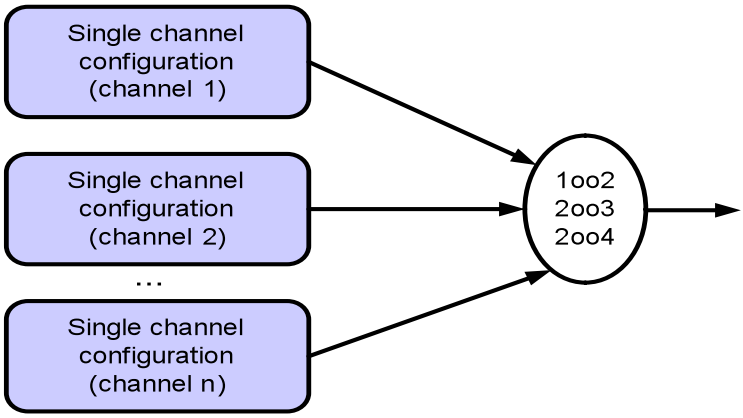

Figure 2 Redundant configuration of the product

4.1.1 Selection of consulting company

The analysis conducted for selection of consulting company showed that there is a company which satisfies all major criteria. Exida is one of the world's leading product certification and knowledge companies specializing in automation system safety. Exida has strong reference list and quite familiar with Canadian nuclear market. The first meeting between RPC Radiy team and Exida representatives has been conducted in March 2010.

4.1.2 Gap analysis of RPC Radiy on compliance with the requirements of IEC 61508

Gap analysis meeting have been conducted in Kirovograd in June 2010. Basically gap analysis was concentrated on two main areas of compliance: product and design processes of RPC Radiy. In total there are approximately 250 requirements that must be met for a product to get IEC 61508 SIL 3 certification. About 60% (150) of the requirements are process requirements.

Gap analysis for the product has been conducted through system failure mode and effect analysis (System FMEA) session. A System FMEA examinesthe overall system architecture in order to identify potential failure modes and their impact on the safety of the system. It also identifies known safety

integrity measures that can help to mitigate the impact of any dangerous failure modes. The results of System FMEA have been documented in corresponding report. The general conclusion of FMEA report is that only minor design changes for the product would be needed to meet SIL2 requirements (in terms of reliability indicators and diagnostic features) in a single channel configuration .

Gap analysis for the design processed has been conducted through independent audit called «Process Gap Analysis». This audit was focused on all main design attributes of complex FPGA-based solutions, including:

- requirements management;

- architecture design;

- detailed design and implementation;

- verification and validation;

- configuration management;

- modification and change management;

- selection and use of software tools;

The results of the analysis were quite positive. The main findings of process gap analysis are the following:

- life cycle is consistent with IEC 60880 and many aspects of IEC 62566 «Nuclear Power Plants– Instrumentation and control important to safety–Development of HDL-programmed integrated circuits for systems performing category A functions» are considered;

- IEC 61508-specific documentation (e.g. Functional safety management plan, safety requirement specification) is not generated;

- IEC 61508-specific design considerations (e.g. safe failure fraction) are not included.

4.1.3 Identification and implementation of corrective actions related with fulfilling of identified gaps

The list of corrective actions has been identified using the reports developed as a result of gap analysis.

During July-October 2010 the reengineering of Radiy's design processes in accordance with IEC 61508 requirements was conducted. It included correction of existing company standards to be SIL-oriented as well as issue of new IEC 61508-specific company standards (e.g. VHDL design and coding guidance) and procedures.

In October 2010 an extensive corporative training of Radiy personnel in functional safety was conducted. The training was provided by certified functional safety coach from Exida. During 2 weeks significant part of Radiy team involved in licensing project (more than 50 persons) was studying the functional safety concepts. In the framework of the training a set of workshops, concerning the details of IEC 61508 safety lifecycle implementation, has been conducted with key

persons of the Radiy team. These workshops resulted in detailed plan concerning further activities to eliminate the gaps.

In November 2010 the development process of FPGA-based modules design and corresponding firmware to comply with SIL2 requirements (SIL3 for redundant configuration) has started as well as the development of SIL3 compatible design documentation for the product. By the end of January 2011, SIL3 documentation related to project's start up phase, including product concept, functional safety management plan, document plan, personnel plan, configuration management plan, tool selection and evaluation report, security analysis report have been developed. The final independent assessment of the product is planned in 2012.

4.2 CANDU Shutdown System 1 (SDS 1) test specimen based on Radiy Platform for AECL

This project involves collaboration efforts of RPC Radiy and AECL targeted to develop a qualified trip unit, based on FPGA platform, for possible use in future CANDU safety system applications. The beginning of this project goes to the 2nd IAEA workshop on application of FPGAs in NPP I&C systems which had been held in 2009 on the basis of RPC Radiy. During this event 90 representatives of industry, regulators and academia from 14 countries discussed various issues concerning application of FPGA in development and modernization of safety-related NPP I&C systems. In the framework of the workshop presentations of Radiy equipment and facilities, as well as technical tour to South Ukrainian NPP to see Radiy's I&C systems in operation have been conducted. This helps AECL team to recognize RPC Radiy as mature vendor of FPGA-based safety I&C Platform as well as turnkey applications for NPPs. As a result the technical meeting between representatives of RPC Radiy and AECL has been planed and the project has started.

In March 2010 first formal technical meeting between RPC Radiy and AECL teams was organized. The principal position of AECL during the meeting was in ability to configure the safety applications based on Radiy Platform in-house (in Canada by AECL engineers) with all corresponding consequences. The outputs of the meeting helped to identify some key project targets listed below:

- Evaluate and test the Radiy Platform (develop and procure Radiy Platform–based test specimen to AECL);

- Develop methods for VHDL-based design process to be used by AECL;

- Develop suitable verification and validation approaches to be used by AECL;

- Work towards certification of Radiy Platform.

CANDU-9 SDS1 trip logic (similar to Darlington) has been selected as a target application for the test specimen. Close cooperation and mutual understanding between partner sides ensure quite rapid development of the test specimen. In September 2010 test specimen has been procured to AECL facilities and testing environment for the test specimen has been deployed. A National Instrument PXI System is used to stimulate the FPGA platform inputs and monitor its outputs. The public presentation of the test specimen and testing environment has been organized at the end of September 2010 in Hamilton, Canada during the 3rd IAEA workshop on application of FPGAs in NPP I&C which has been hosted by AECL and Mc Master University.

As mentioned before, AECL requested from Radiy the technology transfer in terms of FPGA design and V&V methodologies to configure safety applications based of Radiy platform by internal team of AECL. These methodologies are based on experience of RPC Radiy in corresponding subject domain. The adaptation and extension of FPGA design and V&V methodologies will involved experts from Mc Master university. One of the most important features, which were planned to be implemented, is formal verification of FPGA electronic designs.

Another significant milestone in the framework of Radiy-AECL collaboration was the audit conducted by AECL procurement department, on-site of RPC Radiy. The audit took place in July 2010 and consisted of assessment of RPC Radiy quality management system (QMS) on compliance with ISO 9001 and CAN-Z299 series standards. During the audit, AECL auditors examined Radiy's standards, procedures, as well as implementation of corresponding processes and operations in real production activities. As a result of the audit, RPC Radiy was included into AECL's official supplier list. This fact essentially increases the confidence in RPC Radiy for potential customers and may be considered as a step towards SIL certification of Radiy Platform.

5. Conclusion

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 Radiy Platform has been successfully used for modernization of Nuclear Installations including PWR units and Research Reactors. The platform is being certified in accordance with IEC 61508 ed.2 SIL3, as well as feasibility analysis concerning development of Radiy Platform-based safety applications for CANDU reactors is being conducted. The I&C systems for CANDU reactors on the basis of the Radiy platform can include adjusted FPGA-based input signals processing modules, logic control modules, output signals modules, and actuators control modules. RPC Radiy is considering Canadian nuclear market as a strategic marketing direction and will be moving towards starting-up new projects within the market.

6. References

[1] J. Lach, W. Mangione-Smith, M. Potkonjak, "Enhanced FPGA Reliability through Efficient Run-Time Fault Reconfiguration", IEEE Trans. on Reliability, Vol. 49, 2000, pp. 296-304

[2] G. Doerre, D. Lackey, "The IBM ASIC/SoC Methodology – A Recipe for First-time Success", IBM Journal of Research and Development, Iss. 6, 2002, pp. 649-660.

[3] M.A. Yastrebenetsky (edit), "Safety of Nuclear Power Plants: Instrumentation and Control Systems", Technika, Kyiv, Ukraine, 2004.

[4] V. Kharchenko, V. Sklyar (edits), "FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment", RPC Radiy, National Aerospace University "KhAI", State STC on Nuclear and Radiation Safety, Kharkiv, Ukraine, 2008.

[5] I. Bakhmach, V. Kharchenko, A. Siora, V. Sklyar, A. Andrashov, "Experience of I&C systems modernization using FPGA technology", Proceedings of the NPIC&HMIT 2010, Las-Vegas, Nevada, USA, November 7-11, 2010.