Safety-critical Certification of FPGA-based Platform against Requirements of U.S. Nuclear Regulatory Commission (NRC): Industrial Case Study

Vladimir Sklyar

National Aerospace University "KhAI", Kharkiv, Ukraine
vvsklyar@ukr.net

Abstract. Instrumentation and Control systems play important role in operation and maintenance of Nuclear Power Plants. A challenge in such systems implementation is certification and licensing against national safety regulatory requirements. A considered case describes certification of Instrumentation and Control platform of Ukrainian company Radiy against the United States nuclear safety requirements. General framework is described. Research activities of the project are presented.

Keywords: certification, licensing, FPGA, NPP I&C system

Key terms. MathematicalModeling, MathematicalModel, SoftwareSystems

1 Introduction

Nuclear energy is still one from the essential sources in energy agenda of many countries. In Ukraine, for example, up to 50% of energy is generated at Nuclear Power Plants (NPP). Instrumentation and Control (I&C) systems play important role in NPP safety and security assurance as well as in effective control of energy production. Safe and cost-effective operations of NPPs require the modernization of I&C systems to cope with obsolescence and age-related degradation. A computation core of the most parts of I&C systems are generic programmable platform also named as Programmable Logic Controllers (PLCs) [1].

Research and Production Corporation (RPC) Radiy (Kirovograd, Ukraine) has a long history of working with operating NPPs and installing new I&C systems during turn-key projects. RPC Radiy provides a wide variety of I&C solutions ranging from full-scope turn-key modernization projects to reverse engineering and printed circuit board-level. Also like-for-like replacements and equipment to solve ageing and obsolescence problems are implemented for both safety and non-safety applications. RPC Radiy uses Field Programmable Gate Array (FPGA) technology in its digital platform to implement customized solutions for NPPs I&C systems. RPC Radiy's proven technological expertise has been demonstrated in over 100 systems installed to date.

ICTERI 2016, Kyiv, Ukraine, June 21-24, 2016

RPC Radiy's I&C systems have been installed in safety related systems of all operating NPP sites in Ukraine and Bulgaria [2].

FPGA-based safety I&C platform RadICS is the main product of RPC Radiy. The RadICS Platform is designed to be functionally and physically similar to currently installed I&C systems. Such platform capabilities include input processing, customizable control logic, and output processing. The RadICS Platform continuously monitors system status through signals that are received from field sensors. It performs logic computations to create control commands. It also converts control commands to output signals that are applied to field actuators. The RadICS Platform has a modular and scalable design that can be configured to meet the needs of safety I&C applications in NPPs [3].

A big part of efforts to provide I&C systems for utility is licensing efforts. I&C systems have to comply with state-of-the-art standards. A licensing permission process lies in consideration of appropriate documentation related with I&C system design. A challenge is each country has its own set of regulation requirements. So I&C vendors face to make a new licensing case with penetration to any new market. For I&C vendors there are the most challenging licensing barriers at the United States (U.S.) nuclear market. From the one hand the U.S. operate more than one hundred reactors what is the biggest nuclear fleet in the world. From the other hand the U.S. Nuclear Regulatory Commission (NRC) implements one form the strongest regulatory framework in the word, and it is a reason why the biggest part of the nuclear community respects the U.S. NRC licensing permission.

In 2015 RPC Radiy started a project to certify RadICS platform against the U.S. NRC requirements. This paper contains description of the project framework and states some obtained results.

An essential part of the mentioned certification process is a deep University-Industry Cooperation (UIC) conducted between RPC Radiy and National Aerospace University (Kharkiv, Ukraine). Academicians are involved in all parts of RadICS platform certification what is one from the main factor of successful project running. Conclusion of this paper contains a list of researches directed to support of industrial certification activities.

Available references in the investigated area are mainly technical reports available from the U.S. NRC documentation system ADAMS (www.nrc.gov/reading-rm/adams.html).

2 FPGA-based I&C Safety Platform RadICS

The RadICS Platform is a state-of-the-art digital product specifically designed for safety-related control and protection systems of NPPs. A modular and distributed FPGA-based architecture is one from the RadICS Platform features. There is a set of general purpose building blocks (modules) that can be configured and used to implement application specific functions of I&C systems (see Fig. 1).

The basic architecture of the RadICS Platform consists of instrument chassis containing a logic module, as well as up to 14 other Input/Output (I/O) and fiber optic

communication modules. Logic module gathers input data from input modules, execute application specific logic, and update the value driving the output modules. Logic module is also responsible for gathering diagnostic and general health information from all I/O modules. The I/O modules provide interfaces with field devices (e.g., sensors, transmitters, and actuators). The functionality of each module is defined by the logic implemented in the FPGA that are part of the above modules. The backplane of the RadICS Platform provides interfaces to power supplies, process I/Os, communication links, and indicators. The internal backplane provides interfaces to the various modules installed within each chassis by means of a dedicated, isolated, point-to-point low voltage differential signaling (LVDS) interface.

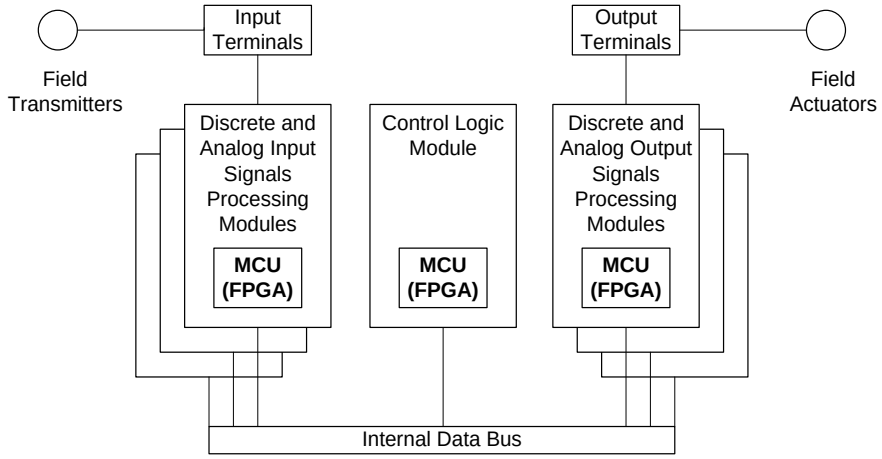

Fig. 1. Typical structure of Instrumentation and Control system based on Microcontroller Unit (MCU) or Field Programmable Gates Array (FPGA)

For application development, RPC Radiy provides a tool called Radiy Product Configuration Toolset (RPCT). This tool can be used to configure logic for various applications using the Application Functional Block Library (AFBL).

In addition, the RadICS Platform includes extensive on-line self-surveillance and diagnostics at various levels, including control of FPGA power, watchdog timer, cyclical redundancy check (CRC) calculations, and monitoring of the performance of FPGA support circuits, I/O modules, communications units, and power supplies.

Safety Life Cycle (LC) of the RadICS Platform is presented on Fig. 2. The RadICS Platform LC implements specific stages of FPGA design development and verification. Specific technique of fault insertion testing has been performed for both hardware and software parts. This LC complies with requirements traceability concept which requested the following:

- Every requirement has a child (either a lower level requirement or a solution);
- Every lower level requirement or solution has a higher level requirement (and opposite, an orphan represents unjustified functionality);
- Every requirement has been tested.

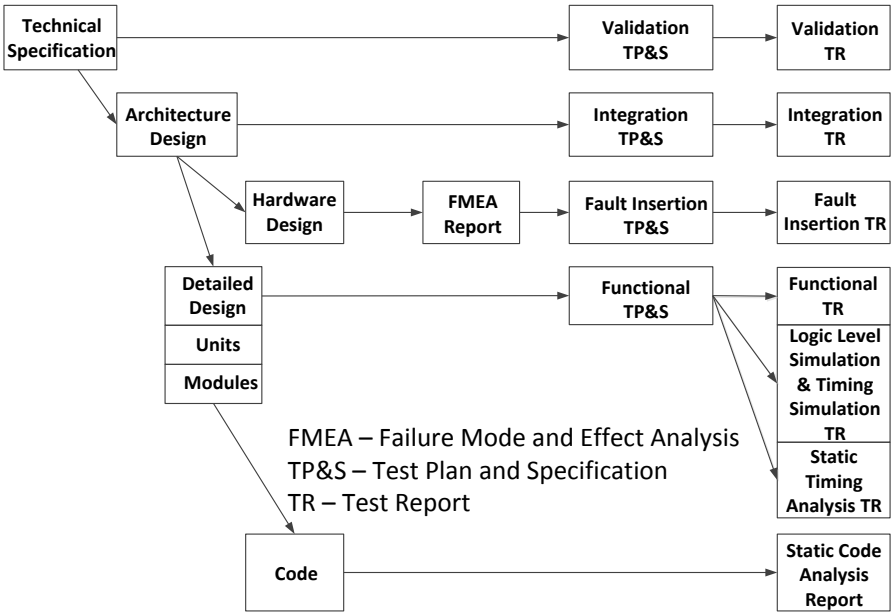

Fig. 2. Safety Life Cycle of FPGA-based RadICS Platform

3 General Approach to Certify I&C Safety Platform in the U.S.

Firstly RPC Radiy established RadICS in 2012, as a wholly owned Limited Liability Company (LLC). The Company RadICS business focus is the design and delivery of I&C systems for NPPs using the RadICS Platform equipment. Company RadICS, based together with RPC Radiy in Kirovograd, Ukraine, is responsible for all RadICS-based application project activities except the manufacturing of the RadICS Platform equipment. Such approach allows to focus certification efforts only on target processes for safety assurance.

After that the basic U.S. licensing strategy is to demonstrate that the generic RadICS Platform and the associated quality and software life cycle processes comply with U.S. nuclear safety requirements. As it is mentioned above, the RadICS Platform has been already licensed in Ukraine and Bulgaria. Difference of the U.S. regulatory requirements was analyzed. Licensing activities workflow was built on the base of results of such analysis, as it is shown it Table 1.

Actions to demonstrate compliance with the U.S. licensing requirements are presented at Fig. 3. An umbrella document for licensing activities is the Topical Report. Some details of the RadICS Topical Report are discussed in the next part.

It should be noticed, the U.S. NRC requires conducting technical meetings for discussion of the provided documents. Since the U.S. NRC has a specific philosophy of I&C systems consideration, additional research have been performed to fulfill this gap (see the Conclusions).

Table 1. Results of Analysis of the U.S. Licensing Specific Part

Difference in requirements	Actions to meet requirements
The U.S. NRC requires to implement a specific Quality Management Program (QMS) in accordance with regulations 10 CFR Part 50 Appendix B	Establish RadICS QMS in compliance with the U.S. NRC requirement. It should be noted U.S. NRC requirements to QMS are different from widely used ISO 9001 QMS, so many efforts are spent to adopt specific requirements in accordance with regulations 10 CFR Part 50 Appendix B "Quality Assurances Requirements for Nuclear Power Plants and Fuel Reprocessing Plants" and ASME NQA-1-2008, "Quality Assurance Program Requirements for Nuclear Facilities". The RadICS QMS governs the system design, integration, and delivery of I&C systems for NPPs using the RadICS Platform equipment
The U.S. NRC requires to implement a specific process for Commercial Grade Dedication for as named commercial components. RadICS Platform components at the RPC Radiy site are commercial since they are produced under not nuclear ISO 9001 QMS	Dedicate the generic RadICS Platform, which was not originally developed under a 10 CFR Part 50 Appendix B QMS, in accordance with the basic requirements for Commercial Grade Dedication. RadICS is employing the commercial dedication processes described in Electric Power Research Institute (EPRI) Technical Report (TR)-107330 "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants" and EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications"
The U.S. NRC requires to submit the Topical Report which has to represent the main platform features	Develop the RadICS Topical Report. The purpose of the RadICS Topical Report is to demonstrate that the RadICS Platform and the associated quality and programmable logic life cycle process comply with NRC requirements
The U.S. NRC requires to submit a set of documents which support the Topical Report argument	Submit to the U.S. NRC the RadICS Topical Report with sets of relevant documents. These documents have to be submitted in three phases. The main part of such documents have been already developed before
The U.S. NRC requires to provide a representative (QTS)	Design, produce and dedicate from RPC Radiy the Qualification Test Specimen (QTS) with the with the Data Acquisition System (DAS)
The U.S. NRC requires to perform a set of qualification tests for the QTS	Perform QTS Equipment Qualification Testing in one from the U.S. testing laboratory recognized by NRC

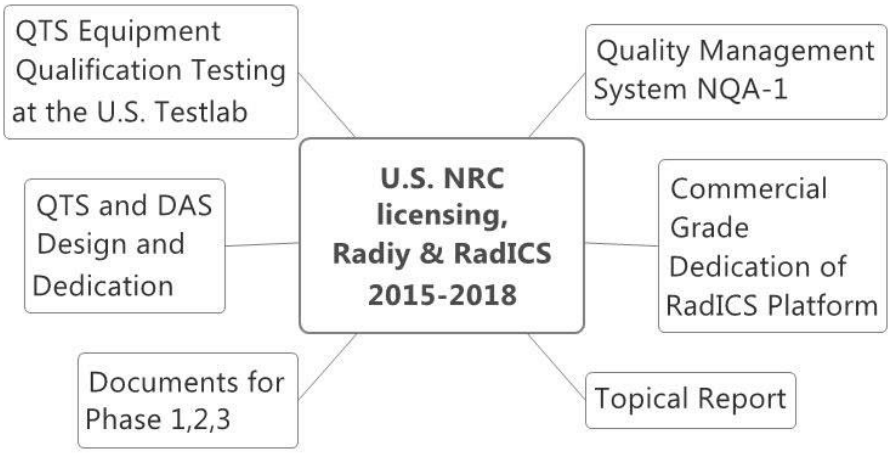

Fig. 3. Parts of Licensing Approach against the U.S. NRC Regulatory Requirements

4 Content of the Topical Report

The RadICS Topical Report is the summary licensing document for the RadICS Platform digital safety I&C platform. It presents design, performance, and qualification information for the RadICS digital safety I&C platform developed by RPC Radiy. The RadICS Platform is a generic digital safety I&C platform dedicated to the implementation of Class 1E (the highest safety class) safety I&C functions in the U.S. NPPs.

The RadICS Topical Report has been divided into 12 chapters and 3 appendices (see Fig. 4). The most important issues of this Topical Report are the following:

- An overview of RadICS development and operational use in international NPPs where it is currently deployed in a variety of digital safety I&C applications. This information is provided to illustrate the safety I&C developments that led to the RadICS Platform;
- An overview of the quality program and the quality process employed to dedicate the generic RadICS Platform hardware and associated programmable logic and develop systems for delivery to U.S. customers;
- An overview of the commercial grade dedication program used to dedicate the generic RadICS Platform hardware and associated platform programmable logic;
- A description of the RadICS Platform operation and how it can be applied in NPP safety-related applications. It also provides descriptions of the hardware and associated generic programmable logic that comprise the RadICS Platform. In addition, details are provided on how digital communications and testability are implemented in the RadICS Platform;
- A description of the hardware development process with associated planning documents and component testing process;

- A description of the RadICS Platform generic programmable logic development life cycle, planning documents, and the verification and validation process. The RadICS programmable logic life cycle processes were examined in more detail as part of the functional safety certification;
- An overview of the generic equipment qualification program for the RadICS Platform. The RadICS qualification "envelope" is designed to meet or exceed the environmental qualification requirements for NPPs in the U.S.;
- An overview of the RadICS approach to platform diversity;
- A summary of a RadICS Platform vulnerability analysis and the secure development and operational environment controls provided by RPC Radiy;
- A conformance summary of the RadICS design and development processes for the key regulatory guidance documents;
- The plant-specific system design guidance for use of the RadICS Platform, including recommended practices and any restrictions;
- A compliance matrix for the U.S. NRC regulatory document DI&C-ISG-04 "Highly Integrated Control Rooms – Digital Communication Systems" with the requirement listed as well as RadICS Platform compliance to each criterion defined;
- A list of the RadICS Platform design documents associated with the Electronic Designs for the RadICS Modules and identifies an initial set of documents planned for submittal to NRC to support the review of the RadICS Topical Report.

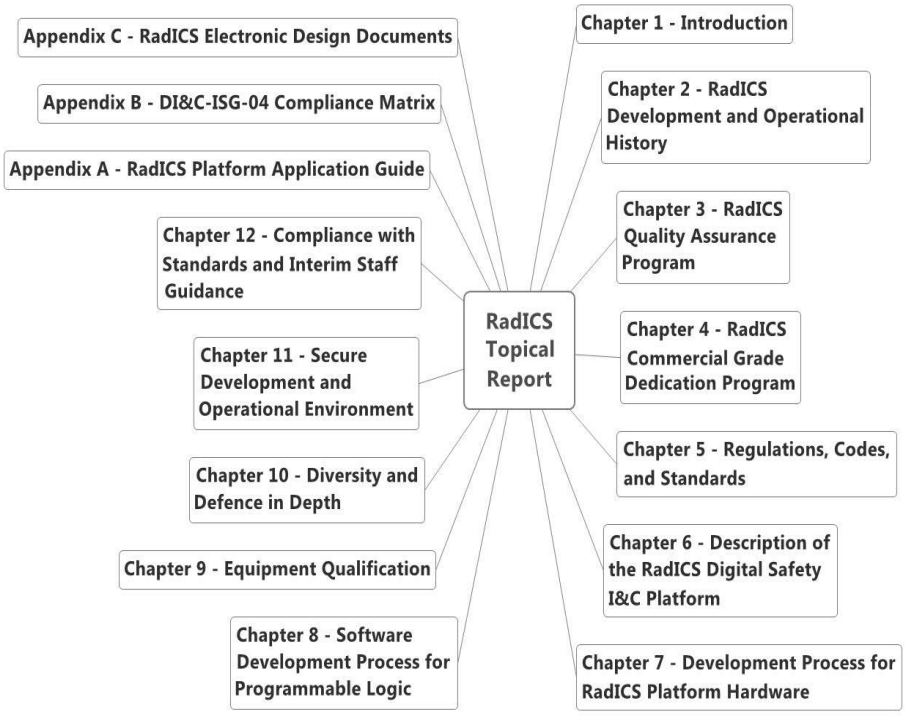

Fig. 4. A Structure of the RadICS Topical Report

5 Conclusions

As well as I&C platform is a high tech product, certification and licensing of such product requires innovative approach followed with research activities. A good basis for such researches provides UIC conducted between RPC Radiy and National Aerospace University. The following research directions have been chosen as priorities to support safety-critical certification:

- Research in FPGA and design tools safety features to support safe use of FPGA chip as a logic control core;
- Research in combination of different testing methodology with different coverage criteria to support effective verification and validation of I&C platform through life cycle;
- Research in efficient power consumption of I&C platform with optimization of used algorithms [4];
- Research in security of I&C platform to protect safety critical application from malware injection;
- Research in Safety and Security Case [5] methodology as a tool to support integral safety evaluation.

References

1. Kharchenko V.S., Sklyar V.V. (Edits). FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment / Bakhmach E.S., Herasimenko A.D., Golovyr V.A., Kharchenko V.S., Rozen Yu.V., Siora A.A., Sklyar V.V., Tokarev V.I., Vinogradskaya S.V., Yastrebenetsky M.A. 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 p.

2. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security / Yastrebenetsky M., Kharchenko V. (Edits). – IGI Global. – 2014. – 470 p.

3. Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring by Vyacheslav Kharchenko, Olexandr Siora and Volodymyr Sklyar in the book "Nuclear Power - Control, Reliability and Human Factors" edited by Pavel Tsvetkov, Texas A&M University, USA , 2011.

4. Kharchenko V., Gorbenko A., Sklyar V., Phillips C. Green Computing and Communications in Critical Application Domains: Challenges and Solutions // Proceedings of the 9th Digital Technologies International Conference “DT 2013”. – Žilina, Slovakia, May 29–31, 2013. – P. 241-247, on CD-ROM, ISBN 978-80-554-0682-4.

5. T. Kelly, Arguing Safety: A Systematic Approach to Managing Safety Cases, PhD thesis, Univ. of York, 1998.