UDC 681.513.3

V.V. SKLYAR, A.V. KHARYBIN, A.M. YURTSEVICH

Research and Production Corporation Radiy, Kirovograd, Ukraine

APPLICATION OF FPGA-BASED ROD CONTROL SYSTEM FOR NUCLEAR POWER PLANTS SAFETY IMPROVEMENT

Field Programmable Gates Arrays (FPGAs) are used as components of Nuclear Power Plants (NPP) safety systems since 1990s. During the last fifteen years FPGAs have recommended itself as reliable proven in use solutions which are able to increase safety of Instrumentation and Control (I&C) systems. Research and Production Corporation (RPC) Radiy is a designer and manufacturer of FPGA-based I&C platform and systems for NPP. The present paper discusses features of FPGA-based Rod Control System (RCS) as an example of NPP safety increasing with using FPGA technologies.

***Key words**: Field Programmable Gates Array (FPGA), Rod Control System, Instrumentation and Control systems, Nuclear Power Plant Safety.*

Introduction

Field Programmable Gates Arrays (FPGAs) are used as components of Nuclear Power Plants (NPP) safety systems since 1990s. FPGA-based technologies have specific beneficial properties regarding NPP applications [1]:

- Implementation of safety functions without the use of any operation software and operating system,
- Reduction in the time necessary for software verification in the design phase;
- Parallel processing of all control algorithms within one cycle, and proven deterministic timing characteristics due to parallel operation of control algorithms;
- Flexibility of the I&C platform which can be configured for any type of functions and reactor designs;
- Easy modification of control logic without any need for hardware modification;
- Possibility of implementing all safety requirements in integrated safety I&C systems;
- Resistance to internal failures and external environmental impacts;
- Resilience to obsolescence due to the portability of the Hardware Description Language (HDL) code between various FPGA-chips produced by different manufacturers;

FPGAs also have specific beneficial properties regarding cyber security that are different from those of Programmable Logic Controller (PLC) based technologies [2]:

- Use of HDL codes (usually in VHDL or Verilog) without the need for an operating system for FPGA programming. At the present time, there are no known viruses and malware for HDL;
- FPGA-based designs and operation do not rely on an operating system and therefore do not have hidden, unused capabilities that can be attacked;
- HDL code is located in flash memory (separated chip) without having a 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, as it was in case with the w32.Stuxnet worm;
- FPGA-based devices have simpler and transparent designs (compared to conventional PLC-based solutions). Malicious designs can be more likely detected by V&V processes.

Instrumentation and Control (I&C) systems made by Research and Production Corporation (RPC) Radiy (including the Rod Control Systems) is state of the art systems, which are designed on the basis of FPGAs, which is easy to operate, maintain upgrade and expand in the future, and also have the capabilities and flexibility to handle common regulatory requirements and customer specific requirements for the different NPPs [3].

Based on the fifteen years experience of FPGA-based systems implementation Radiy designed the Rod Control System (RCS) which has been successfully commissioned at the Unit 1 of the South-Ukraine NPP with WWER-1000 reactor [4].

The main objective of the RCS modernization was safety improvement on the base of risks elimination of the obsolete equipment. Such objective can be achieved with use of FPGA-based I&C advantages which are described above [1,3].

The present paper objective is to describe FPGA-based RCS design and features as an example of NPP safety increasing with using FPGA technologies.

© V.V. Sklyar, A.V. Kharybin, A.M. Yurtsevich

1. Overview of FPGA-based Rod Control System

Modern safety standards state the following requirements to RCS [4]:

– Single failure criterion compliance;

– Full redundancy of the monitoring, indication, rod drives control logic and control channels;

– Physical separation (galvanic isolation) of system inputs/outputs (I/Os);

– Independency between redundant channels;

– Easy and practical human-system interfaces excepting misunderstanding cases and human-factor errors;

– Monitoring and testability features implementation;

– Redundant, high speed, industry standard communication interfaces and protocols to transfer real-time data (such as safety parameters, field inputs, alarms, and RCS status) for monitoring and display, logging and trending for field diagnostics purposes;

– High reliability and availability (99.99%) with no single point of failure;

– online diagnostics with over 99% coverage;

– online repair using hot-swappable modules;

– Easy to maintain, modify and add future enhancements;

– Easy to upgrade and expand in the future without affecting existing field elements and wiring.

– Measurement resolution for measurement channels, signaling channel etc. should be not less than 0.1% from measurement range;

– Summary operational cycle for Rods positions monitoring and Rod Drives command signals forming processes should be less than 20 ms;

– Equipment qualification against environmental, seismic, electromagnetic and other external impacts.

RCS is designed on the basis of Digital FPGA-based safety I&C platform RADIY, it's the distributed I&C System, in which functions of control logic, rod drive, and rod position signaling are implemented on the basis of typical functional modules (platform approach), which are assembled into typical chassis and cabinets.

RCS in general consist of Rods Position Indication System / Subsystem (RPIS) and Rods Drives Control System / Subsystem (RDCS) with control logic processing equipment power supply subsystem and also can include its own Rod Drives Electric Power Supply Subsystem (System) (RDEPSS) made by RPC Radiy (or any other type of RDEPSS).

RPIS indicate all reactor control and safety rods position operation parameters and real rods position in case of emergency TRIP (emergency shutdown) of the reactor.

RDCS perform all Rod Drives control functions and include TRIP Portion (set of the Rod Drives power supply breakers).

RDEPSS, built on the basis of RPC Radiy equipment, is performs the following functions:

- Uninterrupted electric power supply of Rod Drives in normal operation mode;

- Switching off the Rod Drives electric power supply by Emergency Protection (EP) signals in case of normal operation failure which requires reactor shift to the subcritical state.

RCS has 2 or 3 redundant channels depending on the design basis of the nuclear reactor, and it can implement a voting logic of 1oo2 or 2oo3.

RCS scope of the equipment (depending on configuration requirements) includes a set of Rods Position Indication Cabinets (RPIC), Rod Drives Control Logic Cabinets (RD CLC), RDEPSS equipment (Rod Drives Power Supply Cabinets (RD PSC) with Rod Drives Control TRIP Portion breakers), software-based Workstation Cabinets (RCS WSC) for monitoring & data archiving and interconnections with other safety-related and non-safety systems functions, RCS Rods Position Indication Panels and Operators Workplaces in the Main Control Room (MCR) and Emergency Control Room (ECR) with power supply for all these Human Machine Interface (HMI) components directly from RCS cabinets, internal cable (electric and fiber-optic) connections between all RCS cabinets, and also the necessary hardware and software, which provide diagnostics, testing and RCS configuration. Each of the chassis installed in the RCS cabinets contains one Logic Module (LM), one Diagnostic Module (DM) and can include up to 14 I/O modules of various types – Rod Position Indication Module (RPIM), Rod Drive Control Module (RDCM), Rod Drive Power Supply Module (RD PSM). LM collects data from input modules, executes user configured control logic, and updates the states of the output modules. DM collects diagnostic and performance information from all I/O Modules and the LM. The I/O modules provide interfaces with field devices (Rod Position Sensors and Rod Drives).

RDEPSS include a set of cabinets with installed electric power distribution equipment, in which power supply functions are performed on the demand of emergency protection from Reactor Shutdown/Trip/Protection System. Scope of the RDEPSS equipment also includes internal cable connections, which provide electric power distribution connections between components included in the RCS, and necessary software and hardware, which provide diagnostics and configuration functions for RDEPSS.

RCS has on-line monitoring and maintenance capabilities. It can correct its voting logic in case faults are detected, so that system availability is optimized without compromising safety.

RCS has a self-diagnostic subsystem, which includes troubleshooting assistance functions for easy localization of faults. In case of failure, RCS puts itself in the safe state, signaling actuation for reactor shutdown.

RCS support manual Rod Drivers deactivation (power-off mode) for the Reactor TRIP from the Main Control Room (MCR) or Emergency Control Room (ECR) using independent Rod Drivers power supply lines breakers.Generic RCS architecture scheme for PWR-type reactors is presented on Fig. 1.

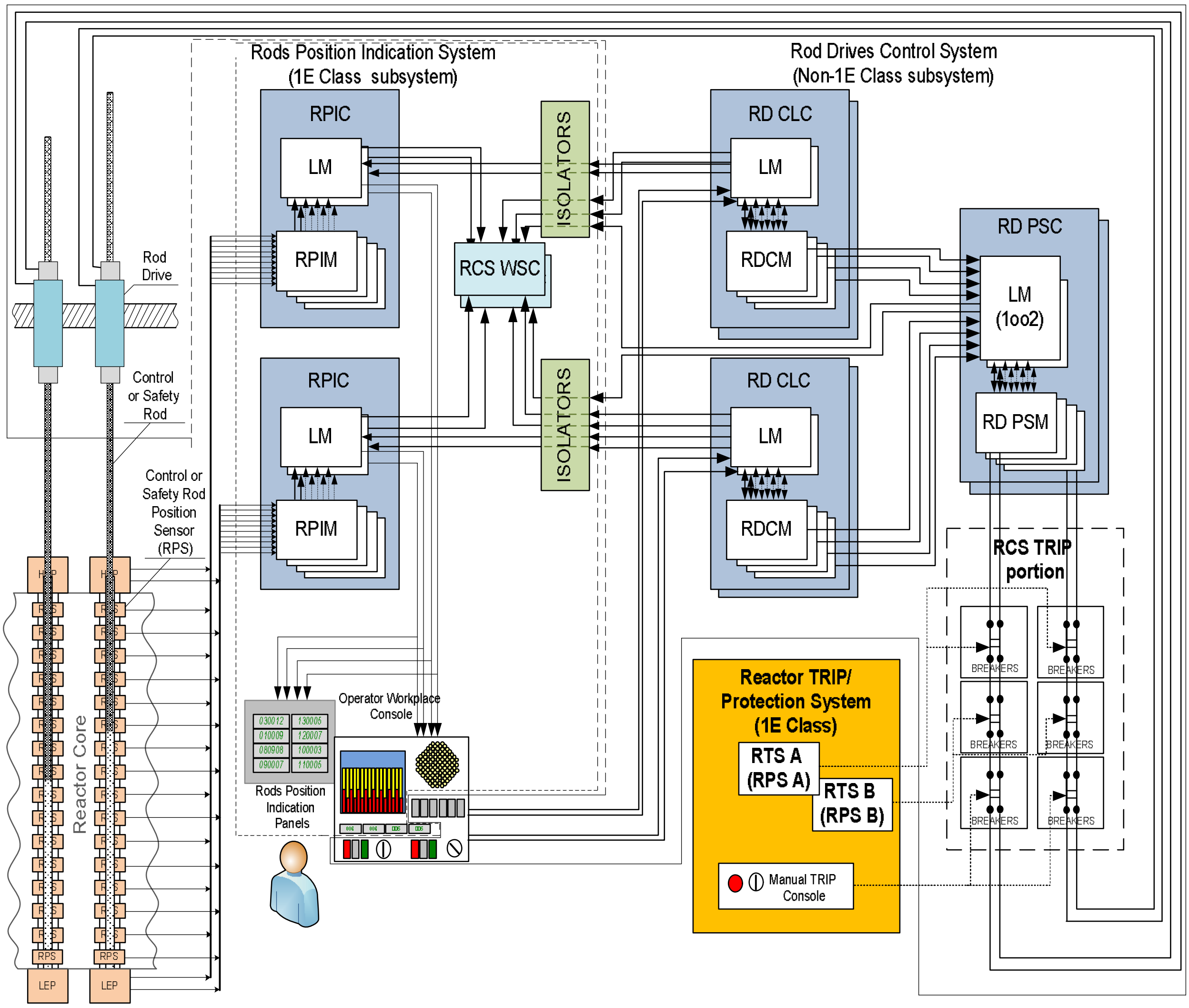

Fig. 1. Generic architecture of RCS two-channel configuration in 1oo2 voting logic version for PWR Unit

2. Main functions of FPGA-based Rod Control System

– Reading, raw and precise processing the signals from the Rod Position Sensors in real-time mode;

– Continuously monitoring all the Rods positions and data archiving;

– Indication of Rods positions on the Rods Position Indicators Panel and Operator workplace in the MCR and ECR;

– Automatic or manual Rod Drives Control (including Rod Drives power-off for reactor TRIP by EP signals from RTS);

– Automatic Rod Drives power-off actuation for reactor TRIP by the manual commands from the MCR and ECR;

– Providing operational and diagnostic data for different Human-System Interfaces and Unit/Plant monitoring systems;

Rods positions monitor software application is designed to collect, process, analyze and visualize at the operator workplace displays the main operating parameters of the Control and Safety Rods Positions in their groups or all at once in the reactor core mode.

Software application provides the functions like:

– On-line real Rods positions situation monitoring and proper/abnormal functioning of the control logic algorithms monitoring;

– Providing visualization of Rods precisely defined positions and analysis tools for RD control logic status information visualization based on the on-line data processing or using archive records from WSC servers;

– Monitoring data documenting (using printing or recording on hard driver).

Conclusion

RPC Radiy has fifteen years of experience in design, production and support of FPGA-based safety I&C systems for NPPs. Such systems provide mature state-of-the-art solutions for NPP safety improvement.

Mentioned above RCS meets the requirements of international safety standards [4].

References

1. NUREG/CR-7006, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems [Text]. – U.S. Nuclear Regulatory Commission (2010).

2. Kharchenko, V. FPGA-based NPP Instrumentation and Control Systems [Text] / V. Kharchenko, V. Sklyar (Edits), Development and Safety Assessment, Research and Production Corporation "Radiy", National Aerospace University named after N.E. Zhukovsky "KhAI", State Scientific Technical Center on Nuclear and Radiation Safety (2008).

3. EPRI TR1019181, "Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems [Text]. – Electric Power Research Institute (2009).

4. EPRI TR1022983, "Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant I&C Systems [Text]. – Electric Power Research Institute (2011).

Поступила в редакцию 8.02.2013, рассмотрена на редколлегии 6.03.2013

Рецензент: д-р техн. наук, проф., зав. каф. компьютерных систем и сетей В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

ЗАСТОСУВАННЯ СИСТЕМИ ГРУПОВОГО ТА ІНДИВІДУАЛЬНОГО УПРАВЛІННЯ ОРГАНАМИ РЕГУЛЮВАННЯ НА БАЗІ ПЛІС ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ АЕС

В.В. Скляр, О.В. Харибін, О.М. Юрцевіч

Програмовані логічні інтегральні схеми (ПЛІС) використовуються в системах безпеки атомних станцій (АЕС) з 1990х рр. За останні 15 років ПЛІС зарекомендували себе як надійні перевіренні часом рішення, здатні підвищити безпеку інформаційних і керуючих систем. Науково-виробниче підприємство "Радій" є розроблювачем і виробником інформаційно-управляючої платформи й систем на базі ПЛІС для АЕС. У дійсній статті на прикладі характеристик системи групового та індивідуального керування (СГІУ) на базі ПЛІС обговорюється питання підвищення безпеки АЕС із використанням ПЛІС-технологій.

Ключові слова: програмовані логічні інтегральні схеми (ПЛІС), інформаційні та управляючі системи, система групового та індивідуального управління, атомна електростанція.

ПРИМЕНЕНИЕ СИСТЕМЫ ГРУППОВОГО И ИНДИВИДУАЛЬНОГО УПРАВЛЕНИЯ ОРГАНАМИ РЕГУЛИРОВАНИЯ НА БАЗЕ ПЛИС ДЛЯ ПОВЫШЕНИЯ БЕЗПЕКИ АЕС

В.В. Скляр, А.В. Харыбин, А.М. Юрцевич

Программируемые логические интегральные схемы (ПЛИС) используются в системах безопасности атомных станций (АЭС) с 1990х гг. За последние 15 лет ПЛИС зарекомендовали себя как надежные проверенные временем решения, способные повысить безопасность информационных и управляющих систем. Научно-производственное предприятие «Радий» является разработчиком и производителем информационно-управляющей платформы и систем на базе ПЛИС для АЭС. В настоящей статье на примере характеристик системы группового и индивидуального управления (СГИУ) на базе ПЛИС обсуждается вопрос повышения безопасности АЭС с использованием ПЛИС-технологий.

Ключевые слова: программируемые логические интегральные схемы (ПЛИС), информационные и управляющие системы, система группового и индивидуального управления, атомная электростанция.

Скляр Владимир Владимирович – д-р техн. наук, доцент, технический директор ЗАО «НПП «Радий», Кировоград, Украина, e-mail: v.sklyar@radiy.com.

Харыбин Александр Викторович – канд. техн. наук, начальник конструкторского бюро ЗАО «НПП «Радий», Кировоград, Украина, e-mail: havral@radiy.com.

Юрцевич Александр Максимович – зам. Генерального конструктора АСУ ТП ЗАО «НПП «Радий», Кировоград, Украина, e-mail: uamax@radiy.com.