Nuclear Installation's Instrumentation and Control Systems on the Basis of Advanced RADIY™ Platform

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

Abstract

The following are results of applying an advanced RADIY™ platform for modernization of Instrumentation and Control (I&C) systems at Nuclear Sights. RADIY™ platform was designed and developed by Research and Production Corporation (RPC) Radiy, located in Ukraine. The main feature of the platform is the use of Field Programmable Gate Arrays (FPGA) as programmable components for logic control operations.

1. Introduction

FPGAs are widely used for safety-critical applications, which include safety systems at nuclear installations. These circuits are advantageous as they use Hardware Design Languages (HDL) for electronic design development [1,2]. Our experience in developing, installing and operating FPGA-based I&C systems, is important for the international nuclear community, as it gives an example of state-of-the-art modernization of nuclear reactor units.

The following points will be discussed:

- Features and advantages of implementing RADIY™ platform for safety I&C systems.
- Ukrainian and Bulgarian experience of applying RADIY™ platform for modernization of I&C systems.
- Design and implementation stages of I&C systems' modernization.
- Licensing and safety assessment of RADIY™ platform.

2. Features and advantages of implementing RADIY™ platform for safety I&C systems

Digital Safety I&C RADIY™ platform is comprised of upper and lower levels [3,4]. The upper level was created on purchased IBM-compatible industrial workstations, with software developed by RPC Radiy and loaded to the workstations. The upper level workstation performs the following functions:

- receipt of process and diagnostic information,
- creation of man-machine interface in the Control Room,
- display of process information for each of the control algorithms relating to control action executed by I&C system components,

- display of diagnostic information on failures of I&C system components,
- registration, archiving and visualization of process and diagnostic information.

The lower level of RADIY™" platform consists of standard cabinets and functional modules (blocks). The platform is comprised of the following standard cabinets:

- Normalizing Converters Cabinets (NCC) – perform inputting 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 formation of output control signals,
- Cross Output Cabinets (COC) – receive signals from three control channels (signal formation cabinets) and form output signals by "two out of three" mode,
- Remote Control Cabinets (RCC) – control 24 actuators on the basis of Control Room signals, automatic adjustment signals and interlocks from signal formation 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),
- Intermediate Clamp Cabinets (ICC) – for signal switching.

The platform includes the following main modules:

- Power Supply Modules,
- Analog Signals Input Modules,
- Normalizing Converter Modules for Thermocouple Signals,
- Normalizing Converter Modules for Resistive Temperature Detector (RTD) Signals,
- Discrete Signals Input Modules,
- Potential Signals Input Modules,
- Logic Control Modules,
- Analog Signals Output Modules,
- Discrete Signals Output Modules,
- Potential Signals Output Modules,

– Actuator Control Modules,

– Optic Communication Modules,

– Diagnostic Modules,

– Fan Cooling Modules,

– chassis and backplanes,

– terminal blocks, cables, wire and fiber optic sets,

– power distribution hardware.

I&C systems' configuration on the basis of RADIY™ 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 cabinet sets,

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.

An example of one I&C rack configuration with modules of RADIY™ platform is given on Figure 1.

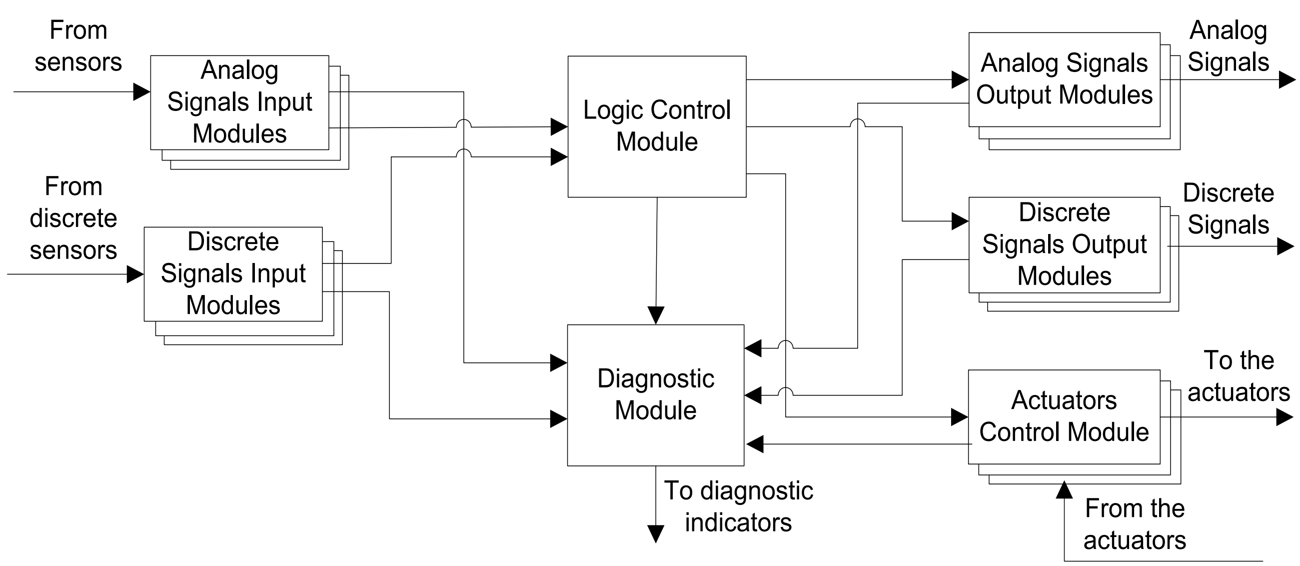


Figure 1 Block diagram of one rack of I&C system.

Applying RADIY™ platform with the use of FPGA technology provides the following opportunities:

- To execute control and other safety-critical functions without software, but on the basis of FPGA technology with implemented electronic design.
- To use software only for diagnostics, archiving, signal processing, data reception and transfers between I&C systems' components. Failures of these functions do not affect execution of basic I&C systems' control functions, and an operation system is not applied at I&C systems' lower levels. Man-machine interface is provided.
- To reduce verification of software process.
- To simultaneously process all control algorithms within one cycle, while maintaining high system performance (e.g. processing cycle of Reactor Trip System is 10 ms) and proven determined temporal characteristics.
- To develop the software-hardware platform in such a way that it becomes a universal interface for I&C systems of any reactor type.
- 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 easily modify the I&C systems after commissioning. For example, to conduct algorithm alterations, without any interference in I&C systems' hardware structure.
- To monitor and control actuator circuits (gates, engines, pumps, valves, etc.) in industries where very high action speed and reliability are required.
- To reduce the number of contact and terminal connections by up to 10 times. Contact and terminal connections cause many operational equipment failures on account of wide use of integrated solutions and fiber optic communication lines.
- To deepen diagnostics of I&C systems' equipment permitting quick and unambiguous detection of place, time and character of failure and hazard degree of equipment operability violation.
- To ensure efficient energy consumption and minimal heat radiation.

3. Ukrainian and Bulgarian experience of applying RADIY™ platform for modernization of I&C systems

RADIY™ platform was 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.

RADIY^{TM} platform was first commissioned in 2003 for Ukrainian NPP unit Zaporozhe-1. During the last six years, 46 applications of RPC Radiy's systems were installed in 17 nuclear power units in Ukraine and Bulgaria. These systems are commissioned in Pressurized Water Reactor (PWR) plants 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 largest project completed by RPC Radiy is modernization of six ESFAS for Bulgarian NPP Kozloduy (three ESFASs for Kozloduy-Unit 5 and three ESFASs for Kozloduy-Unit 6). ESFAS based on RADIY^{TM} platform performs the following control functions [5,6]:

– Forming and outputting process safety and interlock signals for automatic control of actuators in accordance with process algorithms.

– Forming and outputting discrete signals for automatic control of actuators when the monitored process parameters exceed their limit values in accordance with prescribed algorithms.

– Remote control of actuators from the Control Room in accordance with process algorithms.

– Transmission of discrete signals to other systems.

The following outlines mounting and commissioning timelines for Bulgarian NPP:

– August to September 2008 – ESFAS-2 for Kozloduy-6,

– April to May 2009 – ESFAS-2 for Kozloduy-5,

– August to September 2009 – ESFAS-1 and ESFAS-3 for Kozloduy-6,

– April to May 2010 – ESFAS-1 and ESFAS-3 for Kozloduy-5.

The first ESFAS for Kozloduy NPP successfully passed Factory Acceptance Testing (FAT) in July 2008. Mounting of the first ESFAS at the site (ESFAS-2 at Kozloduy-6) started in August 2008. Installation prior to commissioning must be finished in an extremely short period (about one month). The four commissioned ESFASs (ESFAS-1, ESFAS-2, ESFAS-3 at Kozloduy-6, and ESFAS-2 at Kozloduy-5) are now successfully operating. FAT for the last two ESFASs (ESFAS-1 and ESFAS-3 for Kozloduy-5) is planned for February 2010.

4. Design and implementation stages of I&C systems' modernization

The above mentioned modernization project for Kozloduy NPP is characterized by completing the ESFAS design, production, acquisition and commissioning in record time, exhibiting Radiy's strong managerial practices. Figure 2 displays design, implementation and commissioning schedule for

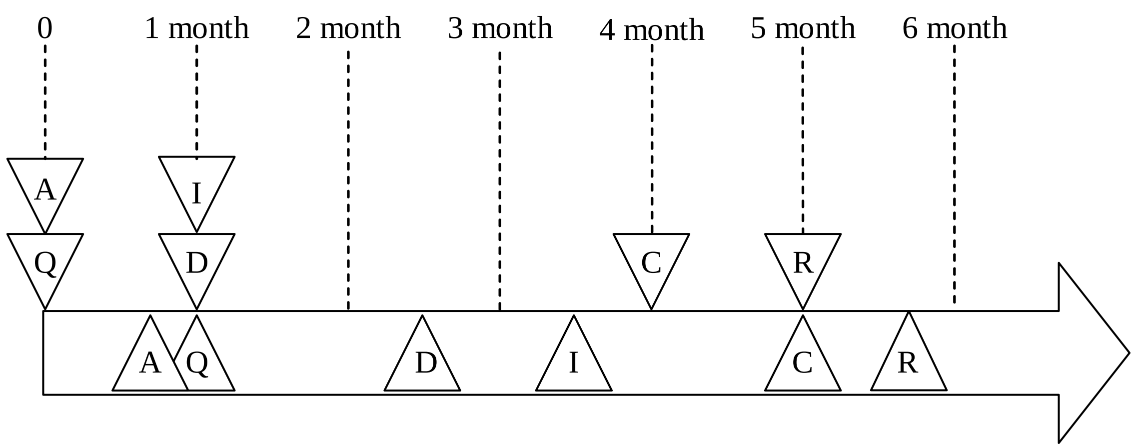
ESFAS. The life cycle of the below I&C system excludes the operation process. All steps are generally completed within six months. The main components of I&C system life cycle processes are discussed below. Quality Assurance (QA) program entails the following:

– organizational structure of QA participants, stating their subordination connections,

– structure, processes, stages and tasks of I&C life cycle and its components, with sequence descriptions of stages and tasks within the processes framework,

– duties and responsibilities of participants responsible for quality assurance of I&C life cycle,

– order and scope of I&C life cycle processes documentation.



Processes	Start	Finish	Processes	Start	Finish
Quality Assurance Program Development	▽ Q	△ Q	I&C Implementation	▽ I	△ I
Basic Data Acquisition	▽ A	△ A	I&C Commissioning	▽ C	△ C
I&C Design Development	▽ D	△ D	Documentation amendment	▽ R	△ R

Figure 2 Design, implementation and commissioning schedule of I&C system.

Basic data is provided by the customer in a standardized log book (questionnaire) containing:

– a list of input and output analogues and discrete signals,

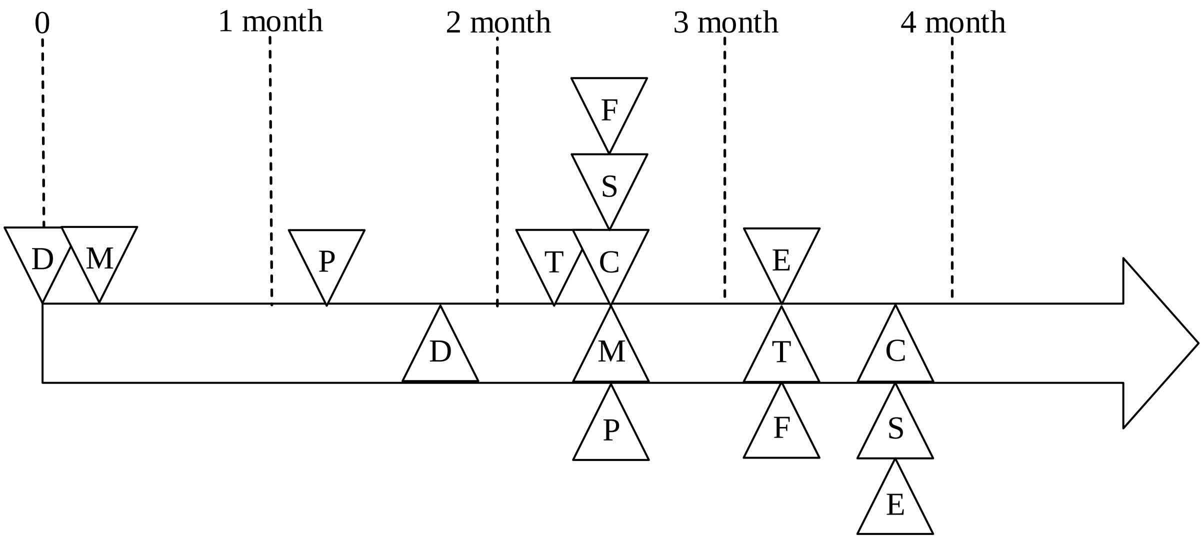
– a list of existing actuators,

– a list of existing cable connections,

– a list of existing alarm elements.

The supplier provides technical specifications that are subject to independent expert assessment. I&C system is generally implemented in four months. Implementation consists of the following processes (see Figure 3):

- development of equipment composition, design, operational and program documentation,
- manufacture of I&C system equipment and development of FPGA electronic design and software,
- development of Factory Acceptance Testing plans,
- training of NPP specialists on equipment operation, maintenance and repair,
- development of start-up and adjustment programs,
- development of preliminary Safety Analysis Report (SAR),
- Factory Acceptance Testing of I&C system,
- supply of I&C system.



Processes	Start	Finish	Processes	Start	Finish
Development of equipment structure and documentation	▽ D	△ D	Development of start-up and adjust-ment programs	▽ C	△ C
Manufacturing of equipment, develop-ment of software	▽ M	△ M	Development of safety analysis report	▽ S	△ S
FAT plan develop-ment	▽ P	△ P	FAT	▽ F	△ F
Utility's personnel training	▽ T	△ T	I&C supply	▽ E	△ E

Figure 3 I&C system implementation schedule.

I&C system is generally commissioned in twenty five days. Commissioning consists of the following processes (see Figure 4):

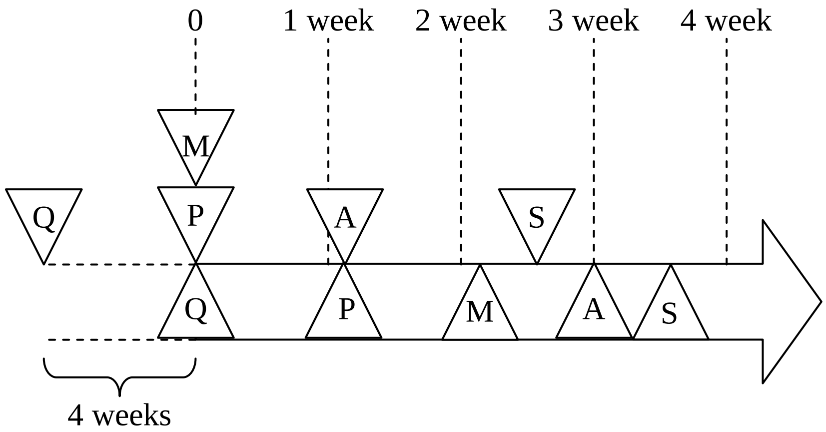
– development and settlement of Quality Assurance program with the customer during installation,

– preparation of mounting site, dismounting of old equipment,

– mounting of equipment and cable routes,

– equipment adjustment,

– Site Acceptance Testing (SAT).



Processes	Start	Finish	Processes	Start	Finish
Installation Quality Assurance Program Development	▽ Q	△ Q	Equipment Adjustment	▽ A	△ A
Preparing On-site Premises, Dismantling of Old Equipment	▽ P	△ P	Site Acceptance Testing	▽ S	△ S
Cable routing, Equipment Mounting	▽ M	△ M			

Figure 4 I&C system commissioning schedule.

Llicensing and safety assessment of RADIY™ platform

The RADIY™ platform is licensed for NPP application in Ukraine and Bulgaria. When licensing FPGA-based I&C systems, the FPGA-chip is considered the hardware and the FPGA electronic design is considered a special kind of software with specific development and verification stages [7,8]. RPC Radiy's FPGA-based hardware is in compliance with International Electrotechnical Commission's (IEC) standards, which include:

– radiation exposure withstand testing,

– environmental qualification, including high and low temperature and humidity, testing,

– seismic testing,

– electromagnetic interference / radiofrequency interference (EMI/RFI) qualification, including different types of conducted emissions, radiated emissions, conducted susceptibility, and radiated susceptibility testing,

– electrical fast transient testing,

– surge withstand testing,

– electrostatic discharge testing,

– safety functions to non-safety functions isolation testing,

– operability and performance testing.

FPGA electronic design has a V-shape life cycle in accordance with requirements of standard IEC 62566 "NPP – I&C important to safety – Selection and use of complex electronic components for systems performing category A functions". Software development stages are replaced by the following specific FPGA electronic design development stages:

– development of signal formation algorithm block-diagrams,

– development of electronic design parts (development of signal formation algorithm program models in design environment),

– integration of electronic design (integration of signal formation algorithm program models into design environment),

– implementation (loading) of integrated electronic design to the FPGA chip.

Each electronic design development stage is terminated by Verification and Validation (V&V) of the obtained product. Functional testing of control logic is a part of V&V process. A third party assessment is performed in accordance with International Atomic Energy Agency (IAEA) and IEC standards to confirm the adequacy of RADIY^{TM} platform and platform-based application for safety requirements. The safety assessments are conducted by Ukrainian State Scientific Technical Centre on Nuclear and Radiation Safety (SSTC NRS), which is the supporting organization of Ukrainian Regulatory Authority. SSTC NRS's experts have considerable experience in assessing FPGA-based safety systems, as they have performed reviews of all thirty three FPGA-based safety systems supplied to Ukrainian NPP units since 2003.

Conclusion

RADIY^{TM} platform was successfully used for modernization of Nuclear Installations including PWR units and Research Reactors. The flexibility and commonality of the above described platform makes it suitable for modernization of CANDU reactors. I&C systems for CANDU reactors on the basis of RADIY^{TM} platform can include adjusted FPGA-based input signals, processing modules, logic control modules, output signals modules, and actuator control modules.

RPC Radiy's success in I&C modernization projects lays in:

– detailed specification of activities, converted into schedules and assignment of responsibilities to personnel,

– highly skilled and qualified personnel that strives on team work,

– efficient installation and resourcing due to fewer pieces of equipment,

– ability to independently perform assembly and adjustment of application logic and hardware,

– uniform structure of cabinets and modules beneficial for integration and adjustment of I&C systems,

– extensive quality control.

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, V. Tokarev, "Advanced I&C Systems for NPPs Based on FPGA Technology: European Experience", Proceedings of the 17th International Conference on Nuclear Engineering "ICONE 17", Brussels, Belgium, 2009, 12-16 July.

[6] V. Kharchenko, A. Siora, V. Sklyar, "Design and Testing Technique of FPGA-Based Critical Systems", The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv, Ukraine, 2009, pp. 305-314.

[7] M. Yastrebenetsky, V. Sklyar, Yu. Rozen, S. Vinogradskaya, "Safety assessment of FPGA-based ESFAS for Kozloduy NPP", Proceedings of the Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Knoxville, Tennessee, USA, 2009 April 5-9.

[8] A. Siora, V. Sklyar, Yu. Rozen, S. Vinogradskaya, M. Yastrebenetsky, "Licensing Principles of FPGA-Based NPP I&C Systems", Proceedings of the 17th International Conference on Nuclear Engineering "ICONE 17", Brussels, Belgium, 2009, 12-16 July.