Reliability and Availability Analysis of FPGA-based Instrumentation and Control Systems

Volodymyr Sklyar, Vyacheslav Kharchenko, Alexander Siora, Sergey Malokhatko, Victor Golovir, Yuriy Beliy

Abstract - **In this paper a method for choice of reliability and availability models is adopted for FPGA-based I&C systems.**

Keywords - **FPGA, I&C system, reliability and availability model.**

I. Introduction

The objective of this paper is to present results of reliability and availability assessment of Field Programmable Gates Arrays (FPGA) Instrumentation and Control (I&C) systems. FPGA is an advanced technology which permits to configure I&C application including safety critical applications like for Nuclear Power Plants (NPP) and others [1,2].

Regulatory safety requirement to safety critical systems includes requirement to reliability and availability. In accordance with International Electrotechnical Commission (IEC) and International Atomic Energy Agency (IAEA) standards these requirements contain:

– Requirements to process of reliability and availability assurance during system life cycle,

– Requirements to reliability and availability indicators values,

– Requirements to reliability and availability qualification methods including in-operation qualification.

Ukrainian Research and Production Corporation (RPC) Radiy is a designer and manufacture of FPGA-based I&C systems [3,4].

The first commissioning of application based on Radiy platform was done in 2003 for Ukrainian NPP unit Zaporozhe-1. Up to now more than fifty I&C systems based on Radiy platform have been installed at seventeen nuclear power units in Ukraine and Bulgaria.

Typical requirements to reliability and availability of NPP I&C systems are the following [5]:

– Mean time between failures: 20000-50000 hours,

– Mean time to repair: 1 hour,

– Availability: 0.9997-0.99999,

– Storageability: 3 years,

– Life time: 30 years.

The paper includes the following chapters:

– Structure and components of Radiy platform,

– Qualification of Radiy platform,

– Requirements to NPP I&C systems reliability and availability,

– A method for choice of I&C systems reliability and availability reliability models,

– Examples of I&C systems reliability and availability assessment.

II. Structure and Components of Radiy Platform

Digital Safety I&C Radiy platform is comprised of upper and lower levels (see Fig. 1). The upper level is based on purchased IBM-compatible industrial workstations, equipped with software developed by RPC Radiy. The upper level workstation performs the following functions [6]:

– Reception and processing of diagnostic information,

– Providing of man-machine interface in the Control Room,

– Displaying process information for each of the control algorithms relating to control action executed by I&C system components,

– Displaying of diagnostic information on failures of I&C system components,

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

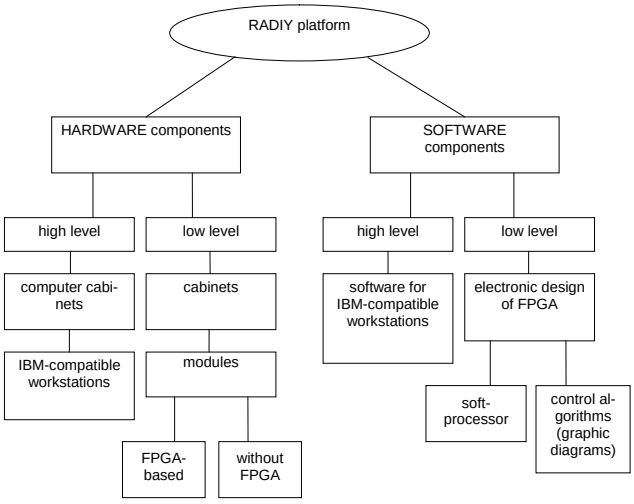

Fig. 1 FPGA-based Radiy Platform: Structure of platform.

The lower level of Radiy platform consists of standard cabinets and functional modules (blocks). The platform is comprised of the following standard cabinets (see Fig. 2):

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

Vyacheslav Kharchenko, Volodymyr Sklyar – Computer Systems and Networks Department, National Aerospace University "KhAI, 17, Chkalova Str., Kharkiv, 61070, UKRAINE,
E-mail: V.Kharchenko@khai.edu
Alexander Siora, Sergey Malokhatko, Victor Golovir, Yuriy Beliy – Research and Production Corporation Radiy, 29, Geroyev Stalingrada Str., Kirovograd, 25006, UKRAINE,
E-mail: marketing@radiy.com

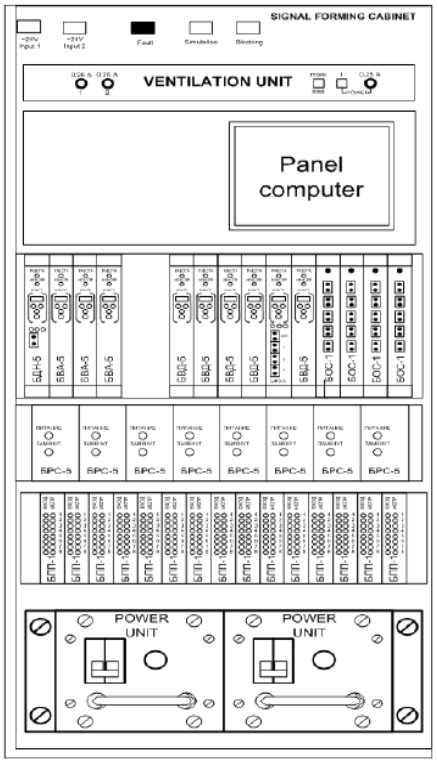

Fig. 2 FPGA-based Radiy Platform: An example of cabinet (Signal Forming Cabinet).

– 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 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,

– Alarm Cabinets (AC) – form control signals for process alarm panel at Control Room,

– Power Supply Cabinets (PSC),

– Unified Current Signal Distribution Cabinets (CDC),

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

The platform includes the following set of modules and hardware:

– Analog Signals Input Modules,

– Thermocouple Signals Input Modules,

– Resistive Temperature Detector (RTD) Signals Input Modules,

– Neutron Flux Detector Signals Input Modules,

– Discrete Signals Input Modules,

– Potential Signals Input Modules,

– Logic Control Modules,

– Diagnostic Modules,

– Optic Communication Modules,

– Analog Signals Output Modules,

– Discrete Signals Output Modules,

– Potential Signals Output Modules,

– Actuator Control Modules,

– Power Supply Modules,

– Fan Cooling Modules,

– Chassis and Backplanes,

– Terminal Blocks, Cables, Wire and Fiber Optic Sets,

– Power Distribution Hardware.

An example of one I&C rack configuration with modules of Radiy platform is given on Fig 3.

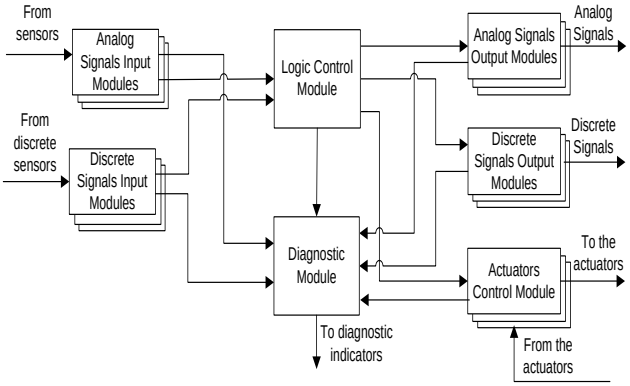

Fig. 3 Block diagram of one rack of I&C system.

The main actions for turnkey application development are system configuration from the existing hardware and software of Radiy platform. 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 cabinets set,

4) Configuration of internal links (wires and fiber optics),

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

An example of configured FPGA-based RTS is presented on Fig. 4. RTS has three tracks and includes three Signal Forming Cabinets and one Cross Output Cabinet.

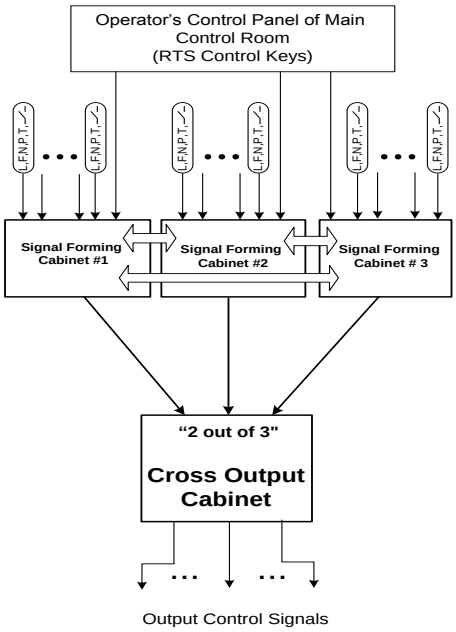

Fig. 4 A Structure of FPGA-based Reactor Trip System.

RTS performs the following functions:

– Storage of setpoints and conditions of reactor trip initiation,

– Automatic monitoring of technological parameters and equipment states,

– Forming of reactor trip signals in case of breaking of setpoints and conditions,

– Data exchange with I&C systems of reactor,

– Indication of technological parameters, reactor trip information and alarm signals at Main Control Room and Emergency Control Room,

– Data archiving, registration and visualization,

Self-diagnostic and visualization of diagnostic data.

Safety critical systems implemented on basis of said platform receive different technological parameters, such as (see Fig. 4): level (L), flow rates (F), neutron flux density (N), pressure (P), temperature (T), and different dry contact discrete signals (⁄–).

III. QUALIFICATION OF RADIY PLATFORM

FPGAs is a complex programmable component which includes two entities [7,8]:

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.

V-shape life cycle of FPGA electronic design is described in the standard IEC 62566 "Nuclear Power Plants – Instrumentation and control important to safety – Selection and use of complex electronic components for systems performing category A functions". This life cycle duplicates V-shape software life cycle, but with development and verification stages relevant to electronic design. Software development stages are replaced by the following specific FPGA electronic design development stages:

development of signal forming algorithm block-diagrams,

development of electronic design parts (development of signal forming algorithm's program models in design environment),

integration of electronic design (integration of signal forming algorithm's program models into FPGA electronic design in 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.

Quality assurance, configuration management, development tools qualification and risks analysis activities are also performed for FPGA electronic designs [7,8].

A third party assessment is performed in accordance with International Atomic Energy Agency (IAEA) and IEC standards to confirm the adequacy of Radiy 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 fifty three FPGA-based safety systems supplied to Ukrainian NPP units since 2003.

Qualification tests performed for FPGA-based Radiy platform include the following [5]:

– Radiation Exposure Withstand testing,

– Environmental testing including: High Temperature and High Humidity testing, Low Temperature and Low Humidity testing, Ambient Temperature and Ambient 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,

– Class 1E to Non-1E Isolation testing.

Additional types of qualification analysis for FPGA-based Radiy platform include the following:

– Critical Digital Review,

– Reliability and Availability Analysis,

– Failure Modes and Effects Analysis,

– Aging and Obsolesce Analysis.

Radiy platform has been qualified against requirements of IEC and IAEA standards.

IV. REQUIREMENTS TO NPP I&C SYSTEMS RELIABILITY AND AVAILABILITY

This chapter describes details about qualification of NPP I&C systems against requirements of IAEA NS-G-1.3 "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants" [9].

The requirements for design require that all structures, systems and components that are items important to safety be designed such that their reliability and availability are commensurate with their classification. In particular, reliable I&C systems important to safety are necessary to prevent undue challenges to the integrity of physical barriers and to ensure the reliability of engineered protective systems.

To ensure that the design basis reliability requirements for I&C systems important to safety are met, a suitable combination of probabilistic and deterministic design criteria should typically be applied. For hardware related failures of systems, quantitative reliability figures should typically be provided. In the design of I&C systems important to safety, design features such as tolerance of random failure, tolerance of common cause failures, fail-safe design, independence of equipment and systems, selection of high quality equipment, testability and maintainability should be considered as appropriate.

In practice a certain amount of trade-off of some of these factors may be necessary in order to optimize goals such as minimizing outage time for repair and reducing frequency of testing. Regardless of how an I&C system is optimized, it should still meet its reliability requirements.

The greater the reliability of the individual components within an I&C system, the greater the reliability of the overall system. There are, however, practical limits to the levels of reliability of individual components. Higher reliability is achieved by the use of redundancy or diversity. For example, it may be possible to monitor reactor power with multiple channels or by diverse means such as measurement of neutron flux or temperature and fluid flow or pressure. The use of redundancy provides protection against random failures. Use of diversity provides protection against certain common cause failures.

The reliability required of each system depends upon the importance to safety of the system's functions and should typically be specified in the design basis. The more important to safety an I&C system is, the higher its reliability should be. One approach to specifying the required reliability is to assign a numerical reliability figure to each systems class. Another approach is to specify deterministic design criteria for the various classes by judging on the basis of engineering experience, assigning the systems to the classes, and then establishing the set of requirements that apply to each class. All systems of the same class are then compared with the typical ones. In most cases deterministic and probabilistic criteria are applied in combination.

Safety systems should comply with the single failure criterion, and the potential for common cause failures should be considered. In some cases, minimum redundancy requirements below which operation would not be permitted may be imposed. In the design of the safety systems, the potential causes of failure should be carefully identified and examined to determine where it is appropriate to apply the principle of diversity.

For all systems important to safety, the degree of redundancy, diversity, testability and robustness should be justified as being adequate to achieve the required reliability of the safety functions to be performed by the systems. This demonstration may be based on a balance of deterministic criteria and quantitative reliability analysis.

In the assessment of the reliability of digital I&C systems, the effects of possible hardware and software failures should be considered, as well as the design features provided to prevent or to limit their effects. Hardware failure conditions to be considered should include failures of parts of the computer itself and failures of parts of communication systems. Both permanent failures and transient failures should be considered.

The contribution of component failure to an I&C system's unavailability should be determined to an appropriate degree of confidence, e.g. by a specified confidence level when a probabilistic approach is used.

V. A Method for Choice of I&C Systems Reliability and Availability Models

A problem of accuracy and integrity increasing for reliability and safety indicators of a system is actual problem in areas of modern reliability theory and critical I&C systems safety theory. This problem can be solved in two ways: first way is in choosing of the most appropriate model from the set of existing models, and the second way is in developing of new models. Variety of existing reliability models of different types arises the necessity to develop an integrated classification for the models, as well as for procedures of model choice depending on system's type. A proposed method is based on classification in a form of model matrix and implementation of choice procedure.

Generalization of research results for the last 10 years in the area of reliability analysis of complex systems with different types of redundancy led to the necessity to perform procedures of structure and parametric synthesis at a set of existing prototypes.

Classification of I&C systems, in terms of the models we used in calculations, is the following:

1) recoverability: a system can be recoverable or nonrecoverable,

2) number of channels and voting logic: a system can be non-redundant, redundant without voting or redundant with voting (the last class is widely used for critical systems),

3) a presence of network voting: a system can have network (coincidence) voting,

4) version redundancy (VR): single-diverse systems with diversity of hardware (HW) or software (SW), multi-diverse systems with simultaneous implementation of HW and SW diversity, multi-diverse systems based on processes' diversity, which use diversity types in according to classification in [10],

5) adaptation against faults: a system can be adaptive or non-adaptive,

6) impact of HW and SW faults on values of reliability indicators (models can consider faults),

7) impact of check and control (CC) errors on values of reliability indicators (models can consider CC errors),

8) availability of operator: system can include operator.

Developed classification is a basis for I&C system reliability model matrix, which includes the following fields (see Table 1):

1) classification identifier of a system – it has eight variations in according to the classification proposed above,

2) classification identifier of a model and description – includes the possible types of the models that consider classification identifiers of the systems,

3) type of a model – reliability block diagram (RBD) for nonrecoverable I&C systems and Markov (or semi-Markov) models for recoverable I&C systems are the basic types; additional types of models expand basic types and allow to consider specified feature depending on the system type,

4) model application method – includes comment concerning integration of both basic and additional types of models for analysis and calculation of reliability for the specified system type.

Derived matrix can be expanded with new rows and fields without changes in application concept.

A model, which is classified in according to the I&C system reliability model matrix, has to be described by a tuple of classification identifiers.

Derived I&C system reliability model matrix includes several thousands of model versions, therefore the problem of I&C system reliability model choosing is actual and must be solved (see Fig. 5).

TABLE 1

A FRAGMENT OF I&C SYSTEM RELIABILITY AND AVAILABILITY MODEL MATRIX

Classification identifier of a system	Classification identifier of a model and description	Type of a model	Model application method
1. Recoverability	Model of nonrecoverable system – <NR>	RBD	Combinatorial formulas for fault tolerance indexes calculation
	Model of recoverable system – <R>	Markov and semi-Markov	Formulas for availability indexes calculation, on the basis of differential and algebraic combined equations
2. Number of channels and voting logic	Model of non-redundant system – <1oo1>; Model of parallel system – <1oo2>; Model of majority-redundant system «2 out of 3» – <2oo3>; Model of majority-redundant system «2 out of 4» – <2oo4>	RBD, Markov and semi-Markov	This type of systems is based on classical approaches for calculation of recoverable and unrecoverable systems
3. Network majorization	Model of a system without network voting logic – <WNV>	RBD, Markov and semi-Markov	Unavailability of network majorization does not introduce additional components into the system model
	Model of a system with network voting logic – <NV>	RBD, Markov and semi-Markov	This type of systems is based on classical approaches for calculation of recoverable and unrecoverable systems with consideration of bridge circuits
4. Version redundancy	Models of single-version systems: Model of two-version system with SW VR – <2SW>; Model of three-version system with SW VR – <3SW>; Model of four-version system with SW VR – <4SW>; Model of two-version system with HW VR – <2HW>; Model of three-version system with HW VR – <3HW>; Model of four-version system with HW VR – <4HW>	Venn diagram, RBD, Markov and semi-Markov	Revealing of relative, group, and absolute defects in RBD, Markov and semi-Markov models considered using metrics of product diversity obtained via Venn diagrams
	Models of multidiverse systems on the basis of product diversity: Model of two-version system with VR of SW and HW – <2SWHW>; Model of three-version system with VR of SW and HW – <3SWHW>; Model of four-version system with VR of SW and HW – <4SWHW>	Venn diagram, RBD, Markov and semi-Markov	Appearance of relative, group, and absolute defects in RBD, Markov and semi-Markov models considered using metrics obtained via Venn diagrams of product diversity
	Models of multidiverse systems on the basis of process diversity: a combination of the following diversity types is considering: - Project diversity – <PD>; - Functional diversity – <FD>; - Signal diversity – <SD>; - Lifecycle diversity (subjective) – <LCD>	Graph of multiversion lifecycle (network model)	Impact of diversity types on fault tolerance and availability indexes considered using metrics of process diversity

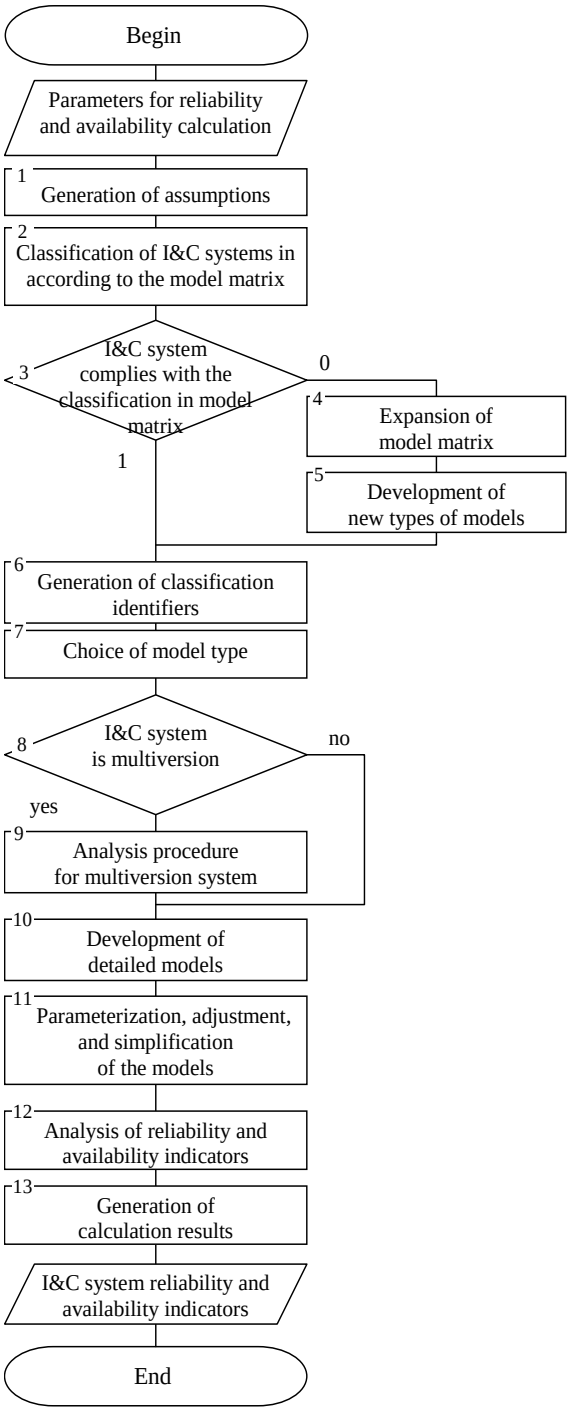

Fig. 5 Stages of method of reliability and availability models choice.

Derivative data for implementation of the method are parameters of I&C system that are required for calculation of reliability indexes. Output data of the method are calculated numerical values of reliability indexes.

Newness of proposed method is based on using of «system-model-assumption» approach. This approach is in generation of assumptions for such reliability model that is the most adequate for the system under assessment. Derived model matrix and synthesis model are the basis for designing of expert system for analysis and calculation of I&C system reliability and functional safety.

VI. Examples of I&C Systems Reliability and Availability Assessment

A usual practice of systems dependability analysis includes function-by-function calculation of reliability and availability indicators. For example, for Reactor Trip System (Fig. 5) function of Alarm Signal Conditioning can involve such set of equipment of SFS as it is marked out on Fig. 6.

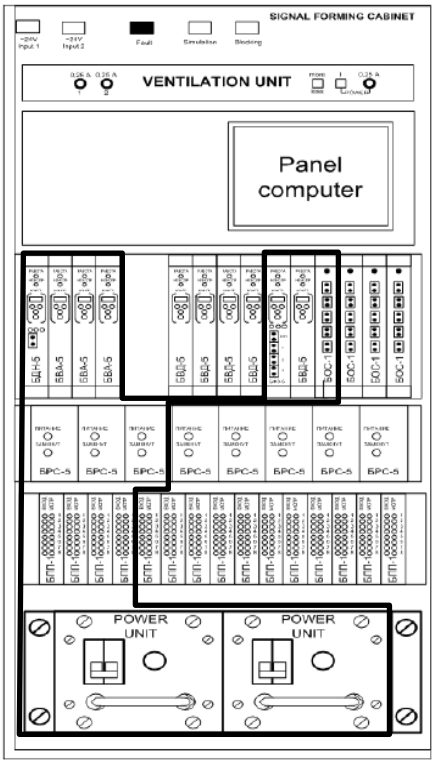

Fig. 6 An approach to function-by-function calculation of reliability and availability.

After a set of equipment definition its calculation can be fulfilled for function failure intensity like:

$$\Lambda_F = \sum_{i=1}^{N} \lambda_i , \quad (1)$$

when λi is a failure intensity of separated functional module, N is a number of functional module in a set of equipment of equipment related to an analyzed function.

Fig. 7 present RBD of diverse Reactor Trip System which includes to sets like on Fig. 5. Calculation of reliability of such system includes three stages:

1) Calculation of three channels reliability:

$$P_{3SFC} = 3P_{SFC}{}^2 - 2P_{SFC}{}^3 , \quad (2)$$

$$P_{3SFC\,D} = 3P_{SFC\,D}{}^2 - 2P_{SFC\,D}{}^3 , \quad (3)$$

2) Calculation of separated sets reliability:

$$P = P_{3SFC} \cdot P_{COC} , \quad (4)$$

$$P_D = P_{3SFC\,D} \cdot P_{COC\,D} , \quad (5)$$

3) Calculation of the whole system reliability:

$$P_S = \left[1-(1-P_{SFC} \cdot P_{COC}) \cdot (1-P_{SFC\,D} \cdot P_{COC\,D})\right] \cdot P_{OR} . \quad (6)$$

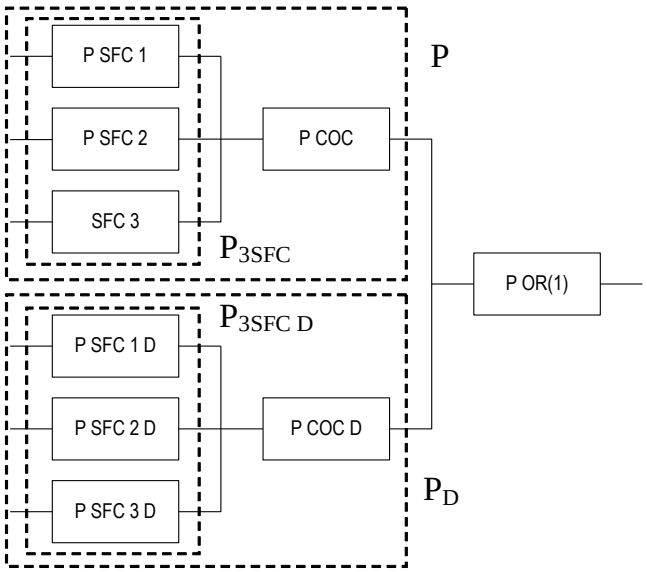

Fig. 7 RBD of diverse Reactor Trip System included two sets.

An example of Markov Model for Reactor Trip System is presented on Fig. 8. This Markov Model is simplified and includes only the following stations:

S_0 – all modules are in operation,
S_1 – OR element failure (system failure),
S_2 – the main set of system failure,
S_{2D} – the diverse set of system failure,
S_3 – the main and the diverse sets of system failures (system failure).

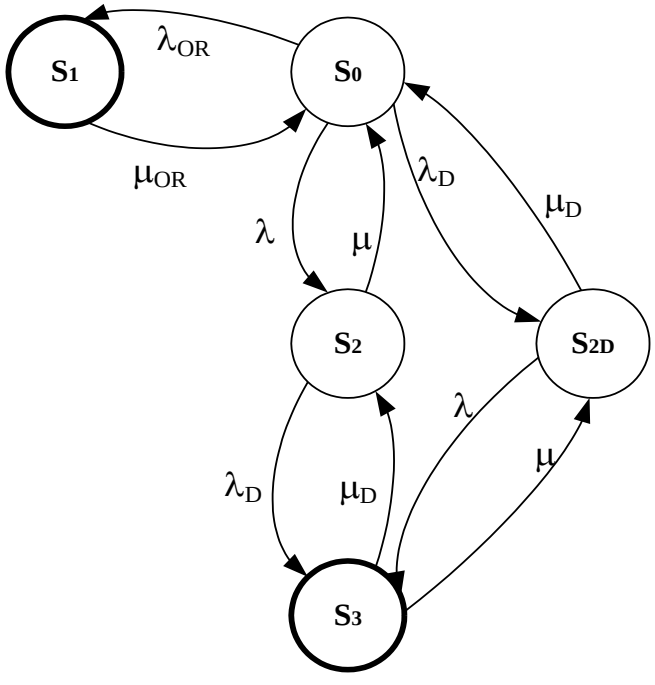

Fig. 8 Markov Model of diverse Reactor Trip System included two sets.

REFERENCES

[1] "Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems. EPRI TR 1019181", 2009.

[2] "Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems. NUREG/CR-7006", 2010.

[3] 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.

[4] 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.

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

[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] "Altera. Reliability Report 49 Q1", 2010.

[8] "Actel. Quality Manual QM-1 Rev. 12.5P", 2010.

[9] "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. IAEA NS-G-1.3", 2002.

[10] "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems. NUREG/CR-7007", 2010.

VII. CONCLUSION

Information and Control Systems manufactured by RPC Radiy have evolved over 15 years. Application of FPGA technology has made considerable progress: from diagnostic functions to implementation of safety related control, processing and communication functions. This evolution resulted in creation configurable and scalable FPGA-based platform with diversity and high reliability features.

Experience in designing, manufacturing and supplying of control systems for Ukrainian and European NPP power units allows to talk about following advantages of digital I&C systems manufactured by RPC Radiy:

– Safety and reliability, that is in accordance with requirements of updated international standards,

– Compactness, scalability and comparatively low price,

– Considerable reduction of the installation time,

– System-Off-The-Shelf Technology based on product (FPGA-based platform) and process (development and installation arrangement) has proved its efficiency and opens the opportunity to develop future generation of digital I&C systems for NPP and other critical applications.