Proceedings of the 18th International Conference on Nuclear Engineering
ICONE18
May 17-21, 2010, Xi'an, China

ICONE18-29754

DIVERSITY-ORIENTED FPGA-BASED NPP I&C SYSTEMS: SAFETY ASSESSMENT, DEVELOPMENT, IMPLEMENTATION

Vyacheslav S. Kharchenko
Centre of Safety Infrastructure-Oriented Research and Analysis
Kharkiv, Ukraine
v_s_kharchenko@ukr.net

Eugenii S. Bakhmach
Research and Production Company "Radiy"
Kirovograd, Ukraine
marketing@radiy.com

Alexandr A. Siora
Research and Production Company "Radiy"
Kirovograd, Ukraine
marketing@radiy.kr.ua

Vladimir V. Sklyar
Centre of Safety Infrastructure-Oriented Research and Analysis
Kharkiv, Ukraine
vvsklyar@mail.ru

Viktor I. Tokarev
Research and Production Company "Radiy"
Kirovograd, Ukraine
victok@hotmail.ru

ABSTRACT

Key challenges caused by implementation of diversity-oriented approach and FPGA technology are discussed in context of NPP I&C systems safety. National and international standards containing the requirements to diversity application in NPP I&C systems are analyzed. A few evolution stages of multi-version NPP I&C systems (Reactor Trip Systems) are described taking into account different types of version redundancy (hardware, software, FPGA diversity). Main attention is attended to the methods of increasing tolerance of NPP I&C systems to physical and design faults using multi-version technologies. A life cycle model and multi-version technologies of FPGA-based I&C systems development are analyzed. Implementation results of safety-critical NPP I&Cs developed by RPC "Radiy" using FPGA technology are described. The FPGA-based platform RADIY™ ensures scalability system functions, dependability and diversity. More than 20 different FPGA-based I&C systems were successfully developed, produced and implemented on the NPPs of Ukraine and Bulgaria during last five years.

INTRODUCTION

The diversity principle is used to ensure reliability, functional safety of I&C computer-based systems for NPPs (reactor trip systems, first of all), aerospace equipment (on-board control systems, autopilots), railway automatics (interlocking and block signal systems) and other critical applications [1-4]. In this case different software and hardware are applied to develop redundant channels. It allows decreasing the risks of the most dangerous incidents - Common Cause Failure (CCF). The most probable sources of CCF are software design faults or multiple physical faults of different channels. Probability of common cause failure (CCF) of safety-critical systems may be essentially decreased due to application of different types of diversity if failures of redundant channels (versions) are maximum independent [1,3]. A lot of international and national standards contain the requirements to use diversity in safety-critical systems. For example, the standard IEC 60880: 2006 defines the use of diversity "as a means of enhancing the reliability of some systems and reducing the potential for certain CCF".

The problems of CCF, application of diversity and NPP I&Cs safety ensuring as a whole should be analyzed taking into account trends of computer technologies development. One of the contemporary trends is dynamically growing application of novel complex electronic components, particularly, Field Programmable Gates Arrays (FPGAs) in NPP I&Cs, aerospace systems and other critical areas.

FPGA is a convenient technology not only for implementation of auxiliary functions (transformation and preliminary processing of data, diagnostics, etc). This technology is effective means to realize safety important control functions of NPP I&Cs. Application of the FPGA technology is more reasonable than application of software-based technology (microprocessors) in many cases [5].

The following FPGA peculiarities are important for safety and dependability assurance:

- development and verification are simplified due to: apparatus parallelism in control algorithms implementation and execution for different functions; absence of cyclical structures in FPGA projects; identity of FPGA project presentation to initial data; advanced testbeds and tools; verified libraries and IP-cores;

- existing technologies of FPGA projects development (graphical scheme and library blocks in CAD environment; special hardware describing languages VHDL, Verilog, Java HDL, etc; microprocessor emulators which are implemented as IP-cores) allow increasing a number of possible options of different project versions and multi-version I&Cs;

- fault-tolerance, data validation and maintainability are improved due to use of: redundancy for intra- and inter-crystal levels; possibilities of implementation of multi-step degradation with different types of adaptation; diversity and multi-diversity implementation; reconfiguration and recovery in the case of component failures; improved means of diagnostics;

- FPGA reprogramming is possible only with the use of especial equipment (it improves a security); stability and survivability of FPGA projects are ensured due to the tolerance to external electromagnetic, climatic, radiation influences, etc.

Plural nature is characteristic for modern NPP I&Cs because their architectures include hardware, software and FPGA-based components [5]. It gives new possibilities and new challenges for safety assessment and assurance in context of diversity approach application.

First of all, there are some problems related to specifying of multi-version I&C taxonomy, normative and methodical support of diversity-oriented development and assessment, selection of diversity type and volume of version redundancy, etc.

Objectives of this paper are:

- analysis of challenges caused by need of diversity approach and FPGA-technologies application in NPP I&Cs and other safety-critical areas;

- discussion of assessment, development and implementation aspects of diversity-oriented decisions for FPGA-based NPP I&Cs.

Structure of the paper is presented below. Some aspects of multi-version systems theory, application in safety-critical areas and challenges caused by implementation of diversity-oriented approach and FPGA technology in the NPP I&Cs are discussed the first section. The second section elaborates the methods of diversity estimation and assessment of multi-version systems safety, features of diversity metrics for FPGA-based systems. Models of one- and two-version FPGA-based systems life cycle and features NPP I&Cs development using the FPGA-based RADIY™ platform are described in the third section. The results of implementation of this platform and FPGA-based NPP I&Cs produced by RPC "Radiy" are analysed in the forth section. Last section summarizes the paper and present directions of future researches.

DIVERSITY-ORIENTED SAFETY CRITICAL NPP I&C SYSTEMS: SOME ASPECTS AND CHALLENGES

Taxonomy Aspect of Multi-Version Computing

A set of concepts concerning diversity may be united by term "multi-version computing" (similar to "dependable computing"[6]). It is a part of dependable computing based on use of diversity approach. Taxonomy scheme of multi-version computing is shown in Figure 1. General concepts of multi-version computing are as follows [4,7].

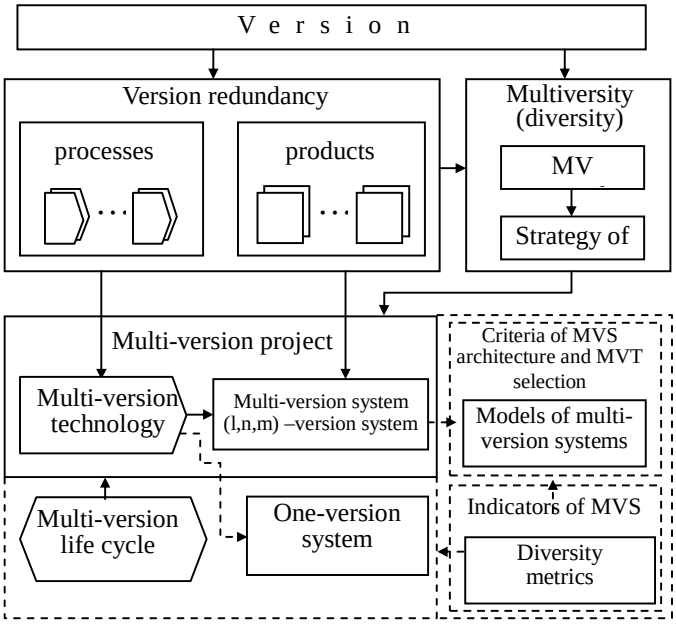

Figure 1. TAXONOMY OF MULTI-VERSION COMPUTING

Versions and Version Redundancy. *Version* is an option of different realization of identical task (product or process); examples of version are software, hardware (or FPGA-based) components performing functions of I&Cs.

Version redundancy (VR) is a kind of redundancy in which different versions are used; there are a lot of VR kinds and a few VR classification schemes described in [2-5].

The most system classification of diversity kinds based on NUREG/CR-6303 includes: *human life* or *cycle diversity* (different design companies, management teams, designers, testers and other personnel); *design diversity* (different technologies, architectures, etc); *software diversity* (different algorithms, operating system, computer languages, etc); *functional diversity* (different underlying mechanisms, logic, actuation means, response time scale, etc); *signal diversity* (different reactor or process parameters, physical effects, sensors, etc); *equipment diversity* (different design,

manufacturers, CPU and bus architectures, printed circuit board designs, etc).

FPGA-based I&C diversity classification includes the following VR kinds [5]: *diversity of electronic elements* (different electronic elements manufactures, technologies of electronic elements production, electronic elements families, electronic elements from the same family); *diversity of CASE-tools* (different developers, kinds and configurations of CASE-tools); *diversity of projects development languages* (joint use of graphical scheme languages, hardware description languages (HDL) or/and IP-cores, different HDLs); *diversity of specifications* (different specification languages).

Diversity or multiversity (MV) is the principle providing use of several versions to perform the same function by two or more options and processing of data received in such ways for checking, choice or formations of final or intermediate results and decision-making on their further use.

Multi-Version Systems. *Multi-version system* (MVS) is a system in which a few versions-products are used; multi-diversion system (MDVS) is a MVS in which two kinds of version redundancy are used. MVS W_n is defined by 5 variables [4]:

$$W_n = \{X, F, U, V, Z\}, \qquad (1)$$

where X, U – sets of input and output signals; $F = \{f_d, d = 1,\ldots, k\}$ – set of I&C functions; $V = \{v_i, i = 1,\ldots, n\}$ – set of versions with output signals $U_1,\ldots, U_n$; Z – displaying function U_{id} in U_d if the function is performed f_d, i.e. $U_d = Z(U_{1d},\ldots,U_{nd})$.

Generalization of MVS (or MDVS) is *(l,n,m)*-version system with l hardware channels, n versions and m types of VR described by the follow formula:

$$W_{n,m} = \{X, F, U, V, R, \theta, Z\}, \qquad (2)$$

where $R = \{r_q, q=1,\ldots, m\}$ – set of VR types, θ – their mapping onto set elements $v_j(\Delta R_j) \in V$, $\Delta R_j \subset R$.

MVS dynamic models can be supplemented by the set of algorithms A(π) of one- and multi-parametric adaptation to the different failures which effect on Z function type:

$$W_{n,m} = \{X, F, U, V, R, \theta, Z, \mathrm{A}(\pi)\}, \qquad (3)$$

where π is a set of adaptation parameters (threshold of majority, number of redundant parts, of used versions,…).

Besides, FPGA-based I&C performing safety critical functions may be represented by a composition of two interconnected automata (monitoring or checking and control automata) [5,6]. Monitoring automaton analyses output signals X from monitoring object and forms its status code Z_C. Control automaton forms control signals Z in accordance with signals Z_C. Several options of MVS architectures are possible for a FPGA-based I&Cs.

Those options may be classified according with *degree of diversity coverage* (I&Cs with a complete and partial diversity) and *diversity depth* (I&Cs with a *common* and *separate diversity*); it should be noted that this feature is applicable only to full system diversity.

Multi-Version Systems and Projects. *Multi-version technology* (MVT) is set of the interconnected rules and design actions in which in a few versions-processes leading to development of two or more intermediate or end-products are used; thus for development of MVS should be used MVT, for development one-version systems can be used both multi-version and one-version technology.

Description of multi-version technology by a graph (MVT graph) is convenient model to solve tasks of development, systematization, and choice of MVTs [4,7]. MVT graph is a E-level bipolar graph with initial node L_u, intermediate nodes L_p ($|L_p| = \prod H_e$, $e=1,\ldots, E$, H_e – a number of version redundancy types on stage e, E – a number of life cycle stages, on which VR application is possible) and finite node L_κ. Edges of graph are determined by the compatibility relation of VR types mapped by contiguous levels (stages of life cycle). Each node of graph is associated with diversity metric d_{eq} and cost metric c_{eq} ($q=1,\ldots,H_e$,). Diversity metric is the degree of MVS version independence and determined by the probability of failure of two and more versions [4,8].

Multi-version project (MVP) is a project in which the multi-version technology is applied (version redundancy of processes is used) leading to creation of one- or multi-version system, i.e. use of version redundancy in end product.

Multi-version life cycle (MVLC) is life cycle of MVP. MVLC is described by life cycle models just as for the one-version projects. V model and other models are used for projects of multi-version software- and FPGA-based I&Cs. The last model was the most wide-spread. MVLC model developing is performed by the use of specific G generation and S versions selection operations. The examples of such models for MVSs are described in [5].

Strategy of diversity (MV) is a collection of general criteria and rules defining principles of formation and selection of version redundancy kinds and volume, i.e. selection of MVT (way in MVT graph).

Choice of optimal MVT selection are carried out according with criteria “diversity(safety)-reliability-cost” using algorithms of dynamical programming [5,7].

Application and Evolution of Multi-Version Systems

Analysis of MVS Applications. There are a lot of examples of multi-version systems and multi-version technologies application in different safety critical areas. Generalized results of MVS application analysis are presented by matrix “kinds of diversity – areas of multi-version I&Cs application” in Table 1.

Table.1 RESULTS OF MVS APPLICATION ANALYSIS.

Kinds of diversity (NUREG 6303)	Multi-version I&C systems application												
	Space		Aviation				Rail. Trans	Chemic. Indystry	Defense	Power Plants	NPP		eCom-mers
	Shuttle	ISS	MC JVC	FAA FCS	Airbus A320	Boeng 777	SCB	CCPS	MICS	Electr. Grid	RTS	ESFAS	WSOA
Design													
Equipment													
Function													
Human													
Signal													
Software													
Others													

These results are based on information presented in [9,10]. Kinds of diversity (diversity redundancy) are classified according to NUREG 6303 and painted by different colors. Last row of the matrix corresponds to other kinds of diversity (including diversity of FPGA project for Reactor-Trip Systems produced by RPC Radiy [5]). MVS are used in space systems (Shuttle, … (ISS)), aviation equipment (… (MC JVC), … (FAA FCS), Airbus and Boeing on-board systems), railway automatics (signaling, centralization and blocking systems (SCB), chemical industry (CCPS), defense systems, power plants (electricity grid), NPPs (RTS and ESFAS), e-commerce and e-science (web-systems with diverse target web-services). The prevailing VR kinds are human, function, software and equipment diversity.

Evolution of Multi-Version NPP I&Cs Stages in Context of FPGA Technology. The results of transformation of multi-version I&Cs for the last decades are very interesting in context of hardware-software technologies development. There are a few diversity implementation evolution stages in safety-critical NPP I&Cs. Analysis of these stages allowed to formulate a low “negation of negation” (Fig. 2) [6,10]:

- stage 1 (1980s), transition from hardware-based systems with identical subsystems to systems with hardware primary subsystem and microprocessor (software)-based secondary subsystem;

- stage 2 (1990s) – use of primary and secondary subsystems with software diversity (I&C platforms produced by Siemens, WH and other companies); it was the first cycle of “negation”;

- stage 3 (2000s, first half) – transition to FPGA-based primary and secondary subsystems with equipment, design and software diversity (I&C platforms produced by RPC Radiy); it was the second negation, i.e. “negation of negation”);

- stage 4 (2000s, second half) – application of different FPGA-oriented soft processors for primary and secondary subsystems, development using IP-diversity (next “negation”).

- stage 5 may be probably stipulated by advancement of electronic technologies (nanotechnologies) and perspectives and possibilities for development of diversity-oriented decisions using so called “naturally dependable chips (NDCs) [11].

Normative Aspect of Multi-Version FPGA-Based NPP I&Cs

Review of Standards. There are the following standards contained requirements to diversity:

- IEC 61513: 2001. NPPs - I&Cs important to safety – general requirements for systems;

- IEC 60880: 2006. NPPs - I&Cs important to safety - SW aspects for computer-based systems performing category A functions;

- IAEA NS-G-1.3: 2002. I&Cs important to safety in NPPs;

- IEEE std.7-4.3.2:1993. IEEE standard criteria for digital computers in safety systems of NPPs;

- NUREG/CR-6303:1993. Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems;

- DI&C-ISG-02, Diversity and Defense-in-Depth Issues, Interim Staff Guidance, BTP 7-19, Guidance for Evaluation of D&DiD In Digital I&C Systems (USA);

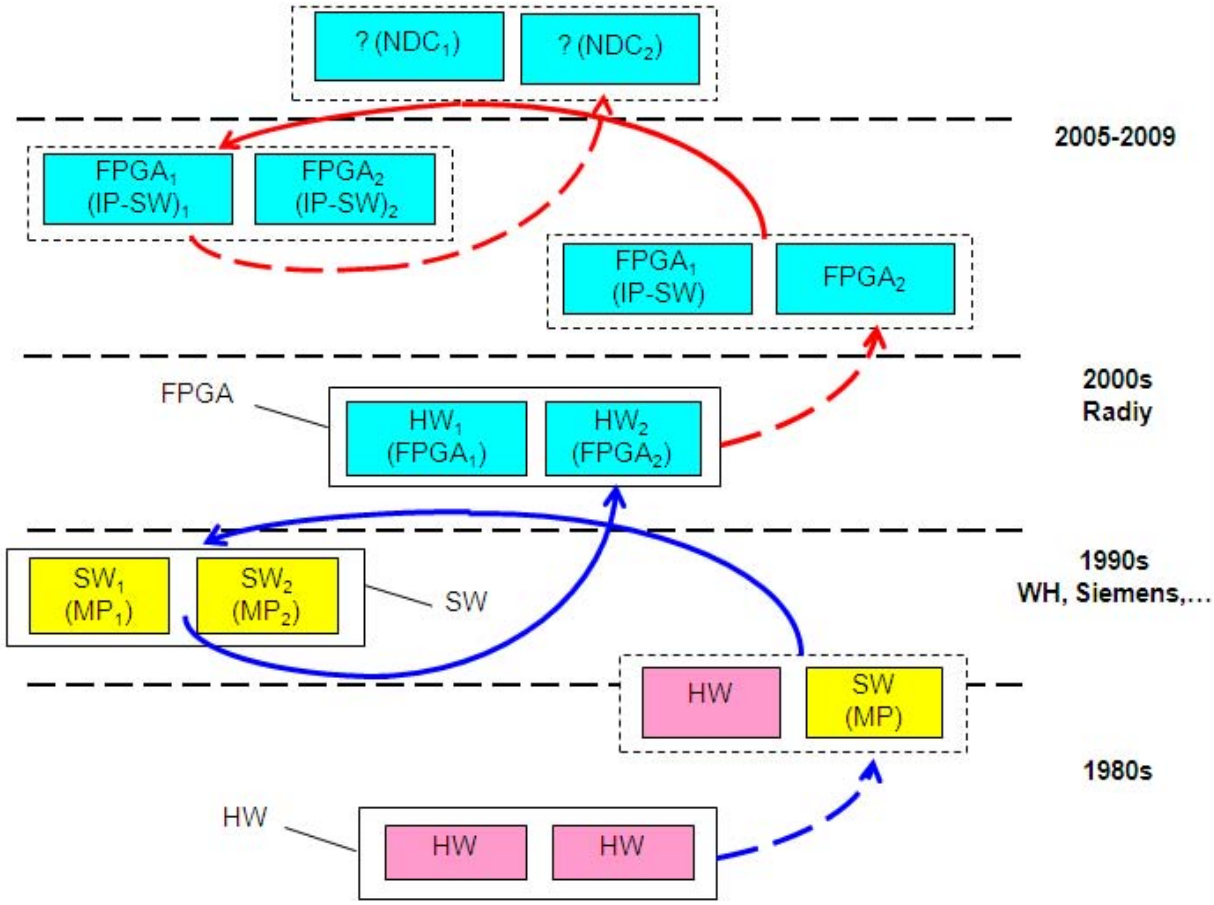

Figure 2. EVOLUTION OF MULTI-VERSION NPP I&CS STAGES: LOW "NEGATION OF NEGATION"

- NP 306.5.02/3.035: 2000. Requirement on nuclear and radiation safety to I&Cs important to safety in NPPs (Ukraine), etc.

These standards contain general requirements concerning:

- systems which must/should be developed using diversity approach (RTS);
- kinds of diversity used to develop NPP I&Cs and to decrease CCF probability;
- features of diversity implementation, determination of kinds and volume of diversity;
- assessment (justification) of real level of diversity in developed systems;
- drawbacks and benefits connected with the use of diversity.

The standards are not enough detailed to make all necessary decisions concerning diversity. It's important to develop additional detailed techniques of assessing diversity and choosing optimal kinds and volume of diversity according to criterion "safety-reliability-cost".

Key challenges. Main conclusions concerning FPGA-based MVS development and implementation experience are the following:

- FPGA-based multi-version I&Cs are used in NPPs during 6-7 last years, i.e. these systems are new object of analysis and still more unique one;
- FPGA technologies give additional possibilities to develop MVSs and ensure high safety and reliability;
- processes of FPGA project development are similar to processes of SW-based project development. FPGA project product is similar to HW-based project product (hard logic);
- there are not any international standards determined requirements to use of diversity for I&Cs development and application taking into account FPGA features.

Results of comparative analysis of challenges caused by development and application of software- and FPGA-based multi-version systems are presented in Table 2.

Table 2. KEY CHALLENGES FOR SOFTWARE-BASED AND FPGA-BASED MVSs

Challenges connected with use of diversity	Software-based multi-version I&C	FPGA-based multi-version I&C
Detailed standards	There are standards determining general requirements to use of diversity	There are no special standards
Experience of development and operation	More 20 years	5-7 years
Accuracy and trustworthiness of diversity assessment	Methods of expert-based, metrical assessment, probabilistic methods using SRGMs	Methods of expert-based, metrical, probabilistic (RBD), deterministic methods
Development of diversity-oriented I&C	Choice of diversity kinds, generation of really diverse software versions	Number of diversity kinds increases
Verification of diversity-oriented I&C	Verification activities volume are significantly increased	Verification is more simple due to simplifying of version verification

ASSESSMENT OF DIVERSITY-ORIENTED FPGA-BASED NPP I&C SYSTEMS

Classification of diversity assessment methods

There are a few methods of diversity assessment and estimation of MVS dependability and safety [11].

Theoretical-set metrics methods. These methods are based on:

- Eiler's diagram for sets of version design, physical and interaction faults (including vulnerabilities for assessment intrusion-tolerance and security as a whole);
- matrix of diversity metrics for sets of different faults (individual, group and absolute faults of versions);
- calculation and analysis of diversity metrics; metrics are calculated by use of Eiler's diagrams or other data about results of testing and faults of different versions.

Probabilistic and statistic methods. To assess MVS dependability and calculate required indicators are used reliability block-diagrams (RBDs) and their modifications (survivability and safety block-diagrams). RBD and metric-based assessment includes:

- reliability block diagram development taking into account MVS architecture (SW and HW versions, kind of diversity, check and reconfiguration means) and sets of different faults;
- calculation of reliability and safety indicators.

Other probabilistic technique of diversity assessment is founded on Bayesian method [12]. Statistic methods are based on testing data and consists of the following operations:

- receiving and normalization of version fault trends using testing data;
- choice of software reliability growth model (SRGM) taking into account features of version development and verification processes and fitting SRGM parameters;
- metrics diversity assessment;
- calculation of reliability and safety indicators.

Fault injection-based assessment. This method is applied to assess MVS using all-known fault-injection technique taking into account profile of version faults. Main stages of assessment are the following:

- analysis of developed project and receiving version fault profiles (kinds and relation between number of different kinds of faults);
- performing of faults injection procedure;
- proceeding of data and metrics diversity calculation;
- calculation of reliability and safety indicators.

Expert and other methods. Expert method is used, first of all, to assess diversity metrics. There are two groups of metrics:

- diversity metrics for direct assessment of versions and MVS reliability and safety (direct diversity metrics);
- indirect diversity metrics (product complexity metrics and process metrics); values of these metrics may be used to assess direct diversity metrics.

Expert method is added other techniques founded on interval mathematics-based assessment of diversity metrics and MVS indicators, soft computing-based assessment (fussy logic, genetic algorithms), risk-oriented approach and so on.

Features of Multi-Version FPGA-Based Systems Assessment

To assess multi-version FPGA-based system dependability and safety it is necessary to take into account the following features of FPGA projects:

- architecture of system and functions carried on FPGA components;
- kinds of used product and process diversity;
- data about faults received during different stages of development, verification and operation of system;
- data about FPGA chip reliability, etc.

Key problem is assessment of diversity metrics for FPGA multi-version projects. To solve this problem may be used information about kinds of diversity and expert assessment of their preference. Example of preference (nonnormalized values of diversity metrics D_{ij}) for different kinds (i) and subkinds (j) of diversity is shown in Table 3.

Table 3. DIVERSITY METRIC FOR FPGA-BASED I&C SYSTEMS

Kind of diversity	Subkind of diversity (mode of diversity implementation)	D_{ij}
Diversity of electronic elements (a)	Diversity of firm-developers of electronic elements (a1)	4
	Diversity of technologies of electronic elements producing (a2)	3
	Diversity of electronic elements families (a3)	2
	Diversity of electronic elements from the same family (a4)	1
Diversity of case-tools (b)	Diversity of developers of case-tools (b1)	3
	Diversity of case-tools (b2)	2
	Diversity of configurations of case-tools (b3)	1
Diversity of projects development languages (c)	Diversity on the base of graphical language and hardware description language (c1)	2
	Diversity of hardware description languages (c2)	1
Diversity of specification (d)	Diversity of specification languages (d1)	1

Detailed technique of diversity and FPGA-based MVS as a whole assessment based on this approach was described in [5].

DEVELOPMENT OF DIVERSITY-ORIENTED FPGA-BASED I&C SYSTEMS

Model of FPGA-Based System Life Cycle

Features of Development and Verification. In development of FPGA-based I&C systems life cycle (LC) it should be taken into consideration that, from the one side, FPGA-based systems are software-hardware products, thus having much in common with software. Therefore, in analysis and development of FPGA-based I&Cs life cycle the postulates of software engineering standards are reasonably useful. From the other side, FPGA project as a specific I&C component have some peculiarities different from software. Therefore the postulates of existing standards regulating software structure cannot be mechanically taken for construction of FPGA-project LC.

Analysis of software LCs showed that for FPGA it should study the LC stages beginning from I&C specification and up to integration of system. Such actions may be performed in parallel to software development.

Besides, verification after each stage of development is obligatory for both FPGA project and software. FPGA project is developed on the grounds of System Requirements Specification with due consideration of distribution of function and non-functional safety requirements between FPGAs and other hardware. The developed FPGA-based components must be integrated within the I&C system, and in future it should be treated as an integral part of I&C system software and hardware.

Example of Life Cycle Model. Let's describe example of LC model using FPGA-based I&Cs produced by RPC Radiy [7]. Development of these systems consists of such stages:

– development of signal formation algorithm block-diagrams;

– development of signal formation algorithm program models in design environment which is determined depending on type and/or manufacturer of FPGA realization environment applied;

– integration of signal formation algorithm program models (development of digital device integrated program model) into design environment;

– implementation (loading) of integrated program model to FPGA chip.

The key term here is «signal formation algorithm block-diagram» implying a certain functionally finite project module presented in the form of a graphic diagram or a listing in hardware description language (HDL). The result of each step is a new product, the final result being a FPGA with implemented logic structure. At each step the developed product must be verified.

The model of FPGA-based I&C system development and verification are shown in Fig. 3.

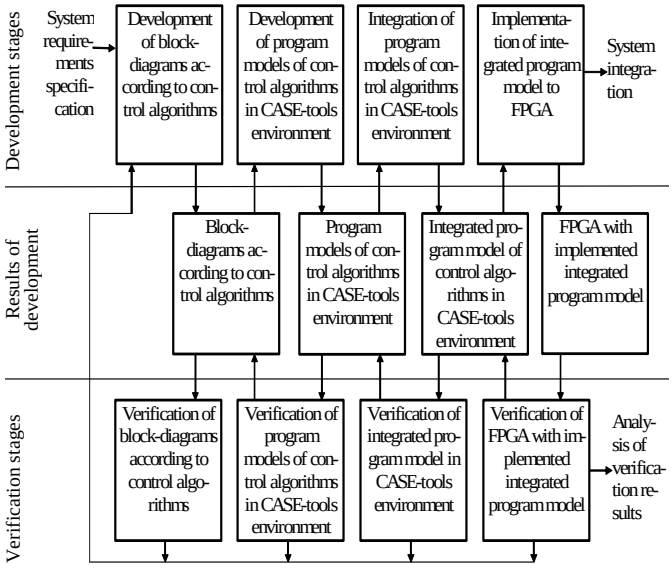

Figure 3. A LIFE CYCLE OF FPGA-BASED I&C SYSTEM

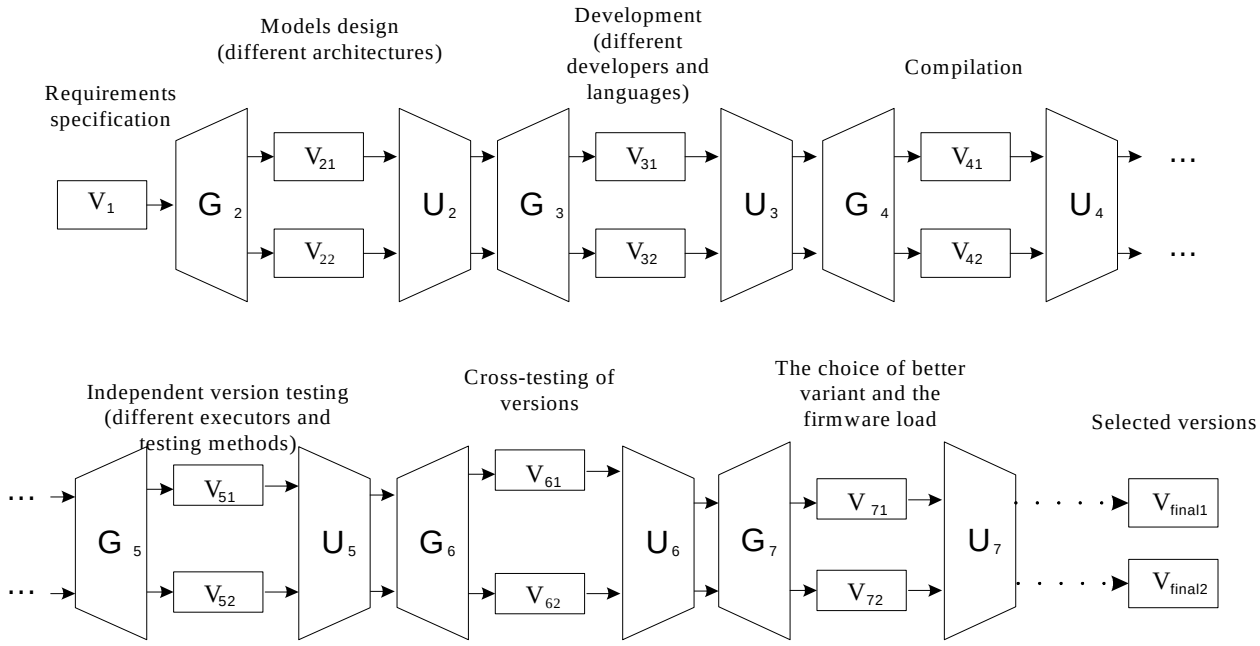

Figure 4. A MODEL OF TWO-VERSION FPGA-BASED I&C LIFE CYCLE

Multi-Version Life Cycle Model. A model of MVS life cycle is based on operations of version generation G, aggregation and selection U at various stages [13]. Example of the two-version life cycle model is shown in Fig. 4 taking to account some FPGA features (V_{ij} are different versions obtained on different stage of development) [5,13].

Development of Multi-Version FPGA-Based NPP I&C Systems by Use of RADIY™ Platform

General Description of RADIY™ Platform. The FPGA-based I&C RADIY™ platform comprises both upper and lower levels [14]. The upper level has been created on purchased IBM-compatible industrial workstations. The software for the upper level RADIY™ platform was developed by RPC Radiy and is loaded on the workstations. The functions of the upper level workstations are the following:

– receipt of process and diagnostic information;

– creation of man-machine interface in the Control Room;

– display of process information on 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 the RADIY™" platform consists of standard cabinets including standard functional modules (blocks). The RADIY™ platform comprises the following standard cabinets:

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

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

– Cross Output Cabinets (COC) receives signals from three control channels (signal formation cabinets) and forms output signals by "two out of three" mode;

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

– Signalling Cabinets (SC) forms control signals for process annunciation panel at Control Room and others.

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

Opportunites of the RADIY™ platform. Application of the RADIY™ platform with the use of FPGA technology provides the following opportunities:

– to implement control and other safety-critical functions in the form of FPGA with implemented electronic design, without software;

– to use software only for diagnostics, archiving, signal processing, data reception and transfer between I&C systems components; failures of those 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;
– to process parallel of all control algorithms within one cycle, thus ensuring high performance of the system (for instance, a processing cycle of Reactor Trip System is 20 ms) and proven determined temporal characteristics;
– to develop the software-hardware platform in such a way that it becomes a universal interface to create I&C systems for any type of reactors;
– 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 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 reduce by more than 10 times the number of contact and terminal connections which cause many operational failures of equipment on account of the wide use of integrated solutions and fiber optic communication lines, etc.

IMPLEMENTATION OF FPGA-BASED NPP I&C SYSTEMS

Licensing of the RADIY™ platform

The RADIY™ platform has been licensed for NPP application in Ukraine and in Bulgaria. The main idea for licensing FPGA-based NPP I&C systems lays in consideration of FPGA-chip as hardware and FPGA electronic design as a special kind of software with specific development and verification stages [5,7].

Qualification tests of FPGA-based hardware in accordance with International Electrotechnical Commission (IEC) standards requirements include:

– radiation exposure withstand qualification;
– environmental (climatic) qualification;
– seismic and mechanical impacts qualification;
– electromagnetic compatibility qualification.

Results of qualification tests confirmed FPGA-based hardware compliance with IEC safety requirements.

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".

The safety assessments have been conducted by Ukrainian State Scientific Technical Centre on Nuclear and Radiation Safety (SSTC NRS), which is the supporting organization of Ukrainian Regulatory Authority. Experts of SSTC NRS have considerable experience in the area of FPGA-based systems safety assessment, as they have performed reviews of all thirty three FPGA-based safety systems supplied to Ukrainian NPP units since 2003.

Implementation of RADIY™ Platform-Based NPP I&Cs

RADIY™ platform has been applied to the following systems which perform reactor control and protection functions:

– Reactor Trip System (RTS); these I&Cs were developed as two-version systems consisting of two triple module redundant subsystems;
– 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.

The first commissioning of the RADIY™ platform was done in 2003 for Ukrainian NPP unit Zaporozhe-1. In six years since that time, 46 applications of RPC "Radiy" systems have been 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 realized by "Radiy" Corporation is the modernization of six ESFAS for Bulgarian NPP Kozloduy (three ESFASs for Kozloduy-Unit 5 and three ESFASs for Kozloduy-Unit 6).

ESFAS based on the RADIY™ platform performs the following control functions:

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

NPP site mounting and commissioning schedule has been as follows:

– August – September 2008 – ESFAS-2 for Kozloduy-6;
– April – May 2009 – ESFAS-2 for Kozloduy-5;
– August – September 2009 – ESFAS-1 and ESFAS-3 for Kozloduy-6;
– April – 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 of Kozloduy-6) started in September 2008. Installation prior to commissioning should be finished in an extremely short period (about one month). All the four commissioned ESFASs (ESFAS-1, ESFAS-2, ESFAS-3 of Kozloduy-6, and ESFAS-2 of 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.

CONCLUSIONS

In this paper we discussed basic concepts and taxonomy scheme of multi-version computing in context of development of FPGA-based NPP I&C systems. Key challenges related to diversity-oriented and FPGA-based systems are the following:

- existing standards are not enough detailed to make all necessary decisions concerning diversity (all the more FPGA-based decisions);
- multi-version I&Cs are still unique, failures occurred rarely and information about failures is not enough representative;
- methods of diversity assessment and kind selection, as a rule, are based on expert approach.

FPGA technology allows developing:

- multi-version systems with different product-process version redundancy,
- diversity scalable multi-tolerant decisions for safety-critical NPP I&Cs.

Discussed models of MVSs and MVTs are base:

- to choice cost-effective technique,
- to develop rational architecture taking into account requirements to diversity, safety, reliability and different limitations.

These theoretical issues were used on development of FPGA-based I&C platform RADIY™. The peculiarities of the platform are realization of control and other safety-related functions without software and ensuring dependability- and diversity-scalable decisions of safety-critical I&C. Existed experience of development, production and operation of RADIY™ platform-based NPP I&C systems has proved effectiveness of proposed theoretical and engineering decisions.

REFERENCES

[1] Littlewood, B., Strigini, L., 2000. A Discussion of Practices for Enhancing Diversity in Software Designs, Technical report LS_DI_TR-04, City University, London, Great Britain.

[2] Preckshot, G., 1994. Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems. NUREG/CR-6303, LLNL, Livermore, USA.

[3] Pullum, L., 2001. *Software Fault Tolerance Techniques and Implementation*, Artech House Computing Library.

[4] Kharchenko, V. (edit), 2002. *Multi-version Systems, Projects and Technologies*, National Aerospace University "KhAI", Kharkiv, Ukraine.

[5] Kharchenko, V., Sklyar, V. (edits), 2008, *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-Kirovograd, Ukraine.

[6] Kharchenko, V., Siora, A., Bakhmach, E., 2008. "Diversity-scalable decisions for FPGA-based safety-critical I&Cs: from Theory to Implementation". In Proceedings of the 6th Conference NPIC&HMIT, Knoxville, Tennessee, USA.

[7] Kharchenko, V., Sklyar, V., Siora, A., Tokarev, V., 2008. "Scalable Diversity-oriented Decisions and Technologies for Dependable SoPC-based Safety-Critical Computer Systems and Infrastructures". In Proceedings of the IEEE International Conference on Dependability of Computer Systems, Szklarska Poreba, Poland, pp. 339-346.

[8] Kharchenko, V., Yastrebenetsky, M., Sklyar, V., 2004. "Diversity Assessment of Nuclear Power Plants Instrumentation and Control Systems". In Proceedings of the 7th PSAM and ESREL Conference, Berlin, Germany, Vol.3, pp.1351-1356.

[9] Wood, R., Bobrek, M., 2009. "Design Approaches for FPGAs in Safety-Related Applications". In Proceedings of the Regional Workshop on Impact of Digital I&C Technologies on the Operation and Licensing of Nuclear Power Plants, Portoroz, Slovenia.

[10] Kharchenko, V., Bakhmach, I., Siora, A., Tokarev, V., 2009. "Diversity-oriented FPGA-based NPP I&C systems: challenges and decisions". In Proceedings of the 2nd IAEA Workshop on the Applications of FPGAs in Nuclear Power Plants, Kirovograd, Ukraine.

[11] Kharchenko, 2009. "Dependable Systems and Multi-Version Computing: Aspects of Evolution", *Radioelectronic and Computer Systems*, No7, Vol.8, pp. 13-27.

[12] Littlewood, B., Popov, P., 2001. "Modelling software design diversity - a review", *ACM Computing Surveys*. No33, pp. 177-208.

[13] Volkovoj, A., Lysenko, I, Kharchenko, V., Shurygin, O, 2009. *Multi-Version Systems and Technologies for Critical Applications*, National Aerospace University "KhAI", Kharkiv, Ukraine.

[14] Bakhmach, I., Kharchenko, V., Siora, A., Sklyar, V., Tokarev, V., 2009. "Advanced I&C Systems for NPPs Based on FPGA Technology: European Experience". In Proceedings of the 17th International Conference on Nuclear Engineering "ICONE 17", Brussels, Belgium.

[