2

Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring

Vyacheslav Kharchenko[1], Olexandr Siora[2] and Volodymyr Sklyar[2]
[1]*National Aerospase University KhAI,*
Centre for Safety Infrastructure-Oriented Research and Analysis,
[2]*Research and Production Corporation RADIY,*
Ukraine

1. Introduction

1.1 Problem of decreasing common cause failure probability for nuclear power plant instrumentation and control systems

To guarantee required level of dependability, safety and security of computer-based systems for critical (safety-critical, mission-critical and business-critical) applications it is used diversity approach. This approach implies development, choice and implementation of a few diverse design options of redundant channels for created system. Probability of common cause failure (CCF) of safety-critical systems may be essentially decreased due to selection and deployment of different diversity types on the assumption of maximal independence of redundant channels realizing software-hardware versions.

This circumstance calls forth that a lot of international and national standards and guides contain the requirements to use diversity in safety-critical systems, first of all, in nuclear power plant (NPP) instrumentation and control systems (I&Cs) (reactor trip systems), aerospace on-board equipment (automatic/robot pilot, flight control systems), railway automatics (signalling and blocking systems), service oriented architecture (SOA)-based web-systems (e-science) etc. (Pullum, 2001; Wood et al., 2009; Gorbenko et al., 2009; Kharchenko et al., 2010; Sommerville, 2011).

Application of the modern information and electronic technologies and component-based approaches to development in critical areas, on the one hand, improve reliability, availability, maintainability and safety characteristics of digital I&Cs. On the other hand, these technologies cause additional risks or so-called safety deficits. Microprocessor (software)-based systems are typical example in that sense. Advantages of this technology are well-known, however a program realization may increase CCF probability of complex software-based I&Cs. Software faults and design faults as a whole are the most probable reason of CCFs. These faults are replicated in redundant channels and cause a fatal failure of computer-based systems. It allows to conclude that, "fault-tolerant" system with identical channels may be "non-tolerant" or "not enough tolerant" to design faults. For example, software design faults caused more than 80% failures of computer-based rocket-space systems which were fatal in 1990 years (Kharchenko et al., 2003) and caused 13% emergencies of space systems and 22% emergencies of carrier rockets (Tarasyuk et al., 2011).

The CCF risks may be essential for diversity-oriented or so-called multi-version systems (MVSs) (Kharchenko, 1999) as well if choice of version redundancy type and development

of channel versions are fulfilled without thorough analysis of their independence and assessment of real diversity degree assessed by special metrics, for example, β-factor (Bukowsky&Goble, 1994).

1.2 Complex electronic components and FPGA technology for NPP I&Cs development

An analysis of development and introduction trends of computer technologies to NPP I&Cs has specified a number of important aspects affecting their safety, peculiarities of development, update and licensing. Such trends include, among others (Yastrebenetsky, 2004): introduction of novel complex electronic components (CECs); expanded nomenclature of software applied and increased effect of its quality to I&Cs safety; realization of novel principles and technologies in I&Cs development; advent of a large number of novel standards regulating the processes of I&Cs development and safety assessment. During recent decades the application of microprocessor techniques in NPP I&Cs design has substantially expanded. Microprocessors are used both in system computer core and in realization of intellectual peripherals – various sensors, drives and other devices with built-in programmable controllers.

Another contemporary trend is dynamically growing application of programmable logic technologies, particularly, Field Programmable Gate Arrays (FPGA) in NPP I&Cs, onboard aerospace systems and other critical areas. FPGA as a kind of CECs is a convenient mean not only in realization of auxiliary functions of transformation and logical processing of information, but also in execution of basic monitoring and control functions inherent in NPP I&Cs. This approach in some cases is more reasonable than application of software-controlled microprocessors (Kharchenko&Sklyar, 2008). In assessment of FPGA-based I&Cs it should be taken into consideration that application of this technologies somewhat levels the difference between hardware and software, whereas obtained solutions are an example of a peculiar realization of so called heterosystems – systems with "fuzzy" software-hardware architecture and mixed execution of functions. This circumstance and other features of FPGA technology increase a number of diversity types and enlarge a set of possible diversity-oriented decisions for NPP I&Cs.

1.3 Work related analysis

Known works, related to the current problem and taking into account features of NPP I&C systems, are divided into three groups: (1) classification and analysis of version redundancy types and diversity-oriented decisions; (2) methods and techniques of diversity level assessment and evaluation of multi-version systems safety in context of CCFs; (3) multi-version technologies of safety critical systems development.

1. A set of diversity classification schemes (general, software and FPGA-based) was analyzed in (Kharchenko et al., 2009). First one is based on NUREG technical reports and guides, samples two-level hierarchy and includes seven main groups of version redundancy (Wood et al., 2009): signal diversity (different sensed reactor or process parameters, different physical effects, different set of sensors); equipment manufacture diversity (different manufacturers, different versions of design, different CEC versions, etc); functional diversity (different underlying mechanisms, logics, actuation means, etc); logic processing equipment or architecture diversity (different processing architectures, different component integration architectures, different communication architectures, etc); logic or software diversity (different algorithms, operating system, computer languages,

etc); design diversity (different technologies, approaches, etc); human or life cycle diversity (different design organizations/companies, management teams, designers, programmers, testers and other personnel). Software diversity types are classified in according with following attributes (Pullum, 2001; Volkoviy et al., 2008): life cycle models and processes of development (for example, V-model for main version and waterfall model with minimum set of processes for duplicate version); resources and means (different human resources, languages and notations, tools); project decisions (different architectures and platforms, protocols, data formats, etc). Next one FPGA-based classification includes the following types of diversity (Kharchenko&Sklyar, 2008; Siora et al., 2009): diversity of electronic elements (different electronic elements manufactures, technologies of production, electronic elements families, etc); diversity of CASE-tools (different developers, kinds and configurations of CASE-tools); diversity of projects development languages (different graphical scheme languages, hardware description languages and IP-cores); diversity of specifications (specification languages) and others.

2. There are following methods of diversity level assessment and evaluation of MVS dependability and safety (Kharchenko et al, 2009). Theoretical-set and metric-oriented methods are based on: Eiler's diagram for sets of version design, physical and interaction faults (including vulnerabilities for assessment intrusion-tolerance); matrix of diversity metrics for sets of different faults (individual, group and absolute faults of versions); calculation of diversity metrics by use of Eiler's diagrams or other data about results of testing and faults of different versions. Probabilistic methods use reliability block-diagrams (RBDs), their modifications (survivability and safety block-diagrams), Markovian chains, Bayesian method, etc. Statistical methods include the following procedures: 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 consists of: receiving project-oriented fault profiles; performing of faults injection procedure; proceeding of data and metrics diversity calculation; calculation of reliability and safety indicators. Expert-oriented methods use 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 methods are 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.
3. Multi-version technologies (MVTs) of diversity types selection and application, development of MVSs as a whole are based on (Siora et al., 2009; Wood et al., 2009) use of diversity types and strategies table, a model of multi-version life cycle (MVLC), a special graph of diversity types and their modifications, and procedures of diversity type and volume choice according with different criteria. The set of diversity strategies developed in the (Wood et al., 2009) consists of three families of strategies: different technologies—Strategy A (digital vs analog), different approaches within the same technology—Strategy B (microprocessor vs FPGA) and different architectures within the same technology—Strategy C (IP-based vs VHDL). Each of the strategy families is characterized by combinations of diversity criteria that may provide adequate mitigation of potential CCF vulnerabilities according with metrics determined by expert way.

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 "types of diversity – areas of multi-version I&Cs application" in Table 1 (Wood et al., 2009; Kharchenko et al., 2010).

Diversity types	Multi-version I&C systems application												
	Space		Aviation				Railways	Chemic. industry	Defense	Power Plants	NPPs		e-Commers
	Shuttle	ISS	MC JVC	FAA FCS	Air-bus A320	Boeng 777	SCB	CCPS	MICS	Electr. Grid	RTS	ESFAS	WSOA
Design													
Equip-ment													
Func-tion													
Human													
Signal													
Soft-ware													
Others													

Table 1. Matrix "types of diversity – areas of multi-version I&Cs application"

Types of diversity (diversity redundancy) are classified according to NUREG 6303 and painted by different colors. Last row of the matrix corresponds to other types of diversity. MVSs 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).

1.4 Goal and structure of the chapter

In spite of the intensive researches in area of multi-version systems and long-term experience of their application there are some problems of diversity approach implementation in context of FPGA technology application in NPP I&Cs, videlicet: specifying of concepts used; selection of diversity types and required volume of version redundancy; joint use of different diversity types taking into consideration state-of-the-art technologies; assessment of real diversity degree and effectiveness of MVSs, etc. Goal of the chapter is analysis of concepts in multi-version computing and diversity-scalable decisions for FPGA-based NPP I&Cs. Structure of the chapter is following. The section 2 elaborates the FPGA peculiarities in context of safety critical applications and evolution aspect of

FPGA-technology and diversity approach conformably to NPP I&Cs. The standards containing requirements to application of diversity approach in NPP I&Cs and key challenges in this area are analyzed in the section 3. The taxonomy of multi-version computing and models of MVSs and MVTs are represented in the section 4. General approach to assessment of diversity and MVS safety is described in the section 5. Features of FPGA-based platform RADIY™ and results of implementation of multi-version I&Cs in NPPs are analyzed in the section 6. Finally, the section 7 concludes the chapter and presents directions of future researches.

2. An evolution of FPGA technology and diversity application in NPP I&Cs

2.1 FPGA peculiarities in context of dependability and safety

FPGA architecture topologically originates from channeled Gates Arrays (GA) (Altera, 2001). In FPGA internal area a set of configurable logic units is disposed in a regular order with routing channels there between and I/O units at the periphery. Transistor couples, logic gates NAND, NOR (Simple Logic Cell), multiplexer-based logic modules, logic modules based on programmable Look-Up Tables (LUT) are used as configurable logic blocks. All those have segmented architecture of internal connections.

System-On-Chip architecture appeared due to two factors: high level of integration permitting to arrange a very complicated circuit on a single crystal, and introduction of specialized hardcores into FPGA. Additional hardcores may be: additional Random Access Memory (RAM) units; JTAG interface for testing and configurating; Phase-Locked Loop (PLL) – frequency control system to correct timing relations of clock pulses as well as for generation of additional frequencies; processor cores enabling creation of devices with a control processor and a peripheral.

Analysis of dependability assurance possibilities in FPGA-based systems allows to determine the following FPGA peculiarities (Kharchenko&Sklyar, 2008; Bobrek et al., 2009).

1. Simplification of development and verification processes: apparatus parallelism in control algorithms execution and realization of different functions by different FPGA elements; absence of cyclical structures in FPGA projects; identity of FPGA project presentation to initial data; advanced testbeds and tools; verified libraries and Intellectual Properties (IP)- cores in FPGA development tools.
2. There are three technologies of FPGA-projects development: development of graphical scheme with using of library blocks in CAD environment; development of software model with using of especial hardware describing languages (VHDL, Verilog, Java HDL, etc); development of program code for operation in environment of microprocessor emulators which are implemented in FPGA as IP-cores. It does allow increasing a number of options of different project versions and multi-version I&Cs.
3. Assurance of fault-tolerance, data validation and maintainability due to use of: redundancy for intra- and inter-crystal levels; diversity implementation; reconfiguration and recovery in the case of component failures; improved means of diagnostic.
4. Security assurance: FPGA reprogramming is possible only with use of especial equipment. Stability and survivability assurance due to: tolerance to external impacts (electromagnetic, climatic, radiation); possibilities of implementation of multi-step degradation with different types of adaptation.

2.2 FPGA technology application in safety-critical systems and NPP I&Cs

Due to these peculiarities area of FPGA technology application essentially has expanded. We can say about a affirmative answer to question "Expansion of FPGA-technology application in safety-critical systems for the last decades: evolution or revolution?" It is confirmed by (Bakhmach et al., 2009):

substantial increase of applying the technologies based on programmable logic (FPGA, CPLD, ASIC);

FPGA technology is improved and ensures new possibilities to develop more reliable and effective systems; application FPGA technology for development of military (B-1B, F-16, etc) and civil aircraft control systems (Boeing 737, 777, AN70, 140), space control systems (satellites FedSat, WIRE; the Mars-vehicle Spirit), etc;

application of FPGAs in NPP I&Cs (Ukraine, Russia, Bulgaria: 1999-start, 2002 – 1000, 2006 – 6000, 2008-2010 – more than 8000 chips every year).

Besides, the illustration of FPGA expansion is evolution of the NPP I&Cs produced by RPC Radiy during 2000-2008 years (Kharchenko&Sklyar, 2008).

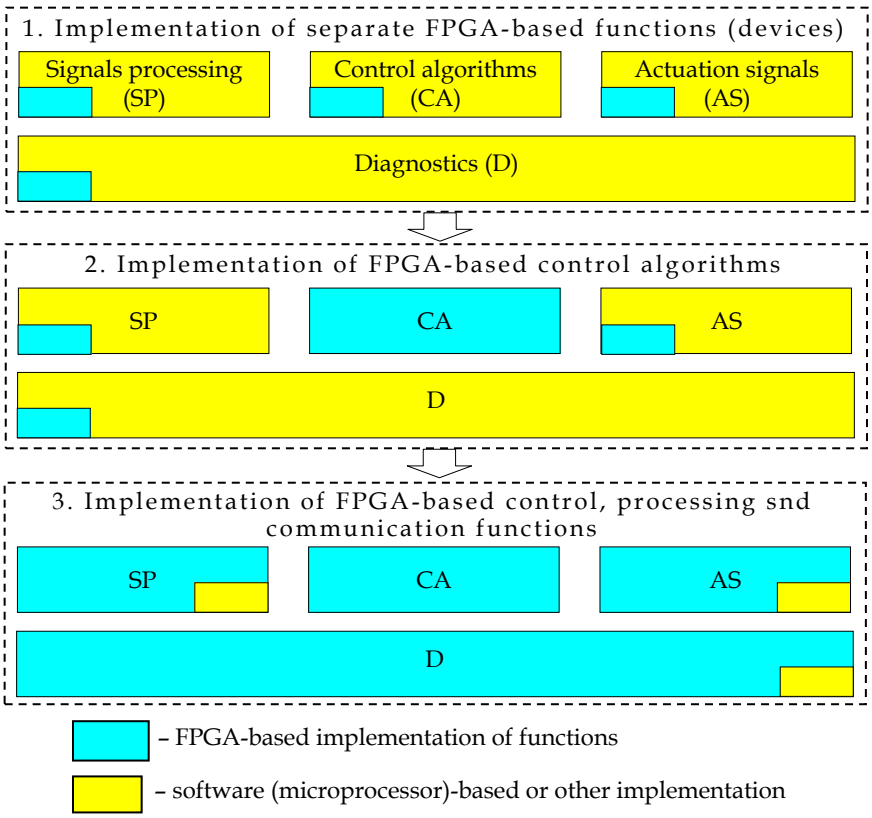


Fig. 1. Application of FPGA technology in the NPP I&Cs produced by RPC Radiy

There are three stages of the evolution (Fig.1): from implementation of separate FPGA-based functions in I&Cs (signals processing (SP), control algorithms (CA), actuation signals formation (AS) and diagnostics (D)), stage 1, and implementation of FPGA-based CA, stage 2, to preferred implementation of FPGA-based SP-, CA-, AS-, D- and communication functions, stage 3.
Analysis of industrial application experience of FPGAs in NPP I&Cs is described in technical report prepared by EPRI (Naser, 2009).

2.3 A law "negation of negation": Stages of diversity approach implementation evolution in NPP I&Cs

Interesting are the results of transformation of multi-version I&Cs for the last decades in context of hardware-software-FPGA technologies development. There are a few diversity implementation evolution stages in safety-critical NPP I&Cs, in particular, reactor trip systems. Analysis of these stages allows formulating (or demonstrating truth) a law "negation of negation" (Kharchenko et al., 2009) (Fig.2):

- stage 1 (1970-1980s) – use of hardware (hard logic, HL)-based one-version systems and transition from hardware (HW)-based systems with identical subsystems to systems with hardware (HL)-based primary subsystem and software (microprocessor, MP)-based secondary subsystem; it was the first "negation";
- stage 2 (1990s) – use of primary and secondary subsystems with software (SW) diversity (I&C platforms produced by Siemens, WH and other companies); example of multi-version systems with software diversity is two-version system consisting of subsystems developed using microprocessors Intel and Motorola (languages C and Ada); it completed the first cycle of "negation of negation";
- stage 3 (2000s, first half) – transition to FPGA-based primary and software-based secondary subsystems with equipment, design and software diversity (first generation of the I&C platforms produced by RPC Radiy); it was next "negation";
- stage 4 (2000s, second half) – application of FPGA-oriented soft processors for primary subsystem and FPGA project developed using HDL-oriented language (hard logic) for creation of secondary subsystem (next generation of the I&C platform produced by RPC Radiy); it completed the second cycle of "negation of negation";
- stage 5 (beginning of 2010s) – application of different FPGAs (hard logic) produced by different manufacturers (and other types of diversity) for primary and secondary subsystems correspondingly; it is next "negation".

What will be the next step? Probably, advancement of electronic technologies, in particular, nanotechnologies, naturally dependable, safe and secure chips will create new perspectives and possibilities for development of diversity-oriented decisions. Actel, Altera and others companies inform about creating first chips called nano FPGAs allowing to develop fault-tolerant projects using large-scale means.

3. Normative base and key challenges connected with diversity application in NPP I&Cs

3.1 Analysis of diversity related standards

There are the following standards and guides 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;

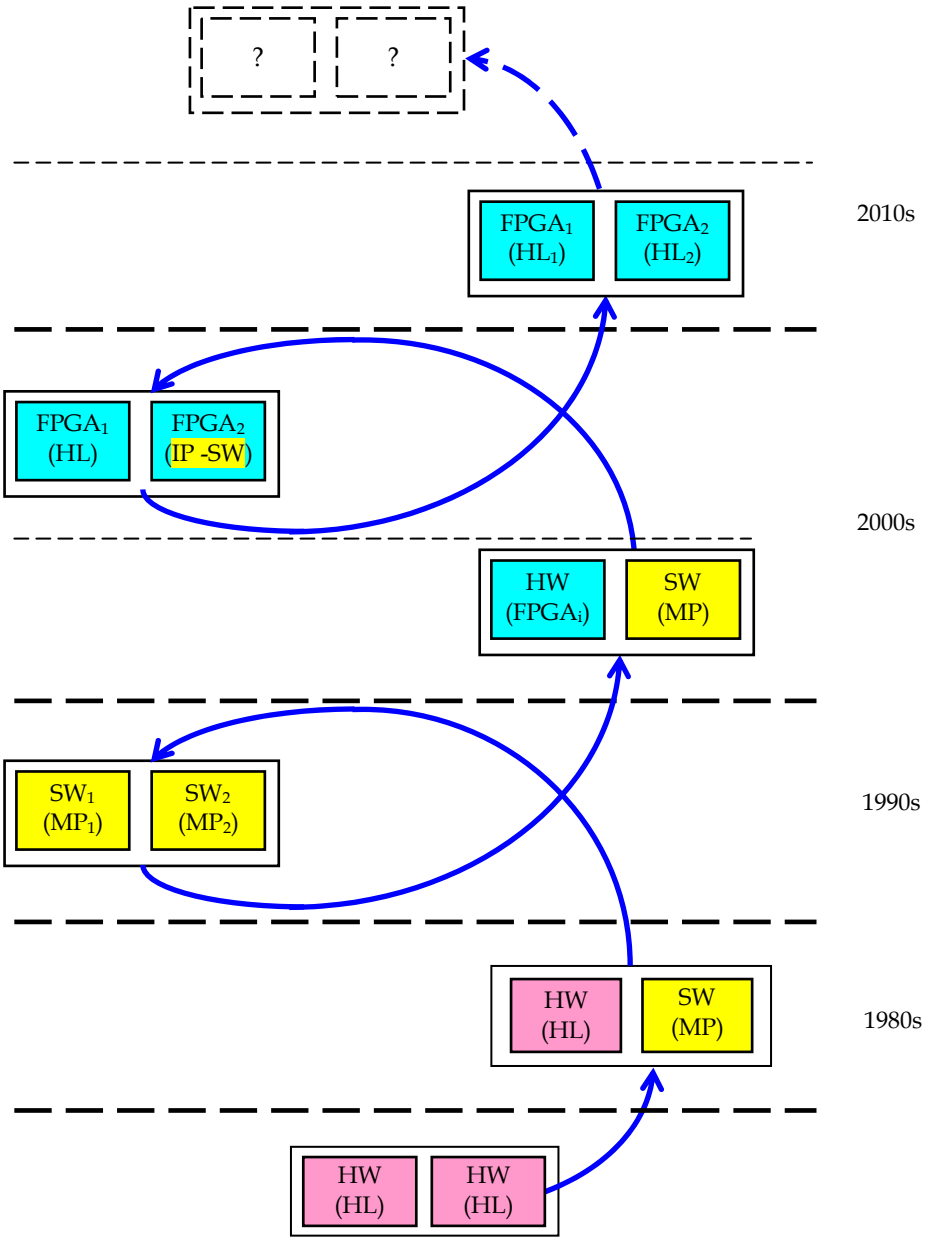


Fig. 2. Stages of diversity approach implementation evolution in safety-critical NPP I&Cs

- 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);
- 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 (Reactor Trip Systems); types of diversity used to develop NPP I&Cs and to decrease CCF probability; features of diversity implementation, determination of types 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".

3.2 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 6-8 last years, i.e. these systems are new object of analysis and still more unique one;

FPGA technology gives 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.

4. Main concepts and models of multi-version computing

4.1 Taxonomy scheme of multi-version computing

A set of concepts concerning diversity may be united by general term "multi-version computing" on the analogy with "dependable computing" (Avižienis et al., 2004). Multi-version computing is a type of dependable computing organization based on use of diversity approach. Taxonomy scheme of multi-version computing developed taking into consideration concepts in this area described in international standards includes the following elements (Kharchenko et al, 2009) (Fig.3).

Version is an option of the different realization of identical task (by use software, hardware or FPGA-based products and life cycle processes); identical versions of structure redundancy-based system are trivial. Version redundancy (VR) is a type of product and process redundancy allowing to create different (non-trivial) versions; product VR is realized jointly with structure, time and other types of non-version redundancy.

Challenges	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	6-8 years
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 MVSs	Choice of diversity kinds, generation of really diverse software versions	Number of diversity kinds increases
Verification of MVSs	Verification activities volume are significantly increased	Verification is more simple due to simplifying of version verification

Table 3. Key challenges for software-based and FPGA-based MVSs

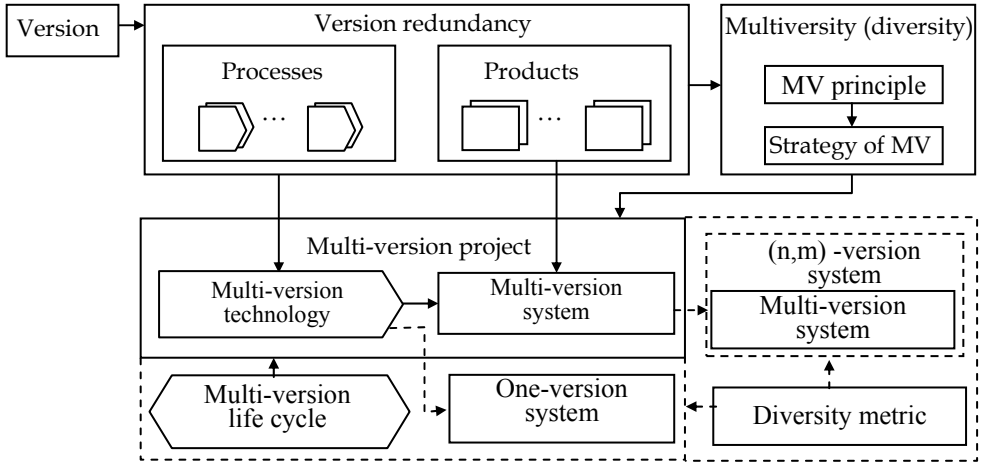


Fig. 3. Taxonomy scheme of multi-version computing

Diversity or multiversity (MV) is a principle providing use of several non-trivial versions; this principle means performance of the same function (realization of products or processes) by two and 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 system (MVS) is a system in which a few versions-products are used; one-version systems may be redundant but consists of a few trivial versions. Multi-diversion system (MDVS) is MVS in which two or more VR types are applied. Multi-version

technology (MVT) is set of the interconnected rules and design actions in which in accordance with MV strategy 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.
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 (realization of version redundancy of products). Strategy of diversity (MV) is a collection of general criteria and rules defining principles of formation and selection of version redundancy types and volume or/and choice of MVTs. Besides, important elements of multi-version computing are concepts "multi-version life cycle", "diversity metric". More detailed interpretation of these concepts will be done below.

4.2 Diversity type classification schemes

Different variants of diversity type classifications were described above. The analysis of the considered classifications allows approving that:

- they are presented by classifications of mixed facet-hierarchical or matrix (network) types;
- the NUREG-based classification presented in (Wood et al., 2009) is the most detailed and systematic, though the principle of attributes orthogonality is not sustained in full in it; for example, subsets of design and software, functional and signal version redundancy are crossed and dependent;
- variety of product (system, hardware and software components) and of process (technologies of development, testing and maintenance) version redundancy cause complexity of VR selection and MVS development.

More general diversity type classification scheme is so-called "cube" of diversity described by matrix MVR = $||\, vr_{ijk} \,||$ in three-dimensional space (Fig. 4). The scheme has coordinates: stage of LC (i); level of project decisions (PD, j) and type of VR (project decision).
Example of two-space matrix presented a cut of "cube" for FPGA-based systems is shown on the table 3. This table contains variants of joint application of one or two diversity types (items 1.4.2-1.4.4, 2.3.3-2.3.8, 3.3.3-3.3.8, 4.2.4-4.2.15; for example, last combinations correspond to 12 = 4 (kinds of EE diversity) x 3 (kinds of CASE-tool diversity) couples).

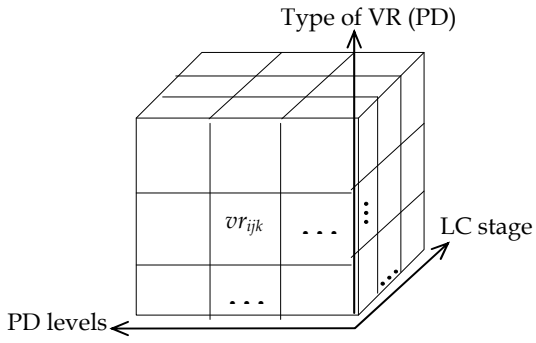


Fig. 4. Cube" of diversity-oriented decisions

Stages of FPGA-based I&C life cycle	Kinds of version redundancy			
	1 Diversity of electronic elements (EE)	2 Diversity of CASE-tools	3 Diversity of project development languages	4 Diversity of scheme specification (SS)
1 Development of block-diagrams according with signal formation algorithms		1.2.1 Different developers of CASE-tools 1.2.2 Different CASE-tools kinds 1.2.3 Different CASE-tools configurations		1.4.1 Different SSs 1.4.2-1.4.4 Combination of couples of diverse CASE-tools and SSs
2 Development of program models of signal formation algorithms in CASE-tools environment		2.2.1 Different developers of CASE-tools 2.2.2 Different CASE-tools kinds 2.2.3 Different CASE-tools configurations	2.3.1 Joint use of graphical scheme language and HDL 2.3.2 Different HDLs 2.3.3-2.3.8 Combination of diverse CASE-tools and HDLs	
3 Integration of program models of signal formation algorithms in CASE-tools environment		3.2.1 Different developers of CASE-tools 3.2.2 Different CASE-tools kinds 3.2.3 Different CASE-tools configurations	3.3.1 Joint use of graphical schemes and HDL 3.3.2 Different HDLs 3.3.3 – 3.3.8 Combination of couples of diverse CASE-tools and HDLs	
4 Implementation of integrated program model in FPGA	4.1 Different manufacturers of EEs 4.2 Different technologies of EEs production 4.3 Different families of EEs 4.4 Different EEs of family	4.2.1 Different developers of CASE-tools 4.2.2 Different CASE-tools kinds 4.2.3 Different CASE-tools configurations 4.2.4-4.2.15 Combination of diverse CASE-tools and EEs		

Table 2. Matrix of diversity-oriented FPGA-based decisions

4.3 Models multi-version systems

One-version W(1) and multi-version W(n) systems are defined by 4 and 6 variables (Kharchenko et al., 2010):

$$W(1) = \{X, Y, Z. \Phi\}, \quad (1)$$

$$W(n) = \{X, Y, Z. \Phi, V, \Psi\}, \quad (2)$$

where X, Y, Z – sets of input signals, internal conditions (states) and output signals correspondingly; $\Phi = \{\varphi_i, i=1, ..., a\}$ – a set of I&C functions (for examples, actuation functions or algorithms of reactor trip system); $V = \{v_j, j=1, ..., n\}$ – a set of versions with output signals $Z_1,\ldots, Z_n$ (or signals Z_{id} , $d = 1,\ldots, n_i$; n_i is a number of versions for function φ_i; $\forall\varphi_i \sim v_j = \{ v_{ij}, j =1,...,n_i\}$); $\Psi = \{\psi_s, s=1, ..., в\}$ – mapping $Z_i \rightarrow Z$.

If the function φ_i is performed, local mapping is true: $\psi_s:\{z_i(v_{i1}),..., z_i(v_{in_i})\}\rightarrow Z_i^{(S)}$. Taking into account formulas (1) and (2), multi-version system and one-version system are connected by relationship:

$$W(n) = \{W(1), V, \Psi\}. \quad (3)$$

System W(1) may be structure-redundant and contain usual means Ψ for signals processing from identical channels (versions). In this case card V=1. For system W(n) is true that: $\forall_j=\overline{1,a} : \exists_j: n_i>1$.

Mapping ψ_s is generally described by: a subset of versions $\Delta v_s \subset v_j$ for receiving output signal Z_i; a vector $\vec{t}_s$ of version v_{ij} initialization time ($\vec{t}_s = \{t(v_{i1}),..., (v_{in_i})\}$); a mean of transforming η_s values $z_i(v_{i1}),..., z_i(v_{in_i})$ in output signal Z_i^S. Hence,

$$\forall\psi_s\in\Psi:\psi_s = \{\Delta vs, \vec{t}_s, \eta_s\} \text{ and } Z_i^{(S)} = \eta_s [z_i(v_{ij}), \vec{t}_s], v_{ij}\in\Delta v_s.$$

There are the following means of transforming η_s: (a) the conjunctive, when $Z_i^S = Vz_i(v_{ij})$; (b) the time conjunctive, when $Z_i^S = Vz_i(v_{ij})\sigma_{ij}$, where $\sigma_{ij}=1$, if $t=t(v_{ij})$, and if not $\sigma_{ij}=0$; (c) the majority, when $Z_i^S = M[z_i(v_{ij})]$, where M is a majority function k out of *l* (or k out of n); (d) the majority-weighted, when weights of versions $\omega(v_{ij})$ are additionally defined on majorization; (e) the functional, when $Z_i^S = f[z_i(v_{ij})]$, where f - some function of transforming output signals of every version.

The model (2) describes system with n versions that, $n = \sum_{i=1}^{a} n_i$. This model does not take into account the possibility of applying several diversity kinds. A set of version redundancy kinds $R=\{r_d, d=1,..., m\}$ may be decomposed on subsets for versions of products $v_{prd}(t_j)$ and processes $v_{prc}(t_j)$: $R=(\bigcup_j \Delta R_{prdj}) \cup (\bigcup_j \Delta R_{prcj})$, where ΔR_{prdj} and ΔR_{prcj} – appropriate subsets.

Thus, different diversity kinds, $r\in R$, are accumulated in final versions of a multi-version system. It is described by special mapping $\Theta : R \rightarrow V$. Mapping Θ may be presented by Boolean matrix $\|\theta d_j\|$, $d=\overline{1,m}; j=\overline{1,n}$, where $\theta_{dj}=1$, if diversity kind r_p is used in version v_j, and if not $\theta_{dj} = 0$. Then multi-version system W(n,m) or multi-diversion system is described by formula:

$$W(n,m) = \{ X, Y, Z, \Phi, V, \Psi, R, \Theta \} = \{W(n), R,\Theta \} = \{W(1), V, \Psi,R, \Theta \}. \quad (4)$$

It is important to describe correspondence between a set of versions V and a set of redundant channels $C=\{c_q, q=1,...,l\}$. This correspondence may be defined by mapping $Q:V\rightarrow C$. This mapping is presented by Boolean matrix $Q = \|\omega_{jg}\|$, $d=\overline{1,m}$, $g=\overline{1,l}$, where $\omega_{gj} = 1$, if version v_i is realized by channel c_j, and if not $\omega_{gj} = 0$. Then model of multi-version (multi-diversion) system is the following:

$$W(n,m,l) = \{ X, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q \}= \{ W(n,m), C, Q \}. \quad (5)$$

MVSs with temporal redundancy and p iterations of algorithms are indicated as W(n,m,n,p) dividing number of parallel (structural) versions n_c, and sequential versions realized by using one channel. Set X may be decomposed for different versions if

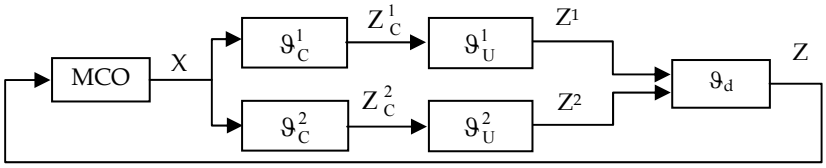
$$X = \bigcup_j X_j \ , \ \forall j_1 j_2 \in \overline{1,n} \ , \ j_1 \neq j_2 : \ X_{j1} \cap X_{j2} \ , X_{j1} \cap X_{j2} = \phi .$$

Such MVSs are called multi-version systems with naturally divided input alphabet:

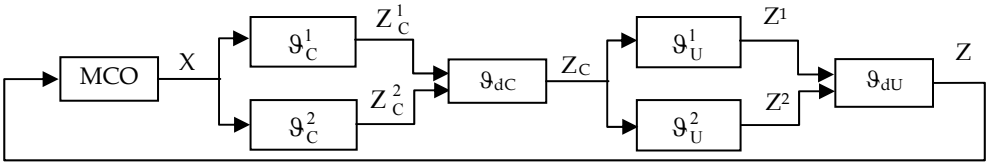
$$W_{NX} = \{ \{X_j\}, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \quad (6)$$

If versions process data presented in different notations, such MVSs are called multi-version systems with artificially divided input alphabet WAX. A special function-transformer Πx (Πxj) should be specified in addition to alphabet X :

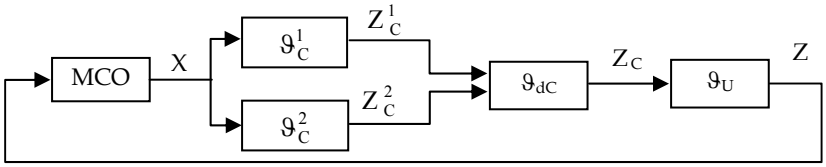
$$W_{NX} = \{X, \{\Pi xj\}, Y, Z, \Phi, V, \Psi, R, \Theta, C, Q\}. \quad (7)$$



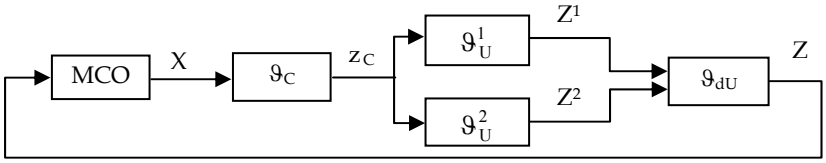
a) two-versions system with full common diversity, ϑ_{FO}



b) two-versions system with full separate diversity, ϑ_{FS}



c) two-versions system with partial diversity (for ϑ_C), ϑ_{PC}



d) two-versions system with partial diversity (for ϑ_U), ϑ_{PU}

ϑ_C^1 , ϑ_C^2 - the first and the second versions of a monitoring automaton;

ϑ_U^1 , ϑ_U^2 - the first and the second versions of a contril automaton;

ϑ_{dC}, ϑ_{dU}, ϑ_d - solver for union of two versions results.

Fig. 5. Architecture variants of two-version I&C systems

Besides, I&Cs performing safety-critical functions may be represented by a composition of two interconnected subsystems – monitoring (checking) subsystem and control subsystem (monitoring and control automata). Monitoring automaton ϑ_C analyses output signals X from monitoring and control object (MCO) and forms its status code Z_C.
Control automaton ϑ_U 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 such attributes (see Fig. 5):
degree of diversity coverage (I&Cs with a full ϑ_F and partial ϑ_P diversity);
diversity depth (I&Cs with a common ϑ_O and separate ϑ_S diversity); it should be noted that this feature is applicable only to full system diversity.

4.4 Models of multi-version life cycle and technology

A model of MVS life cycle (or multi-version LC model) is based on operations of version generation G, aggregation and selection U at various stages (Kharchenko et al., 2007). Example of the two-version life cycle model is shown on Fig. 6 taking to account some FPGA-oriented design features (V_{ij} are different versions obtained on different stage of development) (Prokhorova et al., 2008).

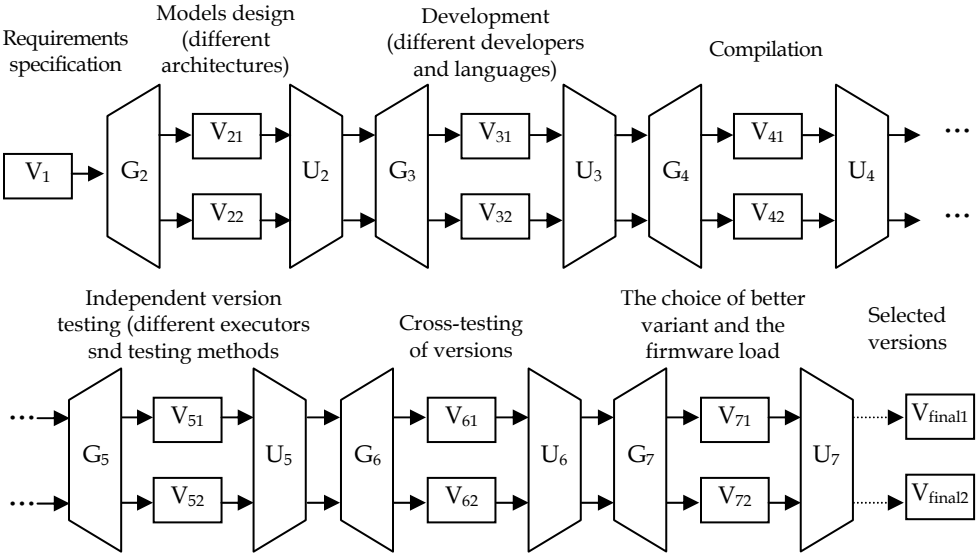


Fig. 6. FPGA-system multi-version life cycle

In general case I&C system LC is a sequence of N stages. At each i-th stage of a multi-version I&C system LC Mi of diversity types may be applied. From Mi, i = 1,...,N; diversity types only a single j-th type, j = 1,...,Mi, may be selected. Besides, at each i-th stage of LC a single-version development technology may be selected. Each j-th diversity type at each i-th LC stage is characterized by two indices: diversity metrics (depth) dij and cost of respective diversity type application (cost increase as compared to single-version option of each i-th LC stage).

Thus, a set of solutions on selection of diversity kind is described by two matrices: diversity metrics values D = || d_{ij} || and cost values C = || c_{ij} ||. Hence MVS LC may be presented as a bipolar N-level graph (Fig.7) called graph of multi-version technologies (Sklyar &Kharchenko, 2007). MVT corresponds to non-zero way in this graph.
Algorithms of MVT (optimal way in the graph) selection according with criteria "diversity (safety)-reliability-cost" are described in (Kharchenko&Sklyar, 2008).

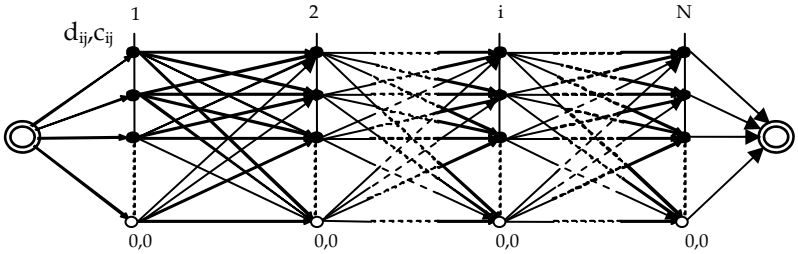


Fig. 7. Graph of MVTs

5. Assessment of multi-version FPGA-based systems safety

5.1 General approach to assessment

Assessment of diversity level and MVS safety is based on the following basic procedures analysis and evaluation:

- check-list-based analysis of applicable diversity types (CLD); initial data for the CLD analysis are I&C design and documentation, a table of diversity types (subtypes) was developed in advance; a result of the CLD analysis is a formalized structured information about used diversity types and subtypes in analyzed I&C system;
- metric-based assessment of diversity (MAD); initial data for the MAD procedure are results of the CLD analysis and values of metrics and weight coefficients for diversity types (subtypes) used in I&C systems; a result of the MAD assessment is a value of general diversity metric;
- Reliability Block Diagram (RBD) and Markovian model (MM)-based assessment taking into account results of MAD.

5.2 Stages of assessment

The main stages and operations of diversity analysis and MVS assessment depend on the type of the evaluated system. The first stage is a Check-list-based analysis of MVS design and documentation. This stage contains two operations:

1. Analysis of I&C specification and requirements to system, definition of system safety class; requirements to diversity (necessary for diversity application);
2. Analysis of I&C design and development process that involves activities: (a) identification of MVS types: which of the subsystems are FPGA-based and which are software and microprocessor-based; (b) identification of product diversity; for FPGA-based MVSs: manufacturer of chips; FPGA technology; FPGA families; FPGA chips, languages; tools, etc); (c) identification of process diversity kinds.

Results of analysis are entered in a check-list in accordance with rule Yes (if corresponding diversity type is used in a system) / No (in opposite case) and is presented as a n-bit Boolean vector.

The second stage is a metric-based assessment of diversity. This stage contains two operations:

1. Determination of metric values for different types of applied diversity, i.e. performing two activities: (a) determination of metric values (local diversity metrics μ_i for diversity type d_i and local diversity metrics μ_{ij} for diversity subtype d_{ij}); the metric values may be predefined; (b) correction of metric values in accordance with development and operation experience.
2. Calculation of general diversity metric μ for a system: (a) determination (correction) of weight coefficients ω_i (ω_{ij}) of metrics (taking into account multi-diversity aspect); sum of weight coefficients ω_i (ω_{ij}) is equal 1; (b) convolution (additive or more complex) of metrics and calculating value of general diversity metric $\mu = \Sigma\, \omega_i \Sigma\, \omega_{ij}\, \mu_{ij}$, i = 1,…, n; j = 1,…$n_i$.

Thus, result of this stage is a value of general diversity metric μ, which is some approximation of β, and can characterize the diversity effect on CCF probability.

The third stage is a probabilistic RBD- or MM-based (RDM) assessment of MVS reliability and safety. Initial data for the RDM procedure are I&C design and documentation, results of the CLD and MAD analysis; results of the RDM procedure are values of safety and dependability indicators. Detailed description of the RDM procedure is given in (Kharchenko et al., 2004).

6. Implementation of FPGA-based safety-critical NPP I&Cs

6.1 General description of the FPGA-based RADIY™ platform

The platform RADIY™ produced by RPC Radiy is an example of a dependable and scalable FPGA-based I&C platform ensuring possibility of development of multi-version systems. Dependability assurance feature of the I&C platform RADIY™ is multi-diversity implementation through the following diversity types: equipment diversity is provided by different electronic components, different programmable components (FPGAs and microcontrollers) and different schemes of units; software diversity is provided by different programming languages and different tools for development and verification; life cycle (human) diversity is provided by different teams of developers.

Scalability of the I&C platform RADIY™ permits to produce different types of safety-critical systems without essential changing of hardware and software components. The I&C platform RADIY™ provides the following types of scalability: scalability of system functions types, volume and peculiarities by changing quantity and quality of sensors, actuators, input/output signals and control algorithms; scalability of dependability (safety integrity) by changing a number of redundant channel, tiers, diagnostic and reconfiguration procedures; scalability of diversity by changing types, depth and criteria of diversity choice.

The FPGA-based I&C RADIY™ platform comprises both upper and lower levels (Kharchenko&Sklyar, 2008). 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 (Bakmach et al., 2009):

- Normalizing Converters Cabinets performs inputting and processing of discrete and analog signals as well as feeding sensors;
- Signal Forming Cabinets performs inputting and processing of discrete and analog signals, processing of control algorithms, and formation of output control signals;
- Cross Output Cabinets receives signals from three control channels (signal formation cabinets) and forms output signals by "two out of three" mode;
- Remote Control Cabinets controls 24 actuators on the basis of Control Room signals, automatic adjustment signals and interlocks from signal formation cabinets;
- Signalling Cabinets forms control signals for process annunciation panel at Control Room and others.

The platform includes the following main modules: chassis and backplanes; power supply modules; analog input modules; normalizing converter modules, thermocouples; normalizing converter modules, resistive temperature detector; discrete input modules; discrete information input modules, pulse; potential signals input modules, high voltage; protection signal forming modules (logic modules); analog output modules, voltage; analog output modules, current; discrete output modules; potential signal output modules; solid-state output modules; relay output modules; actuator control modules; fiber optic communication modules; system diagnostic modules; fan cooling modules etc.

6.2 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.

6.3 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 (Siora et al., 2009b).

Qualification tests of FPGA-based hardware in accordance with International Electrotechnical Commission (IEC) standard 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.

6.4 Implementation of the RADIY™ platform-based I&Cs in NPPs

The RADIY™ platform has been applied to the following NPP I&Cs 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; these I&Cs were developed as one-version systems consisting of triple module redundant subsystems.

The first commissioning of the RADIY™ platform was done in 2003 for Ukrainian NPP unit Zaporozhe-1. In seven years since that time, more than 50 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 design companies of 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 RPC Radiy is the modernization of six ESFASs for Bulgarian NPP Kozloduy (three ESFASs for Kozloduy-Unit 5 and three ESFASs for Kozloduy-Unit 6).

7. Conclusion

Development and implementation of multi-version FPGA-based systems is new stage of evolution in area of improving safety of NPP I&Cs. In this chapter we discussed basic concepts of diversity as a key approach to decreasing probability of common cause failure of

safety-critical I&Cs and the taxonomic scheme of multi-version computing as a part of dependable, safe and secure computing.

Known version redundancy classification schemes were generalized in three-space matrix ("cube of diversity") taking into account features of FPGA technology. It is unique technology allows to simplify NPP I&C development and verification, realize multi-reconfiguration (dynamical function- and dependability-oriented architecting, multi-parametrical space-structural adaptation, etc.), to propose decisions with different product-process version redundancy.

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 and accessible; 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.

Described models of multi-version systems and multi-version technologies (life cycle) may support selecting of cost-effective technique and optimal architecture according with requirements to diversity, safety, reliability and limitation of applied technologies. These theoretical issues were used on development of FPGA-based I&C RADIY™ platform. Main 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. Experience of RPC Radiy has proved effectiveness of these decisions.

8. References

Altera Data Book (2001). *APEX II Programmable Logic Device Family. Data Sheet*, Ver.1.3.

Avizienis A.; Laprie J.-C., Randell, B. & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, vol.1, (2004), pp. 11-33.

Bakhmach, E.; Kharchenko, V., Siora, A., Sklyar, V. & Tokarev, V. (2009). Advanced I&C Systems for NPPS Based on FPGA Technology: European Experience. *Proceedings of 17th International Conference on Nuclear Engineering (ICONE 17)*. ISBN: 978-0-7918-3852-5, Brussels, Belgium, July, 2009.

Bobrek, M.; Bouldin, D; Holkomb, D. et al. (2009). *Review Guidelines for FPGAs in Nuclera Power Plants Safety Systems*, NUREG/CR-7006 ORNL/TM-2009/020.

Bukowsky, J. & Goble, W. (1994). An Extended Beta Model to Quantize the Effects of Common Cause Stressors, *Proceedings of ISAFECOMP,* London, October, 1994.

Gorbenko, A.; Kharchenko V. & Romanovsky A. (2009). Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability In *Methods, Models and Tools for Fault Tolerance*, M. Butler, C. Jones, A. Romanovsky, E. Troubitsyna (Eds.), pp. 324-341, LNCS 5454, Springer.

Kharchenko V.; Yastrebenetsky M. & Sklyar V. (2004). Diversity Assessment of Nuclear Power Plants Instrumentation and Control Systems, *Proceeding by 7th International Conference on PSAM and ESREL Conference*, pp.1351-1356, Vol.3, Berlin, Germany, July, 2004.

Kharchenko, V. & Sklyar, V. (Eds.). (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, ISBN 978-966-96770-2-0, Kharkiv & Kirovograd, Ukraine.

Kharchenko, V. (1999). Multi-version Systems: Models, Reliability, Design Technologies, *Proceeding of 10th ESREL Conference*, pp. 73-77, Vol.1, Munich, Germany, September, 1999.

Kharchenko, V.; Bakhmach, E. & Siora, A. (2009). Diversity-scalable decisions for FPGA-based safety-critical I&C systems: From theory to implementation. *Proceedings of the 6th Conference NPIC&HMIT*, Knoxville, Tennessee, American Nuclear Society, LaGrange Park, IL. ISBN: 978-0-89448-067-6, April, 2009.

Kharchenko, V.; Siora, A., Sklyar, V. & Tokarev, V. (2010). Diversity-Oriented FPGA-Based NPP I&C Systems: Safety Assessment, Development, Implementation, *Proceeding by 18th International Conference on Nuclear Engineering (ICONE18)*, Xi'an, China, May, 2010.

Kharchenko, V.; Siora, A., Sklyar, V., Volkoviy, V. & Bezsaliy, V. (2010). Multi-Diversity Versus Common Cause Failures: FPGA-Based Multi-Version NPP I&C Systems, *Proceedings of the 7th Conference NPIC&HMIT*, Las-Vegas, Nevada, USA, November, 2010.

Kharchenko, V.; Sklyar, V. & Tarasyuk, O. (2003). Risk Analysis of Accidents of Space-Rocket Technik: Evolution of Reasons and Tendencies. *Radio-Electronic and Computer Systems*, Vol.3, (May, 2003), pp. 135–149, National Aerospace University KhAI, Kharkiv, Ukraine.

Kharchenko, V.; Sklyar, V. & Volkoviy, A. (2007). Multi-Version Information Technologies and Development of Dependable Systems out of Undependable Components, *Proceedings of International Conference on Dependability of Computer Systems*, pp. 43-50, Szklarsla Poreba, Poland, July, 2007.

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, *Proceeding of IEEE International Conference on Dependability of Computer Systems*, pp. 339-346, Szklarska Poreba, Poland, July, 2008.

Li, B.; Xu, Y. & Choi, J. (1996). Applying Machine Learning Techniques, *Proceedings of ASME 2010 4th International Conference on Energy Sustainability*, pp. 14-17, ISBN 842-6508-23-3, Phoenix, Arizona, USA, May, 2010.

Lima, P.; Bonarini, A. & Mataric, M. (2004). *Application of Machine Learning,* InTech, ISBN 978-953-7619-34-3, Vienna, Austria.

Naser (Ed.) (2009). *Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems*, EPRI, Palo Alto, CA: 2009 1019181.

Prokhorova, Y.; Kharchenko V.; Ostroumov, B.; Ostroumov, S. & Sidorenko, N. (2008) Dependable SoPC-Based On-board Ice Protection System: from Research Project to Implementation, *Proceeding of IEEE International Conference on Dependability of Computer Systems*, pp. 312-317, Szklarska Poreba, Poland, July, 2008.

Pullum L. (2001). *Software Fault Tolerance Techniques and Implementation*, Artech House Computing Library.

Siora, A.; Sklyar, V., Rozen Yu., Vinogradskaya, S. & Yastrebenetsky, M. (2009). Licensing Principles of FPGA-Based NPP I&C Systems, *Proceedings of 17th International*

Conference on Nuclear Engineering (ICONE 17), Brussels, Belgium, ISBN: 978-0-7918-3852-5, July, 2009.

Siora, A.; Krasnobaev, V. & Kharchenko, V. (2009). *Fault-Tolerance Systems with Version-Information Redundancy*. Ministry of Education and Science of Ukraine, National Aerospace University KhAI. ISBN 978-966-96770-7-5.

Sklyar, V. & Kharchenko, V. (2007). A Method of Multi-version Technologies Choice on Development of Fault-Tolerant Software Systems. *Proceeding of Workshop on Methods, Models and Tools for Fault Tolerance*, pp.148-157, Oxford, UK, July, 2007.

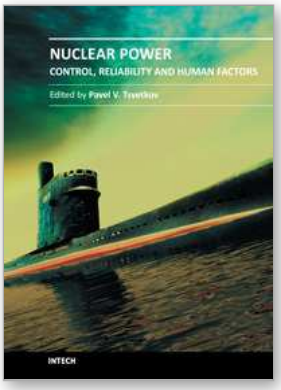
Sommerville, J. (2011). *Software Engineering*. 9th edition, Addison-Wesley, ISBN 9-780-13-703515, England.

Tarasyuk, O., Gorbenko, A., Kharchenko, V., Ruban, V. & Zasukha, S. (2011). Safety of Rocket-Space Engineering and Reliability of Computer Systems: 2000-2009 Years. *Radio-Electronic and Computer Systems,* Vol.11, (March, 2011), pp.23-45, National Aerospace University KhAI, Kharkiv, Ukraine.

Volkovij, A.; Lysenko, I., Kharchenko, V. & Shurygin, O. (2008). *Multi-Version Systems and Technologies for Critical Applications,* National Aerospace University KhAI, Kharkiv, Ukraine.

Wood, R..; Belles, R., Cetiner, M. & et al, (2009). *Diversity Strategies for NPP I&C Systems*, NUREG/CR-7007 ORNL/TM-2009/302.

Yastrebenetsky, M. (Ed.) (2004). *Safety of Nuclear Power Plants: Instrumentation and Control Systems*, Technika, Kyiv, Ukraine (Translated by NRC, USA, 2007).



Nuclear Power - Control, Reliability and Human Factors
Edited by Dr. Pavel Tsvetkov

ISBN 978-953-307-599-0
Hard cover, 428 pages
Publisher InTech
Published online 26, September, 2011
Published in print edition September, 2011

Advances in reactor designs, materials and human-machine interfaces guarantee safety and reliability of emerging reactor technologies, eliminating possibilities for high-consequence human errors as those which have occurred in the past. New instrumentation and control technologies based in digital systems, novel sensors and measurement approaches facilitate safety, reliability and economic competitiveness of nuclear power options. Autonomous operation scenarios are becoming increasingly popular to consider for small modular systems. This book belongs to a series of books on nuclear power published by InTech. It consists of four major sections and contains twenty-one chapters on topics from key subject areas pertinent to instrumentation and control, operation reliability, system aging and human-machine interfaces. The book targets a broad potential readership group - students, researchers and specialists in the field - who are interested in learning about nuclear power.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Vyacheslav Kharchenko, Olexandr Siora and Volodymyr Sklyar (2011). Multi-Version FPGA-Based Nuclear Power Plant I&C Systems: Evolution of Safety Ensuring, Nuclear Power - Control, Reliability and Human Factors, Dr. Pavel Tsvetkov (Ed.), ISBN: 978-953-307-599-0, InTech, Available from: http://www.intechopen.com/books/nuclear-power-control-reliability-and-human-factors/multi-version-fpga-based-nuclear-power-plant-i-c-systems-evolution-of-safety-ensuring

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821