Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies
NPIC&HMIT 2010, Las Vegas, Nevada, November 7-11, 2010, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2010)

MULTI-DIVERSITY VERSUS COMMON CAUSE FAILURES: FPGA-BASED MULTI-VERSION NPP I&C SYSTEMS

Vyacheslav Kharchenko, Alexander Siora, Volodymyr Sklyar,
Andriy Volkoviy, Volodymyr Bezsaliy
Research and Production Corporation "RADIY"
Centre for Safety Infrastructure-Oriented Research and Analysis,
29 Geroev Stalingrada Street, Kirovograd, 25006, Ukraine
v_s_kharchenko@ukr.net, marketing@radiy.com, v.sklyar@csis.org.ua

ABSTRACT

Key challenges and existed decisions in area of development, assessment, certification of multi-version NPP I&C systems are analyzed in context of: common cause failure (CCF) problem; experience of architecting and application of diversity-oriented software- and FPGA-based safety-critical systems; analysis of the national and international standards including diversity aspect. Some principles, methods and techniques for assessing and decreasing risks of CCF by use of multi-diversity approach are described. Multi-diversity ("diversity of diversity") is an approach based on concerted application of a few kinds of process-product version redundancy. Application of every diversity kind ensures reduction of CCF probability. Mathematical models of multi-version (MVS) and multi-diversion (MDVS) systems using different kinds of structure, temporal and version redundancy are generalized. Features of the architectures of FPGA-based MDVSs (MVFSs) are analyzed. To assess diversity (multi-diversity) level, safety and dependability of MDVSs as a whole the following methods and techniques are reviewed: set-theoretical and metric-based methods (using direct and indirect metrics); probabilistic and statistic methods; expert-based technique and combined application of different techniques. Metric-based technique for CCF vulnerabilities analysis and assessment is proposed taking into consideration of MDVS features. Experience of development and application of the NPP MVFSs based on the platform RADIY^{TM} is analyzed.

Key Words: common cause failure, multi-diversity, multi-version system, model, metric

1 INTRODUCTION

1.1 Challenges in Area of Multi-Version NPP I&C Systems

Diversity is one of the general principles of fault- and intrusion-tolerant computer-based systems designing and increasing dependability [1,2]. It is used jointly with techniques based on application of other redundancy kinds (structural, temporal) to ensure I&C systems functional safety (reliability, availability and security as well) for different critical applications including NPPs (RTSs, ESFASs), aerospace equipment (board and launch-abort control systems), railway automatics (interlocking and block signal systems) and some business-critical applications as well. It allows decreasing the risks of the common cause failure (CCF) and optimizing costs on development of the fault-tolerant systems [3].

The most probable sources of CCFs are, first of all, design faults (of software- or FPGA-based projects), multiple physical faults of redundant hardware channels (microprocessors or FPGA chips) caused by different environment impacts, and intrusions directed at identical vulnerabilities of software components of redundant channels. CCF probability of safety-critical systems may be essentially decreased due to application of one or several different types of diversity [4].

Application of the FPGA technology to develop NPP I&C systems is more reasonable in CCF context than software (microprocessor)-based technology owing to [3]: (a) decreasing risks of design faults due to simplification of development and verification processes: apparatus parallelism in control algorithms execution and realization of different functions by different FPGA components; absence of cyclical structures in FPGA projects; identity of FPGA project presentation to initial data (specification of control algorithms); (b) increasing a number of possible versions due to different technologies of FPGA-projects development using: graphical scheme and library blocks in CAD environment; especial HDL-based techniques; program code for operation in environment of microprocessor emulators implemented in FPGA as IP-Cores.

Besides, there are FPGA subtechnologies (SRAM, flash, anti-fuse) allowing to extend a set of diversity-oriented decisions and implement multi-diversity approach [4]; (c) assurance of fault-tolerance due to use of redundancy on intra- and inter-chip levels and dynamical reconfiguration, and intrusion-tolerant due to that FPGA reprogramming is possible only with the use of especial equipment.

However, there are a few challenges in area of multi-version FPGA-based NPP I&C systems (MVFS) development and implementation caused by the following [6]: (a) MVFSs are used in NPPs during last 6-7 years, i.e. these systems are a new object of analysis and still more unique one; (b) there are not any international standards, which determine requirements to use diversity for I&Cs development and application taking into account FPGA features; (c) FPGA technologies give additional possibilities to decrease CCF risks, but they should propose adequate methods and techniques of diversity assessment and selection of diversity kinds and volume to create multi-version or multi-diversion FPGA-based I&C systems, etc. It is necessary to emphasize that challenges (b) and (c) are common for multi-version systems as a whole because: firstly, existing standards are not enough detailed to make all necessary decisions concerning diversity and contain only general requirements; secondly, there are not standardized techniques of quantitative assessing diversity level and choosing optimal kinds and volume of version-redundancy to ensure required value of safety/reliability indicators and minimal cost.

1.2 Related Works

Known works, related to the current problem and taking into account features of NPP I&C systems, are divided into three groups: classification and analysis of version redundancy kinds and diversity-oriented decisions; methods and techniques of diversity level assessment, D3 analysis and evaluation of multi-version systems safety in context of CCF; multi-version technologies of safety critical systems development.

1. **Diversity classification schemes** were analyzed and generalized in [4,7]. First one is based on NUREG/CR-6303, samples two-level hierarchy and includes six main groups of version redundancy [5]: *human* or *life cycle diversity* (different design organizations/companies, management teams, designers, programmers, testers and other personnel); *design diversity* (different technologies, approaches, architectures); *software diversity* (different algorithms, operating system, computer languages, etc); *functional diversity* (different underlying mechanisms, logics, actuation means, etc); *signal diversity* (different sensed reactor or process parameters, different physical effects, different set of sensors); *equipment diversity* (different manufacturers, different versions of design, different CPU versions, etc).

Software diversity may be classified in accordance with [1,8]: *life cycle (LC) models* and *processes of development* (for example, V-model for main version and waterfall model with minimum set of processes for alternative version); *resources and means* (different human resources, languages and notations, tools); *project decisions* (different architectures and platforms, protocols, data formats, etc).

FPGA-based classification includes the following kinds of diversity [3, 10]: *diversity of electronic components* (different electronic components manufactures, technologies of production, electronic components families, etc); *diversity of CASE-tools* (different 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. General diversity classification scheme [4] was presented by "cube of diversity" with three coordinates: stage of LC, level of project decisions and kind of version redundancy.

2. There are following **methods of diversity level assessment** and evaluation of MVS dependability and safety, which were analyzed in [6]: (a) *set-theoretical and metric-oriented methods* 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; (b) *probabilistic methods* using reliability block-diagrams (RBDs), their modifications (survivability and safety block-diagrams), Markovian chains, Bayesian method, etc; (c) *statistical methods* including: 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; (d) *fault injection-based assessment* consisting of: receiving project-oriented fault profiles; performing of faults injection procedure; proceeding of data and metrics diversity calculation; calculation of reliability and safety indicators; (e) *expert-oriented methods* using 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, that can be used to assess direct diversity metrics). Expert method adds 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 of development** and choice of diversity kinds are based on use of: (a) *a model of multi-version life cycle* (MVLC) [8] and a special graph [9] and their modifications [3,10]; MVLC is presented as a bipolar G-level graph called graph of multi-version technologies (MVT) [3]; each its node corresponds metrics of diversity and cost; way form initial to final node corresponds one of the development process options and one of the architectures, and is characterized by indicators of "summarized" diversity and general costs; algorithms of MVT (optimal way in the graph) selection in accordance with criteria "diversity(safety)-reliability-cost" are described in [3,9,10]; (b) *a table of baseline diversity strategies* [5] and corresponding metrics; strategy of diversity (MV) is a set of general criteria and rules defining principles of formation and selection of version redundancy kinds and volume, i.e. selection of MVT [3]; the classification of diversity strategies developed in the [5] 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 in accordance with metrics determined by expert.

1.3 Goal and Structure of the Paper

In spite of the intensive researches and practical developments in area of MVSs there are some problems of specifying of concepts associated with CCF and multi-version computing, and assessing systems in which several kinds of process-product diversity are applied as well. Besides, it is necessary to take into consideration features of FPGA technology and experience of NPP MVFSs implementation.

Goal of the paper is generalization of CCF concept in context of multi-version computing (MVC) including MVCs based on use of a few version redundancy kinds (multi-diversion systems) and development metric-based models for assessment of such systems. Structure of the paper is the following. Main concepts concerning multi-diversity principle, CCF taxonomy and approach to assessment of CCF probability are discussed in Section 2. Section 3 elaborates the models of multi-version and multi-diversion systems taking into account some features of FPGA technology. The metric-based method of

assessing these systems is described in Section 4. Possibilities of the FPGA-based platform RADIY™ for development of multi-version systems and some results of implementation in NPP I&Cs are analyzed in Section 5. Finally, Section 6 concludes the paper and presents directions of future researches.

2 MULTI-DIVERSITY AND COMMON CAUSE FAILURES: MAIN CONCEPTS

2.1 Multi-Version Computing and Principle of Multi-Diversity

Concept of multi-version computing which is a part of dependable computing based on use of diversity approach includes the following elements [4,7]: *version* – an option of different realization of identical task (product or process); *version redundancy* (VR) – a kind of redundancy in which different versions are used; *diversity or multiversity* (MV) – a principle providing use of several versions and performance of the same function (realization of a product or process) by two and more options; *multi-version system* (MVS) – a system in which a few versions-products are used; *multi-version technology* (MVT) – a 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; *multi-version project* (MVP) – 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; *multi-version life cycle* – a collection of interconnected processes and products realized by use of version redundancy and ensuring development of MVS (or one-version system using MVT) in accordance with specification; *strategy of diversity* – a set of general criteria and rules for selection of MVTs; *diversity metric* – an indicator of local process/product diversity level or summarized MVS diversity level.

Interconnection of the listed concepts is presented by taxonomy scheme suggested in [4]. In addition to described concepts we propose to specify a few terms and models for multi-version computing performed by use of two or more kinds of version redundancy. Such computing is based on principle of *multi-diversity* or "*diversity of diversity*" (Di2). The essence of the Di2 principle consists in concerted application of a few kinds of process-product version redundancy in frameworks of the system. Every kind of diversity is peculiar echelon of defence in depth decreasing risks of CCFs.

2.2 Common Cause Failures and Common Time Failures: Elements of Taxonomy

CCF occurs when e_f (two or more) channels (versions) of redundant *e*-channel (*e*-version) system fail simultaneously and there is a common reason caused this event. Thus, CCF is a multiple failure (MF). It is fundamentally different single failure (SF). On the other hand, multiple failures occur as a result of not only one (common) cause. Multiple failures may be caused by influence of a few different reasons if these reasons concur or spread of influence time values is less than speed of on-line testing and reconfiguration means. In this case MF may be called as a common time failure (CTF). Hence, CCF and CTF are multiple failures or common event failure (CEF).

Taxonomy scheme of multiple failures is shown in Fig. 1. Attributes of the classification form simple hierarchy. CCFs and CTFs may be additionally divided into two groups in accordance with number of failures (partial and full CCFs, i.e. PCCFs and FCCFs, and partial and full CTFs, i.e. PCTFs and FCTFs) and distinguishability of channel output data on failures, i.e. distinguishable (DCCFs, DCTFs) and undistinguishable (UDCCFs, UDCTFs) failures.

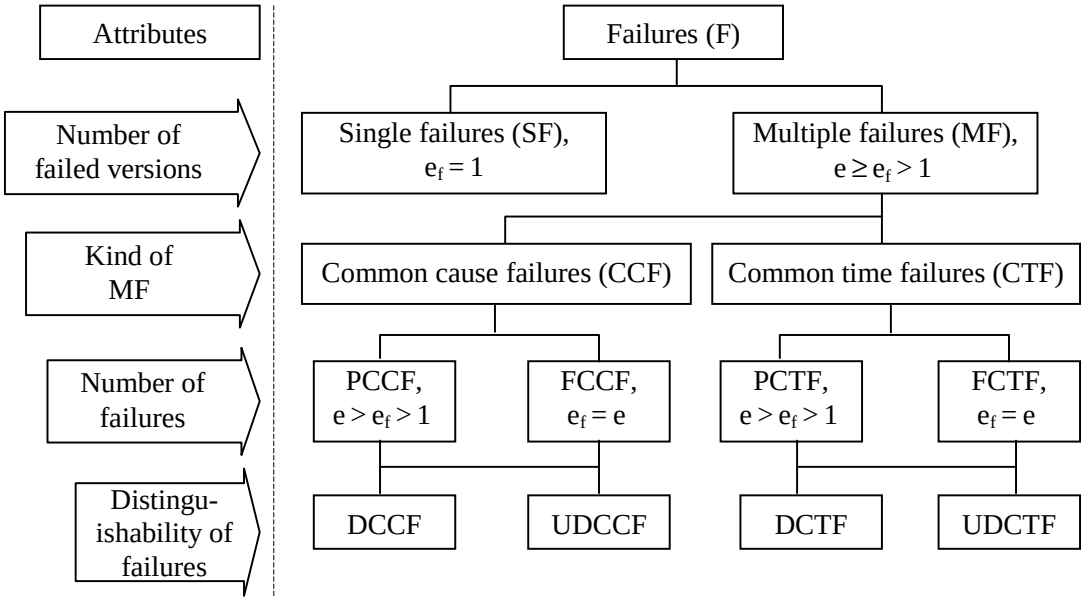

Figure 1. Classification of multiple failures.

Authors of works related to NPP I&C safety problems, first of all, attend to CCFs analysis. However, CTFs are important objective of research as there are examples of serial failures caused by attacks on vulnerabilities of redundant channels and other reasons. Besides, very important problem, in our opinion, is the analysis of distinguishability of effect failures, because it allows determining of moment of partial or full CCFs (or CTFs) by simple means of channel output data comparison.

2.3 Metric-Based Assessment of CCFs

To assess probability of common cause failure it is necessary to calculate the metrics for different CCF vulnerabilities. Convenient form for that is Eiler's diagram (Fig. 2). Circles of these diagrams correspond to sets of version defects (faults) causing failure. For one-version and one-cannel system (Fig. 2,a) number of faults equals N ($N = Card\ F$) and any fault of set F is fatal (and is an equivalent of CCF). In this case metric of CCF β determining relation of number of CCFs to total number of failures equals one (and $\alpha = \beta = 1$).

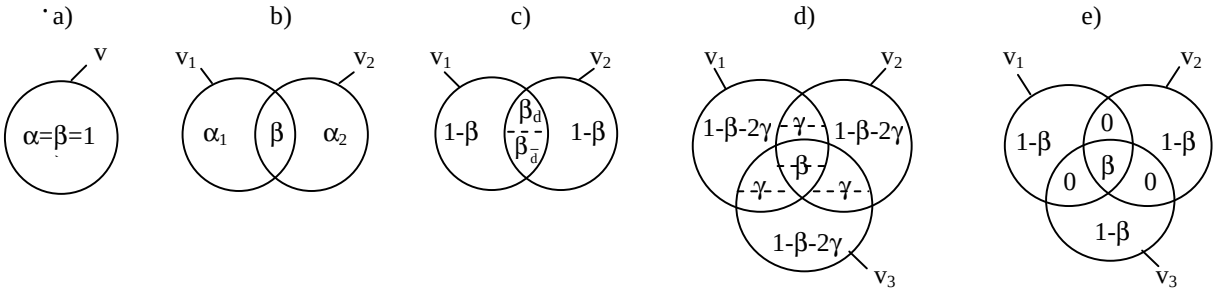

Figure 2. Diagrams of failures of one-version (a), two-version (b,c) and three-version (d,e) systems.

For two-version system (Fig. 2,b,c) CCF metric $\beta = N_{CCF} / N$, $N_{CCF} = Card F_1 \cap F_2$; value of N may be calculated as an arithmetic mean $N = (N_1 + N_2) / 2$, $N_i = Card\ F_i$; SF metric $\alpha_i = 1 - \beta$; DCCF metric $\beta_d = N_{DCCF} / N$; UDCCF metric $\beta_{\bar{d}} = N_{UDCCF} / N$; $\beta = \beta_d + \beta_{\bar{d}}$. Besides, metrics of relative number of DCCFs and UDCCFs may be used: $\beta_d^* = \beta_d / \beta$, $\beta_{\bar{d}}^* = \beta_{\bar{d}} / \beta$.

For three-version system (Fig. 2,d) $\alpha = 1 - \beta - 2\gamma$, where γ is PCCF metric (metric determining part of CCFs of any two versions, $\gamma = N_{PCCF} / N$). Metrics of distinguishable and undistinguishable PCCFs are calculated by analogy β_d and $\beta_{\bar{d}}$. If $\gamma = 0$ (Fig. 2,e), $\alpha = 1 - \beta$. This approach is based on results described in [9] and may be extended to systems in which a set of faults adds a set of vulnerabilities attacked by external system. In Section 4 metric-based assessment will be used to calculate probability of CCF and MDVS safety indicators.

3 MODELS OF MULTI-DIVERSION SYSTEMS

3.1 General Set-Theoretical Models of Multi-Diversion Systems

One-version $W(1)$ and multi-version $W(n)$ systems are defined by 4 and 6 variables [7]:

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

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

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

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

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

System $W(1)$ may be structurally 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: subset of versions $\Delta v_s \subset v_j$ for obtaining output signal Z_i; vector $\vec{t_s}$ of version v_{ij} initialization time ($\vec{t_s} = \{t(v_{i1}),..., (v_{in_i})\}$); mean of transforming η_s values $z_i(v_{i1}),\ldots, z_i(v_{in_i})$ in output signal Z_i^s. Hence,

$$\forall \psi_s \in \Psi: \psi_s = \{ \Delta v_s, \vec{t_s}, \eta_s\} \text{ and } \quad Z_i^{(s)} = \eta_s [z_i(v_{ij}), \vec{t_s}], \ v_{ij} \in \Delta v_s.$$

There are the following means of transforming η_s: (a) the conjunctive, when $Z_i^s = \mathrm{V}\, z_i(v_{ij})$; (b) the time conjunctive, when $Z_i^s = \mathrm{V} z_i(v_{ij})\sigma_{ij}$, 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 – 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, at 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. In this case it is true that

$$m \le \sum_j m_{prdj} + \sum_j m_{prñj} ,$$

where m_{prdj} and m_{prcj} – cardinal numbers of ΔR_{prdj} and ΔR_{prcj} correspondingly.

Thus, different diversity kinds, $r \in R$, are accumulated in final versions of multi-version system. It is described by special mapping $\Theta : R \to V$. Mapping Θ may be presented by Boolean matrix $\| \theta_{dj} \|$, $d = \overline{1,m}$, $j = \overline{1,n}$, where θ_{dj} =1, if diversity kind r_p is used in version v_j, and if not θ_{dj} = 0, than 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 set of versions V and set of redundant channels $C=\{c_q, q=1,..., l\}$. This correspondence may be defined by mapping Q: $V \to C$. This mapping is presented by Boolean matrix $Q = \| \omega_{jg} \|$, $d = \overline{1,m}$, $g = \overline{1,l}$, where ω_{gj}=1, if version v_i is realized by channel c_j, and if not ω_{gj} = 0, than model of multi-version (multi-diversion) system is the following:

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

Multi-version systems with temporal redundancy and p iterations of algorithms (performing functions) are indicated as $W(n,m,n,p)$ dividing number of parallel (structural) versions n_c, and sequential versions realized by use one channel.

Set of input signals X may be decomposed for different versions if

$$X = \bigcup_j \tilde{O}_j , \forall j_1 j_2 \in \overline{1,n}, \; j_1 \neq j_2 : \; X_{j1} \cap X_{j2} \;\; \tilde{O}_{j1} \bigcap \tilde{O}_{j2} = \phi.$$

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 W_{AX}. A special function-transformer Π_x (or transformers Π_{xj}) should be specified in addition to alphabet X for description of such systems:

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

Some schemes of different MVS and MDVS types are shown on Fig. 3.

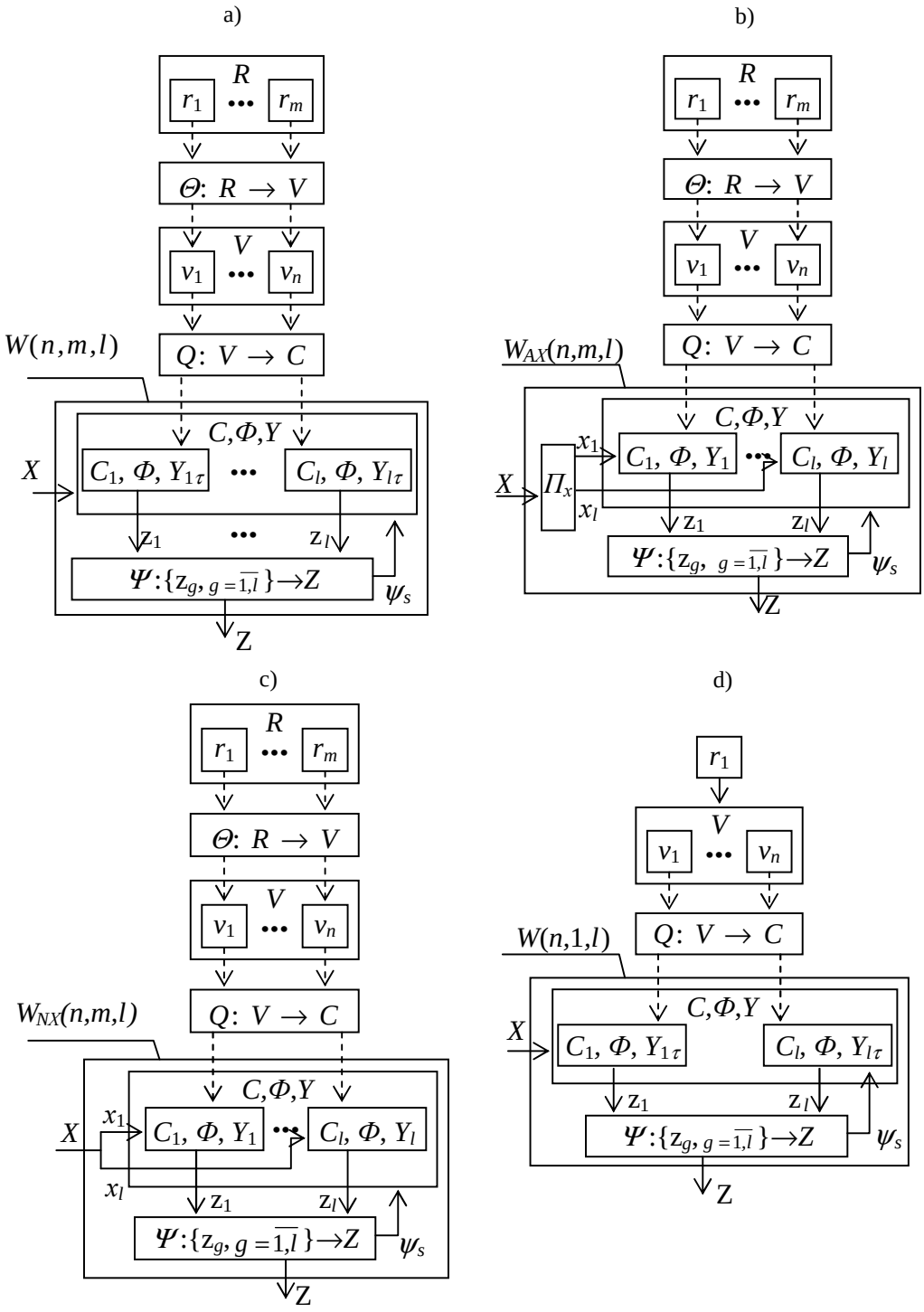

Figure 3. Models of the systems *W (n,m,l)* (a), $W_{AX}(n,m,l)$ (b), $W_{NX}(n,m,l)$ (c), *W(n,1,l)* (d).

3.2 Models of Multi-Diversion FPGA-Based Systems

Every version v_j of multi-diversion FPGA-based system performing safety critical control functions in NPP I&Cs may be represented by a composition of two interconnected automata (monitoring or checking Ξ_{Mj} and control Ξ_{Cj} automata) [3].

Monitoring automaton Ξ_M of the version analyses output signals X (or X_j) from sensors and forms its status code Y_{Cj}. This automaton may be presented as a set of subautomata Ξ_{Mh} processing data from different sensors D_h (groups of sensors). Control automaton Ξ_{Cj} forms control signals Z_j in accordance with signals Y_{Cj}. Automaton Ξ_Ψ processes signals Z_j from automata Ξ_{Cj}. These automata are described by model of finite state machine or HDL-based model. Automata Ξ_{Mj}, Ξ_{Cj} and channel as a whole are realized using different diversity kinds in accordance with section of "cube of diversity" and matrix of project decisions [4,7].

Several options of multi-diversion architectures are possible and effective for FPGA-based I&Cs. Such options may be classified in accordance with degree of diversity coverage (I&Cs with a complete or partial diversity and multi-diversity) and diversity depth (I&Cs with a common or separate diversity and multi-diversity) [3,4].

4. ASSESSMENT OF MULTI-DIVERSION SYSTEMS

To assess MDVS safety in context of CCF let's analyse a system with three types of faults: physical faults of hardware (Hp), design faults of hardware (Hd) and design faults of software (Sd). These faults are assessed by three metrics α_{Hp}, α_{Hd} and α_{Sd}. For one-version (1,0)-system $\beta = \alpha = \alpha_{Hp}+\alpha_{Hd}+\alpha_{Sd} = 1$. Eiler's diagram of fault set for this system is shown in Fig. 4,a.

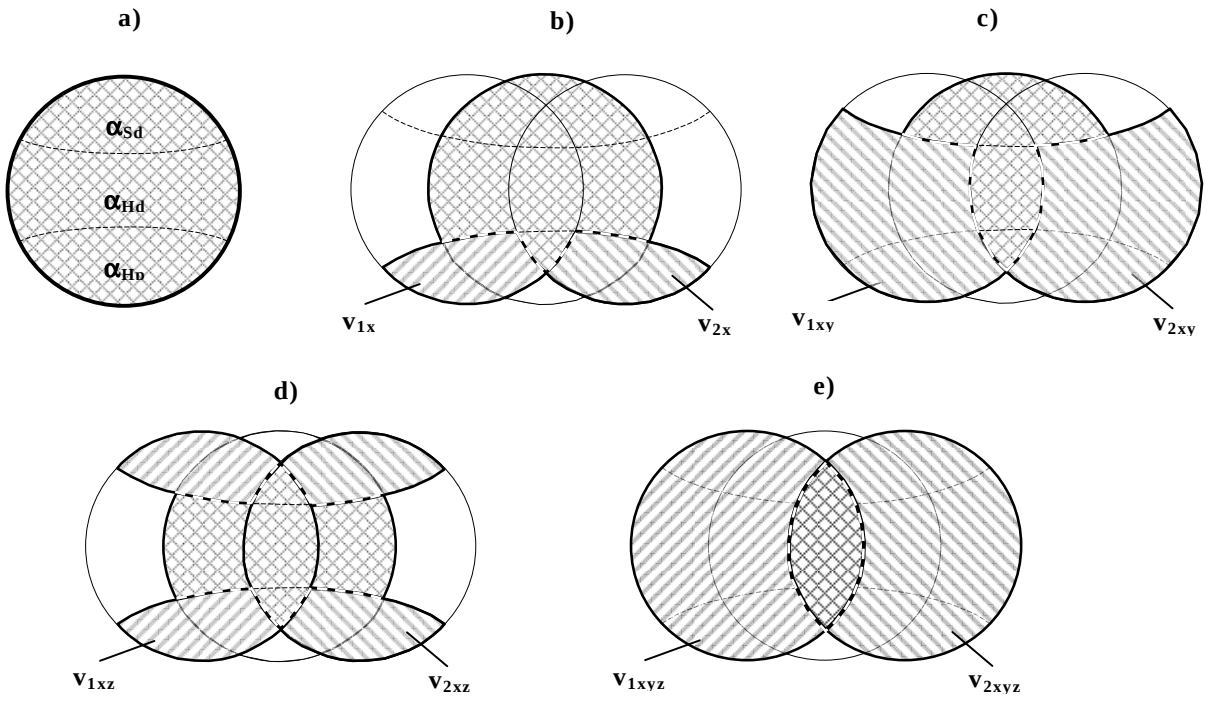

Figure 4. Diagrams of failures of (1,0)- (a), (2,1)- (b), (2,2)- (c,d) and (2,3)- (e) systems.

Eiler's diagrams of fault sets for two-version systems with different kinds of redundancy and diversity are shown in Fig. 4,b-e. Sets of SFs for versions v_1,v_2 marked by different single hatching. Sets of CCFs of two-version systems (common faults for versions v_1,v_2) marked by double (lattice) hatching. Particularly, the following systems are analyzed:

- **(**2,1)-system with one diversity kind *x* for hardware (which may be realized by ordinary structure redundancy) (Fig. 4,b, versions v_{1x}, v_{2x}); $\beta_x = \alpha_{Hd} + \alpha_{Sd} + \beta_{Hp}$, $\alpha_{1x\,(2x)} = \alpha_{Hp} - \beta_{Hp}$;

- (2,2$_{xy}$)-system with two diversity kinds *x*, *y* for hardware (may be realized using of chips from different manufactures, for example, FPGA/SRAM chips of Altera and Actel/Flash) (Fig. 4,c, versions v_{1xy}, v_{2xy}); $\beta_{xy} = \alpha_{Sd} + \beta_{Hd} + \beta_{Hp}$, $\alpha_{1xy\,(2xy)} = \alpha_{Hp} + \alpha_{Hd} - \beta_{Hp} - \beta_{Hd}$;

- (2,2$_{xz}$)-system with structure redundancy/diversity *x* for hardware and diversity *z* of software (which may be realized by use of different languages, different IP cores for FPGA designs, etc.; but chips in this case are identical) (Fig. 4,d, versions v_{1xz}, v_{2xz}); $\beta_{xz} = \alpha_{Hd} + \beta_{Sd} + \beta_{Hp}$, $\alpha_{1xz\,(2xz)} = \alpha_{Hp} + \alpha_{Sd} - \beta_{Hp} - \beta_{Sd}$;

- (2,3)-system with three diversity kinds *x*, *y*, *z* (Fig. 4,e, versions v_{1xyz}, v_{2xyz}); $\beta_{xyz} = \beta_{Hp} + \beta_{Hd} + \beta_{Sd}$, $\alpha_{1xyz\,(2xyz)} = \alpha_{Hp} + \alpha_{Hd} + \alpha_{Sd} - \beta_{Hp} - \beta_{Hd} - \beta_{Sd}$.

Reliability block diagrams for analyzed systems shown in Fig.5, a-e (λ is failure rate of version). Dotted lines of blocks correspond to connected elements of versions.

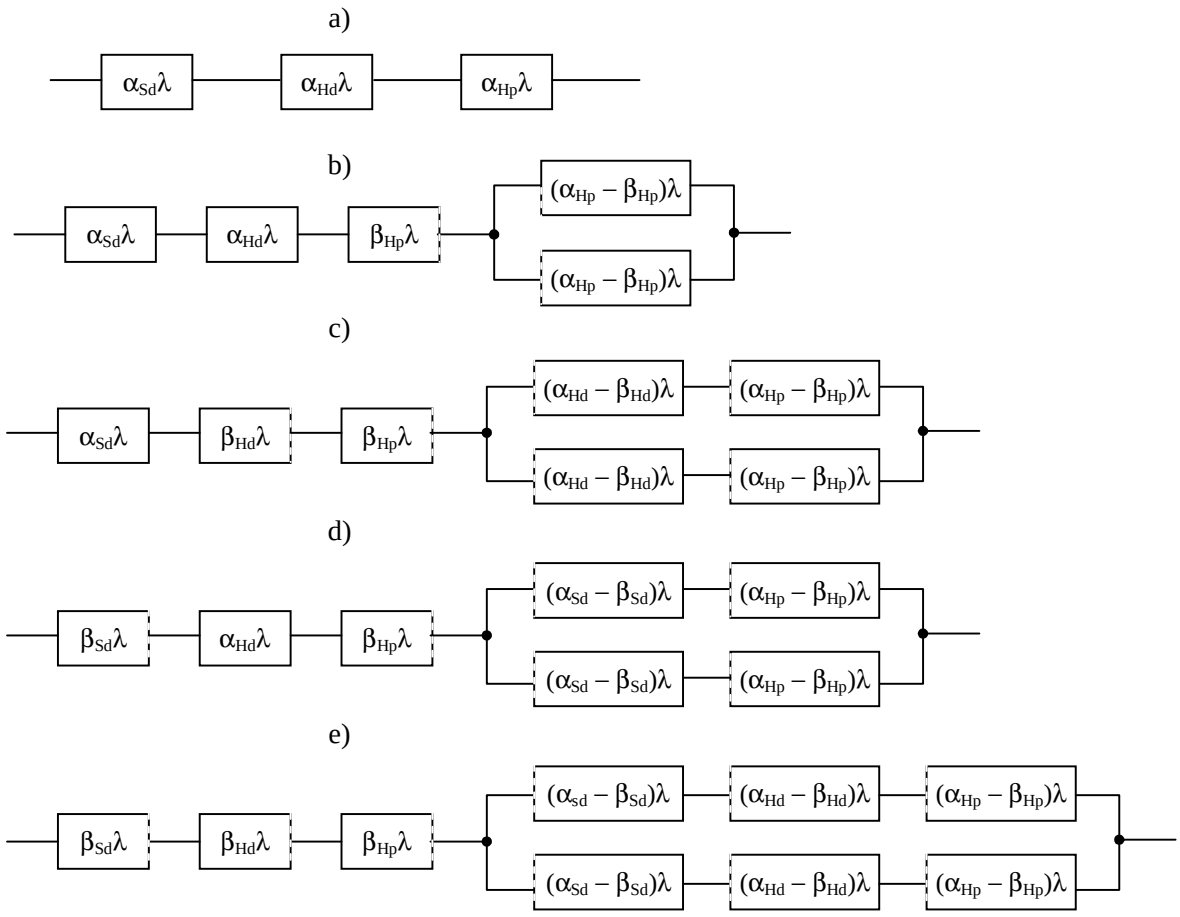

Figure 5. Reliability block diagrams for systems shown in Fig. 4.

Values of metrics α and β are determined using statistics of testing and operation failures, expert methods based on special check-tables, etc. Illustrative results of modeling for MDVSs described above are shown in Fig. 6. The initial data for modeling are the following: $\lambda = 3 \cdot 10\text{-}5$ 1/h, $\beta_{Hp}=0$, $\beta_{Hd} = 0.2$, $\beta_{Sd} = 0.8$; values of SF metrics for one version $\alpha_{hp}= \alpha_{hd} = \alpha_{sd} = 1/3$.

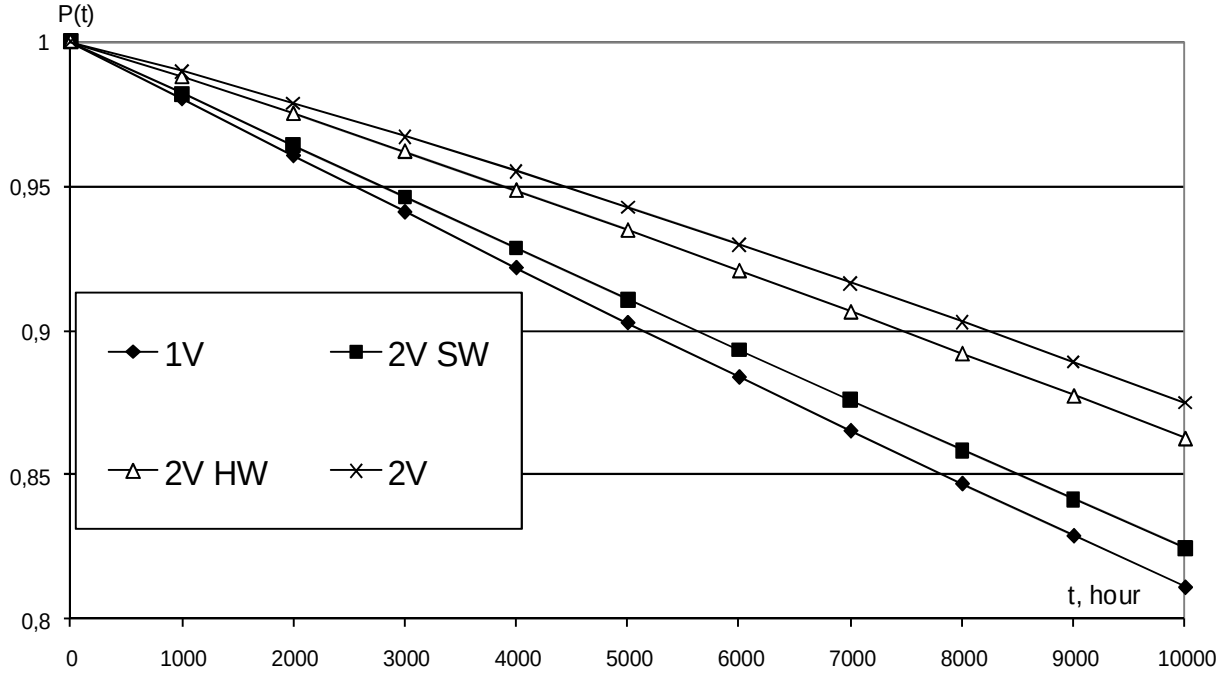

Figure 6. Diagrams for probability of up-state for (2,1)-system (1V), (2,2$_{xy}$)-system (2VHW), (2,2$_{xz}$)-system (2VSW), (2,3)-system (2V).

5 FPGA-BASED PLATFORM RADIY™ FOR MULTI-VERSION NPP I&CS

The platform RADIY™ developed and produced by RPC Radiy is an example of a dependable and scalable FPGA-based I&C platform ensuring designing and manufacturing multi-version systems [3]. Last generation of the FPGA-based I&C systems was developed using principle of multi-diversity. Principle of multi-diversity was realized through the following diversity kinds: (a) equipment diversity is provided by different electronic components from one or different manufactures of FPGA chips, different technologies of programmable components (FPGAs and microcontrollers), different schemes of units; (b) design diversity is provided by different tools for development and verification; (c) life cycle (human) diversity is provided by different teams of developers and verifiers.

Besides, the platform RADIY™ permits to configure a lot of multi-version architectures with ensuring of diversity on their different levels without essential changing of hardware and software modules. This I&C platform RADIY provides scalability of multi-diversity by changing diversity kinds, architecture decisions and criteria of choice of volume diversity. During last seven years 22 main and diverse sets were installed on 11 reactor units of Ukrainian NPPs and confirmed high safety of multi-version systems.

6 CONCLUSION

In this paper some challenges and decisions in area of development and assessment of multi-version NPP I&C systems are analyzed in context of CCF problem were discussed. We proposed and analyzed multi-diversity ("diversity of diversity") approach based on concerted application of a few kinds of process-product version redundancy. This approach allows decreasing risks of CCFs and increasing MVS safety. It is confirmed by experience of development and application of the platform RADIY^{TM}-based NPP I&C systems.

The set-theoretical and automata models of MDVSs using different kinds of structure, temporal and version redundancy were generalized. These models are base for development different software- and FPGA-based architectures. Metric-based technique for CCF analysis and multi-diversity assessment, probabilistic methods may be applied to estimate indicators of safety and dependability of MDVSs. Direction of future research is development detailed technique of D3 analysis of MDVSs and tool for support of safety assessment.

7 REFERENCES

1. L. Pullum, *Software Fault Tolerance Techniques and Implementation*, Artech House Computing Library (2001).
2. B. Littlewood, P. Popov, "Modelling Software Design Diversity - a Review", *ACM Computing Surveys.* **No33**, pp. 177-208 (2001).
3. V. Kharchenko, V. Sklyar (edits), *FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment*, RPC Radiy, National Aerospace University KhAI, State STC on Nuclear and Radiation Safety, Ukraine (2008).
4. V. Kharchenko, A. Siora, E. Bakhmach, "Diversity-Scalable Decisions for FPGA-Based Safety-Critical I&Cs: from Theory to Implementation", *Proceedings of the 6th Conference NPIC&HMIT*, Knoxville, Tennessee, USA (2009).
5. R. Wood, R. Belles, M. Cetiner et al, *Diversity Strategies for NPP I&C Systems*, NUREG/CR-7007 ORNL/TM-2009/302 (2008).
6. V. Kharchenko, A. Siora, V. Sklyar, et al, "Diversity-Oriented FPGA-Based NPP I&C Systems: Safety Assessment, Development, Implementation", *Proceeding by 18th International Conference on Nuclear Engineering (ICONE18)*, Xi'an, China, 10p. (2010).
7. A. Siora, V. Sklyar, V. Kharchenko, "(n,m)-Version Systems: Taxonomy, Models and Technologies", *Bulletin of Kharkiv National University: Mathematical Modelling. Information Technology. Automated Control Systems*, **No4**, pp.34-47 (2008).
8. A. Volkovoy, I. Lysenko, V. Kharchenko, O. Shurygin /V. Kharchenko (ed.), *Multi-Version Systems and Technologies for Critical Applications*, National Aerospace University KhAI, Kharkiv, Ukraine (2009).
9. V. Kharchenko, *Foundation of Defect-Tolerant Digital Systems with Version Redundancy*, Department of Defense, Kharkiv Military University, Ukraine (1996).
10. A. Siora, V. Krasnobaev, V. Kharchenko /V. Kharchenko (ed.), *Fault-Tolerant Systems with Version-Information Redundancy*, National Aerospace University KhAI, Kharkiv, Ukraine (2009).