AUTHORS:
VYACHESLAV KHARCHENKO, OLEXANDR SIORA
VOLODYMIR SKLYAR, ANDRIY VOLKOVIY

Defence-in-Depth and Diversity Analysis of FPGA-Based NPP I&C Systems: Conception, Technique and Tool

Defence-in-Depth and Diversity (D3) as a fundamental principle for NPP safety assurance is analyzed. Reactor trip systems and engineered safety features actuation systems as a I&C part of NPP Defence-in-Depth infrastructure are multiversion systems (MVSs) according to international practice and standards requirements. The features of D3 analysis for multiversion FPGA-based NPP I&Cs are described. The requirements of existed standards are not enough detailed to make decisions concerning D3 and diversity taking into account FPGA features. Standardized and detailed techniques should be developed to assess actual diversity, choose types and volume of diversity according to criterion "required safety/ minimal cost". The technique based on application of CMD (check-list & metrics & reliability block diagrams/Markov's models) approach is suggested to assess MVS safety. Structures of multi-version I&C systems based on the Radiy FPGA platform are assessed by use of these techniques. Tool for D3 analysis of multi-version NPP I&C systems is described.

1.0 INTRODUCTION

1.1 Motivation

Defence-in-Depth and Diversity (D3) is one of the fundamental principles for NPP safety assurance. Reactor trip systems (RTS) and engineered safety features actuation systems (ESFAS) are I&C part of NPP Defence-in-Depth infrastructure [1]. These I&C systems (first of all, RTS) are multi-version systems. FPGA technology allows creating more reliable and safe NPP I&C systems including multi-version systems based on different version redundancy types that are specific for FPGA-oriented products and processes [2]. It is confirmed by industrial experience of FPGA technology application in safety related NPP I&C systems [3]. Hence, features of this technology should be taken into account to carry on D3 analysis of FPGA-based NPP I&C systems.

1.2 Work related analysis

Known works, related to the problem of D3 analysis are divided into following groups: basic concepts of D3 analysis for NPP I&C systems; methods and techniques of diversity assessment as a part of D3 analysis, multi-version systems safety indicators evaluation; experience of development and implementation of FPGA-based NPP I&C.

Basic concepts of D3 analysis for NPP I&C systems were described in [1]. This work specifies features of NPP I&C systems in context of D3.

I&C systems should complement non-I&C features to ensure safety functions. I&C should not degrade the independence between the different barriers to radioactive release. This could be accomplished by separate systems protecting each barrier and D3 within integrated I&C systems. Besides, the D3 strategy should be stated as part of the overall I&C systems architectural design.

Methods of diversity level assessment and evaluation of MVS dependability and safety were analyzed in [4-7]. There are the following methods:

(a) theoretical-set and metricoriented methods based on set diagrams for design, physical and interaction faults and vulnerabilities of versions, calculation of diversity metrics by use of set diagrams and other data about of versions testing;

(b) probabilistic and RBD-based methods, Markovian chains, Bayesian methods;

(c) statistical methods using testing and operation data about version faults and software reliability growth models;

(d) fault injection-based assessment based on project-oriented fault profiles, performing of faults injection procedure, proceeding of data and calculation of reliability and safety indicators.

Multi-version technologies of development are based on use of: (a) a bipolar G-level graph [8], (b) a table of baseline diversity strategies [9] and corresponding metrics. The classification of diversity strategies 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.

Analysis of the references allows concluding that there are not enough detailed techniques to make decisions concerning D3 and diversity taking into account FPGA features.

1.3 Objective and Structure of the Paper

Objective of the paper is to present approach and technique of the D3 analysis for FPGA-based NPP I&Cs. Structure of the paper is the following. The D3 principle in context of NPP I&C and FPGA technology is analysed in the second Section. Features of multi-version FPGA-based I&C systems development are described in the third Section. The technique based on application of CMD (check-list & metrics & reliability block diagrams/Markov's models) approach to assess multi-version systems safety is suggested in the forth Section. Last Section concludes the paper and presents some directions of future researches and developments.

2.0 D3 ANALYSIS IN CONTEXT OF NPP I&C SYSTEMS

2.1 Standards Related to D3 Principle

Main requirements regarding D3 principle and features of its implementation are described in the following standards and technical reports of IAEA:

- NUREG-0493, A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System, March, 1979;
- NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection systems, October, 1994;
- Defence in Depth in Nuclear Safety, report of the International Nuclear Safety, Advisory Group, INSAG-10, Vienna, IAEA, 1996;
- Assessment of Defence in Depth for NPPs, Safety report series, No 46. Vienna, IAEA, 2005;
- NUREG/CR-7007, 2009, Diversity Strategies for NPP Instrumentation and Control Systems, December, 2008.

2.2 Analysis of D3 Principle

Defence in depth (D2) is a hierarchical deployment of different levels of diverse equipment and procedures [1]:

- to prevent the escalation of anticipated operational occurrences,
- to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

D2 consists of a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive material and workers, the public or the environment, during normal operation, anticipated operational occurrences (and, for some barriers, accidents at the plant [10].

INSAG defines five levels of D2:

1. prevention of abnormal operation and failures;

2. control of abnormal operation and detection of failures;
3. control of accidents within the design basis;
4. control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents;
5. mitigation of radiological consequences of significant releases of radioactive material.

2.3 Role of I&C Systems in Employment of D3 Principle

Defence (D-1) in Depth (D-2) and Diversity (D-3) is one of the fundamental principles for NPP safety assurance, and:

- D-1,2: a set of different (diverse) defence echelons (levels, safety-supporting "filters",…);
- D-3: diversity of echelon elements (versions). Hence, D1,2 is diversity as well, but it's "horizontal" diversity (echelon by echelon), D-3 is "vertical" diversity (version by version). Role of I&C systems in employment of D3 principle consists in the following:
  - I&C systems are echelons (one of the echelons or control means for a few echelons);
  - I&C systems (RTS and sometime ESFAS) are multiversion systems according to international practice and standards requirements.

Number of project decisions for multi-version NPP I&Cs as a D3 part increases due to FPGA technologies application, and the following their features [2,3]:

- existed technologies of FPGA projects development (graphical scheme and library blocks in CAD environment; special hardware describing languages VHDL, Verilog, Java HDL, etc; microprocessor emulators which are implemented as IP-cores) allow increasing a number of possible options of different project versions and multi-version I&Cs;
- fault-tolerance, data validation and maintainability are improved due to use of: redundancy for intra- and inter-crystal levels; possibilities of implementation of multi-step degradation with different types of adaptation; diversity and multi-diversity implementation; reconfiguration and recovery in the case of component failures; improved means of diagnostics.

3.0 DIVERSITY AND MULTI-VERSION FPGA-BASED NPP I&C SYSTEMS

3.1 Analysis of standard requirements

Diversity is part of the D3 principle. The diversity principle is used to ensure reliability, functional safety of I&C systems for NPPs and other critical applications (aerospace control systems, railway interlocking and block signal systems, etc.) [5].

The standard IEC 60880: 2006 defines the use of diversity "as a means of enhancing the reliability of some systems and reducing the potential for certain CCF". In this case different software and hardware are applied to develop redundant channels. It allows decreasing the risks of the most dangerous incidents (common cause failure (CCF)).

The most probable sources of CCF are software design faults or multiple physical faults of different channels. A lot of standards and technical reports contain requirements to diversity and recommendations regarding to assessment of multi-version systems:

- 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 comp.-based syst. performing category A functions;
- IAEA NS-G-1.3: 2002. I&Cs important to safety in NPPs.
- IEEE std.7-4.3.2:1993. IEEE standard criteria for digital computers in safety systems of NPPs;
- NUREG/CR-6303:1993. Method for Performing Diversity and Defense-in-Depth Analyses of RPSs;
- NP 306.5.02/3.035: 2000. Requirement on nuclear and radiation safety to I&Cs important to safety in NPPs (Ukraine).
- NUREG/CR-7007 ORNL/TM-2009/302 Diversity Strategies for NPP I&Cs;
- EPRI 1019183 -2009. Effects of Digital I&Cs D3 on Risk in NPPs;
- EPRI 1019182 -2009. Protection Against Digital CCF Combining Defensive Measures and Diversity Attributes;

» EPRI 1019181 -2009. Guidelines on Use of FPGAs in NPP I&Cs.

They concern:

» systems which must/should be developed and produced using diversity approach;

» diversity types to decrease common cause failure probability of NPP I&Cs: there are different classifications;

» features, benefits and limitations of diversity implementation;

» postulation of necessity regarding:

a. determination of required diversity volume;

b. assessment (justification) of real diversity level;

c. risks associated with the use of diversity.

However, the standards are not enough detailed to make assessment procedure. The most representative document is NUREG7007 [9]).

The described technique allows assessing level of diversity using general metrics; values of metrics are determined in advance. But this technique does not permit to calculate safety indicators of MVS safety.

Some aspects and procedures of assessing FPGA-based NPP I&C systems presented in [2,5] taking into account development and verification process features and types of different version redundancy for FPGA projects.

Thus, there are two main problems in the area of diversity approach application:

» choice of product-process diversity types (strategies, types, diversity seeking decisions, etc.);

» assessment of multi-version systems (diversity assessment, safety assessment, reliability assessment, etc.).

Inaccurate evaluation of actual level of diversity (and system safety in whole) is one of the challenges. If the assessment result is underestimated, it causes additional efforts, costs and increases time of implementation. If the assessment result is overestimated, it causes inadmissible increasing of CCF risks.

3.2 Challenges Regarding to FPGA Application in Multi-Version NPP I&C Systems

There are a few challenges regarding to development of NPP I&C systems as a whole and FPGA-based I&C systems in particular (see Table 1). Main conclusions concerning FPGAbased MVS development and implementation experience are the following [5]:

» FPGA-based multi-version I&Cs are used in NPPs during last 10 years, i.e. these systems are new object of analysis and still more unique one;

» FPGA technologies give additional possibilities to develop MVSs and ensure high safety and reliability;

» processes of FPGA project development are similar to processes of SW-based project development. FPGA project product is similar to HW-based project product (hard logic);

» there are no any international standards determined requirements to use of diversity for I&Cs development and application taking into account FPGA features.

3.3 Classification of Diversity Types

General diversity classification includes the following types:

» human life or cycle diversity (different design organizations/companies, management teams within the same company, designers, programmers, testers, installers, or certification personnel);

» design diversity (different technologies, approaches within a technology, architectures);

» software diversity (different algorithms, logic and program architecture, timing, or order of execution, operating system, computer languages);

» functional diversity (different underlying mechanisms, purpose, function, control logic, or actuation means, response time scale);

» signal diversity (different reactor or process parameters sensed by different physical effects, different reactor or process parameters sensed by the same physical effect, the same process parameter sensed by a different set of similar sensors);

Table 1 | Challenges of FPGA Technology Application in Multi-Version NPP I&C Systems

Aspects	Challenges	Key Questions
New technologies, possibilities and risks	New technologies (including FPGA) ensure new possibilities to implement diversity approach but they can create new risks and deficits of safety.	How we should use these possibilities?
Standards requirements	Existed standards don't contain detailed requirements and techniques to assess and apply diversity approach for FPGAbased NPP I&Cs.	What should be severity of regulation for DA implementation?
CCF risk decreasing	Key problem is decreasing number of common version faults (CVF). The CVF number (CCF probability) may be decreased using several types of diversity (multi-diversity or "diversity of diversity").	What type (types) and how much versions developers should use?
Risk assessment	Problems of CCF risks assessment: inaccurate assessing either increases risk of fatal failure (understated assessment) or increases risk of unreasonable costs.	What approach, indicators, methods, techniques, we should use to assess actual diversity level and multi-version I&C systems safety?
Uniqueness of MVSs	There are a lot of examples of diversity approach implementation but comparative analysis of MVS application is not enough.	How we may compare experience of different DA applications?

» equipment diversity (different manufacturers of fundamentally different designs, different manufacturers of same design, different versions of the same design, different CPU architectures, CPU versions, printed circuit board designs, different bus architectures).

FPGA diversity classification includes the following types [2,4]:

» diversity of electronic elements (different electronic elements manufactures, technologies of electronic elements production, electronic elements families, electronic elements from the same family);

» diversity of CASE-tools (different developers, kinds and configurations of CASE-tools);

» diversity of projects development languages (joint use of graphical scheme languages, hardware description languages (HDL) or/and IP-cores, different HDLs, different IP-cores);

» diversity of specifications (different specification languages), etc.

Further we'll use NUREG-based classification harmonized taking into account FPGA technology features. Fragment of the diversity types classification for FPGA-based I&C systems is presented in the Table 2. In this case four types of diversity for FPGA-based I&C systems are detailed (equipment, design, software and human diversity). There are dependencies between different types of diversity (for example, between A1 and A2, between A1 and C2, it's marked by bold type). Application of Altera chips (A1.1) stipulates use of SRAMFPGA technology producing (A2.1) and Case-tool Quartus II (C2.1). Application of Actel chips (A1.2) stipulates use of Flash-FPGA technology producing (A2.2) and Case-tool Libero (C2.2). Example of two versions for FPGA-based I&C systems is shown on the Fig.1.

4.0 D3 ANALYSIS AND ASSESSMENT OF MULTI-VERSION FPGA-BASED NPP I&C SYSTEMS

4.1 Approach and Technique of D3 Analysis and Diversity Assessment

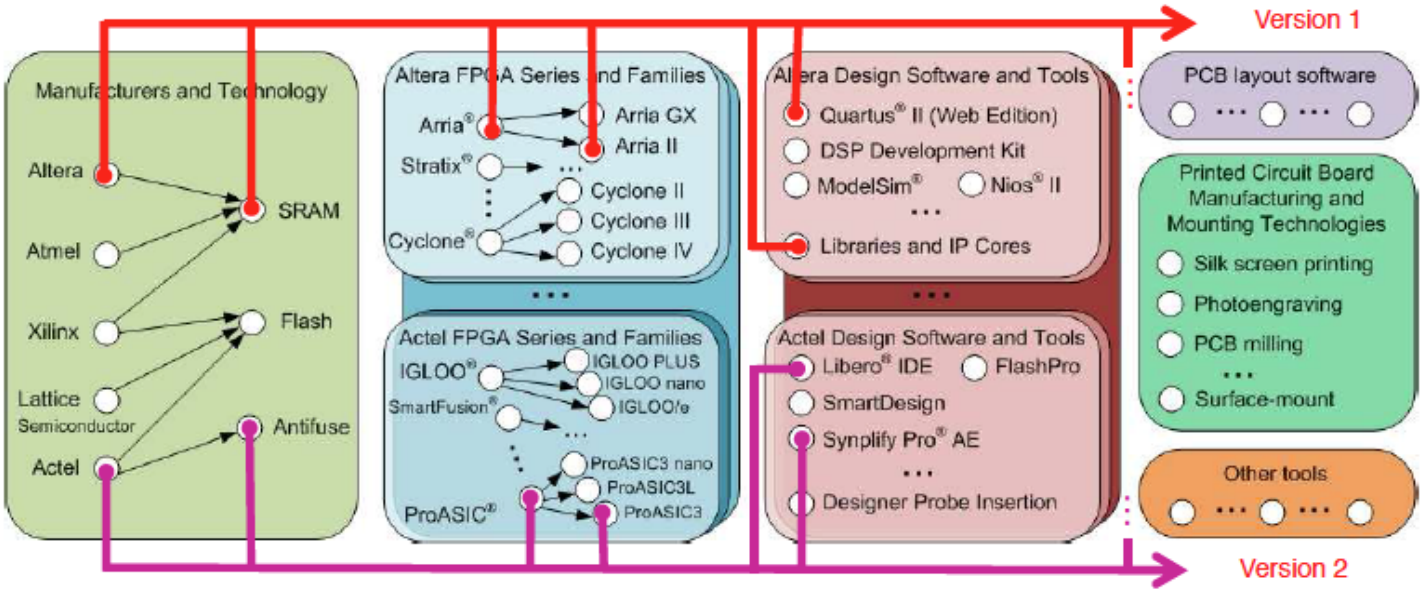
The approach to assessment of diversity level and MVS safety is based on the four basic procedures of analysis and evaluation. The first procedure implements D-1,2-analysis, procedures form the second to the forth implement D-3-analysis [11].

1. Selection of "horizontal" diversity scheme (SDS); initial data is I&C design and documentation; a result of analysis is determination of a set of different (diverse) defence echelons.
2. Check-list-based analysis of applicable diversity types (CLD); initial data for the CLD analysis are I&C design and documentation, 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. CLD stages are the following:

Table 2 | Diversity Types of FPGA-Based I&C Systems

DIVERSITY TYPES			
NUREG6303-Based Types	**FPGA Technology Diversity Types**	**FPGA Technology Diversity Subtypes**	**Examples**
Equipment diversity	Diversity of programmable components (A)	Diversity of manufacturers of FPGA (A1)	Altera (A1.1) vs Actel (A1.2)
		Diversity of technologies of FPGA producing (A2)	SRAM (A2.1) vs Antifuse (A2.2)
		Diversity of FPGA families (A3)	Cyclone vs ProASIC
		Diversity of FPGA from the same family (A4)	Different families
	Diversity of printed circuit boards (PCBs) (B)	Diversity of PCB development technologies (B1)	Different PCB development technologies
		Diversity of PCB Manufacturers (B2)	Different manufacturers (Ukraine vs Republic of Korea)
Design diversity	Diversity of CASE-tools (C)	Diversity of CASE-tools developers (C1)	Altera vs Actel
		Diversity of CASE-tools (C2)	Quartus II (C2.1) vs Libero (C2.2)
		Diversity of CASE-tools configurations (C3)	Different components and tools for design
Software diversity	Diversity of languages of FPGA projects development (D)	Diversity of language kinds (D1)	Graphic notation vs HDL-based
		Diversity of hardware description languages (D2)	VHDL vs Verilog
	Diversity of specification presentation (E)	Diversity of FPGA initial specification languages (E1)	Flow charts vs time diagrams
		Diversity of FPGA specification models (E2)	B&HDL vs Event-B
Human diversity	Diversity of processes (P)	Diversity of development processes (P1)	Different life cycle models, different teams
		Diversity of verification processes (P2)	Different verification teams and used tools
		Diversity of maintenance (P3)	Different development and maintenance teams

Figure 1 | An Example of Two Versions for FPGA-Based I&C System



a. analysis of I&C specification and requirements to system, definition of system safety class; requirements to diversity (necessary for diversity application);

b. analysis of I&C design and development process, that involves activities: (b1) identification of MVS types: which of the subsystems are FPGA-based and which are software and microprocessor-based; (b2) identification of product diversity; for FPGA-based MVSs: manufacturer of chips; FPGA technology; FPGA families; FPGA chips, languages; tools, etc); (b3) identification of process diversity kinds.

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

3. 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.

MAD stages are the following:

a) determination of metric values for different types of applied diversity, i.e. performing two activities: (a1) determination of metric values (local diversity metrics μi for diversity type di and local diversity metrics μij for diversity subtype dij); the metric values may be fixed in advance; (a2) correction of metric values in accordance with development and operation experience;

b calculation of general diversity metric for system: (b1) determination (correction) of weight coefficients of metrics (taking into account multi-diversity aspect); (b2) convolution (additive or more complex) of metrics and calculating value of general diversity metric.

The result of this stage is a value of general diversity metric, which can characterize the diversity effect on CCF probability.

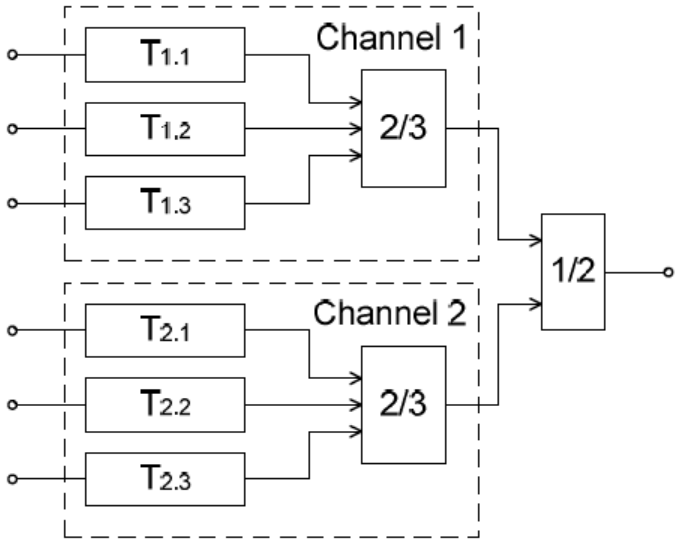
4. RBD and Markovian model-based assessment (RDM); initial data for the RDM procedure are I&C design and documentation, results of the CLD and MAD analysis; results of the RDM procedure are values of safety and dependability indicators.

4.2 RBD-Based Assessment

Probabilistic assessment is considered in terms of Twochannel Reactor Trip System with three parallel tracks (subchannels) of voting logic “2-out-of-3” in each of the channels. A real system produced by enterprises Research and Production Corporation Radiy was taken as a basis (see Fig. 2). Each of the channels of the system independently receives information from sensors and other NPP systems. Each channel is independent and can form reactor trip signal.

Simplified diagram of components of this system is shown in Fig. 2, where $T_{i.j}$ is a track j in channel i.

Figure 2 | Simplified structure of Two-channel Three-track System



Reliability block diagram of Two-channel System that does not use diversity (channel diversity) is shown in the Fig. 3,a. This diagram does not take into account element of voting logic “1- out-of-2” (element OR in the simplest case).

Reliability index $P_{phi.j}$ determines HW reliability of the track $T_{i.j}$ (defined, first of all, by physical failures). Reliability index P_d determines reliability defined by design faults which may be main source of common cause failures (CCF). Majority elements have reliability index P_M. Reliability of the One-version Majority Redundant System is represented by the following formula:

$$P_{1D} = \left\{1 - \left[1 - \left(3P_{ph}^2 - 2P_{ph}^3\right) P_M\right]^2\right\} P_d \,. \qquad (1)$$

If channels are implemented in different HW and SW versions value of P_d will consist of three components (see Fig. 3,b):

- $P_{dr1} = 1 - Q_{dr1}$, where Q_{dr1} – probability of failure caused by relative design faults of the first version;
- $P_{dr2} = 1 - Q_{dr2}$, where Q_{dr2} – probability of failure caused by relative design faults of the second version;
- $P_{da} = 1 - Q_{da}$, where Q_{da} – probability of failure caused by absolute design faults (common faults of the versions).

Reliability of Diverse System is calculated by the formula:

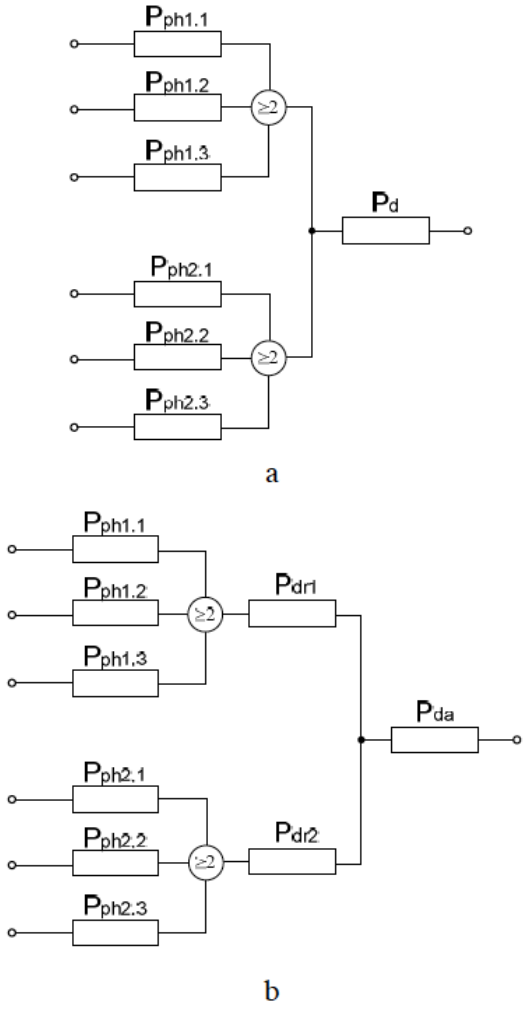
$$P_{2D} = \left\{1 - \left[1 - \left(3P_{ph}^2 - 2P_{ph}^3\right) P_{dr} P_M\right]^2\right\} P_{da} \,. \qquad (2)$$

We consider that $P_{dr1} = P_{dr2} = P_{dr}$ and majority elements are equally reliable.

Diversity is usually applied in such a configuration, where different channels are independently implemented with different types of diversity.

However, this is not the only variant of the redundant circuit. A variant of using redundancy in tracks of one channel is shown in the Fig. 4.

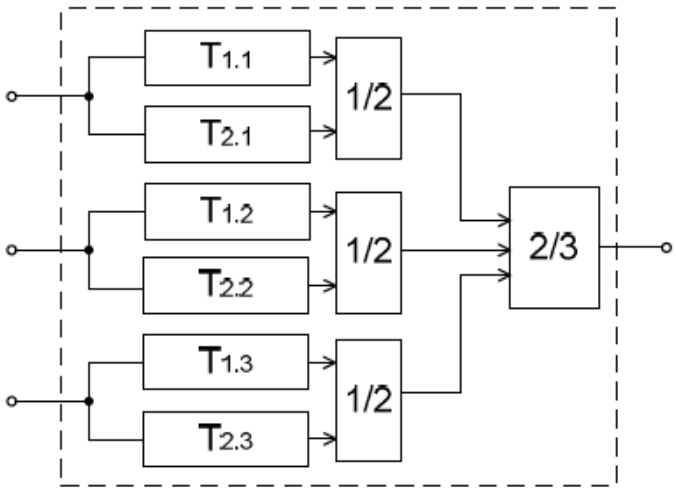
Figure 3 | RBDs of Two-channel Redundant System



Reliability block diagrams for the system, represented in the Fig. 4, are shown in the Fig. 5. Reliability of such system, that use one version for redundancy (Fig. 5,a), can be described by the formula:

$$P_{1M} = \left\{3\left[1-\left(1-P_{ph}\right)^2\right]^2 - 2\left[1-\left(1-P_{ph}\right)^2\right]^3\right\} P_M P_d \,. \quad (3)$$

Figure 4 | Simplified structure of Single-channel Three-track System



In case of using two different versions for $T_{1.i}$ and $T_{2.i}$, system has RBD, shown in the Fig. 5,b, and a formula for reliability calculation:

$$P_{2M} = \left\{3\left[1-\left(1-P_{ph}\right)^2\right]^2 - 2\left[1-\left(1-P_{ph}\right)^2\right]^3\right\} P_M \left[1-\left(1-P_{dr}\right)^2\right] P_{da} \,. \quad (4)$$

If we express the values of reliability (probability of nofailure operation) through failure rates as $P = e^{-\lambda t}$ we can calculate and compare the values of reliability for certain values of λ_{ph}, λ_d, λ_M, λ_{dr}, λ_{da} and ß (the fraction of absolute design faults).

Figure 5 | RBDs of Single-channel Three-track Redundant System

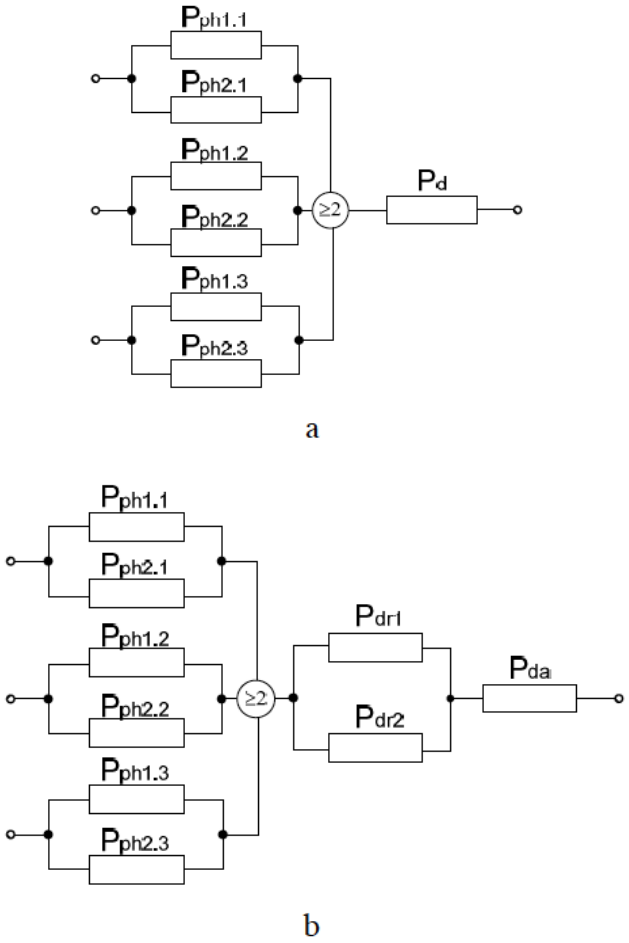
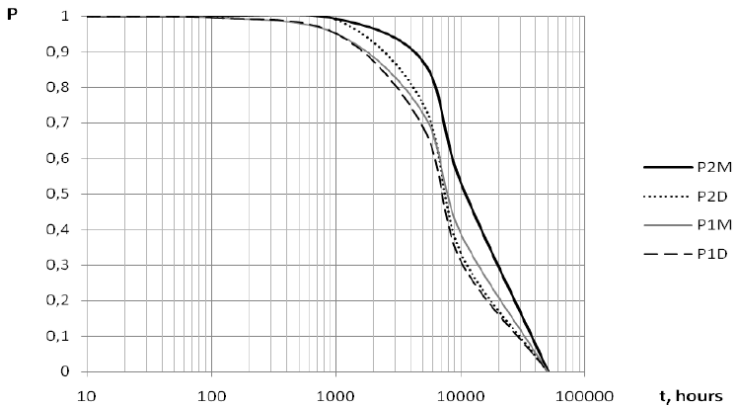


Figure 6 | Dependence of P_{1D}, P_{2D}, P_{1M} and P_{2M} on the time, hours (for systems with diversity ß=0,1)



It should be noted that although the single-channel twoversion three-track redundant system has the greater effect of the use of diversity, its application in many ways violates the principle of independence. Therefore the use of such architecture for safety systems of nuclear power plants is complicated.

In the calculations the following values of the failure rate were used

$$\lambda_{ph}=10^{-4}\ 1/\text{h},\ \lambda_d=\lambda_{ph}/2,\ \lambda_M=\lambda_{ph}/100,\ \lambda_{dr}=(1-\beta)\times\lambda_d,\ \lambda_{da}=\beta\times\lambda_d,$$

where ß=0,1. Graphically dependence of P_{1D}, P_{2D}, P_{1M} and P_{2M} (formulas (1-4)) on the time shown in the Fig. 6.

4.3 Tool for Support of D3 Analysis

Instrumentation support of D3 analysis may be carried out by the tool consisting of version redundancy database (for storage of check-lists and results of assessment of multiversion I&C systems), processing modules for calculation of diversity metrics and safety indicators.

5.0 CONCLUSION

In this paper some problems regarding to D3 analysis and diversity assessment of multi-version I&C systems were discussed. One of the main challenges in this area is a fact that multi-version systems are still unique, failures occurred very rarely, information about failures is not enough representative and is not generalized taking into account development and operation experience for different applications.

Proposed techniques of diversity level and multi-version systems safety assessment are founded on three interconnected approaches. First of them is based on D3 analysis by determining horizontal and vertical diverse echelons. Second one represents metric-based technique allowing to assess diversity level and to compare multi-version systems on application of different kinds and different volume of diversity. Third one is based on the probabilistic models which include key indicator β calculation using metric analysis. This approach and technique allows receiving more accurate assessment of diversity than NUREG7007-based technique due to more detailed presentation of classification attributes.

These theoretical issues were used on development and assessment of FPGA RadICSTM Platform-based I&C systems safety related to NPPs. Next steps of research and development activities may be connected with creation and implementation of tool-based support of all life cycle processes for multi-version systems.

1. Jonson, G., 2010, The INSAG Defense in Depth Concept and D-in-D&D In Instrumentation and Control, In Proceedings of 7th ANS Topical Meeting on NPIC-HMIT, Las Vegas, USA, November, 2010.
2. Kharchenko, V., Sklyar, V. (edits), 2008, FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment. RPC “Radiy”, National Aerospace University “KhAI”, State STC on Nuclear and Radiation Safety, Kharkiv-Kirovograd, Ukraine.
3. EPRI 1019181 -2009, 2009, Guidelines on Use of FPGAs in NPP I&Cs, USA.
4. Kharchenko, V., Siora, A., Bakhmach, E., 2008. “Diversityscalable decisions for FPGA-based safety-critical I&Cs: from Theory to Implementation”. In Proceedings of the 6th Conference NPIC&HMIT, Knoxville, Tennessee, USA.
5. Tsvetkov (ed), P., 2011, Nuclear Power – Control, Reliability and Human Factors, InTech.
6. Littlewood, B., Popov, P., 2001. “Modelling software design diversity - a review”, ACM Computing Surveys. No33, pp. 177-208.
7. Pullum, L., 2001. Software Fault Tolerance Techniques and Implementation, Artech House Computing Library
8. Kharchenko, V., Siora, A., Bakhmach, E., 2008. “Diversityscalable decisions for FPGA-based safety-critical I&Cs: from Theory to Implementation”. In Proceedings of the 6th Conference NPIC&HMIT, Knoxville, Tennessee, USA.
9. NUREG/CR-7007 ORNL/TM-2009/302, 2009, Diversity Strategies for NPP I&Cs.
10. Defence in Depth in Nuclear Safety, 1996, TR of the International Nuclear Safety Advisory Group, INSAG-10, Vienna, IAEA.
11. Kharchenko, V., Bakhmach, E., Siora A., et al., Assessment of Multi-Version NPP I&C Systems Safety: Metric- Based Approach, Technique and Tool, 2011, In Proceedings of the ICONE18, Osaka, Japan, October.