Journal of Energy and Power Engineering 5 (2011) 411-418

Combined Implementation of Dependability Analysis Techniques for NPP I&C Systems Assessment

V. Kharchenko[1], E. Babeshko[1], V. Sklyar[2], A. Siora[2] and V. Tokarev[2]

1. Centre for Safety Infrastructure-Oriented Research and Analysis, Kharkiv 61070, Ukraine

2. Research and Production Company, RADIY, Kirovograd 25009, Ukraine

Received: September 03, 2010 / Accepted: December 10, 2010 / Published: May 31, 2011.

Abstract: Dependability analysis of nuclear power plants information and control systems is an important but challenging task. There are several techniques that can be applied for safety and dependability assessments. All of them have limitations and can't be easily applied in most cases. Sometimes combined usage of different methods is the most appropriate solution. In this paper we consider techniques of dependability assessment and achievement developed and used by research-and-production corporation "Radiy". The elements of the assessment methodology are briefly described.

Key words: NPP information and control systems, dependability, FPGA, FMEA, RBD, Markov modelling.

1. Introduction

Nuclear power production is a safety-critical process that requires reliable and safe operation. Information & control systems (I&CS) of nuclear power plants (NPP) play key roles in stable operation ensuring and therefore should be designed in accordance with international requirements on nuclear and operational safety.

To evaluate and verify this accordance, different standardized techniques of dependability (safety, reliability, availability etc.) analysis and assessment are used. These techniques can be rather simple or quite complicated to implement depending on the problems at hand. Generally, it is difficult to perform NPP I&CS dependability analysis for several reasons, including:

- complex fault-tolerant architecture;
- usage of multiversion technologies;
- large number of different components.

But all assessment techniques are changing and progressing constantly.

Many authors in the field have emphasized the usefulness of particular techniques as well as their restrictions [1-3]. We try to colligate available information on different techniques.

Furthermore, our goal is to discuss the possibilities of development of unified technique for I&CS dependability analysis and assessment. This technique should enable validation and eventual certification of safety, security and reliability of NPP I&CS via modeling and analysis as well as simulation and experimentation. The use of different approaches is important since it confers a high level of confidence in results.

Also, there are many characteristics making the NPP I&CS different from other safety critical control systems. For example, it is not enough to have only a safe nuclear installation, but it also has to be proved to the licensing authorities that the installation really is safe and meets all the necessary requirements.

Finally, the main scope of this paper is to depict methodology developed by research-and-production

Corresponding author: V. Kharchenko, professor, research fields: multiversion design technologies, dependable computing and control systems, fault-tolerance and survivable applications, software reliability assessment and expert analysis. E-mail: V.Kharchenko@csis.org.ua.

corporation (RPC) "Radiy" for safety, reliability and availability assessment in NPP I&CS projects. The approach is based on well-known techniques such as risk analysis, FMECA, probabilistic safety assessments (PSA) as well as on different extensions and combinations of these methods. Among them Intrusion Modes and Effects Analysis (IMEA), extended Failure Modes, Effects and Criticality Analysis, Reliability-Safety-Security Block Diagrams etc.

The proposed elements of methodology were validated during safety assessment of the FPGA-based RADIY^{TM} platform for multi-version NPP I&C systems. Results of this assessment are presented to demonstrate effectiveness and main advantages of methodology.

The rest of the paper is organized as follows. In section 2 we provide short description of FPGA and key advantages of this technology. In section 3 we deal with evolution, main advantages, limitations and possible challenges of dependability analysis and assessment techniques, describe dependability taxonomy. In section 4 diversity and multiversity as key means of dependability achievement are discussed. Finally, we depict FPGA as basis for NPP I&C systems present the FPGA-based RADIY^{TM} platform and discuss licensing issues in section 5 and make conclusions.

2. FPGA: Key Advantages

The problems of NPP I&Cs dependability analysis and ensuring should be discussed taking into account trends of computer technologies development. One of the contemporary trends is dynamically growing application of novel complex electronic components, particularly, Field Programmable Gates Arrays (FPGAs) in NPP I&Cs and other critical areas.

FPGA is a convenient technology not only for implementation of auxiliary functions (transformation and preliminary processing of data, diagnostics, etc.), it is also effective for implementation of safety important NPP I&Cs control functions. Application of the FPGA technology is more reasonable than application of software-based technology (microprocessors) in many cases [4].

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

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

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

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

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

3. Dependability Analysis Techniques

3.1 Dependability Taxonomy

Dependability taxonomy is shown in Fig. 1. According to Ref. [5], dependability is the ability to deliver required service that can justifiably be trusted. Dependability is a complex property, which includes following primary attributes:

- safety – absence of catastrophic consequences for

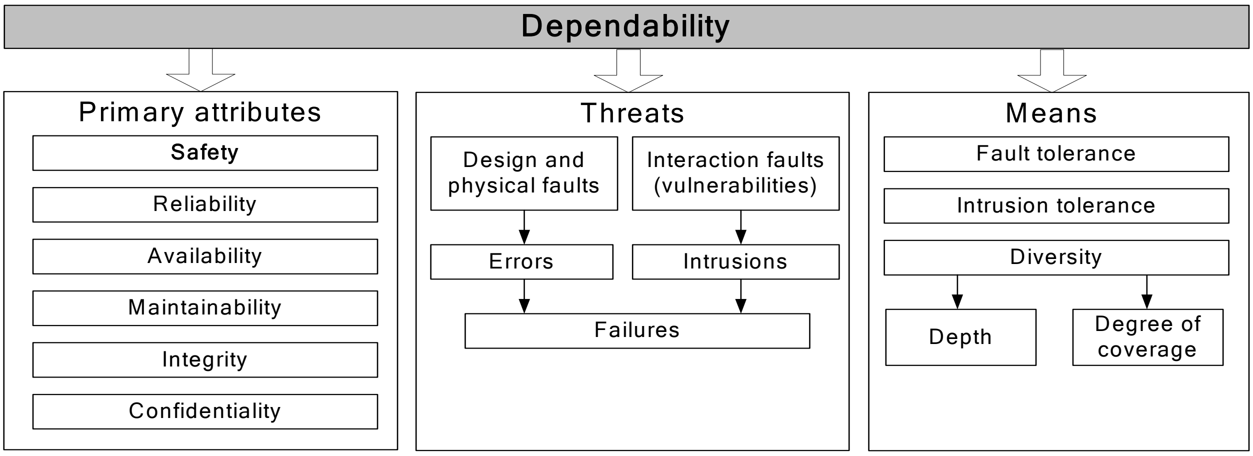

Fig. 1 Dependability taxonomy.

the users and the environment; safety is the most important dependability attribute for NPP in general and thus for NPP I&CS;

- reliability – continuity of correct service;
- availability – readiness for correct service;
- other attributes (maintainability, integrity, confidentiality).

Fault tolerance, the ability of a system to continue operation in the presence of faults, can be achieved by usage of multiple functionally equivalent components (diversity). Intrusion tolerance, the ability of a system to prevent interaction faults from leading to a system failure via possible vulnerabilities, is also can be achieved by usage of diversity. So diversity is a key mean of NPP I&CS dependability achievement.

Diversity can be classified by:

- diversity coverage (I&CS with a complete and partial diversity);
- diversity depth (I&CS with a common and separate diversity).

Diversity issues will be discussed later in Section 4.

3.2 Combined Usage of Dependability Analysis Techniques

There are a lot of well-known techniques that can be used for NPP I&CS dependability analysis and assessment of its attributes. Using these techniques it is possible to perform quantitative and/or qualitative assessments. Qualitative assessments though lacking the ability to account, are very effective in identifying potential failures within the I&CS. We have performed some work to identify possible combination of techniques, results are shown in Fig. 2. To carry out dependability analysis it is necessary to have I&CS technical documentation (this information is obtained from I&CS project) and reliability data of I&CS components (is obtained from component vendors).

The first stage of NPP I&CS dependability analysis is FMECA (Failure modes, effects and criticality analysis). During this stage all possible failure mechanisms and failure rates for all components involved and quantify failure contribution to overall NPP reliability and safety are analysed.

In FMECA qualitative and quantitative results (see Fig. 2) are obtained. Failure mode in FMECA refers to the way a failure might occur. Failure effect is the consequence of failure from the system’s point of view. Failure criticality is assigned to each failure mode to get quantitative parameters.

FMECA is carried out early in the NPP I&CS development life cycle to find ways of mitigating failures and thereby enhancing reliability through design.

A traditional FMECA uses potential component failures as the basis of analysis. Component failures are analysed one by one, and therefore important combinations of component failures might be overlooked. Environmental conditions, external

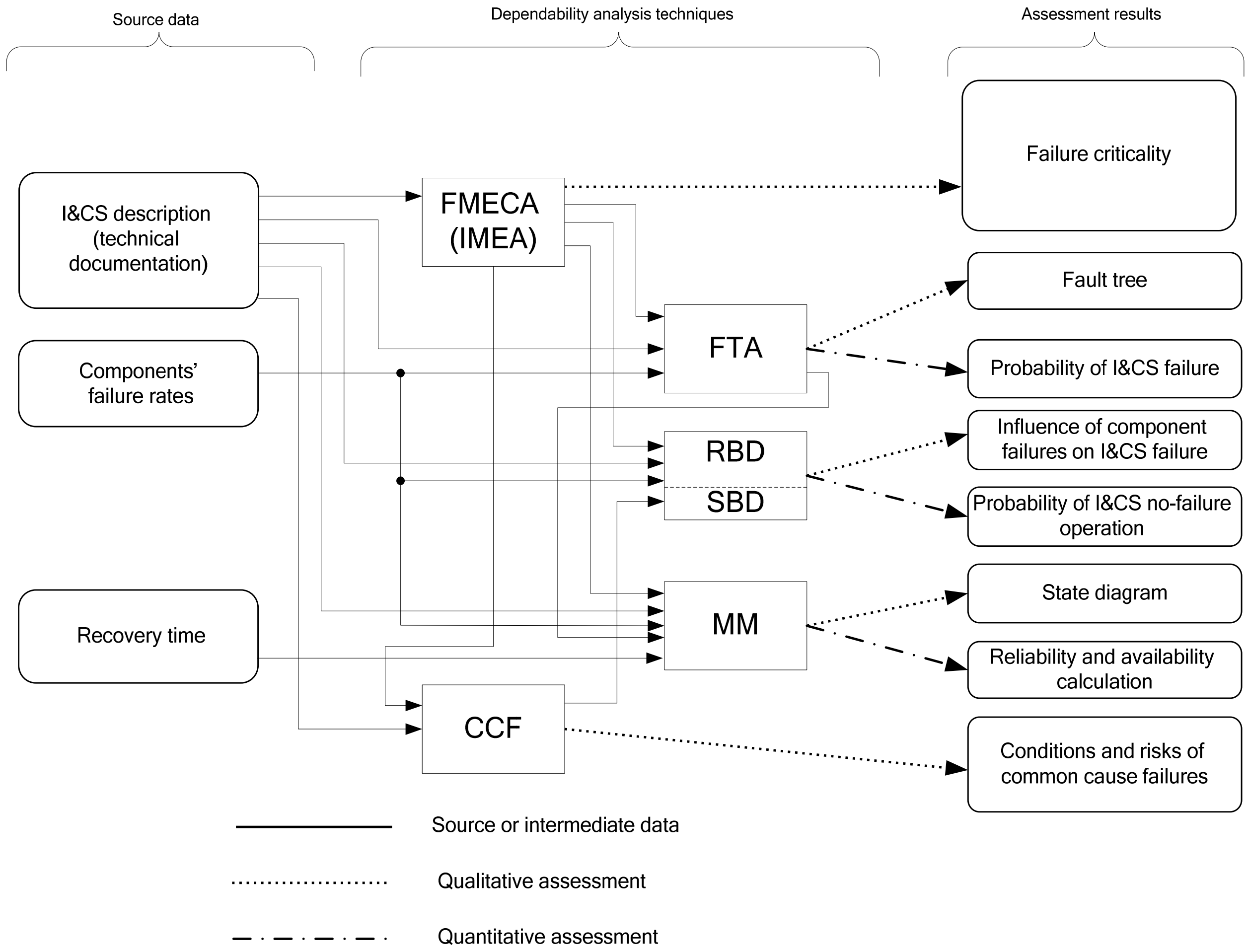
Source data
Dependability analysis techniques
Assessment results
I&CS description (technical documentation)
Components' failure rates
Recovery time
FMECA (IMEA)
FTA
RBD
SBD
MM
CCF
Failure criticality
Fault tree
Probability of I&CS failure
Influence of component failures on I&CS failure
Probability of I&CS no-failure operation
State diagram
Reliability and availability calculation
Conditions and risks of common cause failures
Source or intermediate data
Qualitative assessment
Quantitative assessment

Fig. 2 Combined usage of dependability analysis techniques.

impacts and other such factors are analysed in FMECA only if they produce component failures; external influences that do not produce component failures (but may still produce I&CS failure) are often overlooked.

That's why it is not sufficient to use only FMECA during NPP I&CS analysis.

To take into account external impacts it is possible to use IMEA (Intrusion Modes and Effects Analysis). IMEA is a modification of FMECA that takes into account possible intrusions to the system, examples of this analysis are shown in Refs. [6, 7].

Results of FMECA and IMEA are used during further FTA (Fault Tree Analysis), RBD / SBD (Reliability / Safety Block Diagram), CCF (Common Cause Failure Analysis), and also during Markov modeling.

Reliability block diagram (RBD) is a graphical analysis technique, which expresses the concerned system as connections of a number of components in accordance with their logical relation of reliability. Safety block diagram (SBD) is a similar technique that treats safety aspects [3].

Fig. 3 shows RBD and SBD principles. Set of NPP I&CS components is split into the following groups:

- components that can't lead to NPP I&CS failure C_w;
- components that can lead to I&CS failure, but system state would be safe C_{nws};
- components that can lead to I&CS failure, but system state would be unsafe C_{unws}.

While RBD treats all possible failures (both C_{nws} and C_{nwu} are included into RBD), SBD treats only components that can lead to unsafe situation (only C_{nwu} are included). That gives possibility to concentrate on safety aspect and to simplify all following calculations.

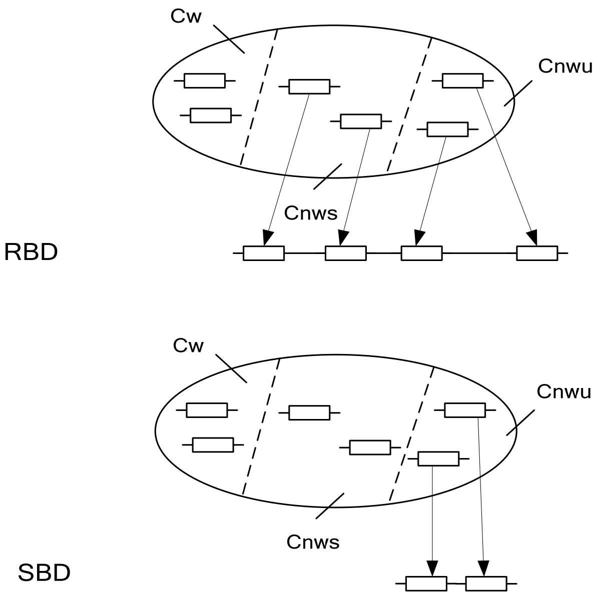

Fig. 3 Reliability and safety block diagrams: principles of development.

During RBD (SBD) it is possible to use list of all components that can cause I&C system failure which has been obtained during FMECA. Then we take into account I&CS architecture (number of components, software and hardware versions, type of diversity, check and reconfiguration means) and sets of different faults and calculate reliability and safety indicators.

In FTA FMECA results are used to get list of all possible failures.

To perform Markov modeling, it is required to know component's failure rates and recovery time so as to get state-to-state transitions. In most cases the NPP I&CS operation may be analyzed using a Markov model.

4. Features of FPGA-based NPP I&Cs Assessment

4.1 Types of Diversity

The threat of common cause failures and necessity of defense means against it have been widely recognized. Ukrainian regulations "Safety Requirements to Safety Important NPP Instrumentation and Control Systems" contain a special chapter with requirements to defense against CCF and a chapter containing observance of diversity of I&CS. According to this document, requirements to diversity are obligatory for reactor protection systems.

FPGA-based I&CS diversity classification includes the following diversity types [8-10]:

- diversity of electronic components (different electronic components manufactures, technologies of electronic components production, electronic components families, electronic components from the same family);
- diversity of CASE-tools (different developers, types 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).

Table 1 summarizes possible diversity types used in systems based on the RADIY^{TM} platform.

4.2 Models of Multi-version Systems

Multi-version system (MVS) is a system in which a few versions-products are used, multi-diversion system (MDVS) is a multi-version in which two types of version redundancy are used. MVS Wn is defined by 5 variables:

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

where X, U – sets of input and output signals;

F = {fd,, d = 1,…, k} – set of I&C functions;

V = {vi,, i = 1,…, n} – set of versions with output signals U1,…, Un;

Z – displaying function Uid in Ud if the function is performed fd, i.e. Ud = Z (U1d,…,Und).

Generalization of MVS (or MDVS) is (l, n, m) — version system with l hardware channels, n versions

Table 1 Diversity implementation.

Equipment diversity	Software diversity	Life cycle (human) diversity
different electronic components	different programming languages	different teams of designers and testers
different programmable components (FPGAs and micro-controllers)	different tools for development and verification	independent verification

and m types of diversity described by the following formula:

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

where $R = \{r_q, q = 1,\ldots, m\}$ – set of diversity types,

θ – their mapping onto set elements $v_j(\Delta R_j) \in V$, $\Delta R_j \subset R$.

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

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

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

Besides, FPGA-based I&C performing safety critical functions may be represented by a composition of two interconnected automata (monitoring or checking and control automata). Monitoring automaton analyses output signals X from monitoring object and forms its status code ZC. Control automaton forms control signals Z in accordance with signals ZC.

Several options of MVS architectures are possible for a FPGA-based I&Cs. Those options may be classified according with degree of diversity coverage (I&Cs with a complete and partial diversity) and diversity depth (I&Cs with a common and separate diversity); it should be noted that this feature is applicable only to full system diversity.

4.3 Assessment of Multi-version Systems

Assessment of diversity metrics is a necessary step of MVS dependability analysis.

Table 2 presents diversity metrics assessment methods.

5. RADIY^{TM}-FPGA-Based Platform for NPP I&CS: Development and Assessment

5.1 Introduction to the RADIY^{TM} Platform

FPGAs are now widely used for safety-critical applications including systems important to nuclear installations safety. FPGA technology allows to develop:

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

Key challenges related to diversity-oriented and FPGA-based NPP I&CS are the following:

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

Table 2 Diversity metrics assessment.

Types of methods	Steps
Theoretical-set metrics methods	Eiler's diagram; matrix of diversity metrics; calculation and analysis of diversity metrics.
RBD and SBD	RBD and SBD development taking into account MVS architecture and sets of different faults; calculation of reliability and safety indicators.
Bayesian method	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; diversity metrics assessment; calculation of reliability and safety indicators.
Fault injection-based assessment	analysis of developed project and receiving version fault profiles; performing of faults injection procedure; proceeding of data and metrics diversity calculation; calculation of reliability and safety indicators.
Expert and other methods	diversity metrics for direct assessment of versions and NPP I&CS 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.

The RADIY^{TM} platform is an example of a dependable FPGA-based I&C platform that ensures possibility of development of multi-version systems (reactor trip systems). Essential dependability assurance feature of the I&C RADIY^{TM} platform is multidiversity 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 RADIY^{TM} platform permits to produce different types of safety-critical systems without essential changing of hardware and software components. The I&C platform RADIY^{TM} platform provides the following types of scalability:

(1) Scalability of system functions types, volume and peculiarities by changing quantity and quality of sensors, actuators, input/output signals and control algorithms;

(2) Scalability of dependability (safety integrity) by changing a number of redundant channel, tiers, diagnostic and reconfiguration procedures;

(3) Scalability of diversity by changing types, depth and criteria of diversity choice.

After 2003 RPC Radiy developed a second generation of I&C platform using FPGAs with a higher degree of integration (1 million gates and more). Since 2003 ten of fifteen Ukrainian nuclear power generating units obtained altogether thirty three I&C systems developed and manufactured by RPC Radiy. All in all, within 2003-2008 in I&C systems of 10 nuclear power generating units with VVER reactors more than 3300 Altera FPGA crystals were used with total operation time 5,600 years (more than 49 million hours). The longest operational time of such equipment at power unit Zaporizhzhya-1 is more than 5 years.

5.2 Safety Assessment and Licensing

Safety assessment of the RADIY^{TM} platform has been carried out using approaches described above in section 2 (see Fig. 1). FMECA-, RBD- and SBD-based analysis and assessments have been performed for all platform blocks. Results of these techniques were used during following Markov modeling and indicators' calculations.

As for NPP I&CS licensing, its basic objective is to assess if these systems are adequately safe. For FPGA-based NPP I&CS main idea lays in consideration of FPGA-chip as hardware and FPGA electronic design as a special type of software with specific development and verification stages [11, 12]. The RADIY^{TM} platform has been licensed for NPP application in Ukraine and in Bulgaria.

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

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

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

FPGA electronic design has a V-shape life cycle in accordance with requirements of coming standard IEC 62566 [13]. Software development stages are replaced by the following specific FPGA electronic design development stages:

- Development of signal formation algorithm block-diagrams;
- Development of electronic design parts (development of signal formation algorithm program models in design environment);
- Integration of electronic design (integration of signal formation algorithm program models into design environment);
- Implementation (downloading) of integrated electronic design to FPGA chip.

Each stage of electronic design development is terminated by verification of the obtained product. A third party assessment has been performed in accordance with IAEA and IEC standard requirements to prove the adequacy of the RADIY^{TM} platform and this platform-based application to safety requirements. 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. Conclusions

To assess dependability and safety of NPP I&C systems, it is not enough to use only one assessment method. Combined usage of different methods and further methods' enhancements are possible solutions. Elements of such methods' usage were presented and discussed in this paper.

Diversity (or multiversity) is a key mean for dependability achievement. Diversity metrics assessment methods were summarized.

Approaches presented in this paper have been applied for development, testing and licensing of FPGA-based I&C systems for nuclear power plants.

References

[1] N.G. Leveson, The need for new paradigms in safety engineering, Safety-Critical Systems: Problems, Process and Practice, Springer London, 2009, pp. 3-20.

[2] L. Tong, X. Cao, Methodology for reliability allocation based on fault tree analysis and dualistic contrast, Nuclear Science and Techniques 19 (4) (2008) 251-256.

[3] H. Yoshikawa, Distributed HMI system for managing all span of plant control and maintenance, Nuclear Engineering and Technology 41 (3) (2009) 237-246.

[4] V. Kharchenko, V. Sklyar (Eds.), 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, 2008, p. 380.

[5] A. Avizienis, J.C. Laprie, B. Randell, C.E. Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE Trans. on Dependable and Secure Computing 1 (2004) 11-33.

[6] A. Gorbenko, V. Kharchenko, O. Tarasyuk, A. Furmanov, F(I)MEA-technique of web services analysis and dependability ensuring, Lecture Notes in Computer Science, 2006, pp. 153-167.

[7] E. Babeshko, A. Gorbenko, V. Kharchenko, Applying F(I)MEA-technique for SCADA-based industrial control systems dependability assessment and ensuring, in: Proceedings of IEEE DepCoS-RELCOMEX Conference, Szklarska Poreba, Poland, June 26-28, 2008, pp. 309-315.

[8] V. Kharchenko, E. Bakhmach, A. Siora, Diversity-scalable decisions for FPGA-based safety-critical I&C systems: From theory to implementation, in: 6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Knoxville, Tennessee, Apr. 5-9, 2009.

[9] V. Kharchenko (Eds.), Multi-Version Systems, Projects and Technologies, National Aerospace University KhAI, Kharkiv, Ukraine, 2002, p. 405.

[10] V. Kharchenko, Dependable systems and multi-version computing: Aspects of evolution, Radio Electronic and Computer Systems 7 (41) (2009) 46-60.

[11] M. Yastrebenetsky, V. Sklyar, Yu. Rozen, S. Vinogradskaya, Safety assessment of FPGA-based ESFAS for Kozloduy NPP, in: Proceedings of the 6th American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, Knoxville, Tennessee, USA, Apr. 5-9, 2009.

[12] A. Siora, V. Sklyar, Yu. Rozen, S. Vinogradskaya, M. Yastrebenetsky, Licensing principles of FPGA-based NPP I&C systems, in: Proceedings of the 17th International Conference on Nuclear Engineering ICONE17, Brussels, Belgium, July 12-16, 2009.

[13] IEC 62566, Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Language Aspects for Systems Performing Category A Functions, CDV, 2010.