UDC 621.3

**E. BABESHKO[1], V. KHARCHENKO[1], A. SIORA[2]**

[1] *Centre for Safety Infrastructure-oriented Research and Analysis, Ukraine*
[2] *Research and Production Corporation Radiy, Ukraine*

# RELIABILITY ASSESSMENT OF FPGA-BASED NPP I&C: EXPERIENCE, METHODS AND TOOLS

*Reliability assessment of instrumentation and control systems (I&Cs) is always one of the most important design and operation activities, especially for critical domains like nuclear power plants (NPPs). Intensive use of relatively new technologies like field programmable gate arrays (FPGAs) in I&C which appear in upgrades and in newly built NPPs makes task to develop and validate advanced reliability assessment methods that consider specific technology features very topical. Increased integration densities make the reliability of integrated circuits the most crucial point in modern NPP I&C. Moreover, FPGAs differ in some significant ways from other integrated circuits: they are shipped as blanks and are very dependent on design configured into them. Therefore, special approaches should be used for comprehensive analysis of FPGAs. This paper summarizes our experience on reliability analysis of FPGA based NPP I&C produced by Research and production corporation Radiy (RPC Radiy). Both analytical and operational reliability analyses are covered.*

***Key words:*** *NPP I&C, reliability assessment, operational reliability, FPGA, FMEA, FTA, RBD.*

## Introduction

To assess the risk of nuclear power plant operation and to determine the risk impact of digital systems, there is a need to quantitatively assess the reliability of the NPP I&C in a justifiable manner [1].

For analytical reliability assessments Markov chain models are typically used [2], the applicability of such models for NPP I&Cs has been surveyed in [3]. Traditionally, application of Markov chain models has been rather straightforward. However, with the implementation of modern I&Cs, there is no common practice on how to use them. In addition, challenges of application of such models for complex systems like FPGA-based NPP I&Cs lie in fact that assessments are based on assumptions the influence of which on the results may be underestimated and not well understood. In FPGA-based systems, a high-level design is implemented with the configurable logic blocks made available by a given FPGA chip. In order to attain a realistic model and satisfactory accuracy of the analysis, it is possible to represent FPGA-based system at this implementation level [4]. Also, different types of models and failure distribution can be considered [5]. Furthermore, combinations of different assessment methods so as to increase assessment accuracy are discussed and presented in [6].

Collecting representative feedback from NPP I&Cs in operation allows validating obtained earlier analytical reliability results. RPC Radiy has used more than 15000 FPGAs in different supplied NPP I&C systems like reactor trip systems, engineered safety features actuation systems, reactor power control and limitation systems etc. Therefore, analysis results are reasonably demonstrative.

The importance of tool support for reliability assessment cannot be overemphasized. In this paper we share experience on tools used by RPC Radiy.

## 1. Reliability Data

Reliability data used for analysis in most cases is provided by the vendor of the particular component. Example of reliability data for FPGA is an Altera Reliability Report [7] that is being updated on a regular basis.

It should be noted that the data provided by vendor is not always detailed enough, i.e., it is not possible to use 'as is' it due to lack of required reliability data.

The following kinds of reliability data may be provided by vendors:

1) reliability data based on operating experience;

2) reliability data based on a part counting method using generic reliability prediction databases such as Military Handbook for "Reliability Prediction of Electronic Equipment" (MIL-HDBK-217F) [8].

MIL-HDBK-217F contains failure rate models for the various part types used in electronic systems, such as integrated circuits, transistors, diodes, resistors, capacitors, relays, switches, and connectors. These failure rate models are based on mathematical models derived from empirical field failure rates that are

gathered for different parts and systems. Those models respect ambient conditions, level of stress, and type of applications.

## 2. Reliability Assessment Methods

### 2.1. General Approach

RPC Radiy performs reliability and availability assessment according to relevant national and international standards. Third parties like Centre for Safety Infrastructure-Oriented Research and Analysis are involved in such assessments.

The assessments are divided into two parts: analytical reliability assessment based on methods like Failure Modes and Effects Analysis (FMEA) and its modifications like XMEA (details are provided in Section 2.2.2), Reliability Block Diagrams (RBD), Markov models, and operational reliability assessment based on reliability data obtained from NPPs that use the RadICS Platform (see Figure 1).

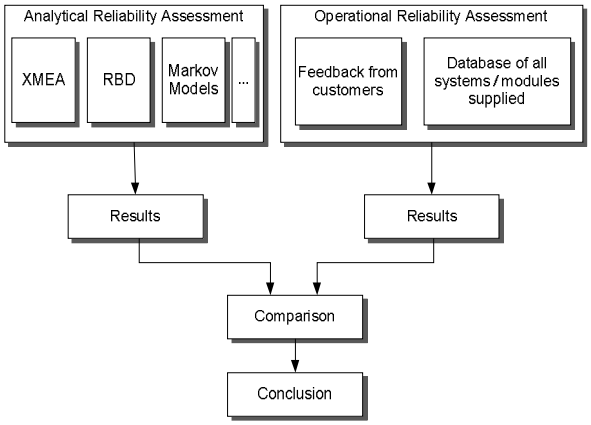


Fig. 1. Reliability Assessment Flow at RPC Radiy

Results obtained by analytical and operational assessments are being compared, and then conclusions on accuracy are made.

### 2.2. Analytical Reliability Assessment

#### 2.2.1. Assumptions

The following typical assumptions are made during analysis:

– all failures are independent;

– only modules critical for safe operation are taken into account (i.e., control consoles, indication control units etc. are not part of reliability analysis scope);

– Mean Time to Repair (MTTR) of 24 hours is achievable due to modular structure of RadICS platforms, possibility of hot swap and availability of spare modules;

– Mean Time to Inspection (MTTI) of 11000 hours is usually assumed in calculations based on experience.

#### 2.2.2. XMEA

FMEA (Failure Modes and Effects Analysis) is a structured, qualitative analysis of a system, subsystem, module, design or function, in order to identify potential failure modes, their causes and their effects on (system) operation, with the objective of improving the design.

We are applying this method not only to failures, but also to other domains like possible intrusions [9]. This generic approach we call XMEA.

#### 2.2.3. RBD

A reliability block diagram (RBD) is a graphical representation of a system's reliability. It shows the logical interconnection of (functioning) components required for successful operation of the system.

RBD allows performing system reliability (no-failure operation) calculation basing on known reliability of its elements.

Probability of no-failure operation in case of series reliability block diagram can be calculated as product of probabilities of no-failure operation of its elements:

$$P_{sys}(t) = \prod_{k=1}^{n} p_k(t), \quad (1)$$

where $p_k$ – probability of no-failure operation of k-th element, n-number of elements in system.

The relation between failure rate and probability of no-failure operation is the following:

$$p(t_0, t) = e^{-\int_{t_0}^{t} \lambda(t)dt}. \quad (2)$$

Basing on formulas (1) and (2) the following expression for failure rate can be obtained:

$$\lambda_{sys}(t) = \sum_{k=1}^{n} \lambda_k(t), \quad (3)$$

where $\lambda_k$ – failure rate of $k$-th element, $n$-number of elements in system.

#### 2.2.4. Fault Tree Analysis

Fault tree analysis is a method to model the chain of causes that lead to an undesired event or effect.

An undesired event is chosen as the top event, e.g., a function event from the event tree. Situations or combination of events that could lead to the top event is connected by logical gates. These second level situations are in turn evaluated and their possible causes determined and connected by logical gates. In this way a tree is built between the top event and a number of basic events and every possible sequence that result in a failing top node is identified.

The basic events are not developed further, they are instead assigned appropriate probability measure that describe their failure probability.

#### 2.2.5. Markov Models

Markov models are based on state transition diagram which represents system behaviour. System is regarded as a number of elements, each of which can assume only one of two states: up or down. As an element fails or is restored, the system moves from one state to another. Based on such state transition diagram system reliability and availability measures can be calculated.

#### 2.2.6. Usage of Combinations of Methods

In [6] we specify approach to usage of combinations of different reliability assessment methods. Figure 2 summarizes basic concept of this approach.

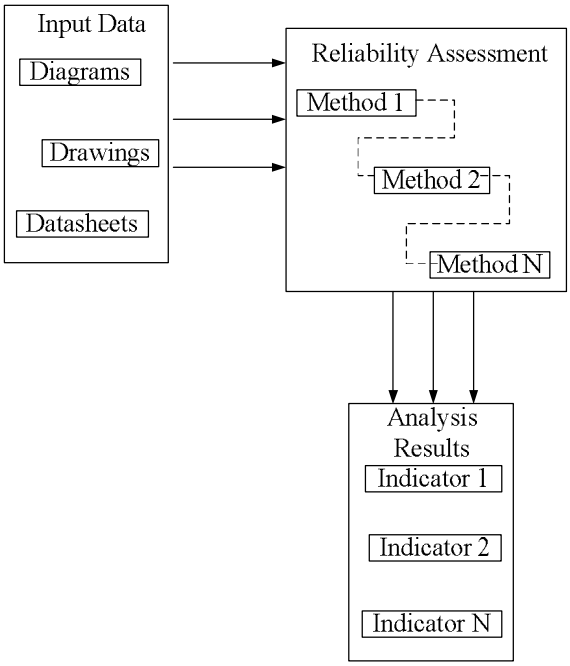


Fig. 2. Concept of Usage of Combinations of Methods

As an example, during RBD it is possible to use list of all components that can cause I&C system failure which has been obtained during XMEA. Then we take into account I&C 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.

Another example is that XMEA results can be used during Fault Tree Analysis (FTA) to get list of all possible failures

### 2.3. Operational Reliability Assessment

Reliability data on supplied I&C systems is collected from RPC Radiy customers on regular basis (usually once in a quarter). Such information includes failure data that is used to calculate operational reliability.

Since 2002 the RadICS Platform is being developed and improved based on technology updates and operational experience.

Between 2004 and 2015, RPC Radiy completed more than 80 turnkey projects and supplied different types of I&C systems for nuclear installations based on the RadICS Platform [10].

In 2010, an independent review of the RadICS Platform was performed by IAEA IERICS Mission.

Since 2010, SIL certification is being performed in several phases to achieve compliance to the second edition of IEC 61508 standard. Actual version of certificate is available at [11].

Figure 3 shows the history of RadICS development, applications, reviews and certification.

The current RadICS operation status is the following:

– operating at 4 Ukrainian NPPs and 1 Bulgarian NPP;

– used as basis for Reactor Trip Systems (RTS), Engineered Safety Features Actuation System (ESFAS), Reactor Power Control and Limitation Systems (RPCLS), Rod Control Systems (RCS), Nuclear and Turbine Island Control Systems;

– combined total operation time is more than 40000000 hours;

– there were no plant shutdowns due to RadICS Platform software or hardware problems;

– there were no RadICS Platform module failures due to FPGA faults.

Operational reliability assessment based on data collected from 2004 to 2015 confirms that actual Mean Time Between Failures (MTBF) values determined from this data are greater than the calculated MTBF values.

## 3. Tools

Review of commercial tools was done in [12]. In addition, Microsoft Excel could be used for simple reliability and availability assessment. Special spreadsheets are developed by RPC Radiy for analytical and operational analysis (see Figure 4).

Also, we have developed a tool that allows to generate reports from database for the specific customer, I&C, RadICS platform module or the particular FPGA chip (see Figure 5).

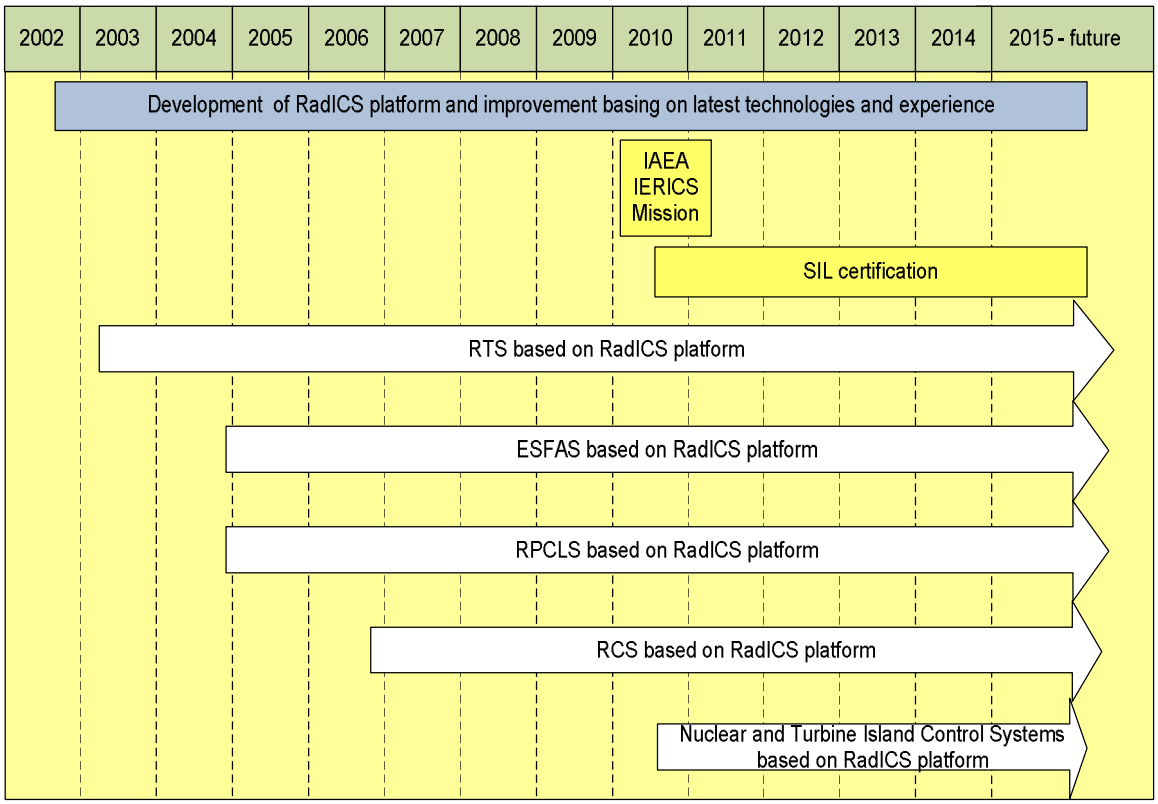


Fig. 3. RadICS Development and Operating History

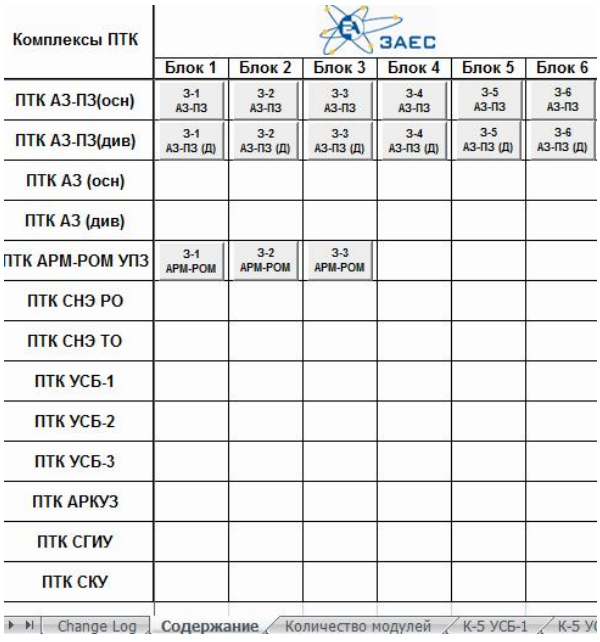


Fig. 4. Spreadsheet for Reliability Assessment

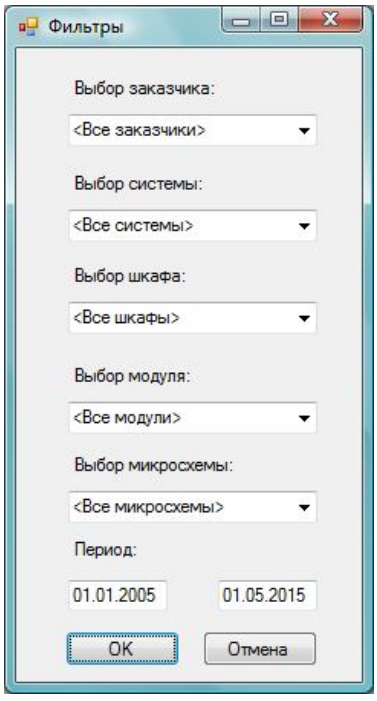


Fig. 5. Operational Reliability Assessment Tool

Figure 6 shows sample chart for total operation time of the particular FPGA type in the particular I&C type.


Fig. 6. Total Operation Time

Exida FMEDA tool is used to carry out FMEA and FMEDA in accordance with IEC 61508 (see Figure 7).

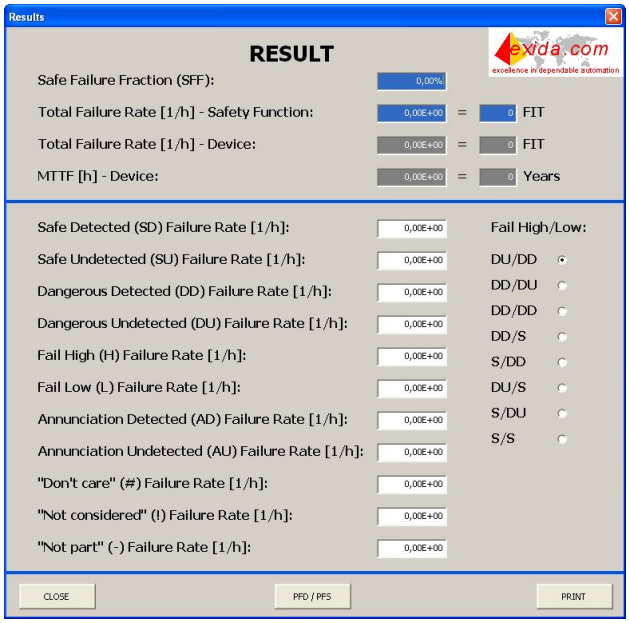


Fig. 7. FMEDA Tool

Outputs of FMEDA tool are Excel spreadsheets that are used further as inputs for Fault Injection Testing (FIT).

## Conclusion

Elements of reliability assessment of NPP I&C done at RPC Radiy were presented.

Among the issues to be solved in order to perform accurate reliability assessment of NPP I&C systems, this work focused on the usage of different reliability assessment method combinations. However, we still have challenges with justifying the most appropriate sequence of method usage and about the several issues not handled in this work. Therefore, the proposed model needs to be extended for a more accurate reliability assessment in further works.

## References (GOST 7.1:2006)

*1. Authen, S. Reliability Analysis Of Digital Systems In A Probabilistic Risk Analysis For Nuclear Power Plants [Text] / S. Authen, J.-E. Holmberg // Nuclear Engineering And Technology. – 2012. – Vol.44, No.5. – P. 471-482.*

*2. Assessment of the Reactor Trip System dependability: Two Markov's chains - Based cases [Text]/ V. Butenko, D. Butenko, V. Kharchenko, O. Odarushchenko, E. Odarushchneko // Proceedings of 10th International Conference on Digital Technologies. – P. 103-109.*

*3. Traditional Probabilistic Risk Assessment Methods for Digital Systems [Text] / T. Chu, G. Martinez-Guridi, M. Yue, J. Lehner, P. Samanta // NUREG/CR-6962. – 2008. – 364 p.*

*4. A Tool for Signal Probability Analysis of FPGA-Based Systems [Text]/ C. Bernardeschi, L. Cassano, A. Domenici, P. Masci // Proceedings of The Second International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking. – 2011. – P. 13-18.*

*5. Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant [Text] / N. Brinzei, G. Deleuze, N. Villaume, J.-F. Petin // Safety and Reliability: Methodology and Applications. – 2015. – P. 2121-2129.*

*6. Combined Implementation of Dependability Analysis Techniques for NPP I&C Systems Assessment [Text] / V. Kharchenko, E. Babeshko, V. Sklyar, A. Siora, V. Tokarev // Journal of Energy and Power Engineering. – 2011. – Vol. 5. – P. 411-418.*

*7. Altera Reliability Report [Electronic resource]. – Available at http://www.altera.com/literature/rr/rr.pdf. – 10.03.2016.*

*8. MIL-HDBK-217F N2. Reliability Prediction of Electronic Equipment [Text]. – 28 February 1995. – 322 p.*

*9. Babeshko, E. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring [Text] / E. Babeshko, V. Kharchenko, A. Gorbenko // Proceedings of the Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX. – P. 309-315*

*10. Radiy Reference List [Electronic resource]. – Available at http://radiy.com/images/news_media/brochures/Reference-list-en.pdf. –10.03.2016.*

*11. RPC Radiy FPGA-Based Safety Controller (FSC) RadICS [Electronic resource]. – Available at http://www.exida.com/SAEL/rpc-radiy-fpga-based-safety-controller-fsc-radics. – 10.03.2016.*

*12. Illiashenko, O. Choice and Complexation of Techniques and Tools for Assessment of NPP I&C Systems Safety [Text] / O. Illiashenko, E. Babeshko // ICONE19-43484.*

## References (BSI)

1. Authen, S., Holmberg, J.-E. Reliability Analysis Of Digital Systems In A Probabilistic Risk Analysis For Nuclear Power Plants. *Nuclear Engineering And Technology*. 2012, vol. 44, no.5, pp. 471-482.

2. Butenko, V. Assessment of the Reactor Trip System dependability: Two Markov's chains - Based cases. *Proceedings of 10th International Conference on Digital Technologies*. pp. 103-109.

3. Chu, T. Traditional Probabilistic Risk Assessment Methods for Digital Systems. *NUREG/CR-6962*, 2008. 364 p.

4. Bernardeschi, C. A Tool for Signal Probability Analysis of FPGA-Based Systems *Proceedings of The Second International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking,* 2011, pp. 13-18.

5. Brinzei, N. Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant. *Safety and Reliability: Methodology and Applications*. 2015, pp. 2121-2129.

6. Kharchenko, V. Combined Implementation of Dependability Analysis Techniques for NPP I&C Systems Assessment. *Journal of Energy and Power Engineering*, 2011, vol. 5, pp. 411-418.

*7. Altera Reliability Report*. Available at http://www.altera.com/literature/rr/rr.pdf (accessed March 10, 2016).

8. MIL-HDBK-217F N2. *Reliability Prediction of Electronic Equipment*. 28 February 1995. 322 p.

9. Babeshko, E., Kharchenko, V., Gorbenko, A. Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring. *Proceedings of the Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX,* pp. 309-315

10. *Radiy Reference List*. – Available at http://radiy.com/images/news_media/brochures/Reference-list-en.pdf (accessed March 10, 2016)

11. *RPC Radiy FPGA-Based Safety Controller (FSC) RadICS*. – Available at http://www.exida.com/SAEL/rpc-radiy-fpga-based-safety-controller-fsc-radics (accessed March 10, 2016)

11. Illiashenko, O., Babeshko, E. Choice and Complexation of Techniques and Tools for Assessment of NPP I&C Systems Safety. *ICONE19-43484*.

*Поступила в редакцию 28.02.2013, рассмотрена на редколлегии 25.03.2013*

## ОЦЕНКА НАДЕЖНОСТИ ИУС АЭС, ОСНОВАННЫХ НА ПЛИС: ОПЫТ, МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА

***Е. В. Бабешко, В. С. Харченко, А. А. Сиора***

Оценка надежности информационно-управляющих систем (ИУС) является одним из важнейших этапов проектирования и эксплуатации систем, особенно для критических объектов, таких как атомные электростанции (АЭС). Интенсивное использование относительно новых технологий, таких как программируемые логические интегральные схемы (ПЛИС), при модернизации существующих и разработке новых ИУС приводит к тому, что разработка и усовершенствование методов оценки надежности, учитывающих специфические особенности технологий, становится весьма актуальной задачей. Надежность интегральных схем становится ключевым фактором современных ИУС АЭС также по причине увеличения плотности интеграции. Кроме того, при анализе следует учитывать, что ПЛИС существенно отличаются от других интегральных схем: они поставляются в виде заготовок и очень сильно зависят от логики, сконфигурированной в них пользователем. Поэтому комплексный анализ систем, основанных на ПЛИС, требует разработки специальных подходов. Данная статья обобщает наш опыт по анализу надежности ИУС АЭС производства НПП «Радий», основанных на ПЛИС. Рассмотрены аналитический анализ надежности и операционная надежность.

**Ключевые слова:** информационно-управляющие системы АЭС, оценка надежности, операционная надежность, ПЛИС, FMEA, FTA, RBD.

## ОЦІНКА НАДІЙНОСТІ ІКС АЕС, ПОБУДОВАНИХ НА ПЛІС: ДОСВІД, МЕТОДИ ТА ІНСТРУМЕНТАЛЬНІ ЗАСОБИ

***Є. В. Бабешко, В. С. Харченко, О. А. Сіора***

Оцінка надійності інформаційно-керівних систем (ІКС) є одним з найважливіших етапів проектування та експлуатації систем, особливо для критичних об'єктів, таких як атомні електростанції (АЕС). Інтенсивне використання відносно нових технологій, таких як програмовані логічні інтегральні схеми (ПЛІС), при модернізації існуючих і розробці нових ІКС призводить до того, що розробка та удосконалення методів оцінки надійності, що враховують специфічні особливості технологій, стає досить актуальним завданням. Надійність інтегральних схем стає ключовим фактором сучасних ІКС АЕС також через збільшення щільності інтеграції. Крім того, при аналізі слід враховувати, що ПЛІС істотно відрізняються від інших інтегральних схем: вони поставляються в вигляді заготовок та дуже сильно залежать від логіки, сконфігурованої в них користувачем. Тому комплексний аналіз систем, побудованих на ПЛІС, вимагає розробки спеціальних підходів. Дана стаття узагальнює наш досвід з аналізу надійності ІКС АЕС виробництва НВП «Радій», побудованих на ПЛІС. Розглянуто аналітичний аналіз надійності та операційну надійність.

**Ключові слова:** інформаційно-керівні системи АЕС, оцінка надійності, операційна надійність, ПЛІС, FMEA, FTA, RBD.

**Бабешко Евгений Васильевич** – ст. науч. сотр., Научно-технический центр исследования и анализа безопасности инфраструктур, Харьков, Украина, e-mail: e.babeshko@csis.org.ua.

**Харченко Вячеслав Сергеевич** – д-р техн. наук, профессор, заслуженный изобретатель Украины, директор Научно-технического центра исследования и анализа безопасности инфраструктур, Харьков, Украина, e-mail: v.kharchenko@csis.org.ua.

**Сиора Александр Андреевич** – канд. техн. наук, генеральный директор НПП «Радий», Кировоград, Украина, e-mail: siora@radiy.com.

**Eugene Babeshko** – Senior researcher, Center for Safety Infrastructure-Oriented Research and Analysis, Kharkiv, Ukraine, e-mail: e.babeshko@csis.org.ua.

**Vyacheslav Kharchenko** – Doctor of Technical Science, Professor, Honor Inventor of Ukraine, Head of Center for Safety Infrastructure-Oriented Research and Analysis, Kharkiv, Ukraine, e-mail: v.kharchenko@csis.org.ua.

**Oleksandr Siora** – Candidate of Technical Science, General director of RPC Radiy, Kirovograd, Ukraine, e-mail: siora@radiy.com.