UDC 681.518:004.312.052 **doi: 10.32620/reks.2020.3.08**

E. BABESHKO[1], V. KHARCHENKO[1], K. LEONTIIEV[2], E. RUCHKOV[2]

[1] ***National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, Ukraine***
[2] ***Research and Production Corporation “Radiy”, Kropyvnytskyi, Ukraine***

PRACTICAL ASPECTS OF OPERATING AND ANALYTICAL RELIABILITY ASSESSMENT OF FPGA-BASED I&C SYSTEMS

Operating reliability assessment of instrumentation and control systems (I&Cs) is always one of the most important activities, especially for critical domains such as nuclear power plants (NPPs). It is an important source of I&C reliability information preferable to lab testing data because it provides information on I&C reliability under real use conditions. That is the reason that now it is a common practice for companies to have an established process of collecting operating reliability data on a large variety of used components on regular basis, maintaining a database with failure information, total operation time, typical failure modes, etc. The intensive use of complicated components like field-programmable gate arrays (FPGAs) in I&C which appear in upgrades and newly-built nuclear power plants makes the task to develop and validate advanced operating 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&Cs. Moreover, FPGAs differ in some significant ways from other integrated circuits: they are shipped as blanks and are very dependent on the design configured into them. Furthermore, FPGA design could be changed during planned NPP outage for different reasons. Considering all possible failure modes of FPGA-based NPP instrumentation and control systems at the design stage is a quite challenging task. Therefore, operating reliability assessment is one of the most preferable ways to perform a comprehensive analysis of FPGA-based NPP I&Cs. Based on information in the literature and own experience, operational vs analytical reliability could be pretty far apart. For that reason, analytical reliability assessment using reliability block diagrams (RBD), failure modes, effects and diagnostics analysis (FMEDA), fault tree analysis (FTA), fault insertion testing (FIT), and other techniques and their combinations are important to meet requirements for such systems. The paper summarizes our experience in operating and analytical reliability assessment of FPGA based NPP I&Cs.

Keywords: *reliability analysis; reliability block diagrams; failure modes, effects, and diagnostics analysis.*

Introduction

For analytical reliability assessments Markov chain models, Reliability block diagrams (RBD) and Fault trees analysis (FTA) are typically used. Traditionally, application of such methods 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 methods 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.

Operating reliability assessment is used for verifying and completing analytical assessment. We compare results that were obtained by analytical calculations with results obtained from operation and propose unified reliability assessment approach.

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, we propose to represent FPGA-based system at this implementation level.

There are a lot of reliability assessment techniques during development and operation stages described by standards MIL [1], IEEE [2], IEC [3] and industrial guides [4]. These techniques can be combined to analyze reliability and evaluate quantitative indicators [5]. Particularities of reliability and safety assessment for FPGA-based I&C are analyzed in [6].

Objective of the paper is to summarize experience on operating reliability analysis of FPGA based NPP I&Cs. In Section 2 we provide overview of analytical and operational reliability assessment methods used at RPC Radiy. Sections 3 and 4 provide details on operating and analytical assessments respectively. The results we obtained illustrate the proposed approach can assess the reliability of the FPGA-based NPP I&Cs reasonably. It also allows performing verification of obtained results by possibility of different methods usage.

In Section 5 we provide details on Failure Modes, Effects and Diagnostics Analysis for FPGA-based I&Cs and discuss the importance of tool support for operating

© E. Babeshko, V. Kharchenko, K. Leontiiev, E. Ruchkov, 2020

reliability assessment that obviously cannot be overemphasized.

Finally, in Sections 6 and 7 we provide an assessment case study and conclusions including future research directions.

1. Reliability Assessment of FPGA-based NPP I&C Systems: Approach

Reliability assessment activities are critical for maintaining system and customers' reliabilities during operation of FPGA-based NPP I&C systems. Reliability assessment typically covers both analytical and operational reliability assessment. RPC Radiy's approach is shown on Figure 1 (FMEDA – Failure Modes, Effects and Diagnostics Analysis, RBD - Reliability Block Diagrams, CCFA - Common Cause Failure Analysis, FTA - Fault Tree Analysis, HAZOP - Hazardous Operations).

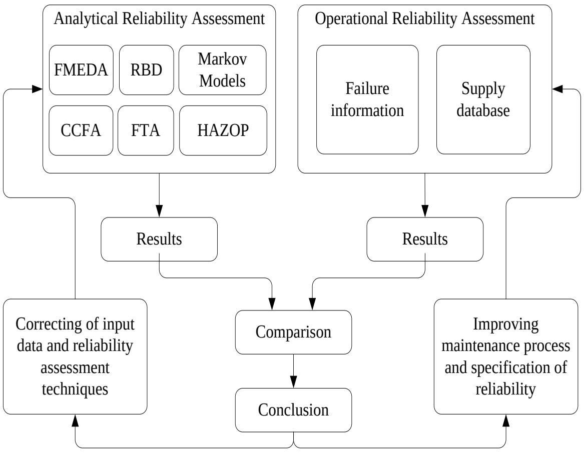

Analytical Reliability Assessment
FMEDA
RBD
Markov Models
CCFA
FTA
HAZOP
Operational Reliability Assessment
Failure information
Supply database
Results
Results
Comparison
Conclusion
Correcting of input data and reliability assessment techniques
Improving maintenance process and specification of reliability

Fig. 1. RPC Radiy's reliability assessment flow

Results obtained by analytical and operational assessments are being compared, and then conclusions are made, providing feedback for possibility of improvement of maintenance process (customer side) and reliability assessment techniques (I&C system supplier side).

During reliability assessment a lot of reliability data is being processed. Figure 2 provides classification of data sources, basic reliability data (obtained from field) and derived reliability data (obtained after performed calculations on basic data).

Thus, the approach is based on combining of the different techniques and data to assess and prove trustworthiness of the assessment results.

2. Operating Reliability Assessment

Reliability data on supplied I&C systems is collected from RPC Radiy customers on regular basis, not less than once in a quarter. Such information includes failure data that is used to calculate operational reliability and can be used for further improvements.

Figure 3 shows toolbox used at RPC Radiy during operating reliability assessment.

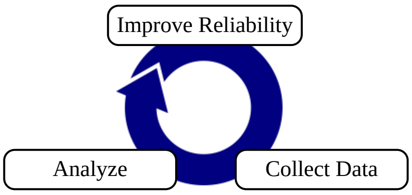


Fig. 3. RPC Radiy's toolbox for operating reliability assessment

During analysis stage the following actions are performed:

– classification of source information by accepted features (operating conditions, type of failed components etc);

– identification of components that reduce the product reliability;

– identification of failure causes;

– efficiency estimation of design-engineering and (or) organizational measures;

– estimation of reliability indices and statistical data processing;

– data processing about usage of spare parts;

– comparison of obtained data with analytical results;

– analysis and classification of data about components failures;

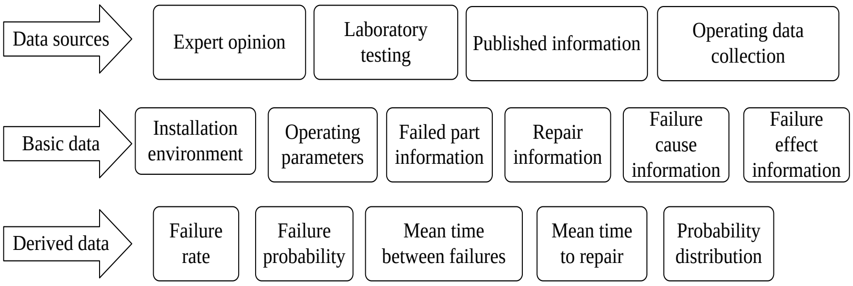


Fig. 2. Reliability data

– identification of possible violations from requirements of maintenance documentation (human errors);

– generation of recommendations on elaboration for removal of detected defects and further improvement of items reliability.

Supply database contains information on supplied I&C systems, including information on beginning of commercial operation of I&C, manufacturing dates of it's parts, information on replacements etc. Figure 4 shows sample report from such database that provides total operation time of NPP I&C systems supplied by RPC Radiy.

3. Analytical Reliability Assessment

As we mentioned in the introduction, there are those areas and reliability assessment tasks that deal with completely new systems or platforms and first-of-its-kind equipment, for which no operating experience exists or it's not representative. For such cases analytical reliability assessment seems to be the only option.

Analytical reliability assessment includes:

– qualitative analysis (identification of failure modes, effects, criticality etc.);

– quantitative analysis (obtaining quantitative reliability indices by calculation);

– evaluation of analysis results.

The following methods are used: CCFA (Common Cause Failure Analysis), FMEDA (Failure Modes, Effects and Diagnostics Analysis), RBD (Reliability Block Diagrams), MM (Markov models), FTA (Fault Tree Analysis), HAZOP (Hazardous Operations).

Figure 5 provides classification of mentioned analytical reliability assessment methods. Basing this classification different attributes of techniques are specified.

Analysis technique of system reliability (no-failure operation) calculation basing on known reliability of its elements was used. Series reliability block diagram was constructed, i.e. failure of any element was considered as failure of the whole system. All failures were considered as independent. Possible software failures were not considered.

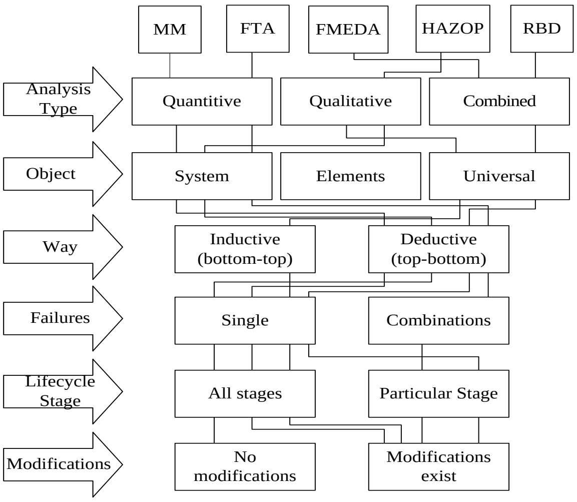


Fig. 5. Classification of analytical reliability assessment methods

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:

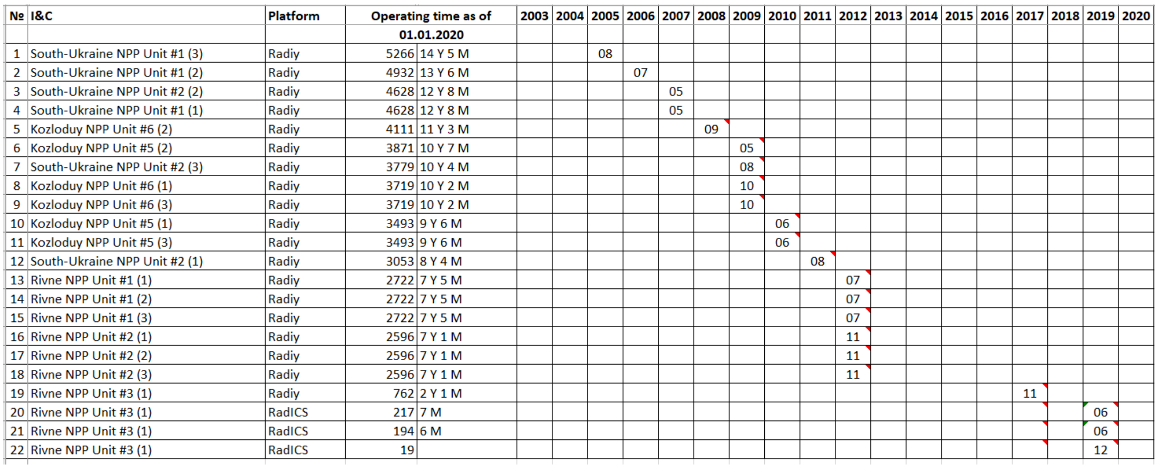
$$P_{sys}(t) = \prod_{k=1}^{n} p_k(t) , \qquad (1)$$

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:

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



№	I&C	Platform	Operating time as of		2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
			01.01.2020																			
1	South-Ukraine NPP Unit #1 (3)	Radiy	5266	14 Y 5 M			08															
2	South-Ukraine NPP Unit #1 (2)	Radiy	4932	13 Y 6 M				07														
3	South-Ukraine NPP Unit #2 (2)	Radiy	4628	12 Y 8 M					05													
4	South-Ukraine NPP Unit #1 (1)	Radiy	4628	12 Y 8 M					05													
5	Kozloduy NPP Unit #6 (2)	Radiy	4111	11 Y 3 M						09												
6	Kozloduy NPP Unit #5 (2)	Radiy	3871	10 Y 7 M							05											
7	South-Ukraine NPP Unit #2 (3)	Radiy	3779	10 Y 4 M							08											
8	Kozloduy NPP Unit #6 (1)	Radiy	3719	10 Y 2 M							10											
9	Kozloduy NPP Unit #6 (3)	Radiy	3719	10 Y 2 M							10											
10	Kozloduy NPP Unit #5 (1)	Radiy	3493	9 Y 6 M								06										
11	Kozloduy NPP Unit #5 (3)	Radiy	3493	9 Y 6 M								06										
12	South-Ukraine NPP Unit #2 (1)	Radiy	3053	8 Y 4 M									08									
13	Rivne NPP Unit #1 (1)	Radiy	2722	7 Y 5 M										07								
14	Rivne NPP Unit #1 (2)	Radiy	2722	7 Y 5 M										07								
15	Rivne NPP Unit #1 (3)	Radiy	2722	7 Y 5 M										07								
16	Rivne NPP Unit #2 (1)	Radiy	2596	7 Y 1 M										11								
17	Rivne NPP Unit #2 (2)	Radiy	2596	7 Y 1 M										11								
18	Rivne NPP Unit #2 (3)	Radiy	2596	7 Y 1 M										11								
19	Rivne NPP Unit #3 (1)	Radiy	762	2 Y 1 M															11			
20	Rivne NPP Unit #3 (1)	RadICS	217	7 M																	06	
21	Rivne NPP Unit #3 (1)	RadICS	194	6 M																	06	
22	Rivne NPP Unit #3 (1)	RadICS	19																		12	

Fig. 4. Total operation time of NPP I&C systems supplied by RPC Radiy

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

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

where λ_k – failure rate of k -th element,

n – number of elements in system.

4. Failure Modes, Effects and Diagnostics Analysis

4.1. Standards

FMEA is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. FMEDA (Failure Mode Effect and Diagnostic Analysis) is an extension of FMEA that combines standard FMEA techniques with the extension to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design.

It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A [1]. The FMEDAs are consistent the FMEA guidance of IEEE Std 352-2016 [2], Sections 4.5.2 and 5.2.

The failure rate data used for the FMEDAs are from the Electrical and Mechanical Component Reliability Handbook [4], which was derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases.

The rates were chosen in a way that is appropriate for safety integrity level verification calculations. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates. For hardware assessment according to IEC 61508 [3], only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures may be excluded from the analysis.

4.2. FPGA Failures

The methods used to estimate the reliability of RadICS (FPGA-based I&C platform produced by RPC Radiy) Modules that are installed in a rack are based on the Electrical and Mechanical Component Reliability Handbook instead of MIL HDBK 217F [10], which is recommended in IEEE Std 352-2016 [2]. The Electrical and Mechanical Component Reliability Handbook provides more current data for modern electronic hardware than MIL HDBK 217F. The FMEDA for each RadICS Module considered the different groups of components that affected module functionality. The following groupings were evaluated:

Common The portion of the RadICS Module that is always used.

Input The portion of the RadICS Module used by one on-board input channel.

Output The portion of the RadICS Module used by one on-board output channel.

LVDS The portion of the logic module providing communication to one input/output module via low-voltage differential signaling.

The following definitions for the failure of the device were considered in order to judge the failure behavior of the RadICS Modules:

Fail-Safe State State where all discrete outputs are de-energized.

Fail-Safe Failure that causes the device to go to the defined fail-safe state without a demand from the process. (abbreviation: S).

Fail-Safe Detected Failure that is detected by automatic self-diagnostics, which causes the output signal to go to the predefined fail-safe state (i.e., output modules de-energized). (abbreviation: SD).

Fail-Safe Undetected Failure that is safe and that is not diagnosed by automatic self-diagnostics. (abbreviation: SU).

Fail Dangerous Failure that does not respond to a demand from the process (i.e., being unable to go to the defined fail-safe state).

Analog Input Failure that deviates the measured input value by more than 2 % of span and leaves the value within active scale.

Fail Dangerous Detected Failure that is dangerous but is detected by automatic diagnostics. (abbreviation: DD).

Fail Dangerous Undetected Failure that is dangerous and that is not being diagnosed by automatic diagnostics. (abbreviation: DU).

No Effect Failure of a component that is part of the safety function but that has no effect on the safety function. (abbreviation: NE) It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508:2010.

Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (e.g., a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm. This condition leads to maintenance, and if the safety channel is not shut down (put into the safe state) during this maintenance, the time must be accounted for in any system level reliability calculation. (abbreviation: AD).
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (e.g., a fault in a diagnostic circuit) and that is not detected by internal diagnostics. AU failures are treated as No Effect failures for Safe Failure Fraction calculation. (abbreviation: AU).
Fail Dangerous Undetected after Surveillance Test	Failure that is dangerous and that is not being diagnosed by either automatic diagnostics or the periodic surveillance test. (abbreviation: DUaPT).

The failure categories listed above expand on the categories listed in IEC 61508:2010 [3], which are only safe and dangerous, both detected and undetected. Under IEC 61508:2010, the No Effect failures cannot contribute to the failure rate of the safety function.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508:2010. It is assumed that the probability model will correctly account for the Annunciation failures; otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508:2010 (worst-case assumption).

4.3. FPGA Failure Modes

FPGA-based systems are analyzed on different implementation level. For example, in [7] failure taxonomy is provided for system level, division level, I&C unit level, I&C module level, while in [8] failure modes are provided for FPGA itself. In order to attain a realistic model and satisfactory accuracy of the analysis, we propose to represent FPGA-based system at the following implementation level: configurable logic blocks made available by a given FPGA chip.

The following failure modes could be considered:

– MUX select;

– Programmable Interconnect Points (PIP) short;

– PIP open;

– buffer off;

– buffer on;

– Lookup Table(LUT) value change;

– control bit change;

– user flip-flop;

– block random access memory (RAM);

– half-latches;

– power network.

4.4. Tool Support

Reliability assessment complexity necessitates development of software tools that assist plant personnel and vendor engineers to manage reliability assessment activities and can provide solutions to various decision making issues.

As was discussed in [9], the following is to be considered during selection of software package:

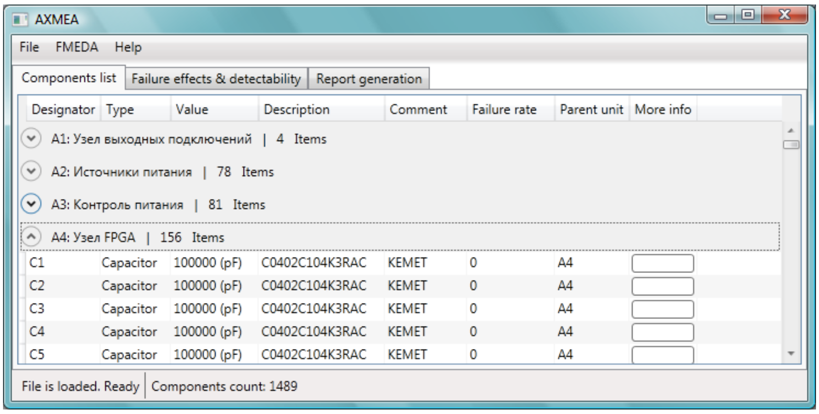
– types of data input (graphically, as a plain text, in a matrix form etc);

– export (import) features;

– supported analysis methods;

– embedded feature of reports generation.

At RPC Radiy we use our own developed tool called AXMEA (Figure 6). So far it supports only FMEDA, but adding other methods and techniques to it is in progress.

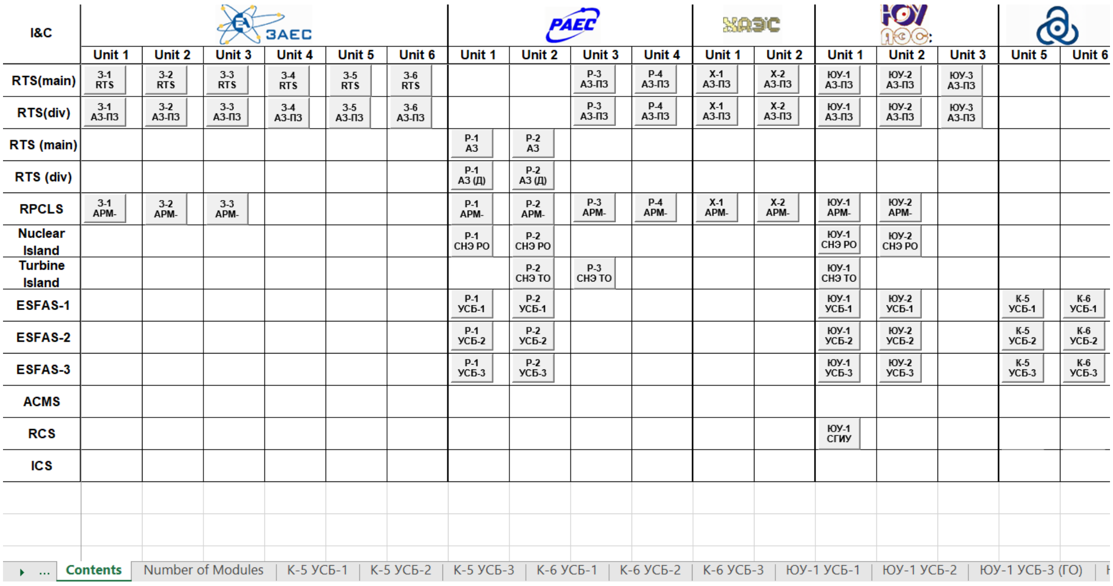


Designator	Type	Value	Description	Comment	Failure rate	Parent unit	More info
A1: Узел выходных подключений | 4 Items							
A2: Источники питания | 78 Items							
A3: Контроль питания | 81 Items							
A4: Узел FPGA | 156 Items							
C1	Capacitor	100000 (pF)	C0402C104K3RAC	KEMET	0	A4	
C2	Capacitor	100000 (pF)	C0402C104K3RAC	KEMET	0	A4	
C3	Capacitor	100000 (pF)	C0402C104K3RAC	KEMET	0	A4	
C4	Capacitor	100000 (pF)	C0402C104K3RAC	KEMET	0	A4	
C5	Capacitor	100000 (pF)	C0402C104K3RAC	KEMET	0	A4	

File is loaded. Ready | Components count: 1489

Fig. 6. AXMEA Tool

For operational reliability assessment is a spreadsheet-based tool is used (Figure 7). This tool summarizes data on all I&Cs supplied by RPC Radiy, providing information on system, module and component level.



I&C	ЗАЕС						PAEC				ХАЭС		ЮУАЭС				
	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5	Unit 6	Unit 1	Unit 2	Unit 3	Unit 4	Unit 1	Unit 2	Unit 1	Unit 2	Unit 3	Unit 5	Unit 6
RTS(main)	З-1 RTS	З-2 RTS	З-3 RTS	З-4 RTS	З-5 RTS	З-6 RTS			Р-3 АЗ-ПЗ	Р-4 АЗ-ПЗ	Х-1 АЗ-ПЗ	Х-2 АЗ-ПЗ	ЮУ-1 АЗ-ПЗ	ЮУ-2 АЗ-ПЗ	ЮУ-3 АЗ-ПЗ		
RTS(div)	З-1 АЗ-ПЗ	З-2 АЗ-ПЗ	З-3 АЗ-ПЗ	З-4 АЗ-ПЗ	З-5 АЗ-ПЗ	З-6 АЗ-ПЗ			Р-3 АЗ-ПЗ	Р-4 АЗ-ПЗ	Х-1 АЗ-ПЗ	Х-2 АЗ-ПЗ	ЮУ-1 АЗ-ПЗ	ЮУ-2 АЗ-ПЗ	ЮУ-3 АЗ-ПЗ		
RTS (main)							Р-1 АЗ	Р-2 АЗ									
RTS (div)							Р-1 АЗ (Д)	Р-2 АЗ (Д)									
RPCLS	З-1 АРМ-	З-2 АРМ-	З-3 АРМ-				Р-1 АРМ-	Р-2 АРМ-	Р-3 АРМ-	Р-4 АРМ-	Х-1 АРМ-	Х-2 АРМ-	ЮУ-1 АРМ-	ЮУ-2 АРМ-			
Nuclear Island							Р-1 СНЭ РО	Р-2 СНЭ РО					ЮУ-1 СНЭ РО	ЮУ-2 СНЭ РО			
Turbine Island								Р-2 СНЭ ТО	Р-3 СНЭ ТО				ЮУ-1 СНЭ ТО				
ESFAS-1							Р-1 УСБ-1	Р-2 УСБ-1					ЮУ-1 УСБ-1	ЮУ-2 УСБ-1		К-5 УСБ-1	К-6 УСБ-1
ESFAS-2							Р-1 УСБ-2	Р-2 УСБ-2					ЮУ-1 УСБ-2	ЮУ-2 УСБ-2		К-5 УСБ-2	К-6 УСБ-2
ESFAS-3							Р-1 УСБ-3	Р-2 УСБ-3					ЮУ-1 УСБ-3	ЮУ-2 УСБ-3		К-5 УСБ-3	К-6 УСБ-3
ACMS																	
RCS													ЮУ-1 СГИУ				
ICS																	

... Contents | Number of Modules | К-5 УСБ-1 | К-5 УСБ-2 | К-5 УСБ-3 | К-6 УСБ-1 | К-6 УСБ-2 | К-6 УСБ-3 | ЮУ-1 УСБ-1 | ЮУ-1 УСБ-2 | ЮУ-1 УСБ-3 (ГО) |

Fig. 7. Spreadsheet for Operating Reliability Assessment

5. Case Study

As an example we take Speed Measuring Device, which block diagram is shown on Figure 8.

Speed Measuring Device includes the following blocks:

– Variable Reluctance Speed Sensor (A0);

– DC/DC converters (A1, A7);

– Variable Reluctance Speed Sensor interface device (A2);

– optocouplers (A3, A5, A8);

– AC/DC converter (A4);

– logic solver (A6);

– output converters (A9);

– relay (A10).

Blocks A3 and A10 are used only to switch device into testing mode and are not used during normal device operation, therefore they are not taken into reliability analysis.

Figure 9 shows reliability block diagram for Speed Measuring Device. Since block A7 is identical to block A1, and block A8 to A5, they are shown on reliability block diagram as 2*A1 and 2*A5 accordingly.

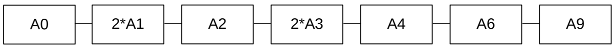


Fig. 9. Reliability Block Diagram
of Speed Measuring Device

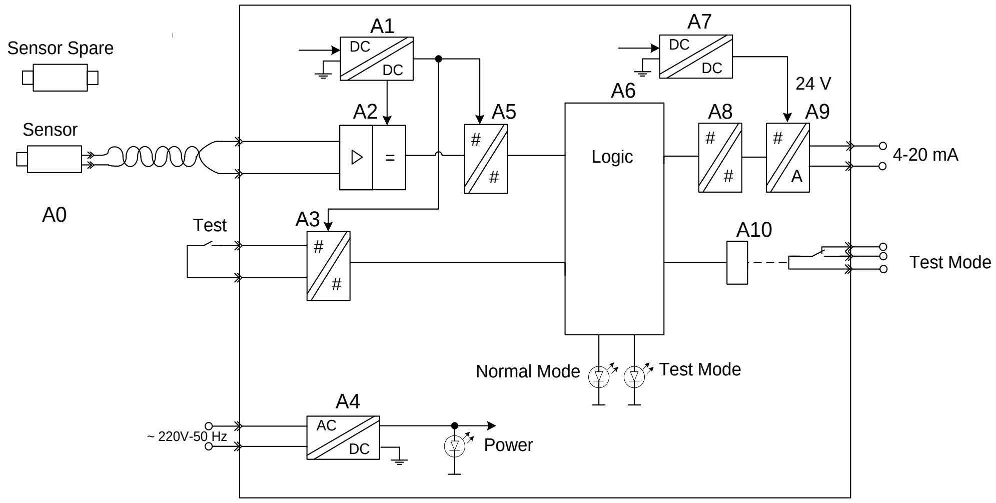


Fig. 8. Block Diagram of Speed Measuring Device

Failure rates for blocks A1-A9 were obtained from supplier documentation. For A0 failure rate MIL-217F [10] was used. The failure rate for this component is defined as:

$$\lambda_p = \lambda_B \pi_T \pi_Q \pi_E / 10^6, \quad (4)$$

Table 1 provides values required for calculation.

Table 1

Values for A0 failure rate calculation

Parameter	Value	Comments
λ_B	0.000050/10^6	Assumed variable inductor (MIL-HDBK-217F [10], Section 11.2)
π_T	3.5	Operation should not exceed +150°C T_{HS} used +150°C (MIL-HDBK-217F [10], Section 11.2)
π_Q	3.0	Commercial component (MIL-HDBK-217F [10], Section 11.2)
π_E	6.0	Assumed “Ground Fixed” environment (MIL-HDBK-217F [10], Section 11.2)

Calculated failure rate of A0 is 3.15E-09.

Table 2 summarizes failures rates for all blocks.

Table 2

Failure rates

No.	Block	Part Type	Quantity of Parts	Failure Rate	Data Origin
1.	A0	VRS SEN-SOR	1	3.15E-09	MIL-HDBK-217F
2.	A1	DC/DC	2	2.23E-07	recom-international.com
3.	A2	AMPL	1	2.24E-08	maximintegrated.com
4.	A3	OPTO	2	1.39E-07	avagotech.com
5.	A4	AC/DC	1	2.78E-06	recom-international.com
6.	A6	FPGA	1	2.98E-07	intel.com
7.	A9	DAC	1	1.43E-09	analog.com

Failure rate of Speed Measuring Device is 3.82898 E-06, and mean time between failures is 261166 hours.

Conclusions

In this paper we have introduced approach to assessment of FPGA-based NPP I&C systems which was implemented by RPC Radiy during last ten years. It is based on combining of the techniques of operational and analytical calculation and assessment of the systems. The most interesting and important points of this approach are renewing of the data for operational assessment and possibilities of comparing results using different techniques and different combinations of the techniques chains.

The future steps will be dedicated to development reliability assessment environment for NPP I&C systems using commercial off-the-shelf and RPC Radiy tools.

Acknowledgement. The authors are grateful to colleagues from RPC Radiy and Computer Systems, Networks and Cybersecurity Department, National Aerospace University “Kharkiv Aviation Institute” for discussion of research results. Besides, this research is supported by the project STARC (Methodology of SusTAinable Development and InfoRmation Technologies of Green Computing and Communication) funded by Ministry of Education and Science of Ukraine.

References (GOST 7.1:2006)

1. MIL STD 1629A, Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis [Text]. – 1980 – 54 p.

2. IEEE Std 352-2016, Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems [Text]. – IEC, 2016. – 155 p.

3. IEC 61508:2010, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems. Parts 1-7 [Text]. – IEC, 2010.

4. Electrical & Mechanical Component Reliability Handbook. Third Edition [Text]. – Exida LLC, 2012. – 132 p.

5.. Combined Implementation of Dependability Analysis Techniques for NPP I&C Systems Assessment [Text] / V. Kharchenko et al // Journal of Energy and Power Engineering. – 2011. – Vol. 5. – P. 411-418.

6. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security [Text] / M. Yastrebenetsky, V. Kharchenko (editors). – IGI Global, USA, 2014. – 470 p.

7. NEA/CSNI/R(2014)16 Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis [Text]. – Nuclear Energy Agency, 2014. – 136 p.

8. An Introduction to Radiation-Induced Failure Modes and Related Mitigation Methods For Xilinx SRAM FPGAs [Text] / H. Quinn, et al // Proceedings of the 2008 International Conference on Engineering of Reconfigurable Systems & Algorithms. –2008. – P. 1-7.

9. Markov's Modeling of NPP I&C Reliability and Safety [Text] / V. Kharchenko et al // Proceedings of The Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management. – 2016. – P. 328-336.

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

References (BSI)

1. *MIL STD 1629A, Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*, 1980. 54 p.

2. *IEEE Std 352-2016, Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, IEC, 2016. 155 p.

3. *IEC 61508:2010, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems.* Parts 1-7, IEC, 2010.

4. *Electrical & Mechanical Component Reliability Handbook*, Third Edition, Exida LLC, 2012. 132 p.

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

6. Yastrebenetsky, M., Kharchenko, V. (editors) *Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*, IGI Global, USA, 2014. 470 p.

7. *NEA/CSNI/R(2014)16 Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis.* Nuclear Energy Agency, 2014. 136 p.

8. Quinn, H., et al. An Introduction to Radiation-Induced Failure Modes and Related Mitigation Methods For Xilinx SRAM FPGAs. *Proceedings of the 2008 International Conference on Engineering of Reconfigurable Systems & Algorithms*, 2008, pp. 1-7.

9. Kharchenko, V. et al. Markov's Modeling of NPP I&C Reliability and Safety. *Proceedings of The Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management*, 2016, pp. 328-336.

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

Надійшла до редакції 17.06.2020, розглянута на редколегії 15.09.2020

ПРАКТИЧНІ АСПЕКТИ ОПЕРАЦІЙНОГО ТА АНАЛІТИЧНОГО ОЦІНЮВАННЯ НАДІЙНОСТІ ІУС НА ПЛІС

Є. В. Бабешко, В. С. Харченко, К. П. Леонтієв, Є. В. Ручков

Оцінювання експлуатаційної надійності інформаційно-управляючих систем (ІУС) є одним з найбільш важливих напрямків діяльності, особливо в критичних областях, таких як атомні електростанції (АЕС). Вона є важливим джерелом інформації щодо надійності ІУС, кращим, ніж дані, отримані за результатами лабораторних випробувань, оскільки надає інформацію про надійність ІУС в реальних умовах використання. Тому у теперішній час для компаній стало звичайною практикою впроваджувати процес збору даних з експлуатаційної надійності на великій кількості використовуваних компонентів на регулярній основі, підтримувати базу даних з інформацією про відмови, сумарним напрацюванням, типовими видами відмов і т.д.

Інтенсивне використання складних компонентів, таких як програмовані логічні інтегральні схеми (ПЛІС) у модернізованих і у новозбудованих АЕС, робить дуже актуальним завдання розроблення та затвердження передових методів оцінювання експлуатаційної надійності, що враховують особливості конкретних технологій. Висока щільність інтеграції призводить до того, що надійність інтегральних схем стає найбільш важливою характеристикою сучасних ІУС АЕС. Більш того, ПЛІС істотно відрізняються від інших інтегральних схем: вони поставляються в вигляді заготовок і сильно залежать від створеної в них конфігурації. Крім того, конфігурація ПЛІС може через змінюватися під час планового відключення АЕС з різних причин. Урахування всіх можливих відмов ІУС на ПЛІС на етапі проєктування – достатньо складне завдання. Таким чином, оцінювання експлуатаційної надійності є одним з найбільш затребуваних способів проведення комплексного аналізу ІУС на ПЛІС. Аналіз літературних джерел і власний досвід показали, що експлуатаційна надійність може істотно відрізнятися від аналітичної. З цієї причини аналітичне оцінювання надійності з використанням структурних схем надійності (RBD), аналізу видів, наслідків і діагностованості відмов (FMEDA), аналізу дерева відмов (FTA), тестування засівом дефектів (FIT) та інших методів і їх комбінацій, є важливим для відповідності вимогам, що пред'являються до таких систем. У даній статті узагальнено наш досвід аналізу експлуатаційної надійності ІУС на ПЛІС.

Ключові слова: аналіз надійності; структурні схеми надійності; аналіз видів, наслідків та діагностованості відмов.

ПРАКТИЧЕСКИЕ АСПЕКТЫ ОПЕРАЦИОННОГО И АНАЛИТИЧЕСКОГО ОЦЕНИВАНИЯ НАДЕЖНОСТИ ИУС НА ПЛИС

Е. В. Бабешко, В. С. Харченко, К. П. Леонтиев, Е. В. Ручков

Оценка эксплуатационной надежности информационно-управляющих систем (ИУС) является одним из наиболее важных направлений деятельности, особенно в критических областях, таких как атомные электростанции (АЭС). Она является важным источником информации о надежности ИУС, более предпочтительным, чем данные, полученные по результатам лабораторных испытаний, поскольку предоставляет информацию о надежности ИУС в реальных условиях использования. Поэтому в настоящее время для компаний стало обычной практикой внедрять процесс сбора данных об эксплуатационной надежности на большом количестве используемых компонентов на регулярной основе, поддерживать базу данных с информацией об отказах, суммарной наработкой, типовыми видами отказов и т.д.

Интенсивное использование сложных компонентов, таких как программируемые логические интегральные схемы (ПЛИС) в модернизируемых и во вновь построенных АЭС, делает очень актуальной задачу разработки и валидации передовых методов оценки эксплуатационной надежности, которые учитывают особенности конкретных технологий. Высокая плотность интеграции приводит к тому, что надежность интегральных схем становится наиболее важной характеристикой современных ИУС АЭС. Более того, ПЛИС существенно отличаются от других интегральных схем: они поставляются в виде заготовок и сильно зависят от созданной в них конфигурации. Кроме того, конфигурация ПЛИС может изменяться во время планового отключения АЭС по разным причинам. Учет всех возможных отказов ИУС на ПЛИС на этапе проектирования - довольно сложная задача. Таким образом, оценка эксплуатационной надежности является одним из наиболее предпочтительных способов проведения комплексного анализа ИУС на ПЛИС. Анализ литературных источников и собственный опыт показали, что эксплуатационная надежность может существенно отличаться от аналитической. По этой причине аналитическая оценка надежности с использованием структурных схем надежности (RBD), анализа видов, последствий и диагностируемости отказов (FMEDA), анализа дерева отказов (FTA), тестирования засевом дефектов (FIT) и других методов и их комбинаций, является важным для соответствия требованиям, предъявляемым к таким системам. В данной статье обобщен наш опыт анализа эксплуатационной надежности ИУС на ПЛИС.

Ключевые слова: анализ надежности; структурные схемы надежности; анализ видов, последствий и диагностируемости отказов.

Бабешко Євген Васильович – канд. техн. наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, професор, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Леонтієв Костянтин Петрович – директор технічний, Науково-виробниче підприємство «Радій», Кропивницький, Україна.

Ручков Євген Валентинович – начальник відділу супроводження КБ АСУ ТП, Науково-виробниче підприємство «Радій», Кропивницький, Україна.

Eugene Babeshko – PhD in Technical Science, Associate Professor of Computer Systems, Networks and Cyber Security Department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: e.babeshko@csn.khai.edu,
ORCID Author ID: 0000-0002-4667-2393, Scopus Author ID: 24823713000, ResearcherID: I-9973-2018,
https://scholar.google.com.ua/citations?user=PO6LPVsAAAAJ.

Vyacheslav Kharchenko – DrS, Professor, Head of Computer Systems, Networks and Cyber Security Department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: v.kharchenko@csn.khai.edu,
ORCID Author ID: 0000-0001-5352-077X, Scopus Author ID: 22034616000, ResearcherID: A-7719-2017,
https://scholar.google.com.ua/citations?user=FQ4dH4EAAAAJ.

Kostiantyn Leontiiev – technical director, Research and production corporation "Radiy", Kropyvnytskyi, Ukraine,
e-mail: ksleontiev@radiy.com, Scopus Author ID: 57195923255

Eugene Ruchkov – head of support department, Research and production corporation "Radiy", Kropyvnytskyi, Ukraine,
e-mail: rev@radiy.com, ORCID Author ID: 0000-0002-4570-9844.