Comparative Reliability Analysis of Reactor Trip System Architectures: Industrial Case

Aleksei Vambol[1] and Vyacheslav Kharchenko[1,2]

[1] Department of Computer Systems, Networks and Cybersecurity,
National Aerospace University «KhAI», Kharkiv, Ukraine
[2] Centre for Safety Infrastructure-Oriented Research and Analysis,
RPC Radiy, Kropyvnytskyi, Ukraine
{o.vambol,v.kharchenko}@csn.khai.edu

Abstract. The aim of this paper is to propose the approach to choosing the most reliable architecture of reactor trip system. The industrial case is based on the systems developed by the use of the platform «RadICS produced by RPC «Radiy». The two-channel three-chassis and three-channel two-chassis architectures were analyzed using their reliability block diagrams (RBDs). The results of analysis show that no architecture among the given ones can be unconditionally considered the most reliable. The choice of the best alternative in terms of reliability can be made using the formulae proposed in the given paper, which allow to take into account the reliabilities of the blocks of RBDs and the percents of common failures for certain types of elements. The analytical expressions for the mean of the advantage and the percent of superiority cases in terms of reliability were obtained for the considered architectures using the aforementioned formulae. The approach to searching the cases of maximal superiority in reliability for the analyzed architectures has been proposed. The aforesaid analysis can be conducted for an arbitrary pair of architectures represented by their RBDs.

Keywords: reliability, reactor trip system, comparative analysis, common cause failure, RadICS

1 Introduction

1.1 Motivation

Reliability of reactor trip systems (RTS) is of great importance for safety of a nuclear power plant. Among such systems the ones based on the FPGA platform RadICS, developed and produced by RPC «Radiy», deserve considerable attention [1, 2]. As this platform allows implementation of systems with different architectures, it is necessary to have an approach to their comparison in terms of reliability. The two-channel three-chassis architecture (2C3), briefly described in [1], and the three-channel two-chassis (3C2) one, outlined in [2], are good examples of the aforesaid multeity. Their reliability block diagrams (RBDs) are given in Figure 1.

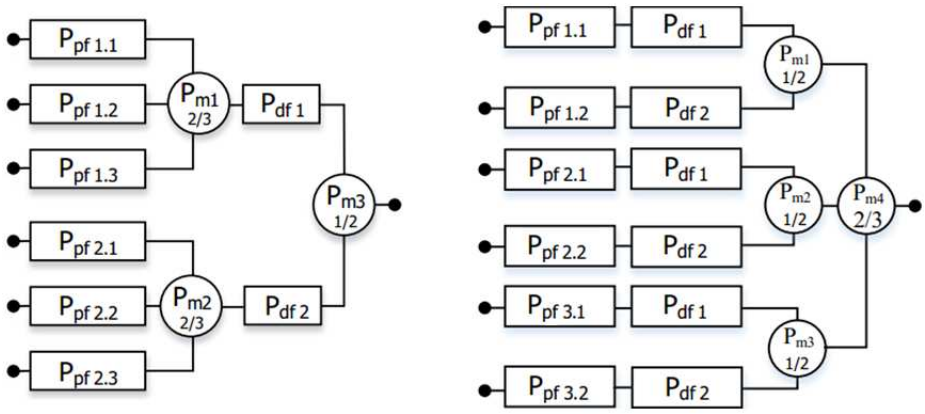

Figure 1. Two-channel three-chassis (left) and three-channel two-chassis (right) RTSes [1, 2].

The signals of RTSes considered in this paper are formed on the basis of output signals of independent channels according to 1-out-of-2 (for 2C3) or 2-out-of-3 (for 3C2) voting logic. The elements implementing these logics are designated in Figure 1 as «1/2» and «2/3» blocks. Each channel uses output signals of its underlying chassis to generate a signal in obedience to one of the aforesaid voting logics [1, 2].

The chassis consist of five components: analogue and digital input modules, logic module, analogue and digital output modules. Each of these components is based on FPGA chips. All modules must be in working states to provide the failure-free operation of the chassis, the reliability of which is affected by physical and design faults. Therefore, the chassis are represented in Figure 1 as serially connected «pf» (physical faults) and «df» (design faults) blocks [2].

Usually RTS is developed using 2C3 architecture. It is caused by special requirements to safety critical systems which are joint by the principle of independence. This principle implies, firstly, independent forming of main and diverse signals for RTS by redundant and diverse channels, and, secondly, their separate placing in different constructions (for example, cabinets) [3]. However, in terms of reliability, 3C2 architecture can be more appropriate. Hence, there are two reasons to compare these architectures:

1) it's possible that there are other application areas where requirements regarding independence are not strong;

2) in terms of safety, the benefits due to higher reliability could be more irrefutable than ones caused by independence.

1.2 Objectives and an approach

The aim of this research is to propose the approach to choosing the most reliable version from the aforementioned pair of architectures. The proposed analysis algorithm can be performed in case of arbitrary pair of RBDs.

Within the scope of this work the elements of the same type are considered to possess equal reliability. In the rest of this paper the RBDs and corresponding architectures are designated as «left» and «right» for the purpose of brevity.

The paper is structured as follows. Sections 2-4 are dedicated to consecutive consideration of three cases, which differ in the number of parameters. The analysis begins with the ideal case, where «1/2» and «2/3» blocks are absolutely reliable, and each next occasion generalizes the previous one. Section 5 is devoted to study of the case in which the underlying elements have such failure rates as in [1] and [2]. The obtained results and possible directions for further research are discussed in Section 6. Besides, this section gives some recommendations for choosing between the analyzed architectures.

1.3 Related work

There are a lot of papers [4-7] where typical KooN (1oo2, 2oo3, etc.) architectures have been researched. However, the RBDs in Figure 1 are more complex and implement the principle of a structural-version redundancy to minimize risk of common cause failures [8].

Besides, the reliability of such structures depends on more initial parameters, in particular, rates of failures due to physical and design faults of channels (versions), failure rates of voting units, diversity metrics and so on.

Hence, choosing the most reliable architecture from the considered pair should be based on a detailed analysis of the effect of the aforesaid parameters on reliability indicators.

2 Ideal case: Absolutely reliable «1/2» and «2/3» elements

Let r denote the reliability of inputs of «1/2» and «2/3» blocks. In this case the reliability formulae for absolutely reliable «1/2» and «2/3» elements are $2r - r^2$ and $3r^2 - 2r^3$ [9]. Thus, the reliability formulae for the left and right RBDs are

$$P_L(p,q) = 2q(3p^2 - 2p^3) - q^2(3p^2 - 2p^3)^2, \quad (1)$$

$$P_R(p,q) = 3(2pq - p^2q^2)^2 - 2(2pq - p^2q^2)^3, \quad (2)$$

where p and q are reliabilities of the blocks prone to potential failures caused by «pf» (physical faults) and «df» (design faults), respectively.

It can be supposed that for some values of p and q the right RBD surpasses the left one in terms of reliability, while for other values of the parameters the left RBD is the most reliable. Optimization algorithms for multivariate functions can be used to find such a pair (p, q) for which the reliability advantage of the right RBD over the left one is maximal (or minimal). This problem can be solved by the search of maximum and minimum of $\Delta P(p,q) = P_R(p,q) - P_L(p,q)$ with the constraints $p, q \in (0; 1]$. The computing environment MATLAB can be used for the given purpose.

The script for searching maximum and minimum of ΔP(p,q) can be written in the following way:

```
dp = @(p,q) ((3*(2*p*q - p^2*q^2)^2 - ...
2*(2*p*q - p^2*q^2)^3) - (2*q*(3*p^2 - 2*p^3) - ...
q^2*(3*p^2 - 2*p^3)^2));
lp = createOptimProblem('fmincon','x0',[0.5,0.5], ...
'objective',@(x)(dp(x(1),x(2))),'lb',[0,0],'ub',[1,1]);
hp = createOptimProblem('fmincon','x0',[0.5,0.5], ...
'objective',@(x)(-dp(x(1),x(2))),'lb',[0,0],'ub',[1,1]);
gs = GlobalSearch();
lr = run(gs, lp);
hr = run(gs, hp);
disp(join([" Minimum: ", lr, newline, "Maximum: ", hr]));
```

The aforementioned computations lead to the results given in Table 1.

Table 1. Cases of a maximal reliability advantage for the left and right RBDs.

Advantageous structure	**p**	**q**	**ΔP**
Left structure	0.75	0.17333	0.1226
Right structure	0.33333	1	0.1317

The plot of ΔP(p,q), which is given in Figure 2, can be built using the given script:

```
dp = @(p, q) ((3*(2*p*q - p^2*q^2)^2 - ...
2*(2*p*q - p^2*q^2)^3) - (2*q*(3*p^2 - 2*p^3) - ...
q^2*(3*p^2 - 2*p^3)^2));
fsurf(dp, [0, 1, 0, 1], "EdgeColor", "none", ...
"MeshDensity", 200);
colormap(gray); xlabel("p"); ylabel("q"); box on;
```

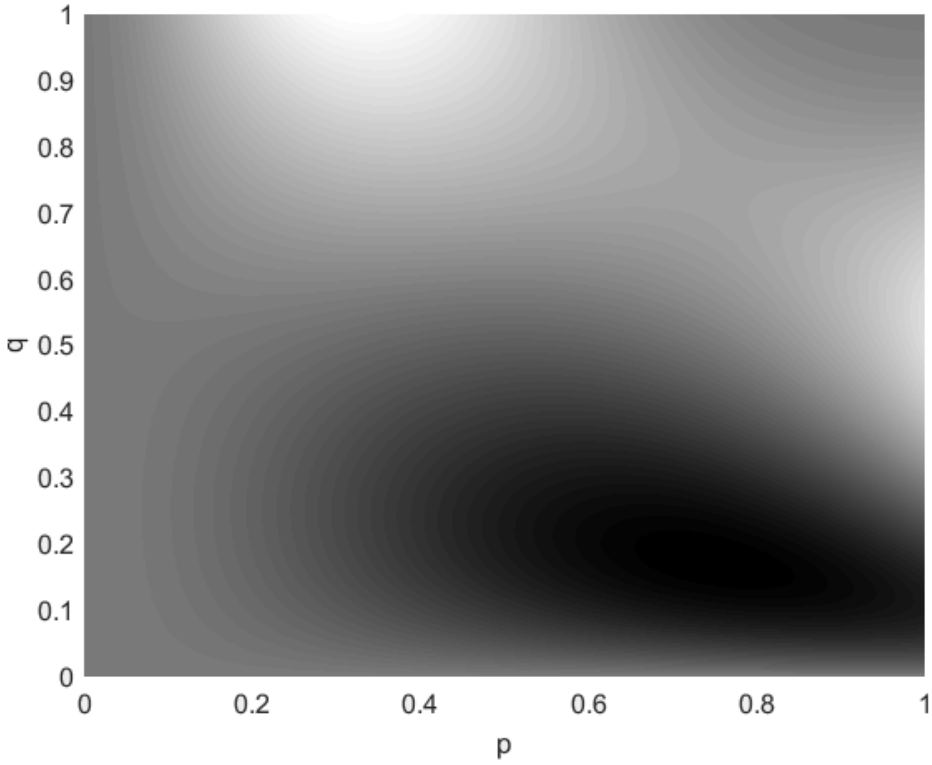

Figure 2. The plot of ΔP(p,q).

Brighter areas of the given plot correspond to higher values of ΔP(p,q), which indicate a greater reliability advantage of the right RBD over the left one.

Consider the expression H(ΔP(p,q)), where H(x) is Heaviside step function, which equals 0 for $x < 0$ and 1 for $x \geq 0$. This composite function is equal to 0 if for a pair (p, q) the left RBD surpasses the right one in terms of reliability. In other cases its value is 1.

Figure 3 represents the plot of H(ΔP(p,q)). The black area corresponds to the value pairs of p and q for which the left RBD is more reliable than the right one. The script for the given plot can be constructed as follows:

```
dp = @(p, q) heaviside((3*(2*p*q - p^2*q^2)^2 - ...
2*(2*p*q - p^2*q^2)^3) - (2*q*(3*p^2 - 2*p^3) - ...
q^2*(3*p^2 - 2*p^3)^2));
fsurf(dp, [0, 1, 0, 1], "EdgeColor", "none", ...
"MeshDensity", 200);
colormap(gray); xlabel("p"); ylabel("q"); box on;
```

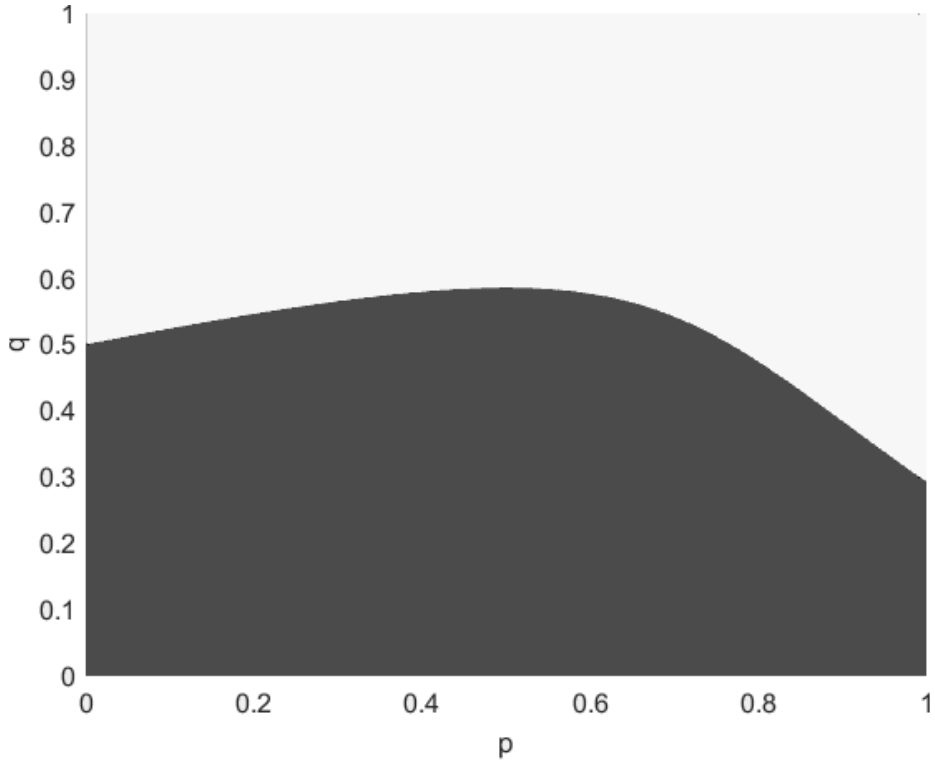

Figure 3. The plot of H(ΔP(p,q)).

Let A denote the average value of ΔP(p,q) over all p, q ∈ (0; 1]. It can be found using the formula from [10] for the average value of a function over a region as follows:

$$A = \int_0^1 \int_0^1 \Delta P(p,q)\, dp\, dq$$

Let S denote the percent of cases in which the right RBD is more reliable than the left one. It can be obtained as multiplied by 100 average value of H(ΔP(p,q)) over all p, q ∈ (0; 1]. By dint of the approach used for A, the following formula is found:

$$S = 100 \int_0^1 \int_0^1 H(\Delta P(p,q))\, dp\, dq$$

The script for calculating the value of A can be written in the following way:

```
syms p q
dp = @(p, q) (3*(2*p*q - p^2*q^2)^2 - ...
```

```
2*(2*p*q - p^2*q^2)^3) - (2*q*(3*p^2 - 2*p^3) - ...
q^2*(3*p^2 - 2*p^3)^2);
vpaintegral(vpaintegral(dp, p, [0 1]), q, [0 1])
```

In the case of S the script can be built as follows:

```
syms p q
hdp = @(p, q) 100*heaviside((3*(2*p*q - p^2*q^2)^2 - ...
2*(2*p*q - p^2*q^2)^3) - (2*q*(3*p^2 - 2*p^3) - ...
q^2*(3*p^2 - 2*p^3)^2));
vpaintegral(vpaintegral(hdp, p, [0 1], "AbsTol", ...
0.001), q, [0 1], "AbsTol", 0.001)
```

The given computations yield A = -0.00537415 and S = 48.15.

3 Ordinary case: Partially reliable «1/2» and «2/3» elements

In the case of not absolutely reliable «1/2» and «2/3» elements, which have reliability values u and v respectively, the reliability formulae for the left and right RBDs can be written in the following way:

$$P_L(p,q,u,v) = u(2qv(3p^2 - 2p^3) - q^2v^2(3p^2 - 2p^3)^2), \quad (3)$$

$$P_R(p,q,u,v) = v(3u^2(2pq - p^2q^2)^2 - 2u^3(2pq - p^2q^2)^3). \quad (4)$$

The aforesaid formulae can be obtained using the modification of the approach for the ideal case, where the reliability formulae for «1/2» and «2/3» elements are replaced with the results of their multiplication by u and v, respectively.

The script for searching global extrema of $\Delta P(p,q,u,v) = P_R(p,q,u,v) - P_L(p,q,u,v)$ with the constraints $p, q, u, v \in (0; 1]$ can be written as follows:

```
dp = @(p, q, u, v)((v*(3*u^2*(2*p*q - p^2*q^2)^2 - ...
2*u^3*(2*p*q - p^2*q^2)^3) - u*(2*q*v*(3*p^2 - 2*p^3) ...
- q^2*v^2*(3*p^2 - 2*p^3)^2)));
lp = createOptimProblem('fmincon','x0',[0.5,0.5, ...
0.5,0.5],'objective',@(x)(dp(x(1),x(2),x(3),x(4))), ...
'lb',[0,0,0,0],'ub',[1,1,1,1]);
hp = createOptimProblem('fmincon','x0',[0.5,0.5, ...
0.5,0.5],'objective',@(x)(-dp(x(1),x(2),x(3),x(4))), ...
'lb',[0,0,0,0],'ub',[1,1,1,1]);
gs = GlobalSearch();
lr = run(gs, lp);
hr = run(gs, hp);
disp(join([" Minimum: ", lr, newline, "Maximum: ", hr]));
```

The aforesaid computations yield the results given in Table 2.

Table 2. Cases of a maximal reliability advantage for the left and right RBDs with partially reliable «1/2» and «2/3» elements.

Advantageous structure	**p**	**q**	**u**	**v**	**ΔP**
Left structure	0.99967	1	1	0.5	0.25
Right structure	0.33333	1	1	1	0.1317

The mean of ΔP(p,q,u,v) is calculated according to the following formula:

$$A = \int_0^1 \int_0^1 \int_0^1 \int_0^1 \Delta P(p,q,u,v)\, dp\, dq\, du\, dv$$

The percent of cases in which the right RBD is more reliable:

$$S = 100 \int_0^1 \int_0^1 \int_0^1 \int_0^1 H(\Delta P(p,q,u,v))\, dp\, dq\, du\, dv$$

These formulae can be obtained using the corresponding approach for the ideal case.

The script for calculating the value of A can be constructed in the following way:

```
syms p q u v
dp = @(p, q, u, v)((v*(3*u^2*(2*p*q - p^2*q^2)^2 - ...
2*u^3*(2*p*q - p^2*q^2)^3) - u*(2*q*v*(3*p^2 - 2*p^3) ...
- q^2*v^2*(3*p^2 - 2*p^3)^2)));
vpaintegral(vpaintegral(vpaintegral(vpaintegral(dp, ...
p, [0 1], "AbsTol", 0.001), q, [0 1], "AbsTol", ...
0.001), u, [0 1], "AbsTol", 0.001), v, [0 1], ...
"AbsTol", 0.001)
```

The value of S can be calculated using the following script:

```
syms p q u v
hdp = @(p, q, u, v) 100*heaviside((v*(3*u^2*(2*p*q - ...
p^2*q^2)^2 - 2*u^3*(2*p*q - p^2*q^2)^3) - ...
u*(2*q*v*(3*p^2 - 2*p^3) - q^2*v^2*(3*p^2 - 2*p^3)^2)));
vpaintegral(vpaintegral(vpaintegral(vpaintegral(hdp, ...
p, [0 1], "AbsTol", 1), q, [0 1], "AbsTol", 1), ...
u, [0 1], "AbsTol", 1), v, [0 1], "AbsTol", 1)
```

The given computations yield $A \approx -0.029$ and $S \approx 5$.

4 Generalized case: Common failures in «pf» and «df» elements

The previous case can be generalized by considering all «pf» and «df» blocks as having 100h% and 100s% of common failures, respectively. The probability of failure-free operation for the given RBDs under the condition of absence of common failure can be calculated using (3) and (4) by substituting

$$x = p / (1 - h(1 - p)) \text{ for } p,$$
$$y = q / (1 - s(1 - q)) \text{ for } q.$$

The formulae for x and y represent the reliability of «pf» and «df» elements provided that situations leading to common failure do not happen.

The probability of common failure absence equals

$$(1 - h(1 - p))(1 - s(1 - q)) = (p / x)(q / y).$$

The aforementioned RBDs are not able to function properly in case of common failure, so their reliability formulae can be written in the following way:

$$P_L(p,q,u,v,h,s) = u(2yv(3x^2 - 2x^3) - y^2v^2(3x^2 - 2x^3)^2)(p / x)(q / y), \quad (5)$$
$$P_R(p,q,u,v,h,s) = v(3u^2(2xy - x^2y^2)^2 - 2u^3(2xy - x^2y^2)^3)(p / x)(q / y). \quad (6)$$

The mean of $\Delta P(p,q,u,v,h,s)$ is calculated as follows:

$$A = \int_0^1\int_0^1\int_0^1\int_0^1\int_0^1\int_0^1 \Delta P(p,q,u,v,h,s)\,dp\,dq\,du\,dv\,ds\,dh$$

The percent of cases in which the right RBD is more reliable:

$$S = 100\int_0^1\int_0^1\int_0^1\int_0^1\int_0^1\int_0^1 H(\Delta P(p,q,u,v,h,s))\,dp\,dq\,du\,dv\,ds\,dh$$

5 Case study: Specified failure rates of «pf» and «df» blocks

In the papers [1] and [2], where the aforesaid architectures have been investigated in terms of Markov analysis, the considered failure rate of «pf» block is 10^{-4} h^{-1}. For «df» elements the examined values of this parameter, given in 10^{-6} h^{-1}, are 10, 25, 50 and 75. Other blocks are regarded as absolutely reliable.

Within the scope of this case study, the analyzed RBDs are considered for parameters chosen as described above. Thus, the reliability formulae for the ideal case, which are given in Section 2, can be used. The probability of failure-free operation during t hours for «pf» and «df» blocks can be calculated using the following expressions:

$$P_{pf}(t) = \exp(-\lambda_{pf} \cdot t),$$
$$P_{df}(t) = \exp(-\lambda_{df} \cdot t),$$

where λ_{pf} and λ_{df} are failure rates of «pf» and «df» elements, respectively [11]. Hence, the reliability values of the considered RBDs at the time moment t can be obtained using (1) and (2) by substituting $P_{pf}(t)$ for p and $P_{df}(t)$ for q.

The aforementioned approach can be used to prove that if $t \geq 7000$ h, each of the analyzed RBDs has reliability less than 0.85 for any of the considered failure rate sets. Thus, the given architectures should not be used during a larger time spans, if their parameters are as described above. Consequently, in this case study it is sufficient to analyze the given RBDs only for t less than 7000 h. Other time intervals are irrelevant to choosing the preferable architecture and therefore not considered.

The script for searching minimum of the difference between the reliability values of the right and left RBDs in a specified range of time spans can be written as follows:

```
LP = 1e-4; LD = 10 * 1e-6; ST = 0; FN = 7000;
p = @(t) exp(-LP * t);
q = @(t) exp(-LD * t);
R = @(t) (3*(2*p(t)*q(t) - (p(t))^2*(q(t))^2)^2 - ...
2*(2*p(t)*q(t) - (p(t))^2*(q(t))^2)^3);
L = @(t) (2*q(t)*(3*(p(t))^2 - 2*(p(t))^3) - ...
(q(t))^2*(3*(p(t))^2 - 2*(p(t))^3)^2);
m = createOptimProblem('fmincon','x0',[(ST+FN)/2], ...
'objective',@(t)(R(t) - L(t)),'lb',[ST],'ub',[FN]);
g = GlobalSearch();
[x, y] = run(g, m);
disp(join([" Minimum: ", y]));
```

The first line of the given code determines such parameters as λ_{pf}, λ_{df} and the examined range of time intervals, which in this study is set to (0; 7000) h. The result returned by this script is nonnegative for each of the aforementioned failure rate sets. Thus, for any time interval less than 7000 h the right RBD is more reliable in all cases examined above. Hence, the right architecture is preferable for all pairs (λ_{pf}, λ_{df}) considered in this section.

6 Conclusion

6.1 Discussion and future steps

No architecture among the given ones can be unconditionally considered the most reliable, so the reliability formulae for their RBDs have been obtained in order to make possible the choice of the most reliable alternative. These formulae allow to take into account the reliabilities of the underlying elements of the aforementioned RBDs and the percents of common failures for «pf» and «df» elements. The aforesaid analytical expressions have been used to obtain the formula for the mean of the reliability advantage of the right RBD over the left one as well as the expression for the percent of cases in which the right architecture is more reliable. The approach to finding the cases of maximal reliability advantage for the left and right architectures has been proposed. The given analysis can be conducted for an arbitrary pair of RBDs.

Future research can be dedicated to development of a decision-making system for choosing between the given architectures, which considers all parameters and standard requirements for RTS or other similar safety-critical systems.

6.2 Recommendations for choosing an architecture

If reliability of the underlying elements can be estimated precisely, a preferable architecture can be chosen using the aforementioned reliability formulas for the analyzed RBDs. In particular, for the case of the underlying blocks having such failure rates as described in the first paragraph of Section 5, the right architecture is recommended.

However, the results of this research also allow to give guidances for some occasions, where the reliability values for elements of the given RBDs are known only partially. The most important of these recommendations are listed below.

In the ideal case, which is described in Section 2, the right architecture should be used if the reliability of «df» block is greater than 0.6, and the left one is preferable if this parameter is less than 0.29.

For the ordinary case, which is considered in Section 3, the left architecture is more reliable for about 95% of all possible reliability parameter sets characterizing the blocks of the given RBDs. Thus, if there is no information about the reliability of the underlying elements (e.g., due to their degradation), the left architecture is preferable.

Acknowledgements

This research is supported by the project STARC (Methodology of SusTAinable Development and InfoRmation Technologies of Green Computing and Communication) funded by Department of Education and Science of Ukraine.

References

1. Butenko, V., Kharchenko, V., Odarushchenko, E., Butenko, D. Metric-based approach and tool for modeling the I&C system using Markov chains. *Proceedings of 23rd International Conference on Nuclear Engineering*, 2015, pp. 1-9.
2. Kharchenko, V., Butenko, V., Odarushchenko, O., Odarushchenko, E. Markov's Modeling of NPP I&C Reliability and Safety: Optimization of Tool-and-Technique Selection. *Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management*, 2016, pp. 328-336.
3. Yastrebenetsky, M., Kharchenko, V. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, 1st Edition. *IGI Global*, 2014, 470 p.
4. Geist, R., Trivedi, K. Reliability estimation of fault-tolerant systems: Tools and techniques. *IEEE Computer*, vol. 23, iss. 7, 1990, pp.52-61.
5. Wang, D., Trivedi, K. Reliability analysis of phased-mission system with independent component repairs. *IEEE Transactions on reliability*, vol. 56, iss. 3, 2007, pp. 540-551.
6. Grottke, M., Sun, H., Fricks, R., Trivedi, K. Ten fallacies of availability and reliability analysis. *Service Availability: 5th International Service Availability Symposium*, 2008, pp.187-206
7. Popov, G., Tashev, T. Comparative Reliability Analysis for TMR «2 out of 3». Fault Tolerance Systems. *Recent Advances in Applied Mathematics and Computational and Information Sciences*, vol. 2, 2009, pp. 357-360.
8. Stott, J., Britton, P., Ring, R., Hark, F., Hatfield, G. Common Cause Failure Modeling: Aerospace vs. Nuclear. *10th International Conference on Probabilistic Safety Assessment & Management*, vol. 3, 2010, pp. 2570-2581.
9. Ferrero, A., Petri, D., Carbone, P., Catelani, M. Modern Measurements: Fundamentals and Applications. *John Wiley & Sons*, 2015, 571 p.
10. Larson, R., Edwards, B. Multivariable Calculus, 11th Edition. *Brooks Cole*, 2017, 1160 p.
11. Gnedenko, B., Belyayev, Yu., Solovyev, A. Mathematical Methods of Reliability Theory. *Academic Press*, 1969, 506 p.