Scholar Publishing Group
Distributed Processing System
https://doi.org/10.38007/DPS.2020.010304
ISSN 2790-0916 Vol. 1, Issue 3: 27-36

Quantitative Analysis Method of Distributed System Vulnerability Based on Reliability Theory

Saravan Sride*

National Polytechnic Institute of Cambodia, Cambodia

**corresponding author*

Keywords: Reliability Theory, Distributed System, System Vulnerability, Quantitative Analysis

Abstract: Under the background of smart grid, there are few studies on the vulnerability analysis of distributed system(DS) integrating information systems, most of which are still in the primary stage of research, and more of them are qualitative assessment of the security operation risk of DSs under the influence of information systems; There are few quantitative analysis(QA) and protection of system vulnerability. This paper focuses on the QA method of DS vulnerability, and puts forward the reliability theory(RT). This paper analyzes the vulnerability of DS and the vulnerability index of DS based on information physical fusion, and discusses the QA method of DS vulnerability based on RT. The effectiveness and feasibility of this method are verified by experiments.

1. Introduction

The positioning point of smart grid is to integrate the advanced network technology and communication technology into the DS to build a new power network, which is based on the traditional DS framework. After the intervention of the information system, the safe, reliable and stable operation of the DS has been affected to a certain extent. After the stability and security of the information system are damaged and threatened, the safe and sustainable operation of the DS will be seriously threatened. Under bad conditions, large-scale power outages and some DSs will be out of operation. Therefore, based on the RT, this paper studies the QA method of DS vulnerability.

The QA method of DS vulnerability based on RT has been studied and analyzed by many scholars at home and abroad. The vulnerability analysis of DS is mainly completed in two steps. First, the interactive system is modeled, and the appropriate theory is selected to determine the vulnerability index based on the system model for vulnerability assessment. Kwon s uses the theory of complex network and the multi-layer complex network model to extract the multi-layer centrality between networks and the shortest electrical path algorithm to evaluate the robustness of the power network [1]. Prabakaran b s uses the improved penetration theory to build the chain fault model of

the system. It analyzes the vulnerability of the chain fault of the DS when the nodes of the fusion system are under random attack from the two levels of the distributed control center and the topological centrality. The vulnerability of the DS is more obvious due to the impact of the system delay [2].

Based on the RT, this paper studies the QA method of DS vulnerability, and proposes the vulnerability index of DS based on the RT and the risk knowledge of DS; The vulnerability of DS based on information physical fusion is analyzed. Through the selected vulnerability indicators and analysis methods, the vulnerability of the DS after the intervention of the information system is analyzed. The analysis results show that the more information nodes are attacked, the more vulnerable the DS is [3-4].

2. Research on QA Method of DS Vulnerability

2.1. DS Vulnerability Index of Information Physical Fusion

Before the vulnerability analysis of DS based on information physical fusion, it is very important to select appropriate vulnerability indicators. In the context of smart grid, the vulnerability of DS needs to consider the impact of information system. The monitoring and control role of information system on DS greatly affects the vulnerability of DS, and has a certain impact on the safe and stable operation of DS, The vulnerability index selected in this paper is a new type of power system structure vulnerability index selected by combining the active power loss of nodes and branches of the DS and the fault node removal rate, and considering the risk vulnerability index under the influence of the information system, the comprehensive power system vulnerability index is selected [5-6].

2.1.1. Vulnerability Analysis of DS Based on Information Physical Fusion

After the intervention of the information system, the intelligence and integration of the DS have been greatly improved, and the overall performance and overall service efficiency of the DS have been significantly improved. However, the vulnerability has also been greatly affected by the information system. For a long time, scholars have made many achievements in the vulnerability analysis of DSs. However, a large number of methods and data show that these studies mainly focus on the primary network of traditional DSs, while the vulnerability research of DSs after the information system constructed by the secondary network is involved is still weak [7].

2.1.2. Requirements for Vulnerability Index Selection of DS

In the DS, the system structure has certain unevenness, the power flow distribution combined with the load size and property difference also has unevenness, the power transmission and distribution capacity of power nodes is significantly different, the status of different power nodes in the system is different, and their importance is also different. At the same time, in the DS interconnection network, the distance between nodes is very long, and when the load power changes, it is mainly obvious in the vicinity of the node, which makes the node's ability to reflect the load change and the exclusive ability of the disturbance amount different, that is to say, the node's anti-interference ability is different. In the DS, the power nodes that bear certain transmission power and have weak anti-interference ability are the key protection objects in the system and also the vulnerable nodes in the system [8-9].

The selection of the vulnerability index of DS nodes needs to meet the importance of the nodes to transmit power and distribute electric energy under the normal operation state of the system, and whether to exit the operation when the nodes are disturbed by the external environment. The structural characteristics of the DS are very obvious. The ability of the system to transmit and distribute power is closely related to the status of the power nodes. According to the steady-state analysis knowledge of the DS and the power distribution of the system on each node, the utilization rate of the nodes can be obtained [10-11]. From this, it can be seen that the DS topology and the system power flow distribution have a correlation effect on the function use of power nodes. The inconsistency of these two aspects directly determines that there is a certain difference in the importance of power nodes [12].

According to the definition of DS vulnerability, the DS vulnerability index is selected to consider the vulnerability of the DS. Different definition methods have different index choices, which can reflect the stable operation ability of the system from different angles. No matter which indicator is selected for evaluation, it should first meet the criteria that the indicator can reflect the system's impact resistance, power flow probability in limited area under fault state, vulnerability set under non impact state, etc. after meeting the above requirements, the vulnerability evaluation of DSs will be more effective [13-14].

2.2. Vulnerability Index of DS

In the DS, the nodes and branches of the power system in the topology structure jointly constitute the flow channel of energy flow. The power flow distribution of the DS, excluding the influence of load factors, mainly depends on the electrical characteristics of the nodes and branches of the DS. The network structure of the DS has a great impact on it. According to the basic knowledge of DS steady-state analysis, the resistance parameter in the power network is far less than the reactance parameter, so the influence of reactance on the system is mainly considered in parameter selection [15-16]. Differential processing for branch parameters: differential processing is performed for a certain electrical branch sh, and the DS segment of the DS n is divided, and the reactance parameter on the DS segment of the DS K is taken as:

$$X_{hk} = \mathrm{Im}(W_{h\cdot k}) \tag{1}$$

Where: wh. K DS represents the impedance parameters on the k-th differential section of the electrical branch sh.

Let uhk be the active power that can be carried by the DS section of the DS K on the electrical branch sh, and UK (I) the DS Max is the maximum value of the active power that can be carried by the DS on the branch. Therefore, the utilization efficiency of the active power on the branch can be obtained:

$$\eta_{hk(I)} = \frac{U_{hk}}{U_{k(I)\max}} \tag{2}$$

let the active power provided by the first section li of the branch sh be Uli, h, and the active

power obtained by the end RJ after passing through the branch sh be URI, h, Then the importance coefficient of the power node to the active power can be obtained as:

$$I_{hi} = \frac{H_{L_{i,h}}}{\sum_{j=1}^{N_R} H_j}, H = 1 \sim N_S \tag{3}$$

$$I_{hj} = \frac{H_{L_{j,h}}}{\sum_{j=1}^{N_R} H_j}, H = 1 \sim N_S \tag{4}$$

In combination with the above analysis, the branch vulnerability parameters on the k-th segment of branch sh are:

$$T_{k(I)h} = X_{h \cdot k} I_{hi} I_{hj} \eta_{hk(I)} \tag{5}$$

The electrical medium can identify the vulnerable branches or nodes in the distributed power system. In combination with the active load loss and chain fault that may be caused by the random attack fault of the power system, the removal probability of the problem branches in the actual system under the action of the security device is defined as the fragile removal probability of the branches [17].

2.3. Vulnerability Judgment Mechanism

This paper uses the DS vulnerability matrix to analyze the vulnerability of the DS. The vulnerability matrix is formed through the evolution of the correlation matrix of the two systems. The analysis process includes the following steps:

Forming the incidence matrix of information system and DS; Through the selection of the vulnerability index, the vulnerability index of the DS under the influence of the information system is calculated to form the system vulnerability matrix; The vulnerability indexes of the DS are sorted and summarized, and the vulnerable node set and the number of nodes of the DS are determined.

Considering the impact of the information system on the vulnerability of the DS, this paper selects random failure as the attack mode. When attacking the information system, the vulnerability of the DS will be affected. The vulnerability of the DS will change with the change of the state of the information node [18]. For the analysis process of system vulnerability, this paper uses computer to process the original data of the system, including the structure and parameters of the network, and focuses on the simulation and equivalence of the relationship between the information network and the power network and their interaction channels to obtain the system incidence matrix; According to the evaluation requirements, the node vulnerability set is divided to obtain the vulnerability set of the power system, and the vulnerability of the DS is studied by combining the vulnerability value results. The vulnerability analysis process is shown in Figure 1.

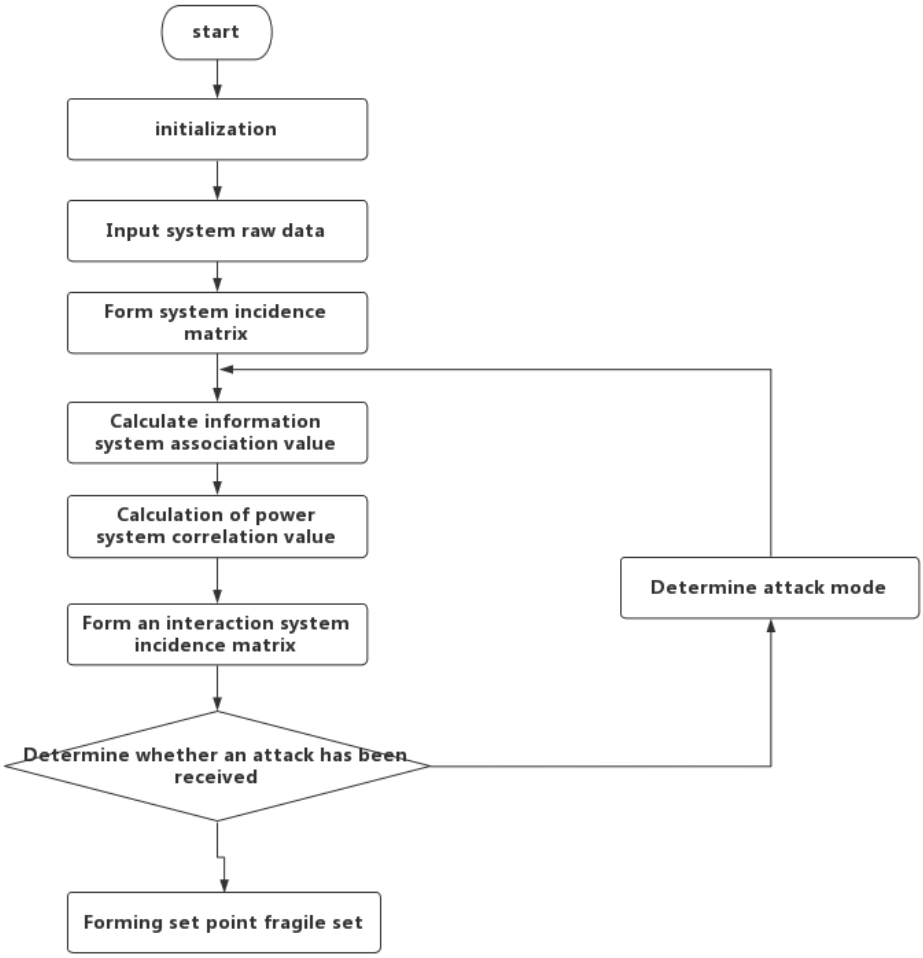

Figure 1. Vulnerability analysis flow chart

3. RT Analysis

3.1. RT

Reliability is a qualitative concept. Usually, reliability is used to quantify reliability, that is, uncertainty factors in specified conditions are used, and random variables subject to certain distribution are used to quantify reliability. The safety factor method of reliability fixed value is to measure the safety degree by the safety factor, which is the ratio of resistance effect a and load effect B. The functional function based on the RT is generally expressed by the difference between the resistance effect a and the load effect B. the resistance effect and the load effect are functions of some independent variables. Therefore, the independent variables of the functional function f Z are the union of the load effect and the resistance effect independent variables. The expression is as follows:

$$f = g(V_1, V_2, ..., V_n) = A - B \tag{6}$$

Where: V1, V2,..., VN are the quantitative expression of uncertainty factors under specified conditions, i.e. random variables. Function function f greater than zero indicates that the product or system is in a reliable state; The function function f is equal to zero, indicating that the product or system is in the limit state; If the function function f is less than zero, the product or system is in a failure state.

3.2. Reliability Index

Reliability index, also known as safety index, is a quantitative index to measure reliability. In the n-dimensional state space, the reliability index is the shortest distance from the n-dimensional limit state surface to the coordinate origin, which is recorded as γ, Where the limit state plane is a plane composed of all points where f = g (V1, V2,..., VN) = 0.

It is assumed that the resistance effect function a and the load effect function B obey normal distribution, i.e. a ~ n (μ a, σ A) B~N(μB, σ B), then the function function f also follows the normal distribution, i.e. f ~ n (μ F, σ F) The corresponding failure probability expression is as follows:

$$H_y = H(F<0) = \int_{-\infty}^{0} y_f(F)dF = \frac{1}{\sqrt{2\Pi}}\int_{-\infty}^{-\gamma_f/\sigma_f} e^{-t^2/2}dt \tag{7}$$

According to the above formula, the reliability index γ Can be expressed as:

$$\begin{cases} \gamma = \dfrac{\mu_f}{\sigma_f} \\ \mu_f = \mu_R - \mu_S \\ \sigma_f = \sqrt{\sigma_R^2 + \sigma_S^2} \end{cases} \tag{8}$$

Us Uf γ Both can express the reliability, but the calculation of us and UF involves complex multiple integrals, and the mathematical processing is difficult. Us Uf γ There is a corresponding relationship between them, γ The larger the failure probability UF, the smaller the reliability probability us. When the γ Value, the failure probability can be obtained by querying the normal distribution table, and the reliability probability can be obtained according to the complementary relationship between the reliability probability and the instability probability.

4. QA of DS Vulnerability based on RT

According to the vulnerability analysis model established above, according to the vulnerability assessment process described in Figure 1, and based on the DS analysis and calculation software, calculate the power grid. The specific DS vulnerability index, information vulnerability index and power information interaction channel vulnerability index are shown in Table 1 and Figure 2.

Table 1. Data table of vulnerability index of node fusion system

	0	2	4	6	8	10	12	14	16	18
Power node vulnerability value	0.28	0.11	0.19	0.64	0.13	0.16	0.26	0.38	0.21	0.06
Information node vulnerability value	0.72	0.91	0.82	0.73	0.56	0.87	0.89	0.75	0.79	0.85

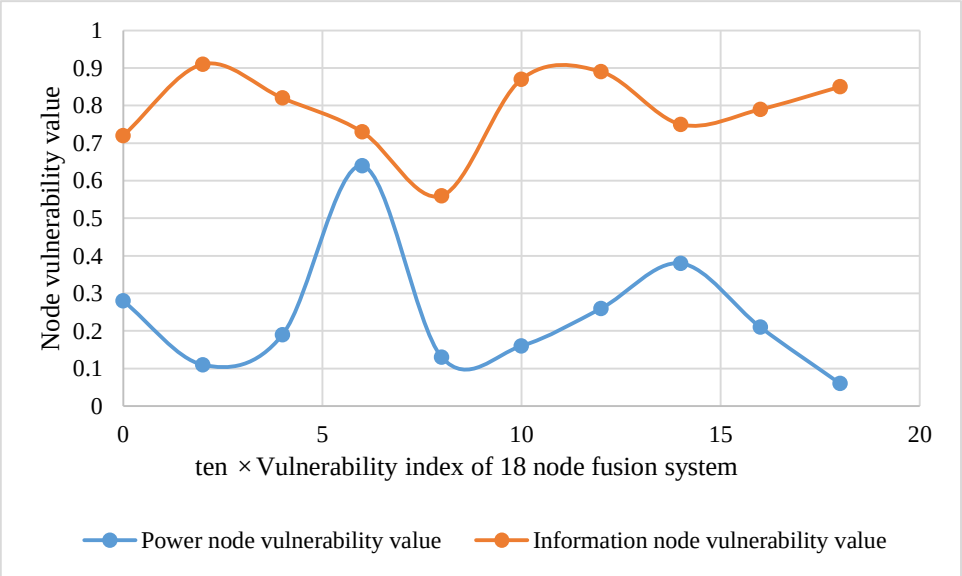

Figure 2. Ten × Vulnerability index of 18 node fusion system

The above chart shows the vulnerability values of the nodes and interaction channels of the information system and the DS in the system. It can be seen from Fig. 2 that the blue curve shows that the vulnerability values of the DS differ greatly on different nodes. For example, compared with the power node "1" and the power node "5", the vulnerability value of the point "1" is smaller than that of the node "5". The vulnerability value of the DS is about 0.5, This is closely related to the nature of nodes and the importance of nodes in the system. Node "1" is a load node or a low-order substation node in the DS, so its vulnerability value is relatively low. The red curve indicates the node vulnerability value of the information system. According to the characteristics of the information system, the information system contains a large amount of information, the information system contains a large number of small signals, and the system capacity and power cannot be infinitely large. Therefore, it is more sensitive to external influences than the DS, and its vulnerability value is much more vulnerable than the DS. The yellow vertical line indicates the fragile relationship of the interaction channel. The length of the vertical line does not represent the size of the vulnerability value, but only the relationship between the interaction channels.

After the intervention of the information system, the vulnerability of the nodes of the DS has changed significantly. The vulnerability value of the nodes has increased on the basis of the original, and the vulnerability value of the power nodes with larger vulnerability value has increased even more. The detailed results of the vulnerability value of the power nodes considering the impact of the information system are shown in Table 2.

Table 2. Information physical fusion power system node vulnerability ranking table

Fragile value sorting	Original power system		After information system intervention	
	Node	Vulnerability value	Node	Vulnerability value
1	5	0.67	5	0.79
2	12	0.45	12	0.54
3	14	0.41	14	0.50
4	3	0.39	1	0.45
5	13	0.32	3	0.44
6	16	0.31	11	0.43
7	1	0.28	4	0.41
8	11	0.24	7	0.39
9	15	0.23	13	0.38
10	6	0.17	10	0.37

Table 2 shows the vulnerability values of power nodes after the intervention of the information system. The vulnerability value of power node "5" has increased from 0.7 of the original DS to 0.85 of the DS, reaching the vulnerability warning value. In other words, when the information node "3" is attacked, it is likely to cause the state failure of power node DS 5. For any node in the system, the failure of the node will produce a series of chain reactions, The stability of the DS will be seriously affected. Take the "5" node as an example, the power nodes associated with it are node "6", node "8" and node "10". Once the state of node "5" is abnormal, Other node voltages associated with node "5" may not continue to meet the basic voltage requirements, and the operation state and data analysis of the entire DS will be reprocessed, which seriously affects the stability of the DS and the safety of system control.

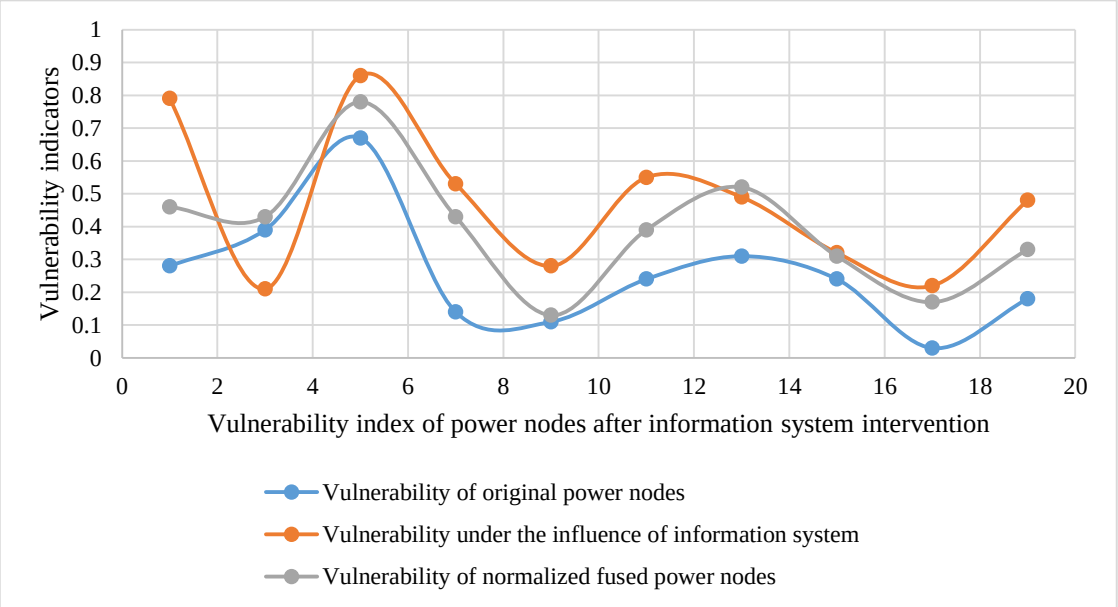

Figure 3. Vulnerability index of power nodes after information system intervention

According to the change of vulnerability value in Figure 3, when a single node is attacked, the

vulnerability value of the power system is compared and analyzed. It is found that when a single node of the information system is attacked, the vulnerability of the nodes of the power system is also affected by the importance and delay characteristics of the information node. For directly connected nodes, the impact is great, because after the information system is attacked, the vulnerability of the power system branch increases, and its vulnerability also increases to a certain extent.

5. Conclusion

In this paper, the QA method of DS vulnerability based on RT is studied, and a vulnerability index of power grid DS considering RT is proposed. Combined with RT, the improved vulnerability index of DS is proposed to identify the vulnerable links of power grid efficiently. Through the QA of the vulnerability of the DS, the experimental data show that the vulnerability of the branch of the DS based on the RT is improved, and its vulnerability is also increased to a certain extent. However, there are also shortcomings in this study. The experiment does not consider the situation of distributed energy grid connection in the real DS, and the impact of intermittent nature on the system reliability, power supply and demand and the identification accuracy of vulnerable links needs to be further studied.

Funding

This article is not supported by any foundation.

Data Availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Conflict of Interest

The author states that this article has no conflict of interest.

References

[1] Kwon S, Lee J H. DIVDS: Docker Image Vulnerability Diagnostic System. IEEE Access, 2020, PP(99):1-1.

[2] Prabakaran B S, Dave M, Kriebel F, et al. Architectural-Space Exploration of Heterogeneous Reliability and Checkpointing Modes for Out-of-Order Superscalar Processors. IEEE Access, 2019, PP(99):1-1.

[3] Mousavizadeh S, Bolandi T G, Haghifam M R, et al. Resiliency analysis of electric distribution networks: A new approach based on modularity concept. International journal of electrical power and energy systems, 2020, 117(May):105669.1-105669.17.

[4] Kaboodvand N, Heuvel M P V D, Fransson P. Adaptive frequency-based modeling of whole-brain oscillations: Predicting regional vulnerability and hazardousness rates. Network Neuroscience, 2019, 3(1):1-26.

[5] Abedi A, Gaudard L, Romerio F. Review of major approaches to analyze vulnerability in power system. Reliability Engineering & System Safety, 2019, 183(MAR.):153-172.

[6] Kishani M, Tahoori M, Asadi H. Dependability Analysis of Data Storage Systems in Presence of Soft Errors. IEEE Transactions on Reliability, 2019, 68(1):201-215.

[7] Konwinski L. Medication Safety and the Independent Double Check: A Work System Analysis and Reliability Engineering Theory Review. Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care, 2020, 9(1):119-120.

[8] Zarghami A, Gunawan I. The Emergence and Evolution of Reliability Theory for Water Distribution Networks. Built Environment Project and Asset Management, 2020, 11(2):251-265.

[9] Wang R, Luo Y. Efficient strategy for reliability-based optimization design of multidisciplinary coupled system with interval parameters. Applied Mathematical Modelling, 2019, 75(Nov.):349-370.

[10] Iranpour M, Hejazi M A, Shahidehpour M. A Unified Approach for Reliability Assessment of Critical Infrastructures Using Graph Theory and Entropy. IEEE Transactions on Smart Grid, 2020, PP(99):1-1.

[11] Gatti A, Stratford P, Brisson N, et al. How to Optimize Measurement Protocols: An Example of Assessing Measurement Reliability Using Generalizability Theory.. Physiotherapy Canada. Physiotherapie Canada, 2020, 72(2):112-121.

[12] al-Nasraween, Dr, mo'en, et al. Information Function for Item and Test and Reliability when Using Three Forms of Multi-Choice Test under Item Response Theory. International Journal for Research in Education, 2019, 43(3):6-6.

[13] Konwinski L. Medication Safety and the Independent Double Check: A Work System Analysis and Reliability Engineering Theory Review. Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care, 2020, 9(1):119-120.

[14] Kozhevnikov V S, Matyushkin I V, Chernyaev N V. Analysis of the basic equation of the physical and statistical approach within reliability theory of technical systems. Computer Research and Modeling, 2020, 12(4):721-735.

[15] Kolios A. Reliability Engineering: Theory and Practice – Eighth edition A. Birolini Springer. 2017. xvii; 651pp. Illustrated 179.99. ISBN 978-3-662-54208-8. Aeronautical Journal -New Series-, 2019, 123(1266):1307-1308.

[16] Mohammadi R, Mashhadi H R, Shahidehpour M. Market-Based Customer Reliability Provision in Distribution Systems Based on Game Theory: A Bi-Level Optimization Approach. Smart Grid, IEEE Transactions on, 2019, 10(4):3840-3848.

[17] Goncharenko A V. Two Entropy Theory Wings as a New Trend for the Modern Means of Air Transport Operational Reliability Measure. Transactions on Aerospace Research, 2020, 2020(3):64-74.

[18] Oudah F, Naggar M E, Norlander G. Unified system reliability approach for single and group pile foundations – Theory and resistance factor calibration. Computers and Geotechnics, 2019, 108(APR.):173-182.