CREATION OF THE IOT ARCHITECTURE FOR SOLVING THE PROBLEM OF GUARANTEED FUNCTIONING OF THE CYBER-PHYSICAL SYSTEM

Nataliya Pankratova, Yuliia Perederii

Abstract: *This paper is aimed to propose the Internet of Things (IoT) architecture for solving the problem of guaranteed functioning of the cyber-physical systems. IoT is the technological basis of cyber-physical systems. IoT is the "brain" of a system which includes billions of nodes in this data and uses it to further control physical elements. The data flow in the proposed architecture is described, which includes the three main layers: physical end points that directly interact with devices; cloud technologies, which is responsible for working with data and providing service; gateway, which serves for transferring data between the two previous levels. As an example of a cyber-physical system for which proposed IoT architecture is applied an electric refrigerator truck used to deliver cargo. It is required to ensure the guaranteed functioning of the electric refrigerator.*

Keywords: *Cyber-physical systems, the Internet of Things, system analysis, multi-factor risks, information technology.*

ITHEA Keywords: *H.4.2. Information System Applications: Types of Systems.*

DOI: https://doi.org/10.54521/ijita28-03-p01

Introduction

A cyber-physical system (CPS) is a complex distributed system, managed and controlled by computer systems, tightly integrated with the Internet and its users. The main principle of the CPS is a deep relationship between its physical and computational elements to make decisions regarding the maintenance of

the functioning of real objects. Every day cyber-physical systems find their application in new areas so that becomes a perspective topic for each researcher. Smart city and homes, pollution control, energy saving, smart transportation and industries — modern solutions in the Internet of Things. Analysis on a cyber-physical system as a management system and review on current trends in its development is shown in the article [Pankratova and Ptukha, 2020].

The technological basis of CPS is the Internet of Things (IoT), which is the "brain" of a system in the form of artificial intelligence and other technologies for analysis, processing of data received from sensors in the real world. The Internet of Things is defined as a paradigm in which objects equipped with sensors and actuators interact with each other to achieve a set goal. Currently, there is no single approach for building an IoT architecture.

The Internet of Things is used in healthcare, education, environmental monitoring, home and transportation automation, and even entertainment. A wide range of IoT application domains and their features are presented in articles [Ray P.P., 2018, Kumar et all, 2019]. Different researchers offer their own concept of architecture, depending on the problem to be solved. For example, a 6-tier architecture is presented in article [Mocrii et all, 2018] for smart home automation. In the work, the aim of which is to improve the mobility and transport of the city, an architecture of 3 main modules, each of which has an internal subsystem, is proposed [Badii et all, 2019].

Regardless of the chosen domain, 3 main layers can be identified in the base of any of the IoT architectures (Figure 1) [Pallavi and Smruti, 2017, Burhan et all, 2018, Yang and Kim, 2019].

Perception or device layer is the physical layer, which contains sensors for the perception and collection of information about the environment, as well as influencing mechanisms. Gateway layer is responsible for the transmission and processing of sensor data. Application layer is responsible for providing application-specific services.

When considering a specific problem to be solved, researchers can extend the architecture of an IoT system with layers for security, data storage, data preprocessing, monitoring, control, etc. [Pallavi and Smruti, 2017].

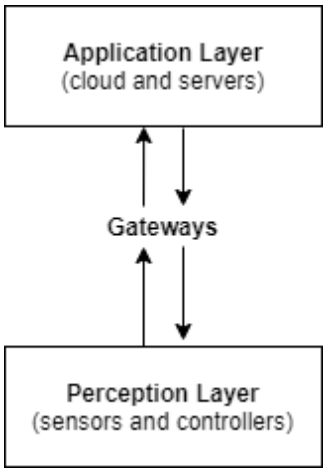


Figure 1. Common three-layer architecture for IoT systems

The proposed IoT architecture

In this work, IoT architecture (Figure 2) to solve the problem of guaranteed functioning of the cyber-physical system is proposed. When building it, the basic needs and features of the system, as well as the advantages of existing architectures, were taken into account.

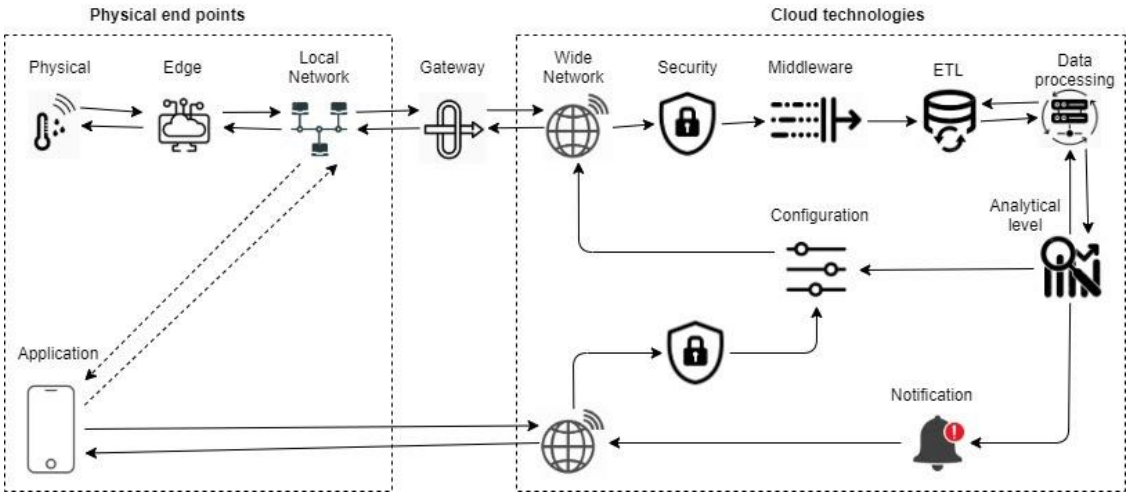


Figure 2. Architecture of IoT system for tasks of guaranteed functioning of the cyber-physical system

As well as existing IoT architectures, this approach is formed based on 3 main layers:

- Physical end points that directly interact with devices;
- Cloud technologies, which is responsible for working with data and providing service;
- Gateway, which serves for transferring data between the two previous levels.

For each of the levels, an internal subsystem of levels is defined, which makes it possible to ensure the fulfillment of the task.

The Physical layer is the physical sensor of the system. It is responsible for collecting information and performing mechanical works.

The Edge layer provides minimal functionality for converting analog information to digital and vice versa and connects to a single sensor or actuator.

Since most peripheral devices are not connected to the mains or wired communication, there is a need for a Local Network layer that will cover the problem of communication between sensors within the system.

There are several reasons for having a Gateway layer in IoT solutions:

- Recording a critical situation and issuing a local response, even without communication with the Cloud Technologies level;
- Interaction with Cloud Technologies to transfer processed information from peripheral devices to the server and obtain configuration data for peripheral devices;
- Saving information about the status of peripheral devices and the data collected by them.

Wide Network layer separates the edge and Cloud Technologies parts of the overall solution. Gateway is mostly connected to Cloud Technologies using mobile wireless like 4G / 5G, but sometimes wired internet is used. This layer also includes DNS server-based balancing and location services and many other components of wireless networks.

The Security layer provides AAA (Authentication, Authorization and Accounting) and encryption / decryption functions along with other services related to connection security.

The Middleware layer provides back-end functionality for load balancing, message queuing, and streaming. The components of this layer must be duplicated and automatically scaled. The layer is implemented mainly based on microservices or PaaS from Cloud providers.

ETL layer - layer of data collection and storage, information lifecycle management including archiving and destruction.

The Data processing layer is responsible for preparing data and forming a knowledge base for further analysis and self-learning.

The Analytic layer extracts situational information from a complete set of peripherals and predicts future events. All computational methods for predicting the system state take place at this stage. Also, its function is to form solutions to avoid emergency situations.

Notification layer forms the subscription notification algorithm. The client application subscribes to the necessary events and, when this happens, receives an information signal - a notification.

Configuration layer - works as a repository for three types of peripheral statuses:

- Current state of the peripheral device;
- The new state of the peripheral to be loaded;
- Peripheral intermediate status - indicates the process of updating from old states to new ones.

An IoT application can have two interaction streams: M2M (machine to machine) and M2P (machine to person). Application layer associated with an M2M stream where information is processed and presented to a customer or support engineer.

The data flow in the proposed architecture can be considered as follows:

1. Various physical sensors of the selected system collect data, send it for transformation and consolidate in the local network;
2. Data is transmitted to a closed Internet network using Gateway;
3. After passing the security check, the data is queued for storage and further processing;
4. Based on the collected historical data and new added data, a knowledge base is formed and a data model is defined;
5. Taking into account the knowledge base, the data model, as well as the latest data obtained, an analysis to predict the occurrence of abnormal and critical situations is performed. Available options for possible changes are formed to prevent such situations;
6. Sending a notification to the client or support engineer about the forecasted situation. At the same time, the system gives the corrections for the sensors necessary to avoid abnormal and critical situations.

The architecture also provides for the ability of a client or a support engineer to influence the cyber-physical system locally or remotely, in case there is a better solution than was suggested by the application. In such cases, the system will save the new solution to the knowledge base for further self-learning.

The subject of the study

As mentioned earlier, the data collected from the sensors is transmitted from Physical end points to Cloud Technologies. This process can be performed according to the proposed architecture without the participation of a system analyst. When the data is transferred to the Data processing and Analytical layers, the knowledge base must be formed, and computational methods must be applied for the given task.

As an example of a cyber-physical system for which this IoT architecture can be applied, an electric refrigerator truck used to deliver cargo is proposed. For this case, it is required to ensure the guaranteed functioning of the system. Thus, the data received from the sensors of the electric refrigerator truck is transmitted downstream in the proposed IoT architecture to the Data processing Date and Analytical layers, in which the methods of system analysis is carried

out and solution options are offered to predict the occurrence of abnormal or emergency situations in the in the system life cycle and ensure the guaranteed functioning of the system. One of the approaches to solving this task is presented below.

The vehicle must distribute perishable goods around the city. The load is distributed in equal parts at four points with different distances between them. Electric vehicle capacity is 800 kg. Each consumer receives the same amount of cargo, weighing 200 kg.

In normal mode, considering the terrain, the vehicle can perform this work when powered only from a fully charged battery. The movement of the vehicle is monitored by the operator of the dispatch center, which has an emergency forecasting system, to make a timely decision on changing the route to the next customer.

Under the terms of the contract between the carrier and the consumer of the goods, the carrier pays a penalty for delay in delivery, which is proportional to the time of delay.

Thus, the first critical parameter that needs to be controlled is the profit from the transportation. The profit can be determined using the formula:

$$Q=Qin-WABCkWh-VBCB-kn1t1-kn2t2-kn3t3-kn4t4-Qa,$$

where Q is profit, Q_{in} is amount received from the customer, W_{AB} is the amount of electricity received from the grid to charge the battery (BAT), $CkWh$is the electricity price (per kWh), V_B is the amount of consumed gasoline in liters, C_B is the gasoline price per liter, knj are coefficients for computing the penalty for each destination, $j=1,\ldots,4$, $t1,\ldots,t4$ – delivery delays of goods to the corresponding destinations, Q_a is fixed expenses for depreciation of equipment, salaries, etc.

With normal delivery, there are no delays, i.e., $t1=t2=t3=t4=0;$ gasoline consumption for charging the battery does not exceed a certain level. In this case, the main expenses include the initial charge of the battery, a small

amount of consumed gasoline, the inevitable depreciation costs, and other fixed expenses.

The situation becomes abnormal when due to traffic conditions or other factors, the delivery of goods is not done on time or the gasoline consumption is too high. This leads to a sharp decrease in profitability due to the payment of penalties to the customer, payment for gasoline.

The situation also becomes abnormal if the estimated remaining range is significantly lower than the remaining travel distance, or the energy reserve in the battery is lower than the permissible one either for a long time or at the beginning of the trip.

In the event of a delay due to traffic congestion, or other factors, the battery can be recharged from a gasoline generator or a stationary charging station.

Battery charging is also possible due to the recuperative braking or descending from the hill. Since the charging current of the battery is limited, the peak bursts of energy are accumulated in a special storage device (the high-capacity capacitor bank), and then distributed among potential consumers.

An emergency situation can happen when losses occur as a result of a late delivery of goods. Abnormal and emergency situations are relative to the profit from the transportation 980 price units and 850 price units, the range of 13000m and 1000m, the energy stored in the battery 20 MJ and 5 MJ.

Evaluation of the guaranteed functioning

The approach of system guaranteed functioning assessment and rational coordination of resources of acceptable risk is used to study the process of functioning of the CPS using an electric refrigerator truck as an example. The state of the vehicle at any time from the given interval is characterized by values of indicators of the profit from deliveries y_1, estimated power reserve y_2, the amount of energy $y3$ in the rechargeable battery. True functional dependencies y_1, y_2, $y3$ are given as discretely specified samples Y1, Y2, Y3, which are functions of discretely specified parameters x_{ij}, shown in Table 1. In

accordance with the IPTG procedures, the input data were pre-processed and transformed into the form required to restore the FD. Functional dependencies $yi=(x1,x2x3),i=1,m$ were restored in terms of functions Y1, Y2, and Y3, discretely specified. An assumption was made about the existence of a relationship between the variable parameters based on the fact that many variables are technologically related, for example, the current speed, average speed and distance to travel, or mechanical shaft power and traction motors current. In connection with this assumption, the restoration of functional dependencies in a multiplicative form was, since in this case the possible relationship between the variables is considered.

Table 1. *Description of dependencies Y1, Y2, Y3 and their variable parameters* x_{ij}

Function	Description	Variable	Description
Y_1	profit from deliveries	x_{11}	average speed
		$x12$	current speed
		x_{13}	distance to point 4
		x_{14}	range
		$x15$	the amount of gasoline consumed
		x_{16}	expenses $-WABCkWh-Qa$
		x_{17}	the amount received from the customer for the transportation of the goods
Y_2	range Estimated power	x_{21}	average travel speed
		$x22$	average battery discharge power

	reserve	x_{23}	the amount of stored energy in the battery
		x_{24}	the total weight of the vehicle
		$x25$	current speed
		x_{26}	current battery discharge/charge power
Y_3	the amount of energy in the battery	x_{31}	mechanical shaft power on traction motors
		$x32$	charge power provided by the generator
		x_{33}	the power consumed by the refrigerator
		x_{34}	the power consumed by other equipment
		$x35$	traction motors current

A linear regression model was chosen as a forecasting model, the parameters for which were calculated using the least squares method. This model was chosen due to the fact that, with the relative simplicity of implementation and low computation costs, it gives fairly accurate results comparable to the results of more costly methods, for example, methods of time series analysis.

Prediction of the values of functions is performed at each step of observation, while $N_0 = 50$ last measurements of variables are used for forecasting, with the help of which prediction is made for $N_1 = 10$ steps ahead. Thus, the dynamic sample for prediction is $ND = N0 + N1 = 60$ values. Prediction dynamically changes at each iteration, so that in the developed program you can monitor the indicators as they change dynamically and their predicted values in 10 steps.

The procedure for detecting an abnormal n_j (or emergency a_j) situation is based on the use of threshold values $yinj$ for the current *j-th* sensor (and not only the current value is used, but also the predicted ones). An abnormal situation occurs if at least one of the sensors satisfies the inequality ∃(yij<(>) $yinj$, depending on whether the minimum or maximum threshold is used. The detection of an emergency situation is similarly accomplished: threshold values $y_i^{a_j}$ are used for sensor *j*, an emergency situation occurs when the inequality ∃(yij<(>) $yiaj$) is satisfied, depending on whether the minimum or maximum threshold is used.

According to the statement of the problem, an emergency is a situation in which losses were incurred as a result of untimely delivery of the cargo. Thus, the only established threshold value for an emergency will be $Y1 < 0$, which has practical meaning, since from the point of view of the company organizing the delivery of the cargo, the complete failure of the task will only be the occurrence of losses as a result; while any other situation can still be turned into profit, for example, by using the economy mode of an electric vehicle, or even by using other cars. Although such a situation, of course, will not be normal, the company will still make a profit as a result.

In the developed software, when an emergency situation is detected, this is immediately reported to the operator by a corresponding message on the screen, and the type (emergency situation, emergency situation in several parameters, etc.) and a description of this emergency situation including which specific threshold has been exceeded / dropped below in the corresponding sensor. The value of the risk factor is also calculated in parallel. This is done according to the formula:

$$\rho ij = yji - yinjyinj - yiaj ,$$

where y_i^j is the current *j* sensor value, $yinj$ is the threshold value for an abnormal situation to occur, $y_i^{a_j}$ is the threshold value for an emergency

situation to occur. In accordance with the obtained value of the function, the current level of danger is determined, and its classification is performed.

Confidence intervals were used to identify the reliability of the information transmitted from the sensors due to sensor failure. The predicted values yif of the critical variables y_i are used to construct the confidence interval *I*. If, during further operation, the values y_i do not fall into this interval, this indicates a sensor failure.

$$I=yif-\Delta,yif+\Delta,\Delta=t\alpha Sy,$$

where S_y is mean square error of the forecast model; t_α is value for t -statistic for probability α, the probability that a value will fall within the confidence interval; in this problem $\alpha = 0.8$. With this method, sensor failures can be detected with a high probability and the error can be prevented from affecting decision making.

The margin of permissible risk, as the duration of functioning of a complex system in a certain mode, during which the degree and level of risk as a result of the possible impact of risk factors do not exceed a priori specified permissible values, is calculated in this work according to the formulas:

$$\Delta i[s]=maxkyi[tk-1]-yi[tk],k<s+nf,$$

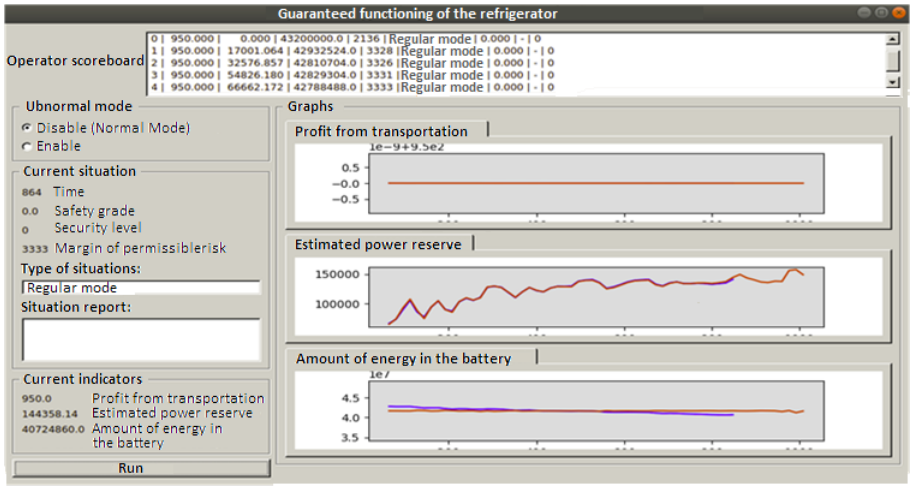
$$T[s]=miniyi[ts]-yiw\Delta i[s]\times T0,$$

where: $T[s]$ is the margin of permissible risk of an abnormal situation at time s,c ; y_{iw} is the value for an abnormal situation level; nf is number of forecasting steps.

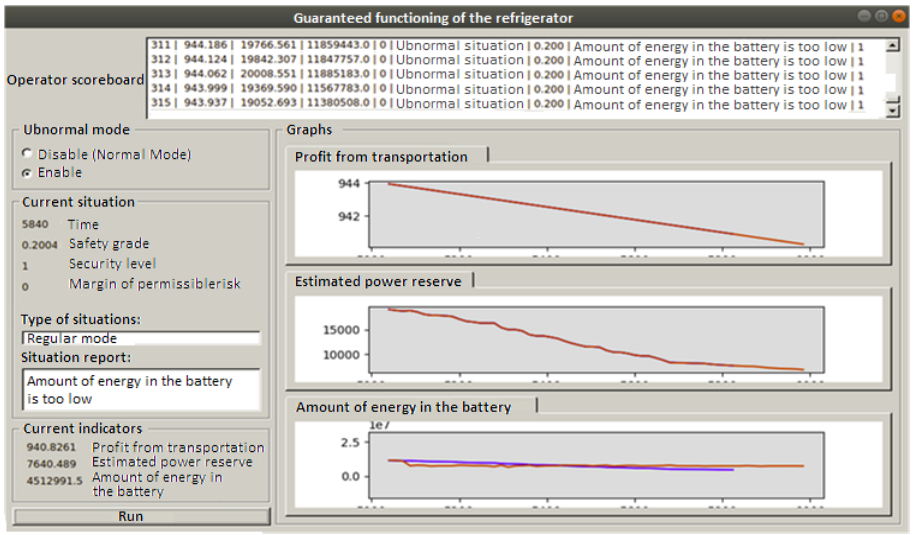
If there is an abnormal situation on the forecast interval, then the margin of permissible risk is 0. That is, first, the maximum change in each indicator y_i for one time interval in an abnormal mode is found for all the data that are available at the moment, as well as the predicted ones. Then the margin of permissible risk is the minimum of the partial difference of the current and abnormal

parameters and its maximum change in the abnormal mode. Simply put, the margin of permissible risk is the time during which an abnormal situation can be controlled in a manageable manner, ensuring the guaranteed survivability of functioning.

Some results of the functioning of an electric refrigerator truck are shown in Figure 3.



a)



b)

Figure 3. Monitoring results in the normal (a) and abnormal (b) modes of operation of the electric refrigerator truck in the form of the distribution of critical variables during operation

As a result of monitoring the functioning of the electric refrigerator truck for a normal situation, the value of the hazard was 0, the level of the hazard – 0, the margin of permissible risk 3333 s (Figure 3a); for an abnormal situation, the value of the hazard was 0.2004, the level of the hazard was 1 (an abnormal situation based on one parameter), the margin of permissible risk was 0 s (Figure 3b). The situation corresponds to the battery energy being too low.

Conclusion

As a result of this work, an IoT architecture is proposed for solving the problem of guaranteed survivability of the cyber-physical system. This architecture has advantages in comparison with the architectures of other researchers studied in the current work, since it covers the most business cases and meets modern requirements and characteristics of IoT systems. It is also allowed that some elements of the architecture can be excluded when developing a most valuable product or customer needs, that makes this architecture flexible in customization.

As an example of the cyber-physical system for evaluation of the guaranteed functioning was an electric refrigerator truck used to deliver cargo. A margin of permissible risk has been introduced as a period of time during which an abnormal mode can be converted into a normal mode, will ensure the survivability of the cyber-physical system operation.

The proposed IoT architecture and forecasting model were considered within the framework of the chosen domain and the given task. It is assumed that such approach can be applied to problems of guaranteed functioning for set of similar interconnected systems. At the same time, minor adjustments may be necessary depending on the specified characteristics of the cyber-physical system.

Bibliography

[Pankratova and Ptukha, 2020] Pankratova, Nataliya & Ptukha, Y. Estimation computational models of the cyber-physical systems functioning. System

research and information technologies. 2020, 28-33. https://doi.org/10.20535/SRIT.2308-8893.2020.1.03

[Ray P.P, 2018] Ray, P.P. A Survey on Internet of Things Architectures. Journal of King Saud University—Computer and Information Sciences, 30, 2018, 291-319. https://doi.org/10.1016/j.jksuci.2016.10.003

[Kumar et all, 2019] Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111, 2019. https://doi.org/10.1186/s40537-019-0268-2

[Mocrii et all, 2018] Dragos Mocrii, Yuxiang Chen, Petr Musilek. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. Internet of Things 1-2, 2018, 81-98. https://doi.org/10.1016/j.iot.2018.08.009

[Badii et all, 2019] Badii, C.; Bellini, P.; Difino, A.; Nesi, P. Sii-Mobility: An IoT/IoE Architecture to Enhance Smart City Mobility and Transportation Services. Sensors, 2019, 19, 1. https://doi.org/10.3390/s19010001

[Pallavi and Smruti, 2017] Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035

[Burhan et all, 2018] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S.). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors (Basel, Switzerland), 18(9), 2018, 2796. https://doi.org/10.3390/s18092796

[Yang and Kim, 2019] Yang H, Kim Y. Design and Implementation of High-Availability Architecture for IoT-Cloud Services. Sensors. 2019; 19(15):3276. https://doi.org/10.3390/s19153276

[Zgurovsky and Pankratova, 2011] Zgurovsky M.Z., Pankratova N.D. System analysis: problems, methodology, applications. – K.: Naukova dumka, 2011. (in Russian)

Authors' Information

Nataliya D. Pankratova *– DTs, Professor, Corresponding member of NASU, Deputy director of Institute for applied system analysis, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Av. Pobedy 37, Kiev 03056, Ukraine;*

e-mail: *natalidmp@gmail.com*

Major Fields of Scientific Research*: System analysis, Theory of risk, Decision-making, Applied mathematics, Applied mechanics, Foresight, Scenario analysis, Strategic planning, Information technology*

Yuliia A. Perederii – PhD student, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Av. Pobedy 37, Kiev 03056, Ukraine*;*

e-mail: *yuliaptuha@gmail.com*

Major Fields of Scientific Research*: System analysis, Decision-making, Information technology*