1. Volodymyr DUBOVOI[1], 2. Maria S. YUKHIMCHUK[1], 3. Nelya M. KYRYLENKO[2], 4. Andrii H. BUKHUN[3], 5. Olena M. HOMONYUK[4], 6. Maksat KALIMOLDAYEV[5], 7. Konrad GROMASZEK[6], 8. Saule SMAILOVA[7]

Vinnytsia National Technical University (1), Vinnytsia Humanities and Pedagogical College (2), National academy of the National Guard of Ukraine (3), Khmelnytsky National University (4), Institute of Information and Computational Technologies CS MES RK (5), Lublin University of Technology (6), East Kazakhstan State Technical University named after D.Serikbayev (7)
ORCID: 1. 0000-0003-0440-3643; 2. 0000-0002-8131-9739; 3. 0000-0001-9039-6616; 4. 0000-0002-9665-1427; 5. 0000-0002-3849-788X; 6. 0000-0003-0025-8880; 7. 0000-0002-3265-3714; 8. 0000-0002-8411-3584

doi:10.15199/48.2021.09.08

Functional safety assessment of one-level coordination of distributed cyber-physical objects

Abstract. *An approach to solving the problem of analysis and improving the functional safety of cyber-physical control systems for distributed continuous objects is proposed. The model of a one-level cyber-physical system of coordination control was developed, the sources of dangers are analyzed and the probability of a dangerous operating mode is estimated.*

Streszczenie. *Zaproponowano podejście do rozwiązania problemu analizy i poprawy bezpieczeństwa funkcjonalnego cyberfizycznych systemów sterowania rozproszonymi obiektami ciągłymi. Opracowano model jednopoziomowego cyberfizycznego systemu sterowania koordynacyjnego, przeanalizowano źródła zagrożeń i oszacowano prawdopodobieństwo wystąpienia niebezpiecznego trybu funkcjonowanie. (**Ocena bezpieczeństwa funkcjonalnego jednopoziomowej koordynacji rozproszonych obiektów cyber-fizycznych**).*

Keywords: *cyber-physical control system, functional safety, coordination control, one-level systems, distributed object.*
Słowa kluczowe: cyber-fizyczny system sterowania, bezpieczeństwo funkcjonalne, sterowanie koordynacyjne, systemy jednopoziomowe, obiekt rozproszony.

Introduction

Cyber-physical systems is the systems which consist of physical objects, facilities of their condition monitoring, facilities of impact on them and facilities of processing information and making control decisions are the basis of modern material production. The significant parts of the physical objects of cyber-physical systems are distributed in space. The distribution factor was often neglected in order to simplify the control system, save technical facilities of control and measurement, simplify control algorithms to ensure their speed. With the development and cheapening of technical facilities of measurement and impact on an object, wireless communications, and the advent of the Internet of Things technologies, it has become possible to equip a distributed object with monitoring and control facilities at many points, resulting in the creation of distributed cyber-physical control systems (DCPCS). However, complications of the cyber physical system can lead to additional vulnerabilities and a decrease in the level of functional safety [1, 2]. The issue of functional safety is the subject of many studies [3]. The main object of these studies is distributed computer systems. Recently, considerable attention has been paid to cyber-physical systems, in particular, the Internet of things systems [4, 5].

Among the distributed objects of cyber-physical systems, there are common objects characterized by the inseparability of elements (continuous objects) partially isotropic in separate coordinates and/or parameters; structural homogeneity; resource dissipativity; additivity of products; additivity of resources. An example of such systems is a system for controlling the thermal regime of multizonal distributed objects [6].

Distributed object control is the subject a lot of research. The frequency methods for the analysis and synthesis of distributed control systems [7], structural methods [8] and others were proposed. The methods for modeling and optimization of DCPCS under uncertainty [9] were developed as well. The greatest attention of researchers is given to the theory of hierarchical systems [10-12]. At the same time, for distributed objects with a large number of measured and controlled points with local control systems (LCS) and one-level coordination systems (P2P systems) are promising. However, the coordination theory in single-level DCPCS has not yet a sufficiently complete formulation.

An analysis of existing works on the theory of general safety and security, cyber-physical systems and distributed control systems has shown that the problem of research and enhancing the functional safety of distributed cyber-physical continuous-object control systems has not yet been solved.

The aim of this work is to develop approaches to solving the problem of analysis and improving the functional safety of distributed cyber-physical systems for control of continuous objects.

Method and Model

The sources of danger for DCPCS can be divided into those which are typical for all control systems, and those which are connected with the distribution of the object and the structural features of DCPCS [13, 14]. In this work, we focus on the sources of functional danger of DCPCS, which lead to the output of the operating modes of a distributed object beyond critical limits.

An analysis of the dangers associated with impaired coordination is feasible on the basis of a statistical model. As an indicator of functional safety, due to the provision of a safe mode of operation of the object, we take the probability $\mathbf{P}_{us}$ of the absence of object parameters beyond critical bounds.

We will develop a statistical model for coordinating the control of spatial objects with these properties in two stages:

- Development of a deterministic model;
- Consider stochastic effects on the characteristics which are possible for the object under consideration: isotropy and dissipation.

Consider the most common type of distributed peer-to-peer systems i.e. systems with regular communications and logistical productive functions of elements, products and resources additivity. The scheme of such DCPCS is shown in Fig. 1, in which: p_0 is the main control resource; $\mathbf{P}_{in}$ is the vector of resources that come to an element from other

elements of a distributed object; $\mathbf{P}_{out}$ is the vector of resources coming from an element to other elements of a distributed object; v is the state of the object element; $\mathbf{V}$ is vector of states of other elements; x is raw materials; y is product.

The object element is been controlled by a local control system (LCS), which mode (specified value of the element state) is set by the coordinator. LCS together with the coordinator is an agent of multiagent DCPCS.

Coordinators form a P2P network, but this network is not fully connected but with regular connections. Each coordinator is only associated with the LCS coordinators of elements that are located in the area of significant interaction.

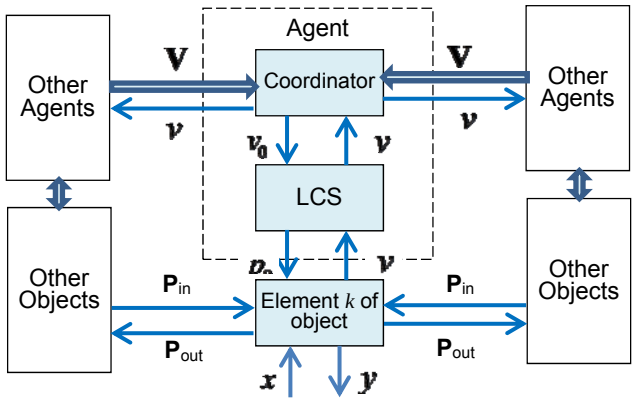

Fig. 1 – Structural model of distributed cyber-physical system

A wave algorithm is proposed to coordinate DCPCS agents. As the coordination wave passes through the P2P system, the coordination parameter v_0 is changed to improve the coordination criterion. The convergence and stability of the wave coordinate algorithm depends on the ratio of the exponent damping ratio λ and the coordination coefficient ζ: $\Delta p_0 = -\zeta \cdot (v - v_0)$, where v_0 is the specified value of the element state.

The scheme of an element of the distributed object is shown in Fig. 2.

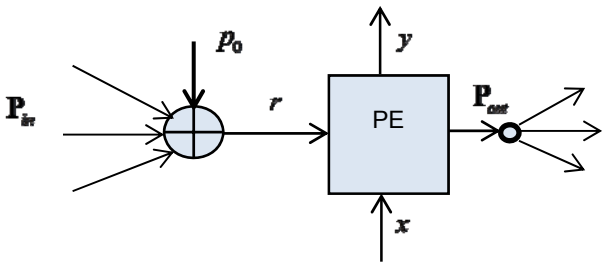

Fig. 2. An element of the distributed object

All elements of an object affect each other, but the sensitivity of an element at each input decreases exponentially depending on the spatial distance between the elements [15].

It is known that the influence of the element with coordinate $\mathbf{Z}_k$ propagates gradually in accordance with the transport equation (Burgers equation, in particular the diffusion and heat conduction equation). The transfer equation has the first order in time and the second order in spatial coordinates. The solution of the distribution equation for various boundary and initial conditions is known [15, 16]. In particular, the instantaneous point effect on an element k is propagated to the element j according to the ratio

$$v(d_k, t) = \frac{V_{0k}}{8(\pi\lambda t)^{3/2}} e^{-\frac{d_k^2}{4\lambda t}}, \quad (1)$$

where λ is the transfer coefficient; $d_{kj} = |\mathbf{Z}_k - \mathbf{Z}_j|$ is the distance from the k-th point of the control impact to the j-th element; V_{0k} is the value of the control impact; $\tau_k = t - t_k$ is the time interval from the moment of impact on the k-th element.

If the impact is $V_{0k} = p_{0k} dt$, where p_{0k} is the value of the control impact, carried out in the area of the radius r_0, then for a non-stationary process can be written

$$\frac{dv_j(t)}{dt} = \frac{p_{0k} + v_k - v_j}{8(\pi\lambda t)^{3/2}} e^{-\frac{d_{kj}^2}{4\lambda t}} \left[1 + \left(\frac{d_{kj}^2}{\lambda t} - 6\right) \cdot \frac{r_0^2}{40\lambda t}\right] \quad (2)$$

Evolution is due to two processes: the distribution of the resource while keeping constant its total amount and the processes of dissipation. Dissipation, in turn, involves the loss of a resource to the environment, the cost of a resource for a production process according to a production function, and the loss of non-production processes.

Based on equation (2), let us write the equation of change of state of the object element under the influence of all other controlled elements and LCS. For a linear object based on the superposition principle we find

$$\frac{dv_j(t)}{dt} = p_{0j}(t) + \sum_{k=1}^{n} \left\{ \frac{p_{0k}(t) + v_k(t) - v_j(t)}{8[\pi\lambda(t - t_k)]^{3/2}} e^{-\frac{d_{kj}^2}{4\lambda t}} \left[1 + \left(\frac{d_{kj}^2}{\lambda(t - t_k)} - 6\right) \cdot \frac{r_{0k}^2}{40\lambda t}\right] \right\}, \quad (3)$$

where t_k is the time moment of control impact on k-th controlled element; n is the number of controlled elements (control points), or

$$\frac{dv_j(t)}{dt} = p_{0j}(t) + \sum_{k=1}^{n} \gamma_{kj}(t) \left[v_k(t) - v_j(t)\right] \quad (4)$$

where

$$\gamma_{kj}(t) = \frac{e^{-\frac{d_{kj}^2}{4\lambda t}}}{8[\pi\lambda(t - t_k)]^{3/2}} \left[1 + \left(\frac{d_{kj}^2}{\lambda(t - t_k)} - 6\right) \cdot \frac{r_{0k}^2}{40\lambda t}\right]. \quad (5)$$

We write equation (4) with the form of Cauchy

$$\frac{dv_j(t)}{dt} = -v_j(t) \sum_{k=1}^{n} \gamma_{kj}(t) + \sum_{k=1}^{n} \gamma_{kj}(t) v_k(t) + p_{0j}(t), \quad j = 1 \ldots n, \quad (6)$$

or in vector-matrix form

$$\mathbf{V}' = \mathbf{V}\Gamma + \mathbf{P}_0 \quad (7)$$

From model (6) by the method of integrating factor, we find the equation of state of an element in time and space.

The limiting distance d_m to the elements which should be considered to be significant influences the ratio

$$\frac{e^{-\frac{d_m^2}{4\lambda\tau_k}}}{8(\pi\lambda\tau_k)^{3/2}} > \varepsilon, \quad (8)$$

where $\varepsilon \ll 1$ - significance indicator.

Dependence (2) must show the maximum at time intervals $d_k^2 / 6\lambda = \tau_k$ from the moment of impact on the object, from which the limit distance should satisfy the condition $\frac{e^{-3/2}}{8\left(\frac{\pi}{6}\right)^{3/2} d^3} > \varepsilon$ or $d < \frac{0.419}{\sqrt[3]{\varepsilon}}$

The state of the object affects the production function. For a linear production function $y=\alpha(v)\cdot x$, this influence is determined by the parameter $\alpha(v)$. The typical production function parameter of the element $\alpha(v)$ is approximated by a function $\alpha(v)=\frac{2\alpha_0 e^{(v-v_0)}}{1+e^{(v-v_0)}}-\frac{e^{(v-v_0)}}{2\alpha_0}$.

The resource that is accumulated in the element of the object is spent on production $dv'=\mu x\cdot dt$ and dissipation processes $dv''=(1-\eta)v\cdot dt$, where μ is the resource consumption per unit of raw material x; η is the coefficient of performance (COP).

Let us find the probability of functional safety violation P_{us} by object parameters become out of critical limits due to stochastic uncertainty.

The sources of stochastic uncertainty are:

- Disruption of coordination due to errors in communication between the coordinators. Shannon's theorem implies the probability of an error in the communication channel between the coordinators

(9) $$P_c=\frac{1}{1+\frac{E_s}{E_n d^2}},$$

where E_s is the energy of the data signal; E_n is the energy of the interferences.

- Random fluctuations in the propagation parameter λ in equation (3). If the statistical characteristics of the fluctuations are the same, then the variance of the state of the object due to these fluctuations

(10) $$\sigma^2_{v_j/\lambda}=\left(\frac{\partial v_j}{\partial\lambda}\sigma_\lambda\right)^2,$$

where σ^2_λ is the dispersion of propagation parameter fluctuations; v_j is determined from the equation of state (8) taking into account the substitution (5) as a function of the parameter λ.

- Random effects of external environment on the state of the elements u. The variance of an object's state as a result of these influences

(11) $$\sigma^2_{v_j/u}=\left(\frac{\partial v_j}{\partial u}\sigma_u\right)^2,$$

where σ^2_u - dispersion of influences. Since the influence of the environment is similar to the influence of adjacent elements of the object, then $\frac{\partial v_j}{\partial u}=\frac{\partial v_j}{\partial v_k}$, where the parameters in equation (8) satisfy the condition $v_k=u$ and d_{kj} is the distance from the element to the object border.

- A systematic error caused by the spatial discretion of affecting a distributed object $\delta_{v/d_{kj}}\left(d_{ij},t\right)$. For the uncontrolled i-th element, which is in the interval between the controlled elements, equation (6) is also valid under condition $p_{0i}(t)=0$. With even placement of control points

(12) $$\delta_{v/d_{kj}}\left(d_{ij},t\right)=\frac{2}{d_{kj}}\int_0^{d_{kj}/2}\left[v_i\left(d_{ij},t\right)-v_j\left(t\right)\right]d\left(d_{ij}\right).$$

- Dynamic errors due to control impact. This error is systematic and is determined by the controller's transfer function and frequency of coordination. If we consider coordination as a regular process, the coordinate signal at the input of the controller will be a periodic sequence of rectangular pulses. The spectrum of such a sequence is $S_{v_0}(\omega)=\frac{2\overline{\Delta v_0}}{\omega T_{co}}$, where $\overline{\Delta v_0}$ is the average correction of the coordinator, T_{co} is the period of the coordination wave. If the transfer function of a regulator is $W_{lc}(j\omega)$, then the transfer function of an error is $W_\delta(j\omega)=\frac{1}{1+W_{lc}(j\omega)W_{ob}(j\omega)}$. Then the mean square error of the controller

(13) $$\sigma_{p_0/\delta}=\int_0^\infty\frac{2\overline{\Delta v_0}}{\omega T}\cdot\left|\frac{1}{1+W_{LCS}(j\omega)W_{ob}(j\omega)}\right|d\omega$$

and

(14) $$\sigma_{v/v_0}=\int_0^\infty\frac{2\overline{\Delta v_0}}{\omega T}\cdot\left|\frac{W_{LCS}(j\omega)W_{ob}(j\omega)}{1+W_{LCS}(j\omega)W_{ob}(j\omega)}\right|d\omega.$$

Let us find the transfer function of an element of an object. From (6) we see that the state of the j-th element is determined by the differential equation

(15) $$\frac{dv_j(t)}{dt}+v_j(t)\sum_{k\in\Omega_\varepsilon}\gamma_{kj}(t)=p_{0\,j}(t)+\sum_{k=1}^{n}\gamma_{kj}(t)v_k(t),$$

where Ω_ε is a set of elements that satisfy condition (8).

Given condition (8), we can consider $t>\tau_k$ and $1/t\approx 0$ then $\gamma_{kj}(t)=\frac{e^{-\frac{d_{kj}^2}{4\lambda t}}}{8\left[\pi\lambda\left(t-t_k\right)\right]^{3/2}}$. From equation (18), using the Fourier transform, we obtain

(16) $$W_{ob}(j\omega)=\frac{1}{j\omega+\sum_{k\in\Omega_\varepsilon}\gamma_{kj}(t)}.$$

Total error

(17) $$\sigma_v=\sqrt{\sigma^2_{v_j/\lambda}+\sigma^2_{v_j/u}+\delta^2_{v/d_{kj}}+\sigma^2_{v/v_0}}.$$

Coordination is designed to reduce this error. Since coordination is accomplished by sequentially solving the problem of minimizing the deflection of the object, this component of the variance is equal to the value of the criterion after one cycle of coordination, consisting of a given number of waves. Since, for stability, the one-wave wave algorithm only partially reduces the error, so $\sigma'_v=k\sigma_v$, over the entire cycle $\sigma'_v=k^m\sigma_v$, where m is the number of waves in the coordination cycle, $0\ll k<1$.

The large number and variety of sources of error make it possible to assume the Gaussian nature of the distribution of the total error. $G\left(v,m_v,\sigma_v\right)$. Accordingly, the likelihood of the object parameters going beyond the critical limits

(18) $$P_{us}=P_c^m\cdot\int_{v_{cr}}^\infty G\left(v,m_v,\sigma_v\right)dv.$$

The analytical solution of the probability P_{us} estimation problem for a system with a large number of control points is difficult due to the large dimension of model. In this regard, the simulation model is developed on the Scilab/Xcos (Scicos) platform.

The basic element of the model implements the model of the controlled element of distributed object. The interaction coefficient is calculated on the basis of (1) by the formula

$$k_\lambda = \left(4\pi\lambda\tau_{0j}\right)^{-3/2} e^{-\frac{|Z_0 - Z_j|^2}{4\lambda\tau_{0j}}} . \quad (19)$$

Analysis

We considered the bioreactor as an object of simulation [16]. The managed resource in the bioreactor is the amount of thermal energy. The simulation results show that at large values of the propagation parameter and the distance between the control elements, the coordination error increases rapidly. An increasing the number of coordination waves when using the wave algorithm reduces the error, but for the system parameters were been used in the model reduces only up to 50%. Fig. 9 shows the dependences of the probability of exceeding the state of the critical value.

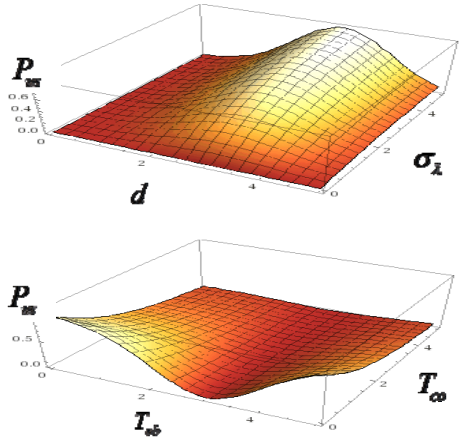

Fig. 9. Dependencies of the probability of a functional safety violation on DCPCS parameters.

It can be seen from the above dependences that there is a dangerous distance d between the places of the control impact on the distributed object. However, with small fluctuations in the propagation parameter, the influence of the distance on the probability of the dangerous mode is not significant. On the other hand, the probability of a dangerous mode can be reduced by the appropriate choice of the interval between coordination waves passages.

Conclusions

As a result of the research, an approach to solving the problem of analysis and improving the functional safety of distributed cyber-physical control systems for continuous objects is proposed. The model of the one-level coordination control in DCPCS was developed and the analysis of the functional safety (using the example of a bioreactor) showed that the probability of a dangerous mode can be reduced by an appropriate choice of system parameters. However, this can lead to a decrease in the overall system efficiency. Finding the best compromise between safety and effectiveness requires further research.

Authors: V.M. Dubovoy, Vinnytsia National Technical University, *Vinnytsia, Ukraine, e-mail: v.m.dubovoy@gmail.com; M. S. Yukhimchuk, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: umcmasha@gmail.com; Nelya M. Kyrylenko, Department of Informatics and Information Technologies in Education Municipal Institution of Higher Education «Vinnytsia Humanities and Pedagogical College», Vinnytsia, e-mail: nelly_112@ukr.net; Andrii H. Bukhun, National Academy of the National Guard of Ukraine, e-mail: Andrew000519@gmail.com; Olena M. Homonyuk, Khmelnytsky National University, elena_gomonyuk29@ukr.net; Mashat Kalimoldayev, Institute of Information and Computational Technologies CS MES RK, Almaty, Kazakhstan, e-mail: mnk@ipic.kz; Konrad Gromaszek, Lublin University of Technology, Lublin, Poland, e-mail: k.gromaszek@pollub.pl; Saule Smailova, East Kazakhstan State Technical University named after D.Serikbayev, Ust-Kamenogorsk, Kazakhstan, e-mail: saule_smailova@mail.ru*

REFERENCES

[1] Loukas G. Cyber-Physical Attacks. A growing invisible threat. Oxford, UK: Butterworh-Heinemann (Elsevier) (2015). p. 65. ISBN 9780128012901.

[2] Ahmad I., Zarrar M. K., Saeed T., Rehman S. Security Aspects of Cyber Physical Systems. 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh (2018), pp. 1-6. doi: 10.1109/CAIS.2018.8442009

[3] Kharchenko V. et al. Integrated Cyber Safety & Security Management System: Industry 4.0 Issue, 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), Leeds, United Kingdom (2019), pp. 197-201. doi: 10.1109/DESSERT.2019.8770010

[4] Cerf V., Ryan P., Senges M., Whitt R. IoT safety and security as shared responsibility. Bus. Inform. (2016) 1, 7–19

[5] Iqbal M. A., Olaleye O. G., Bayoumi M. A. A review on Internet of Things (IoT): security and privacy requirements and the solution approaches. Global J. Comput. Sci. Technol.: E Network, Web & Secur. (2016) 16(7)

[6] Dubovoi V., Yukhymchuk M. et al. Smart control of multi-zone object heating with multi-source system: 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering, UKRCON 2019 - Proceedings (2019), p. 1018-1021, 8879942

[7] Kukharova T. V., Pershin I. M. Conditions of Application of Distributed Systems Synthesis Methods to Multidimensional Object, 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok (2018), pp. 1-5, doi: 10.1109/FarEastCon.2018.8602749.

[8] Butkovskiy G. Structural method for systems with distributed parameters, Avtomat. i Telemekh. (1975), no. 5, 5–27; Autom. Remote Control, 36:5 (1975), 703–721

[9] Dubovoi V. M., Yukhymchuk M. S. Energy efficiency of smart control based on situational models: Control Systems: Theory and Applications (2018), стр. 145-167

[10] Mesarovic M. D., Macko D., Takahara Y. Theory of hierarchical, multilevel, systems. Academic Press, New York and London (1970).

[11] Katrenko A.V., Savka I.V. Mechanisms of coordination in complex hierarchical systems (2008), 156-166 URL: http://vlp.com.ua/files/16_1.pdf

[12] Bayas M. M., Dubovoy V. M. et al. Optimization of hierarchical management of technological processes: Proceedings of SPIE - The International Society for Optical Engineering (2015), 9816, 981622

[13] Dubovoi V., Moskvin O. Impact of the internet resources structure on energy consumption while searching for information: Studies in Systems, Decision and Control, (2017), 74, стр. 125-146

[14] Dubovoi, V.M., Yukhymchuk, M.S. et al. Evaluation of uncertainty of control by measurement with logical conditions: Proceedings of SPIE - The International Society for Optical Engineering (2016), 10031, 100314F

[15] Carslaw H., Jaeger J. Conduction of Heat in Solids. 2 edition. — Oxford University Press, USA, (1959). 510 p.

[16] Dunn I. J., Heinzle E., Ingham J., Prenosil J. E. Biological Reaction Engineering: Dynamic Modelling Fundamentals with Simulation Examples. 2nd edition. — Wiley-VCH, (2003). 508 p. ISBN 3527307591.

[17] Mashkov, V., Smolarz, A., Lytvynenko, V., Gromaszek, K., The problem of system fault-tolerance, *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska* 4 (2014), vol. 4, 41-44. https://doi.org/10.5604/20830157.1130182.