Target Functions of the Conceptual Model of Adaptive Monitoring of Complex Security in Interest of Counteraction Cyber-Physical-Social Threats of «Smart City»

Igor V. Kotenko[1], Igor B. Parashchuk[2]
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS);
St. Petersburg National Research University of Information Technologies, Mechanics and Optics (University ITMO)
St. Petersburg, Russia
[1]ivkote@comsec.spb.ru, [2]parashchuk@comsec.spb.ru

***Abstract*— The problems of mathematical formulation of particular and generalized target functions in the interests of a formal description of the problem of adaptive monitoring of complex security of compound Cyber-Physical-Social Systems are considered. Adaptive monitoring is aimed at countering complex security threats to the «Smart City». Adaptation levels are defined, groups of optimized parameters are described. Particular attention is paid to the parameters in the procedures for watching, evaluating and predicting complex security.**

Keywords*— *target function; monitoring; parameter; quality indicator; complex security; state, watching; evaluating; predicting

I. INTRODUCTION

The concept of «Smart City» («city of the future») should be considered as one of the directions of development of modern large Cyber-Physical-Social Systems (CPSS) and as a new generation of network distributed social, physical and cybernetic infrastructures.

They are aimed at realizing the priorities of Russia's scientific and technological development, ensuring a high quality of people's lives through the use of innovative technologies that provide for the economical, ecological and safe functioning of «Smart City» facilities and the use of urban life systems [1–3].

Problems of the Cyber-Physical-Social (CPS) security of the «Smart City» – the problems of the integrated use of a set of methods and means of security of transport management systems and networks, commercial and public services, digital education and e-government, automated agrarian enterprises, mass media, computerized industrial enterprises, energy, education, medicine. Up to every «Smart House», «Smart Office» and an individual in a «Smart City».

The nature of modern threats to the security of the «Smart City» is complicated – they can acquire the status of complex social- and (or) cyber- and (or) physical threats simultaneously or in different combinations. They can come either from a person (group of people) or from the state – within the framework of the concept of information (hybrid) confrontation between countries, aimed at defeating each other's critical infrastructures [4–6].

«Smart City» is a set of CPS subsystems for life support, health care, education, transport, etc., interlinked in place and in time, in a social, bio- and technological environment. Therefore, the problem of the complexity of threats is added to the problem of their multilevel nature. It manifests itself in the fact that the level of threats is different on different spatial, social, physical and cybernetic sites, as well as in different time coordinates of the functioning of the «Smart City».

To the main directions of ensuring the counteraction of CPS threats to the «Smart City», along with organizational measures to ensure complex security, measures to ensure the security of the CPS management subsystem and security management, include monitoring of complex security.

At the same time, monitoring procedures in the interests of countering CPS threats to the «Smart City» at the present stage should also be complex, multilevel and intelligent.

To detect and recognize threats to a modern «Smart City», security monitoring must be adaptive and optimal. It should cover the social, cybernetic and physical spheres of city life simultaneously.

II. RELEVANT WORKS

Problems of organization and synthesis of optimal algorithms for monitoring complex systems are discussed in a number of works [7–10]. They are aimed at improving the effectiveness of watching, evaluating and predicting procedures in monitoring systems of this class.

Target functions are used as identifiers for extreme tasks [7, 8] for security monitoring. But they do not guarantee high accuracy in assessing the security process.

In work [7] the approach based on adaptive monitoring of security parameters is offered. However, this approach requires consideration of supporting analysis procedures in terms of adaptation, which is not always possible.

This research was supported by the Russian Science Foundation under grant number 18-11-00302 in SPIIRAS.

978-1-5386-5824-6/18/$31.00 ©2018 IEEE

In [8] an expanded approach to network monitoring is presented. But this approach is applicable to communication networks, which narrows the scope of application.

Work [9] is devoted to the approach to monitoring, as to the procedure for registration the parameters of cybersecurity. But this approach is very difficult for practical implementation in the framework of adaptive procedures.

One of the main criteria for the quality of complex security (CS) monitoring is the adaptability (lat. adaptatio – adaptation) of this process. This property of monitoring to change its modes for the purpose of preserving, improving or acquiring new characteristics under conditions of the effects of a changing environment [10].

The adaptability of the monitoring process describes its ability to fit (agree on) algorithms, their behavior, structure and function to the conditions of existence, to unexpected changes in the properties of CS, objectives of CS, objectives of CS management and the environment by changing mode or search for the optimal methods of watching, evaluating and predicting (WEP) [10].

III. THEORETICAL PART – A GENERAL FORMULATION OF THE PROBLEM

The main content of the conceptual model of adaptive monitoring (AM) of CS answers to questions: what parameters of the design and (or) quality indicators (QI) of the properties of the CS, how (according to what criteria and on the basis of which methods) and when to watch, evaluate and predict at various stages of the life cycle of CPSS and under different conditions of the situation.

And also possible ways and methods of adaptation (alignment) of CS monitoring regimes in the context of constructive and destructive influences. The conceptual model of AM of CS is a formal generalized description of the system of views, ideas and principles that determine the general methodology of adaptive monitoring of systems of this class. It is known that monitoring is a set of procedures of WEP of the systemic characteristics of CS.

Using the approaches of decomposition theory, we will consider the adaptation of these procedures consistently, based on the specific conditions for their implementation and relying on the optimization criteria inherent in these procedures.

So, there is a monitoring object – CS. It is subject to the influence of external constructive and destructive factors - the environment; purposes of functioning and application, determined by the super-system, etc.

And internal factors – the number of consumers of CS services and their requirements; current objectives of the CS management; control actions; the failure flow of CS elements and the recovery stream of system resources; intensity of the CS incident flow, etc.

Elements of the automated control system (ACS) of CS are the system of technical operation (STO) and the decision-making system (DMS) [11]. The measurement subsystem is part of the STO of ACS of CS.

It realizes a complex of technical, system and technical-technological measurements, and technical measurements form the basis of the CS technical diagnostics process. The result of technical diagnostics is a vector of the currently diagnosed parameters $\vec{Y}_{\text{dp}}(k)$ of CS. It is a dataset of measurement of parameters of technical condition of elements of the CS. A complex of system and technical-technological measurements is implemented directly in the interest of monitoring of CS, the result of its implementation is the vector of current measured parameters $\vec{Y}_{\text{mp}}(k)$ of the system characteristics of the CS – a dataset on the results of measurements of parameters of the essential properties of CS as a whole.

IV. FORMULATION OF TARGET FUNCTIONS

Realization of the collection through the watching channels of the listed data, their processing (systematization, generalization) is the task of the watching procedure (WP) within the AM of CS. The data is collected at the first level of adaptation, when the parameters of the WP are optimized. However, the list and nomenclature of the watchable parameters $\vec{Y}_{\text{p}}^{\text{w}}(k)$ of CS should be optimized (adapted) in accordance with the requirements of the current management tasks of CS.

They should correspond to the scope and nomenclature of parameters and QI, the estimated values of which are necessary for the ACS at this stage of the implementation of the CS for making an information decision on the security condition (quality). For this purpose, on the second level, when an AM optimized the parameters of the evaluation procedure (EP), the decision on the choice of (forming) the optimal system of evaluated parameters (SEP) of CS:

$$F_{\text{SEP}}(k): \rightarrow \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ \vec{Y}_{\text{p}}'(k)\in\vec{Y}_{\text{p}}^{\text{w}}(k)}}{opt} f(\vec{Y}'_{\text{p}}(k)) = \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ \vec{Y}_{\text{p}}'(k)\in\vec{Y}_{\text{p}}^{\text{w}}(k)}}{opt} f(q_{\text{p}}(k); s_{\text{p}}(k); \Delta\tau_{\text{p}}(k)); \quad (1)$$

$$q_{\text{p}}(k)\in Q_{\text{p}};\ s_{\text{p}}(k)\in S_{\text{p}};\ \Delta\tau_{\text{p}}(k)\in\Delta T_{\text{p}}, \quad (2)$$

where in the expression (1), $f(\vec{Y}'_{\text{p}}(k))$ – function of choosing the optimal vector of parameters $\vec{Y}'_{\text{p}}(k)$, which are necessary of the WEP at the *k*-th step of CS monitoring. It is necessary to watch, evaluate and predict taking into account: uncertainty factors $\varpi(k)$, belonging to the uncertainty set Ω; factors of external and internal influences (vector of influences) $\vec{v}(k)$ on the system, belonging to a set of possible influences (matrix of influences) *V* (environment, operating conditions, etc.); volume and nomenclature of parameters, required by ACS of CS $\vec{Y}'_{\text{p}}(k)\in\vec{Y}_{\text{p}}^{\text{w}}(k)$.

At this step, an adaptation is carried out, with the aim of finding the optimal (2): $q_{\text{p}}(k)$ – the volume of system parameters of the CS, which are necessary of the WEP at the *k*-th monitoring step, belonging to the set of possible system parameters Q_{p}; $s_{\text{p}}(k)$ – nomenclatures (structures, hierarchies) of the system parameters of the CS, which are necessary of the WEP for the *k*-th monitoring step, belonging to the set of possible sets (nomenclatures) of the system parameters of CS S_{p}; $\Delta\tau_{\text{p}}(k)$ – periodicity of the WEP parameters of the CS at the *k*-th monitoring step, belonging to the set of possible of WEP intervals ΔT_{p}.

The result of realization of the AM of CS at this step, is the optimal for these conditions, the vector of parameters $\vec{Y}'_{\text{p}}(k)$, which is necessary of the WEP for the *k*-th step of complex security monitoring. Elements of this vector are used in the future for the realization of the procedures of WEP of the state (quality) CS.

After determining the parameters that need to be watched, the WP parameters are adapted. This stage is realized in accordance with the target functions (3) under the conditions (4):

$$F_{\text{WP}}(k): \rightarrow \underset{\substack{\varpi(k)\in\Omega;\,\vec{\nu}(k)\in V;\\ r'(k)\in R'\\ \vec{Y}_{\text{p}}(k)\in\vec{Y}_{\text{wp}}(k)\in\vec{Y}'_{\text{p}}(k)}}{opt} f(\vec{Y}'_{\text{wp}}(k)) = \underset{\substack{\varpi(k)\in\Omega;\,\vec{\nu}(k)\in V;\\ r'(k)\in R'\\ \vec{Y}_{\text{p}}(k)\in\vec{Y}_{\text{wp}}(k)\in\vec{Y}'_{\text{p}}(k)}}{opt} f(q_{\text{wp}}(k); s_{\text{wp}}(k); \Delta\tau_{\text{w}}(k); m_{\text{w}}(k)); \quad (3)$$

$$q_{\text{wp}}(k)\in Q_{\text{wp}};\ s_{\text{wp}}(k)\in S_{\text{wp}};\ \Delta\tau_{\text{w}}(k)\in\Delta T_{\text{w}};\ m_{\text{w}}(k)\in M_{\text{w}}, \quad (4)$$

where in the expression (3), $f(\vec{Y}'_{\text{wp}}(k))$ – the function of choosing the optimal vector of watched parameters $\vec{Y}_{\text{wp}}(k)$ at the *k*-th step of monitoring of the CS, taking into account a number of factors.

Factors: uncertainties $\varpi(k)$; impacts $\vec{\nu}(k)$; errors of measurement and diagnostics $r'(k)$, belonging to a set of possible errors of such class R', and also volume and nomenclature of really watched system parameters $\vec{Y}_{\text{p}}(k)\in\vec{Y}_{\text{wp}}(k)\in\vec{Y}'_{\text{p}}(k)$.

These are the parameters, the watching of which is realizable and belongs to the set (vector) $\vec{Y}'_{\text{p}}(k)$ of parameters, in the estimated values of which requires ACS of CS. In the general case, expression (4), at this stage of adaptation, occurs the search for optimal: $q_{\text{wp}}(k)$ и $s_{\text{wp}}(k)$ – volume and nomenclature watched at the *k*-th step of monitoring CS parameters; $\Delta\tau_{\text{w}}(k)$ – periodicity of the watch of parameters of the CS at the *k*-th monitoring step, belonging to the set of possible of watch intervals ΔT_{w}; $m_{\text{н}}(k)$ – methods (modes) of watch at the *k*-th step of monitoring the parameters of the CS, belonging to a variety of possible modes of watch M_{w}.

The result of the AM at this adaptation level is the optimal for these conditions of SEP of CS, i.e. a vector of essential system parameters of the CS, to be evaluated, the elements of which belong to the set (vector) of watched parameters $\vec{Y}_{\text{p}}(k)\in\vec{Y}_{\text{wp}}(k)$ of the system properties of the CS. Elements of the vector $\vec{Y}_{\text{p}}(k)$ are used in the future to implement the synthesis of the optimal system of quality indicators (SQI) of the CS, the implementation of procedures for evaluating and predicting the status (quality) of complex security of CPSS.

Realization of the process of formation of the optimal SQI, obtaining of particular and generalized evaluative of the parameters (state) or CS quality, is the task of the EP in the framework of AM security.

At this level of adaptation of the EP parameters, two-stage optimization is performed: first, the problem of obtaining the optimum for these conditions, a consistent and non-redundant SQI is solved, then a decision is made to select the CS status (quality) optimal evaluation method for these conditions.

The procedure for optimizing the volume and nomenclature of SQI within the framework of the AM of CS, may be implemented in accordance with the target function (5) under conditions (6):

$$F_{\text{SQI}}(k): \rightarrow \underset{\substack{\varpi(k)\in\Omega;\,\vec{\nu}(k)\in V;\\ r''(k)\in R''\\ \vec{Y}_{\text{p}}(k)\in\{Y_{\text{p}}\}}}{opt} f(\vec{Y}_{\text{QI}}(k)) = \underset{\substack{\varpi(k)\in\Omega;\,\vec{\nu}(k)\in V;\\ r''(k)\in R''\\ \vec{Y}_{\text{p}}(k)\in\{Y_{\text{p}}\}}}{opt} f(q_{\text{QI}}(k); s_{\text{SQI}}(k); \vec{Y}_{\text{QI}}(k)); \quad (5)$$

$$q_{\text{QI}}(k)\in Q_{\text{QI}};\ s_{\text{SQI}}(k)\in S_{\text{SQI}};\ \vec{Y}_{\text{QI}}(k)\in\{Y_{\text{QI}}\}, \quad (6)$$

where in the expression (5), $f(\vec{Y}_{\text{QI}}(k))$ – the function of choosing the optimal (wealthy and non-redundant) vector $\vec{Y}_{\text{QI}}(k)$ QI of CS.

These indicators are subject to evaluation taking into account uncertainties $\varpi(k)$, factors of external and internal influences (impact vector) $\vec{\nu}(k)$ on the system, errors in measurement, diagnostics and watch $r''(k)$, belonging to the set of possible errors of this class R'' and the composition of the elements of the parameter vector $\vec{Y}_{\text{QI}}(k)$, the elements of which belong to the set of possible watchable CS parameters $\{Y_{\text{QI}}\}$.

At the same time, within the framework of the AM of CS, a decision is made to select the optimal method for evaluating (ME) the state (quality) of the CS – $m_{\text{es(q)}}$ in accordance with the target function (7) and under the conditions (8):

$$F_{\text{ME}}(k):\rightarrow \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r(k)\in R\\ \vec{Y}_{\text{p(QI)}}(k)\in\{Y_{\text{p(QI)}}\}}}{opt} f(m_{\text{es(q)}}(k)) = \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r(k)\in R\\ \vec{Y}_{\text{p(QI)}}(k)\in\{Y_{\text{p(QI)}}\}}}{opt} f(\delta_{\text{err}}(k);t_{\text{ev}}(k);\vec{Z}_{\text{ev}}(k)); \quad (7)$$

$$\delta_{\text{err}}(k)\in\Delta_{\text{err}};\ t_{\text{ev}}(k)\in T_{\text{ev}};\ \vec{Z}_{\text{ev}}(k)\in\{Z_{\text{ev}}\}. \quad (8)$$

At this stage of the adaptation, the search for optimal parameters of the EP: $\delta_{\text{err}}(k)$ – the dispersion values of the parameter (QI) evaluation errors at the *k*-th monitoring step of the CS, belonging to the set of possible values of Δ_{err}, characterizes the accuracy of the evaluation; $t_{\text{ev}}(k)$ – the values of the parameters (QI) evaluation time at the *k*-th monitoring step, belonging to the set of possible values of T_{ev}, and characterizing the timeliness of the evaluation; $\vec{Z}_{\text{ev}}(k)$ – elements of the computational resources cost vector for the implementation of the parameters (QI) evaluation procedure at the *k*-th monitoring step, belonging to the matrix (set) of computational costs $\{Z_{\text{ev}}\}$.

The result of AM implementation at this stage is the optimal for these conditions vector of parameter estimates or QI, characterizing the system-wide properties of the CS $\vec{Y}_{\text{p}}(k)$; $\vec{Y}_{\text{QI}}(k)$.

Based on evaluations of these parameters, administrative and operational-technical decisions are made to manage the CPSS CS.

In addition, the current evaluated values of the state (quality) of the CS are the starting point, the initial data for the predicting procedure (PP).

The interrelated system of target functions of the AM of CS can be written in a general form, as a complex function of coherent sequential adaptation, which aims to optimize the parameters of WP, EP and PP in the interest of managing of the CS:

$$F_{\text{AM}}(k):\rightarrow\{F_{\text{SEP}}(k)\}\cup\{F_{\text{WP}}(k)\}\cup \cup\{F_{\text{EP}}(k):\rightarrow\{F_{\text{SQI}}(k)\}\cup\{F_{\text{ME}}(k)\}\}\cup\{F_{\text{PP}}(k)\}. \quad (9)$$

In this case, the complex target function of the AM of CS may be a combination of target functions for adapting the parameters of the relevant monitoring procedures (9): formation of SEP, necessary for ACS $F_{\text{SEP}}(k)$ (1); WP $F_{\text{WP}}(k)$ (3) and (4), EP $F_{\text{EP}}(k)$, which, in turn, is a combination of target optimization functions SQI of CS $F_{\text{SQI}}(k)$ (5) and (6), method for evaluating $F_{\text{ME}}(k)$ (7) and (8), as well as the target function of optimizing the parameters of the PP state (quality) of CS.

V. CONCLUSIONS

Thus, the expression (9) has the physical meaning of the joint dynamic adaptation of the parameters of the complex of procedures for watching, evaluating and predicting (ie, monitoring parameters) of the state (quality) CS in interest of counteraction CPS threats, under the impact of changing evolutionary and operational factors.

Practical implementation of the proposed target functions of the conceptual model will, in our opinion, increase the effectiveness of the system monitoring of CS in interest of counteraction CPS threats.

This will be due to an increase in the non-redundancy, reliability and accuracy of the resulting evaluations and predictions of the state (quality) of the CS, at the expense of reducing the costs of ACS of CS resources, allocated in the interest of security control.

That, in turn, will allow to reduce the costs of financial, time and other management resources in the design, development and operation of CS systems in interest of counteraction CPS threats of big CPSS – «Smart City», as well as to increase the degree of validity of decisions taken to manage the structure, parameters and operating modes of such system.

REFERENCES

[1] Strategic Opportunities for 21st Century Cyber-Physical Systems. // Foundations for Innovation in Cyber-Physical Systems workshop. Chicago, IL, March 13-14, 2012. p. 231.

[2] Graham S., Baliga G., Kumar P.R. Abstractions, Architecture, Mechanism, and Middleware for Networked Control. // IEEE Transactions on Automatic Control, July 2009, vol. 54, no. 7, pp. 1490-1503.

[3] Lee E.A. Cyber-Physical Systems – Are Computing Foundations Adequate. // NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap. Austin, October 16-17, 2006, pp. 342-353.

[4] Ruiz J.F., Desnitsky V.A., Harjani R., Manna A., Kotenko I.V., Chechulin A.A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). Garching/Munich, February, 2012. pp. 261-268.

[5] Desnitsky V.A., Kotenko I.V. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices. // Lecture Notes in Computer Science, 8708(1): 2014. pp.194–210.

[6] Kotenko I.V., Levshun D.S., Chechulin A.A. Event correlation in the integrated cyber-physical security system. // Proceedings of the 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, May 2016. pp. 484-486.

[7] Fry C., Nystrom M. Security Monitoring. Sebastopol, USA, O'Reilly Media Inc., 2009. p. 227.

[8] Bejtlich R. The Practice of Network Security Monitoring. Understanding Incident Detection and Response./ Networking & Cloud Computing, 2013. p. 376.

[9] Creasey J., Glover I. Cyber Security Monitoring and Logging Guide. / CREST Published, 2015. p. 60.

[10] Parashchuk I.B. Parametrization principles of states space of Telecommunications network in the framework of formulation of problem of optimal adaptive networking monitoring. // Modern Science: Development Tendencies. VII International Science-Practical Conference. Part II. Krasnodar, 2014. pp. 142-144.

[11] Al-Shaer E., Ou X., Xie G. Automated Security Management. Berlin. Springer Science & Business Media. 2013. p. 187.