

# Development of Cyber-Physical System Security Management Process Model on the Example of Smart Home

Vyacheslav G. Burlov<sup>1</sup>, Elena S. Grozmani<sup>1</sup> and Sergey V. Petrov<sup>2</sup>

<sup>1</sup>*Peter the Great St. Petersburg Polytechnic University, Saint Petersburg, Russia*

<sup>2</sup>*Joint Stock Company "Research Institute "Rubin", Saint Petersburg, Russia*

**Keywords:** Cyberphysical System, Security, Management, Model, Management Decision.


**Abstract:** Cyber-Physical Systems (CPS) is a hierarchical information technology environment resulting from the convergence of general-purpose telecommunication networks and specialized technological devices designed to control and monitor physical processes. This type of systems is actively implemented in industrial, urban, and residential infrastructure, allowing for more efficient use of resources, improved quality of management and feedback. As complex heterogeneous distributed information management systems, CPSs are susceptible to cyber threats. The peculiarities of construction and functioning of cyber-physical systems require the division of threats and attacks into two classes. The first includes malicious actions aimed at violating the confidentiality, availability, and integrity of data processed in the system. Ensuring the security of conventional information systems is aimed at preserving these very properties. The second class includes cyber threats, the successful implementation of which can disrupt or modify the system's management and control processes. Depending on the CPS's objectives and the degree of criticality of the real-world processes it controls, disturbance of flows within it can lead to serious consequences, such as great material damage or threat to human life and health. With the rapid development and improvement of Programmable Logic Controller (PLC) devices and their cost reduction, the smart home concept is becoming increasingly popular. This approach involves integrating PLCs communicating with each other and the control center via multiprotocol computational public access (Internet) networks into the residential infrastructure. Thus, a smart home is built on the basis of CPSs. In this application environment, it is essential to ensure the information security of the cyber-physical systems used. To ensure the required level of security of these objects, it is necessary to effectively solve the problems of managing the process of ensuring their information security. On this basis, the paper proposes an approach to develop a model of the CPS security management process on the example of a smart home.


## 1 INTRODUCTION


Cyber-physical systems are information-technological objects resulting from the fusion of physical process with controlling the programmed environment, created based on developed heterogeneous multiprotocol computer networks, and including productive information systems, which can possess properties of artificial intelligence. On their basis, the control of direct executors (electrical, hydraulic, thermodynamic, climatic, robotic systems and complexes, etc.) is implemented together with

monitoring and data collection necessary for the organization of timely and quality feedback.

On the other hand, CPSs can be considered as a conceptual paradigm of production and technological systems representation in the form of a conglomerate of means of transformation of matter and energy different types and information and telecommunication environment, which provides both information exchange between components and functioning of the entire complex under variable external environment using automated control.

<sup>a</sup> <https://orcid.org/0000-0000-0000-0000>

<sup>b</sup> <https://orcid.org/0000-0000-0000-0000>

<sup>c</sup> <https://orcid.org/0000-0000-0000-0000>

To date, the most prominent examples of CPSs are systems that provide the implementation of the concept of smart home and the Internet of Things (IoT), Industrial Control Systems (ICS), as well as Supervisory Control And Data Acquisition (SCADA). Geographically distributed CPSs include traffic control and management systems. Examples of local cyber-physical systems are the modern automobile and sophisticated medical equipment.

Cyber-physical systems, being information systems, are susceptible to the digital environment's destructive factors - threats to information security. In contrast to conventional information systems designed to provide data processing, the main task of CPSs is to manage and control the physical processes of the real world. This defines a change in the attackers' primary targets. For traditional information systems, it is unauthorized access to protected information and violation of data and services availability. The main targets of attacks on CPSs are to disrupt information flows within the system and intercept the control of the actors (actuators). As a result of changing the attackers' targets, the consequences of successfully executed attacks change as well. For information systems, this is usually a financial and reputational loss. In the case of CPSs, the damage can be quite different, ranging from damage and destruction of technical facilities and objects to harming human health and even endangering human life. The situation is complicated by the fact that targeted computer attacks using zero-day vulnerabilities, social engineering, and specially designed tools can be carried out against cyber-physical systems. The complexity and heterogeneity of CPSs, the presence of multiple cyber threats and attackers with special means and high qualifications, and great potential damage require the implementation of a complex multipurpose information security system.

The protection subsystem is a fully or partially independent metasystem concerning the protected and consists of a set of processes aimed at identifying and neutralizing threats. At the same time, the information security subsystem management process should be viewed as even more high-level. Most of the research focuses specifically on security processes rather than on security management. Simultaneously, in the absence of command decisions adequate to the real situation, even the most perfect system will not be able to achieve its targets with the required indicators.

Another important issue is the selection and justification of the requirements for the CPS protection system. In this situation, it is necessary to

build a mathematical model of the system, which would evaluate the prototype's characteristics even before its creation. Currently, the prevailing approach is to build models based on analysis. In their simpler implementation, these solutions do not take into account all the regularities and conditions of the existence of the target processes within the system. Thus, the implemented security systems do not have the required properties and/or indicators and do not provide the required security level.

Given the above, ensuring the secure functioning of cyber-physical systems is a priority in the context of their rapid development and widespread deployment. At the same time, current approaches to the organization and provision of the CPS safety management processes do not allow achieving management objectives with a guaranteed result. This poses threats of unacceptable damage.

The purpose of this study is to develop a model of the CPS safety management process that allows a guaranteed result. A smart home was used as the object on which the proposed approach was tested.

## 2 PROPOSED METHODOLOGY

At the heart of the management process is a management decision. Any solution is built on the basis of a control process or subsystem model. Thus, if this model is not "good", it becomes impossible to work out the right solution. What criteria does the model have to meet? Its main and most important property is adequacy. A model must sufficiently account for the patterns and attributes of the objects being reflected. When we talk about the management process, which by definition is a continuum, it is crucial to define its conditions of existence. Only with the right solution to this problem is it possible to achieve the management objectives. Whether it is a human or an information management system, which is ultimately the realization of the intentions of its developers, the decision-maker has a conceptual and logical apparatus used in problem-solving (Andreev, Burlov and Grachev, 2019; Burlov, 2020). This process is not an atomic operation but consists of the following steps: decomposition, abstraction or formalization, and aggregation (three-component cognition). At the first stage, the problem is broken down into separate complete blocks, which can be solved using the system's methods. The formalization process moves to a certain level of abstraction by highlighting the properties and their evaluation criteria required to solve each problem. The final step is to process and merge the individual results

obtained. If a system is intelligent, it can carry out the accumulation of "experience", received as a result of aggregation processes, and produce new laws on its basis. The law of preservation of object integrity was used to work out process existence conditions (Burlov, 2017; Burlov, Andreev and Gomazov, 2018). It is expressed in the mutual transformation of its action's object properties and properties under a fixed purpose. In the context of the problem we are solving, the object, action, and purpose are transformed into a setting, an information-analytical work, and a management decision. Let us introduce the following definitions. A management decision is a condition for the subject to ensure the conditions for implementing the purpose of the object he manages in an appropriate environment to achieve the purpose of management. Environment is a set of factors and conditions in which activities are carried out. Information and analytical work is continuous extraction, collection, study, display, and analysis of situation data. For example, marketing, exploration, and monitoring (Burlov and Grachev, 2020; Burlov, Abramov, Istomin, Fokicheva and Sokolov, 2018). Thus, based on the principle of three-component cognition and the law of preserving the object's integrity, it is necessary to proceed to the synthesis of the management decision process model. Its graphical representation is shown in Figure 1.

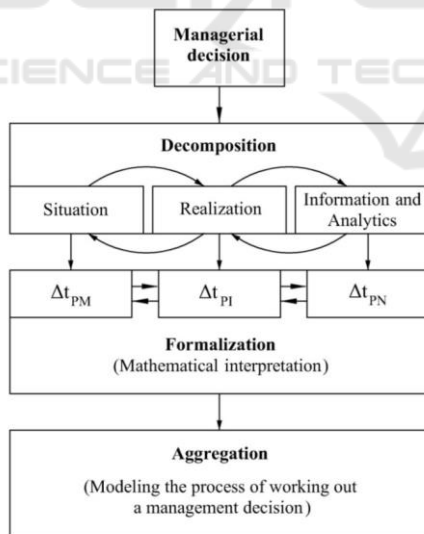


Figure 1: Structure diagram of the interpretation of the synthesis process of the decision mathematical model.

At the first level, applying the decomposition method, we decompose the solution exactly into three elements "environment", "solution" and "information-analytical work", which correspond to "object", "purpose" and "action". Applying the

method of abstraction at the second level, we identify the "object" ("environment") with the periodicity of the problem manifestation for the system -  $\Delta t_{PM}$ , which requires the development of a solution. "Intent" ("Solution") is identified with the periodicity of neutralization of the problem (average time of adequate response to the problem) -  $\Delta t_{PN}$ . "Action" ("Information-analytical work") is identified with the frequency of problem identification (average time to recognize an adverse situation) -  $\Delta t_{PI}$  (Burlov, Uzun, Grachev, Faustov and Sipovich, 2021; Chumakov, Zakharov and Tumanov, 2018). The temporal characteristics are justified by the fact that only temporal resources are irrecoverable. Also, the results of research in the theory of functional systems of the USSR Academy of Sciences Academician P.K. Anokhin (Anokhin, 1979) showed that the decision-maker's decision is formed in the scheme "excitation", "recognition", "reaction to the situation". Therefore, the following diagram of the expression of the decision model formation basic components is used in the paper:

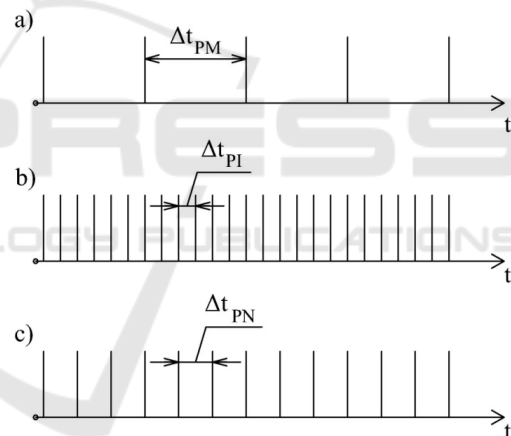


Figure 2: Diagram of the manifestation of the basic elements of decision model formation.

With the help of aggregation the concept of "management decision" is transformed into an aggregate - a mathematical model of management decision of the following kind:

$$P = F (\Delta t_{PM}, \Delta t_{PI}, \Delta t_{PN}) \quad (1)$$

### 3 PROPOSED METHOD

Due to the fact that the basic model of management decision has three elements, let us present the management structural scheme as follows:

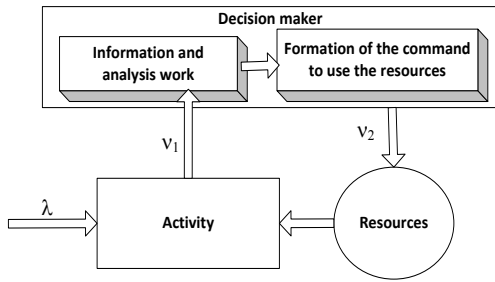


Figure 3: Structure diagram of the control.

$\lambda$ - the value inverse of the average time of manifestation of the problem;

$v_1$  is the value inverse of the average problem identification time;

$v_2$  is the value inverse of the mean problem neutralization time.

The decision-maker, expressed as an information command system, should ensure the fulfillment of existing conditions of the target processes under adverse external conditions by performing the following tasks:

- threat/problem identification (recognition);
- neutralizing (responding to) the threat/problem.

In this regard, four basic states of the decision-maker can be distinguished (Burlov and Popov, 2017; Sokolov, Alimov, Golubeva, Burlov and Vikhrov, 2018):

$A_{00}$  - decision-maker does not identify or neutralize;

$A_{10}$  - decision-maker identifies and does not neutralize;

$A_{01}$  - decision-maker does not identify and neutralize;

$A_{11}$  - decision-maker identifies and neutralizes.

$P_{00}, P_{10}, P_{01}, P_{11}$  - probabilities of being in these states respectively.

To implement this approach, it is necessary to make a system of Kolmogorov differential equations that relate the probabilities of finding the system in different states, and these equations do not work with absolute intervals (time), but with relative - frequencies (inversely proportional to time).

So, let's consider the graph of states of the information-management system:

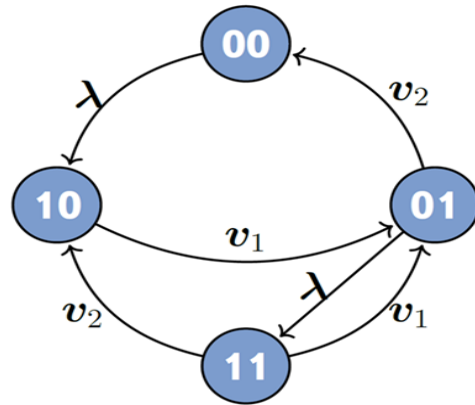


Figure 4: State graph of the management decision-making process.

$\lambda$  is the intensity of the problem manifestation ( $1/\Delta t_{PM}$ );

$v_1$  - intensity of problem identification ( $1/\Delta t_{PI}$ );

$v_2$  - intensity of problem neutralization ( $1/\Delta t_{PN}$ ).

Let us form a system of Kolmogorov differential equations:

$$\frac{d}{dt} P_{00}(t) = -P_{00}(t)\lambda + P_{01}(t)v_2 \tag{2}$$

$$\frac{d}{dt} P_{01}(t) = -P_{01}(t)(\lambda + v_2) + P_{11}(t)v_1 + P_{10}(t)v_1$$

$$\frac{d}{dt} P_{10}(t) = P_{00}(t)\lambda - P_{10}(t)v_1 + P_{11}(t)v_2$$

$$\frac{d}{dt} P_{11}(t) = P_{01}(t)\lambda - P_{11}(t)(v_1 + v_2)$$

The transition from differential equations to algebraic equations is possible if we assume that there are no transients, then the derivatives  $\frac{d}{dt} P_{00}(t) = 0$ , by the condition of function constancy (derivatives equal to zero), besides the sum of all probabilities is equal to one:  $P_{00}+P_{01}+P_{10}+P_{11}=1$ .

$$-P_{00}(t)\lambda + P_{01}(t)v_2 = 0 \tag{3}$$

$$-P_{01}(t)(\lambda + v_2) + P_{11}(t)v_1 + P_{10}(t)v_1 = 0$$

$$P_{00}(t)\lambda - P_{10}(t)v_1 + P_{11}(t)v_2 = 0$$

$$P_{01}(t)\lambda - P_{11}(t)(v_1 + v_2) = 0$$

The sought probabilities are no longer time-dependent. The solution of the linear algebraic system of equations (3) is the following relations:

$$P_{00} = \frac{v_1 v_2}{\lambda(\lambda + v_1 + v_2) + v_1 v_2} \tag{4}$$

$$P_{10} = \frac{\lambda v_2 (\lambda + v_1 + v_2)}{(v_1 + v_2) [\lambda(\lambda + v_1 + v_2) + v_1 v_2]}$$

$$P_{01} = \frac{\lambda v_1}{\lambda(\lambda + v_1 + v_2) + v_1 v_2}$$

$$P_{11} = \frac{\lambda v_1}{(v_1 + v_2) [(\lambda + v_1 + v_2) + v_1 v_2]}$$

Having received the relations defining the probabilities of the system being in  $A_{00}, A_{10}, A_{01}, A_{11}$  states, we can work out the requirements to the

intensity of the processes of recognition of the problem potentially arising in the system and the processes of their neutralization taking into account the supposed frequency of the destructive factors manifestation.

$$P_{00} = P_{INP} = \frac{v_1 v_2}{\lambda (\lambda + v_1 + v_2) + v_1 v_2} \quad (5)$$

$P_{INP}$  - probability of identifying and solving the problem facing the decision-maker.

Three parameters are related in this relationship.

Thus, the analytical dependence of generalized characteristics of environment ( $\Delta t_{PM}$ ), information-analytical activity ( $\Delta t_{PI}$ ) and work on neutralization of destructive factors ( $\Delta t_{PN}$ ), which can be used to assess models of information-analytical systems of information security process management and obtain the estimated values of key properties of these systems, was established.

## 4 EXPERIMENTAL RESULTS

This method has been tested on the example of the Smart House cyber-physical system. Research shows that securing the Smart Home system is one of the biggest challenges facing implementing this system (Robles and Kim, 2010; Yang, Mistretta, Chaychian and Siau, 2017; Li, Gu, Chen, He, Wu and Zhang, 2018).

One possible approach to determine the values of  $\lambda$ ,  $v_1$  and  $v_2$  is the use of network models.

A network model is a graphical representation of a set of interrelated activities performed in a certain sequence. The schedule consists of elements - activities and events (usually indicated by arrows and circles). The event has no duration in time. It marks the completion of one or more activities that determine whether subsequent activities can begin. According to its role in the network schedule, a distinction is made between an initial (initial) event - any work of the considered complex does not precede it; a final (final) event - after which no work within the considered complex is performed; an intermediate event fixing the end of previous work and the beginning of subsequent work.

According to the calculations that were made in the network planning, the following results were obtained:

1) the average time for the problem to appear is:

$$\Delta t_{PM} = 2 \text{ (days)} = 2880 \text{ (minutes)}.$$

$\lambda = \frac{1}{2} = 0.5$  (the inverse of the average problem time).

2) the average time to identify the problem:

$$\Delta t_{PI} = 116 \text{ (minutes)} = 0.08 \text{ (days)}.$$

$v_1 = \frac{1}{0.08} = 12.41$  (the value inverse of the average problem identification time).

3) the average time to neutralize the problem:

$$\Delta t_{PN} = 281 \text{ (minutes)} = 0.195 \text{ (days)}.$$

$v_2 = \frac{1}{0.076} = 5.12$  (the value inverse of the average problem neutralization time).

Let us consider the conditions for the existence of the process for given probabilities:

$$P_{00} = \frac{v_1 * v_2}{\lambda (\lambda + v_1 + v_2) + v_1 * v_2} = 0.876$$

$$P_{10} = \frac{\lambda * v_2 * (\lambda + v_1 + v_2)}{(v_1 + v_2) (\lambda * (\lambda + v_1 + v_2) + v_1 * v_2)} = 0.036$$

$$P_{01} = \frac{\lambda * v_1}{\lambda (\lambda + v_1 + v_2) + v_1 * v_2} = 0.086$$

$$P_{11} = \frac{\lambda * v_1}{(v_1 + v_2) (\lambda + v_1 + v_2) + v_1 * v_2} = 0.016$$

Thus, we obtain a solution model based on the synthesis approach, which allows us to evaluate the information-management system's properties before its construction. This approach ensures that the management objective is guaranteed to be achieved.

## 5 DISCUSSION

In this section, we present for consideration some open issues and shortcomings of the proposed approach.

Cyberphysical systems are dynamic objects. This means that they change over time and space. To ensure the required CPS security level, the information management system must promptly adapt to changes in the protected object. The proposed methodology, which is based on the law of preservation of the object's integrity, makes it possible to provide the required property.

At the same time, the decision-maker is constantly acting in the presence of uncertainty. In the case considered in the article, threats and vulnerabilities used in attacks on CPSs have the property of uncertainty. The presence of unknown attack vectors or zero-day threats significantly reduces information management information security systems' effectiveness. The approach proposed in the article does not take this factor into account at the moment.

The decision-maker, as stated, operates in an environment in which there is some uncertainty or ambiguity. Together with this, the information management system, being a complex object, is also prone to errors and failures. Thus, there is a possibility of misbehavior of the information and control system in which it fails to meet its target task. Refinement of the proposed method taking into

account this factor will improve the accuracy of the results obtained.

## 6 CONCLUSIONS

In this article, the types of attacks on cyber-physical systems have been identified due to their characteristics. It is established that disruption of the processes taking place in the CPSs and interception of control over them can lead to significant material damage and threaten people's lives and health.

To guarantee the achievement of managing the process of ensuring information security of the CPS, it is required to have an adequate model of the information and control system, which acts as a decision-maker.

The paper proposes a methodology and method of constructing this model using a synthesis-based approach. It was tested on the example of the CPS smart house.

This paper can act as a basic guide for developing models of the CPS security subsystems.

The purpose of further research is to refine the parameters of the control process model, in particular, it is required to take into account the probability of making an erroneous decision.

## REFERENCES

- Andreev, A., Burlov, V. and Grachev, M. (2019). "Information technologies and synthesis of the management process model in the enterprise", 2019 International Science and Technology Conference "EastConf", pages 1–5.
- Anokhin, P. (1979). *System mechanisms of higher nervous activity*, M.: Science, p. 453.
- Burlov, V. (2017). *The law of preserving the integrity of the object - the method of the basis for solving the problems of information warfare and ensuring security, Neurocomputers and their applications. Abstracts*, pages 261-263.
- Burlov, V., (2020). "Mathematical model of human decision: A methodological basis for the functioning of the artificial intelligence system", *Proceedings of the European Conference on the Impact of Artificial Intelligence and Robotics*, pp. 38-48.
- Burlov, V., Andreev, A. and Gomazov, F. (2018). Safety management of a technosphere object based on the law of preserving the integrity of the object, Federal State Budgetary Educational Institution of Higher Education "St. Petersburg State University of Economics (SPbSEU)", pp. 56-60.
- Burlov, V. and Grachev, M. (2020). Model of Management Decision Making in Enterprises Implementing Information and Measurement Technologies, *2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, Russia, pages 1-5.
- Burlov, V., Abramov, V., Istomin, E., Fokicheva, A. and Sokolov, A. (2018). The methodological basis for the strategic management of territory development, *18th International Multidisciplinary Scientific GeoConferences SGEM 2018*. Conference proceedings, pages 483-490.
- Burlov, V. and Popov, N., (2017). Space geoformation application management system in the interest of ensuring environmental security of the region, in the collection: *The successes of astronautics*, pages 751-760.
- Burlov, V., Uzun, O., Grachev, M., Faustov, S. and Sipovich, D. (2021). "Web-based power management and use model". *Advances in Intelligent Systems and Computing*, 1258 AISC, pages 629–641.
- Chumakov, N., Zakharov, A. and Tumanov M., (2018). In the collection: *Materials of the XVII All-Russian Scientific and Practical Conference on Planning and Training of Engineering and Technical Personnel for the Industrial and Economic Complex of the Region*, PTES 2018.17.2018, pp. 156-158.
- Sokolov, S. S., Alimov, O. M., Golubeva, M. G., Burlov, V. G. and Vikhrov, N. M. (2018). The automating process of information security management, *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus)*, pages 124-127.
- Li, M., Gu, W., Chen, W., He, Y., Wu, Y. and Zhang, Y. (2018). Smart Home: Architecture, Technologies and Systems, *8th International Congress of Information and Communication Technology (ICICT-2018)*, v. 131, pages 393-400.
- Robles, J. and Kim, T. (2010). Application, systems and methods in smart home technology, A review. *Int. J. Adv. Sci. Technol*, pages 37–48.
- Yang, C., Mistretta, E., Chaychian, S., and Siau, J. (2017). Smart home system network architecture.