Survivability of Organizational Management Systems and the Maintenance of Critical Infrastructure Security

© Aleksandr Dodonov, © Olena Gorbachyk, © Maryna Kuznietsova

Institute for Information Recording of National Academy of Sciences of Ukraine, Kyiv, Ukraine

dodonov@ipri.kiev.ua,
ges@ipri.kiev.ua,margle@ipri.kiev.ua

Abstract. The paper is dedicated to the issue of improving the security of critical infrastructures functioning using the capabilities of their automated organizational management systems. It's substantiated, that security of critical infrastructures functioning depends on the level of survivability of automated organizational management systems (OMS). Increasing the survivability of automated organizational management systems is an essential element of a secure risk management system for critical infrastructures. The survivability property of automated OMS is defined as their ability to retain their functionality by performing the set of functions necessary to achieve the goal of functioning with a given quality, in the context of accumulation of component damages and loss of resources, by changing the behavior of the system. The survivability states of automated OMS are classified. A model is proposed to investigate the survivability of an automated OMS regarding a set of functions aimed at ensuring the security of critical infrastructure functioning. The methodological aspects of the development and implementation of the automated OMS are highlighted, that will function in the conditions of permanent changes of the environment and modernization of the components of the OMS. The criteria of estimation of system qualities of OMS and its components - automated workplaces are offered. An integrated survivability index has been proposed to evaluate the survivability and functional degradation of the OMS. Time constraints for the fulfillment the procedures for building information infrastructure in the OMS are formulated, to ensure the implementation of the functions supporting the critical infrastructure security. The expediency of creation a specialized modeling complex for OMS automation for the development of basic system, design and technological solutions, development of management decisions for the basic processes of organizational management is substantiated. At the specialized modeling complex it is possible to analyze and improve the existing methods of maintaining the security of critical infrastructure functioning, to develop templates for managers' actions in the event of undesirable changes during the critical infrastructure functioning, occurrence and development of emergency situations on the objects of critical infrastructure.

Keywords: survivability, security, critical infrastructure, automated organizational management system.

1 Introduction

Ensuring the security of critical infrastructures is, first and foremost, a reduction to an acceptable level of risk of harm to the environment, the individual, society, and the country. Critical infrastructure objects must be guaranteed to maintain a certain level of security, avoid emergency situations, prevent their transition to dangerous conditions.

Low survivability systems collapse quickly and this can lead to cascading accidents and significant material losses, while systems with high survivability break down gradually, retaining in part functionality, limited performance, and time-consuming adoption for switching to safe mode of operation, emergency shutdown, isolation of damage, preventing their spread, etc. An important part of the security risk management system of critical infrastructures is to increase the survivability of organizational management systems.

Today, all chains of control of critical objects and infrastructures involve complexes of hardware and software, information systems and telecommunication networks, intended to support the solution or solve the problems of operational management and control over various processes and technical objects within the organization of production or technological processes. Computer tools have become an integral part of various management systems, components of complex technical, administrative, economic and other systems of regional and global scale. Computer systems and technologies provide advanced communication tools, support a complex structure of resources, production and management processes automation, various technologies for information processing. Security of management objects depends on the technologies of automated organizational management systems, which are complex sociotechnical systems, that include technical and technological subsystems, relevant systems of activity (systems of roles and functions of service and management personnel), an environment that actively interacts with others compound.

Effective use of the sociotechnical systems components capabilities, taking into account the synergistic effect allows ensure the functional safety of critical infrastructures, to reduce the risk of accidents.

2 Critical infrastructure security dependence on the survivability of organizational management systems

Critical infrastructure security will mean the independence from unacceptable risk [1], that is, the ability of infrastructure, as a system, to minimize the risks of disaster.

Automated organizational management systems (OMS) for critical infrastructures should ensure not only the proper functioning of the infrastructure and the desired end result, but also the adequate response to security incidents occurring at critical infrastructure objects [2]. Tools of the automated OMS should ensure timely recognition of the threat and the moment of occurrence of a critical (emergency) situation, determine an adequate level of their processing, initiate processes of counteraction, compensation or adaptation to continue the functioning of the critical infrastructure in full or in part, and, if necessary, procedures for slow gradual degradation and safe shutdown must be activated.

An analysis of the current trends in the development of automated OMS shows that there is an increasing number of functions that are critical to the security of critical infrastructures that rely on information and communication technologies and computers. Even today, thanks to automation, the implementation of organizational management processes occurs in such a way as to prevent the transition of infrastructure or its components into potentially dangerous states [2-4]. As a rule, the shutdown of a technical object in case of occurrence or realization of a threat of its transition to a dangerous (emergency) state is automatic. Intelligent software products for predicting, assessing and minimizing the security risks of critical objects and structures are available to support and develop management solutions at various levels.

Under the survivability of an organizational management system, we will understand its ability to retain its functionality by performing the set of functions necessary to achieve the goal of functioning with a given quality, in the context of accumulation of component damage and loss of resources, by changing the behavior of the system.

In the general case, the survivability of the OMS depends on the set of parameters that characterize the system, the functions performed by it, the effects of the environment and the type, extent and dynamics of interaction with it. If the OMS is in a "status of survivability," the system performs the set of functions $\phi=(\phi_1,\phi_2,...,\phi_n)$ with the specified quality and required efficiency, that is, the purpose of the function is achieved. The "status of survivability" is characterized by the stability and predictability of the functioning of the system, that is, the critical infrastructure OMS fulfills all managerial functions.

There are three types of system survivability status $|\mathrm{S}|=\{|\mathrm{S}|_t\}, t=1,2,3$, to which the OMS can go, namely [2, 5]:

- system survivability status type $|\mathrm{S}|_1$, in which the OMS provides all the functions of the set $\phi=(\phi_1,\phi_2,...,\phi_n)$ with given quality and required efficiency or with poor quality and less efficiency in any of the states $w_j \in W$, that is

$$\prod_{i\in I} x(\phi_i)=1, \qquad x(\phi_i)=\begin{cases}1, \textit{ if } \phi_i \textit{ is fulfilled}\\ 0, \textit{ otherwise}\end{cases}$$

- system survivability status type $|\mathrm{S}|_2$, whereby only a certain subset of the functions are provided by the OMS $\phi^*\subset\phi$ in any of the states $w_j \in W$, that is

$$\prod_{\phi_i\in\phi^*} x(\phi_i)=1$$

- system survivability status type $|\mathrm{S}|_3$, whereby at least one of the functions of the set is performed in the OMS $\phi=(\phi_1,\phi_2,...,\phi_n)$ in any of the states $w_j \in W$, that is

$$\sum_{i\in I} x(\phi_i) \geq 1 .$$

Transition of the OMS into "status of survivability" types $|\mathrm{S}|_2$ and $|\mathrm{S}|_3$ means that there are violations in the functioning of the system (functional failures of components or "wrong actions" of managers), and there is a narrowing of the functionality of the OMS.

Among the functions of the set $\phi = (\phi_1, \phi_2, ..., \phi_n)$ identify the functions of the OMS, aimed at ensuring the security of critical infrastructure, $\phi^S \subset \phi,\ \phi^S = (\phi_1^s, \phi_2^s, ..., \phi_r^s)$. Functions from the set ϕ^S can be both independent and information related. The ability of the OMS to maintain the secure functioning of the critical infrastructure can be characterized by the OMS 's survivability with respect to a set of functions ϕ^S.

In automated OMS, the automated workstations of managers (AWM) are functional components. Each AWM is a subsystem, the structure of which is determined by its functional purpose. AWM specialization is done by installing the appropriate software and establishing links between system components. The modular principle of software development makes it quite easy to form the required configuration of the AWM, as a subsystem of the OMS, to perform certain management functions. AWM functionality can be expanded as needed by connecting new software modules. This creates a flexible scalable environment for implementing management functions.

To study the survivability of automated OMS with respect to a set of functions ϕ^S, to ensure the critical functioning of the critical infrastructure, the following model can be applied:

$$\overline{\Im} = \left\langle G, \phi^S, \mathrm{Tm}, \mathrm{Can}, \mathrm{Tt} \right\rangle ,$$

where G – a graph that describes the information and communication links in the OMS and may be changed during the operation of the OMS or in the case of changing the functionality of the individual AWM; $\phi^S = (\phi_1^s, \phi_2^s, ..., \phi_r^s)$ – a set of functions implemented in the OMS to maintain the security of critical infrastructure, Tm – some of the time-deficient functions of the last argument, Can – a matrix of functionalities of the totality of AWM, which actually represent an automated OMS; Tt – vector that characterizes the load of the AWM.

Let us denote the set of managerial tasks performed in the OMS of the implementation of the set of functions $\phi^S = (\phi_1^s, \phi_2^s, ..., \phi_r^s)$ with the required quality and the required efficiency through

$$F = \bigcup_{i\in I} F_i = \{f_1, f_2, \dots, f_n\} ,$$

while the AWM Φ_k can potentially perform a number of managerial tasks $\varphi_{\text{н}} : \{1, 2, \dots, p\} \to P(F)$, where $P(F)$ –the set of all subsets F.

If $\varphi_{\text{н}}(k) = \left\{f_{i_1}, f_{i_2}, \dots, f_{i_j}\right\}$, $1 \leq i_r \leq n$, then the functional component of the AWM Φ_k

can perform managerial tasks $f_{i_1}, f_{i_2}, \dots, f_{i_j}$.

Suppose that all the necessary information and communication links between the AWM of the OMS to perform the security support functions of the critical infrastructure can be provided.

At each specific moment of time specific AWM Φ_k implements a subset of managerial tasks $\varphi_{men} : \{1, 2, \dots, p\} \to P(F)$.

At the AWM of the OMS the decision of managerial tasks $f_1, f_2, \dots, f_n$ is supported, if $\varphi_{men}(k) = \{f_{i_1}, f_{i_2}, \dots, f_{i_j}\}$. If $\varphi_{men}(k) = \varnothing$, than AWM of the OMS Φ_k does not perform managerial tasks, the solution of which requires the implementation of functions ϕ^S, which support the security operation of critical infrastructure.

Assuming every managerial task $f_i \in F$ is characterized by some performance efficiency c_i, you can define the performance function for the entire automated OMS on the performance of functions ϕ^S which support the security operation of critical infrastructure: $\psi_{е\phi} : F \times \{1, 2, \dots, p\} \times P(F) \to C$,where C is a certain number set.

If the AWM of the OMS Φ_k is focused on managerial tasks $\varphi_{men}(k) = \{f_{i_1}, f_{i_2}, \dots, f_{i_j}\}$ and performance when fulfilling $f_i \in \{f_{i_1}, f_{i_2}, \dots, f_{i_j}\}$ is equal to c_{i_k}, than: $\psi_{е\phi}(f_i, k, \varphi_{men}(k)) = c_{i_k}$

.

To implement by automated OMS the functions ϕ^S, which support the security operation of critical infrastructure, with the efficiency not lower than the specified, the managerial tasks $f_1, f_2, \dots, f_n$ must be performed with appropriate efficiency, that is, the following conditions must be met [5]:

$$\bigcup_{k=1}^{p} \varphi_{н}(k) \supseteq F, \tag{1}$$

$$\varphi_{men}(k) \subseteq \varphi_{н}(k) \qquad \forall k = \overline{1, p}, \tag{2}$$

$$\sum_{k=1}^{p} \psi_{е\phi}(f_i, k, \psi_{men}(k)) \geq c_i, \quad \forall i = \overline{1, n}, \tag{3}$$

Let us define as a functional failure the impossibility of fulfilling at least one of the managerial tasks in the OMS $f_i \in F$. In the case of functional failure, the status of some AWM Φ_k changes and the corresponding function φ_{men} also changes. Although condition (2) cannot be violated by functional failure AWM Φ_k, but its violation may be caused by errors in management. If the narrowing of the functionality leads to a violation of conditions (1) - (3), then the means of ensuring the survivability of the

OMS must be activated and the system must be adjusted so that conditions (1) - (3) are again fulfilled.

When reconfiguring the OMS, it is advisable to minimize the number of AWM of the OMS involved in failure compensation procedures, i.e. to minimize the number of changes φ_{men}. It is because of the conditions (1) - (3) that the minimum quantity of φ_{men} is changed, the optimality of OMS behavior can be characterized, and the number of compensated functional failures may serve as a criterion for system survivability.

3 Development and implementation of automated high-survivability OMS for critical infrastructure

The problem of ensuring the safety of the functioning of critical objects and infrastructures is complex, but the quality and properties of their automated OMS are of utmost importance, since the security and safety of critical infrastructures depends on management decisions, especially in the event of an emergency situation, i.e. in conditions when there is no possibility of a clear prediction of the results of management impacts. Functional stability of the OMS itself becomes a factor and condition for security and safety of critical infrastructure objects.

Already at the initial stage of development and implementation of automated OMS, it is necessary to define criteria for assessing systemic qualities, in particular, [6, 7]:

- criteria for compliance of the OMS and the individual AWM with the specified indicators of quality of functioning and/or assessment of the degree of its functional degradation;
- criteria for evaluating the performance of dynamic reconfiguration and reallocation of resources;
- criteria for assessing the extent of system recovery after glitches and failures due to mechanisms of reorganization or reconstruction;
- criteria that characterize changes in performance, reactivity, system sensitivity in the conditions of system resources degradation;
- criteria for assessing the adaptability of the system to external and internal changes;
- cost-effectiveness criteria for the use of available resources.

Analyzing the survivability of an automated OMS that operates in a constantly changing external environment and often undergoes modernization, one can obtain the most objective and adequate indicator of the quality of its functioning, because it is in the study of survivability that the system's ability to perform its functions over a long period is revealed, and not just the possibility of continuation of function in gap on recovery after individual glitches or failures. Quantitative assessment of survivability is generally performed on the basis of specific metrics that characterize the loss of functionality (functional degradation) over a certain period of time. Various methodological approaches to calculating such metrics are possible, in particular through quantitative assessments of the system's ability to perform mission-critical functions, through the degree of system degradation, and the like. For example, for the analysis of survivability and the assessment of functional degradation, it is possible to use the integral survivability index, determined by the weighted average of the estimates of performance indicators in the following form [7]:

$$\xi = \frac{1}{N}\sum_{j=1}^{N} z_j(r),$$

where the values of the normalized indicators $z_j(r), j = \overline{1,N}$ are calculated as

$$z_j(r) = \begin{cases} a_j \dfrac{q_j^*(r) - q_j^{TB}}{q_j^{TB}}, j = \overline{1,l}, \textit{ for technical requirements (TR) of the form } q_j \geq q_j^{TB} \\ a_j \dfrac{q_j^{TB}(r) - q_j^*}{q_j^{TB}}, j = \overline{l+1,N} \textit{ for TR of the form } q_j \leq q_j^{TB} \end{cases}$$

where a_j – weighting factor characterizing the degree of significance of the j-th index of survivability for the integrated assessment of the quality of functioning of the automated OMS; r - the number of accumulated functional failures in the OMS over a given period of time (taking into account the recovery); $q_j \subset Q = \{q_1, q_2, \ldots q_S\}$ – element of a set of metrics that should be within the appropriate range, which are defined by the technical requirements, which are formulated, as a rule, in the terms of reference for the development of automated OMS; $q_j(r)$ – the "worst" in understanding the fulfillment of the terms of reference of the j-th indicator value of the quality of functioning when r components failure accumulated in the system.

If there is a restriction for all given survival~~ rat~~es for a given period of time $q_j \geq q_j^{TB}$ or $q_j \leq q_j^{TB}$, $j = \overline{1,N}$, then $\min\limits_j z_j \geq 0, \quad j = 1, N$, and, accordingly, the value of the integral index ξ will be no lower than some critical lower limit ξ_{kp}, the specific value of which may be specified when determining the functionality of the system for a certain period of operation, or as the initial value of the integral index ξ. In this case, a quantitative assessment of the degree of degradation of the system's capabilities may be, for example, the value:

$$S_d = \frac{\xi_{\text{п.}} - \xi_{\text{пот.}}}{\xi_{\text{п.}}} \times 100\% = \frac{\xi_{\text{втр.}}}{\xi_{\text{п.}}} \times 100\%,$$

where $\xi_{п.}$ – quantitative assessment of the initial (design) functionality of an automated OMS, taking into account the weighting coefficients of the significance of the survivability indicators; a $\xi_{пот.}$, $\xi_{втр.}$ – quantification for current (existing) and lost OMS functionality, respectively.

The automation of the OMS involves the introduction of information and communication technologies for the collection, processing, accumulation, systematization, storage, retrieval and dissemination of information [8]. The functioning of an automated OMS can be modeled with help of network model, the nodes of which are the functional components (AWM), and the arcs are the different communication channels (wired, wireless, combined).

The implementation of information and communication technology is ensured by the parallel and sequential operation of a set of functional components that interact with each other and with the external environment through communication channels. Technology should provide the development of management decision, for example, over time T_z, which does not exceed $T_{доп}$ (the maximum time allowed for the collection and processing of information, which depends on the requirements of the subject area). Therefore,

$$T_z = (T_f + T_{об}) \le T_{доп},$$

where T_f – time spent for processing information by functional components, $T_{об}$ – time spent on information interaction.

In the case of undesirable influences on the system or communication channels, the time for implementation of information technology to develop a management decision may increase by $T_{дод}$. The survivability criterion of the OMS may be the feasibility of building the necessary information infrastructure as a set of functional components and communication channels under restrictions

$$(T_f + T_{об} + T_{дод}) \le T_{доп}.$$

For comparison of different variants of automated OMS implementation for the purpose of choosing the most functionally sustainable one can use the survivability index - the number of information infrastructures that allow to implement information technology of management decision making, reducing the risks of occurrence and development of emergency situations in critical infrastructures.

The practical experience of designing and implementing automated OMS shows that all basic system, design, software and technological solutions for the created OMS should be pre-tested, and the managers have to go through the re-education and training stage. It is advisable to make adjustments and approbations of the AWM on the specialized modeling complex. The architecture of the complex depends on the features of the critical infrastructure, systems models and processes involved in the operation of the objects and infrastructure as a whole. Each management task that arises in the operation of critical infrastructure can be reproduced in the modeling complex as a separate functional task, the execution of which in the OMS generates a separate management process. The input for this process can be either the initial management impact, or the output or intermediate data of some other management process. The execution of the management process involves the preparation and development of decisions on the actions ordering, necessary to perform a functional task, into a certain sequence of operations implemented within the relevant technology, determining what people (employees), at what time, what technological processes (operations) perform to ensure the secure functioning of the critical infrastructure. The implementation of the technological process requires not only the specialists with the appropriate level of qualification, but also the technical means, techniques and instructions for their application, software, information and other services, necessary and sufficient for the fulfillment of the functional tasks of management [5].

On the specialized modeling complex could not only be worked out the basic processes of organizational management, but also carried out the selection and testing of practically suitable formalized methods of maintaining the security of critical infrastructure functioning with high promptness of justified management decisions development, clarity of results of management and taking into account the existing system-based subordination and interaction in OMS.

Traditionally in the process of working out and making decisions, managers use "subjective" knowledge of certain events, informal experience of experts, who are involved in the assessment of the current situation in the critical infrastructure.

When working on the specialized modeling complex of basic processes of organizational management, the transition from intuitive estimates to quantitative is possible, that significantly objectifies management decisions and helps to improve their quality. Preliminary analysis of emergency situations on the modeling complex, crashes in the operation of critical infrastructure and erroneous management decisions allows create specific templates of managers' actions, which is important in the conditions of time resource criticality in accidents at the management object [8].

In the future, the specialized modeling complex can become an analytical resource for the OMS, its toolkit can be used to develop strategic management decisions and substantiate current management decisions.

4 Conclusions and recommendations

The use of automated high-survivability OMS in critical infrastructures will reduce the risks of infrastructure transition to disaster states, as such OMS are guaranteed to perform their functions over a long period in the face of permanent environmental change and many frequent upgrades.

The analytical resource developed during the AWM OMS creation, formalized methods of maintaining the security of the functioning of critical infrastructures will allow to increase the efficiency and validity of management decisions, the clarity of the results of management even in the context of unwanted changes in the system of subordination and interaction in OMS, caused by changes in the functioning of critical infrastructure.

References

1. Dodonov,O., Gorbachyk, O., Kuznietsova, M.: Increasing the survivability of automated systems of organizational management as a way to security of critical infrastructures. In: XVIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2018), CEUR Workshop Proceeding (ISSN 1613-0073). Vol. 2318, p.261-270 (2018), http://ceur-ws.org/Vol-2318//, last accessed 2019/11/15.
2. Kharchenko,V.S., Yakovlev,S.V., Gorbachyk,O.S. ,etal.: Provision of Functional Safety of Critical Information-control Systems. Kharkov: Konstanta, 272 p. Ukr. (2019).
3. Kuznietsova, N. V.: Information Technologies for Clients' Database Analysisand Behaviour Forecasting. CEUR Workshop Proceeding (ISSN 1613-0073). Vol. 2067, p.56-62 (2017), http://ceur-ws.org/Vol-2067/, last accessed 2019/11/15.
4. Churyumov, G., Tkachov, V., Tokariev, V., Diachenko, V.: Method for Ensuring Survivability of Flying Ad-hoc Network Based on Structural and Functional Reconfiguration. In: XVIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2018), CEUR Workshop Proceeding (ISSN 1613-0073). Vol.2318, p.64-76, (2018) http://ceur-ws.org/Vol-2318//, last accessed 2019/11/15.
5. Dodonov,O., Kuznietsova, M. Gorbachyk, O.: Complex Systems Survivability: Analysis and Modeling. Kyiv: NTUU "KPI", 264 p. Ukr. (2009).
6. Dodonov,O., Gorbachyk, O., Kuznietsova, M.: System Research of Survivability andSafety for Complex Technical Systems. Data Rec., Storage&Processing. Vol.12, N 2, p.202-208. Ukr. (2010).
7. Dodonov,O., Gorbachyk, O., Kuznietsova, M.: Organizational Management Systems: Information Technology and Security In: XIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2013). V.13, p.5-11. (2013).
8. Dodonov, O.: Computer Modelling of the Process of Organizing Management // Visnyk NANU, N1, p. 69 – 77. (2016).