A Mathematical Model for Information Security of Automated Control Systems for Technical Processes of a Gas Producing Enterprise

A. S. Rimsha
University of Tyumen (UTMN)
RimshaAndrew@gmail.com

A. N. Iuganson
ITMO University
a_yougunson@corp.ifmo.ru

***Abstract*— Currently, gas producing enterprises use automated systems to improve the efficiency and control of the process. The principle of working operation automated control systems for technical processes of a gas producing enterprise is very similar to the solutions used in other industrial enterprises, but nevertheless has its own features. The gas producing enterprises could be concerned with facilities, exposed to different emergencies, which can be caused, among other things, by insufficient protection of automated control systems for technical processes.**

To analyze the level of information security of the typical gas producing enterprise a mathematical model was proposed. This article describes every level of such system, assets are identified and the technology for modeling information security is determined. Few ways of vulnerabilities assets are stated. Main threats are based on these vulnerabilities. Possible ways of implementation of suggested information security systems and their influence on the reduction of possible damage are considered.

Keywords*— *mathematical model; information security; gas productng enterprise; risk assessment; cyber-physical systems

I. INTRODUCTION

To automate the process of producing gas automated control systems for technical processes are used. Very often they are based on programming logical controllers (PLC) [1].

The preliminary analysis of typical information systems of automated control systems for technical processes, network protocols and different reference resources shows the complexity of interoperating between these parts. As a result, there are many potentially vulnerable parts of the information system. [2, 3]

It is difficult to gather a sufficient amount of information about security incidents. That’s why a problem of modeling information security of automated control systems for technical processes of a gas producing enterprise is actual nowadays. The mathematical model will help to assess risks, to optimize expenses on information security in organization, to give some recommendation how to increase information security level by some technical and organizational measures. [4].

Typically, the approach to modeling is chosen, focused on the parameters used as input information, and those results of calculations that are obtained at the output. Usually, input information is based on available statistics for the existing information systems and/or is based on expert data. The deduced models can be used as at the design stage of the information system, so in the phases of operation and maintenance, monitoring and audit of information security systems.

II. METHODOLOGY

To select a specific technology for modeling the information security of automated control systems for technical processes, we formalize some business processes of a typical gas producing enterprise, which is a territorially distributed structure that starts from the gas wells and ends with a central dispatch station.

Management of the technological process requires the use of special technological solutions for the construction of data transmission networks. The simplified structure of automated control systems for technical processes of a gas producing enterprise is built on a hierarchical basis. There are three common levels in this industrial system’s structure [1, 5]:

- *low level* or *input level*. On this level there are sensors (a temperature sensor, a pressure sensor and other) and executive mechanisms (regulating and stop valves and other);
- *middle level* or *level of automate management*. On this level there are industrial controllers, controlling executive mechanisms and, if needed, devices for transmitting data from the sensors to the upper level;
- *high level* or *level of operator’s control*. It is centralized remote control based on SCADA (supervisory control and data acquisition) and modern developments in the field of information technology (including Input/output servers, electric switchboards, different workstations, databases, software for monitoring, visualizing and saving data from automated processes and other).

Let’s introduce some general symbols:

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

$c^{sensor} = \{c_1^{sensor}, \ldots, c_{a_1}^{sensor}\}$ – a set of sensors used in technical processes;

$c^{mechanism} = \{c_1^{mechanism}, \ldots, c_{a_2}^{mechanism}\}$ – a set of executive mechanisms;

$c^{PLC} = \{c_1^{PLC}, \ldots, c_{a_3}^{PLC}\}$ – a set of PLCs;

$c^{server} = \{c_1^{server}, \ldots, c_{a_4}^{server}\}$ – a set of input/output servers;

$c^{network} = \{c_1^{network}, \ldots, c_{a_5}^{network}\}$ – a set of network components;

$c^{workstation} = \{c_1^{workstation}, \ldots, c_{a_6}^{workstation}\}$ – a set of workstations.

Then the set of all types of equipment (the system's components) used in the automated process control system of a gas producing enterprise can be represented in the following form:

$$C = \{c^{sensor}, c^{mechanism}, c^{PLC}, c^{server}, c^{network}, c^{workstation}\} \quad (1)$$

Unlike the proposed generalized mathematical model of automated control systems for technical processes [6] the OSI model will be used to represent the interaction of devices with each other. According to the OSI model every level (physical, data link, network, transport, session, presentation, application) will be corresponded to an adjacency matrix. The dimension of the matrix is defined by the number of system's components |*C*|, and elements of the matrix are represented with network protocols. From there, a set of devices' interactions can be defined as follows:

$$S = \{S^1, \ldots, S^7\} \quad (2),$$

in which $S^k = \begin{vmatrix} 0 & \ldots & s_{1j}^k & \ldots & s_{1i}^k & \ldots & s_{1n}^k \\ \ldots & 0 & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{j1}^k & \ldots & 0 & \ldots & s_{ji}^k & \ldots & s_{jn}^k \\ \ldots & \ldots & \ldots & 0 & \ldots & \ldots & \ldots \\ s_{i1}^k & \ldots & s_{ij}^k & \ldots & 0 & \ldots & s_{in}^k \\ \ldots & \ldots & \ldots & \ldots & \ldots & 0 & \ldots \\ s_{n1}^k & \ldots & s_{nj}^k & \ldots & s_{ni}^k & \ldots & 0 \end{vmatrix}$,

k – the level of the OSI model,

s_{ij} – a network protocol.

All significant assets correspond to a certain value, depending on the degree of its impact on the profit of the organization and the level of damage (in financial, reputational, social, industrial and other ways), which the organization may incur in the event of failure, compromise, or improper functioning of the asset. Let's combine the value of assets in a set:

$$A = \{A_1, \ldots, A_o\}. \quad (3)$$

According to (1) and (2) the potency of this set will be equal to $o = |C| + |S|$.

Talking about automated control systems for technical processes of a gas producing enterprise we can leave out the problem of confidentiality [7]. Thus, the vulnerability is a security issue that can break the integrity and accessibility of information. Let's define a set of vulnerabilities as $V = \{V_1, \ldots, V_m\}$.

Each vulnerability can have different impact on a separate asset [8]. Thereby vulnerability's affects can be presented as a matrix of impacts of vulnerabilities on values assets.

TABLE I. THE MATRIX OF IMPACTS OF VULNERABILITIES ON VALUE ASSETS

	V_1	V_2	…	V_m
A_1	v_{11}	v_{12}	…	v_{1m}
A_2	v_{21}	v_{22}	…	v_{2m}
…	…	…	…	…
A_o	v_{o1}	v_{o2}	…	v_{om}

An impact of single vulnerability on the set of value assets could be calculated as follows:

$$V_j = \sum_{i=1}^{o} v_{ij} \times A_i\,, \quad (4)$$

in which v_{ij} – an impact of the vulnerability V_j on the value asset A_i.

Let's define a set of threats as $T = \{T_1, \ldots, T_g\}$ and let's define a set of threat's characteristic including probability characteristics as $P = \{p_1, \ldots, p_g\}$, $h = 1, 2, \ldots, g$. Each threat is an aggregate of vulnerabilities, but also every vulnerability can have it's own influence on the implementation of the threat. Thus let's define the coefficient of potential vulnerability impact on the threat – *d*.

The technological process could be broken when the treat is realized. Thus, the failure of the system components may occur. The damage done in this case is an aggregate of all the vulnerabilities of a specific threat, taking into account the potential impact of each vulnerability [9]. The matrix of connections between vulnerabilities and threats can be determined as follows:

TABLE II. THE MATRIX OF CONNECTIONS BETWEEN VULNERABILITIES AND THREATS

	V_1	V_2	…	V_m
T_1	t_{11}	t_{12}	…	t_{1m}
T_2	t_{21}	t_{22}	…	t_{2m}
…	…	…	…	…
T_g	t_{g1}	t_{g2}	…	t_{gm}

Since under damage we mean the implementation of a threat, the assessment of the damage from a specific threat will be determined by the set of vulnerabilities that are associated with it:

$$T_h = \sum_{j=1}^{m} t_{hj} \times V_j = \sum_{j=1}^{m} \left(t_{hj} \times \sum_{i=1}^{n} v_{ij} \times A_j \right), \quad (5)$$

in which t_{hj} – an impact of vulnerability V_j on the threat T_h.

Let's define risk as the possibility that an unfavorable event will occur that has a consequence (damage) T_h with the probability p_h [10]. Further we mean that the risk depends on the implementation of the threat T_h. Thus, the overall assessment of the system's risk can be determined as a union of implementing all threats:

$$R = \sum_{i=1}^{g} R_i = \sum_{i=1}^{g} p_i \times T_i \, . \tag{6}$$

To fully assess the organization's damage, it is necessary to take into account not only the value of the risk depending on the implementation of threats, but also the possible damage from ignoring the legislative requirements concerning information security of automated control systems for technical processes and critical infrastructure protection. Since this damage is assessed not only quantitatively but also qualitatively, and the requirements are mandatory for the organizations operating the critical infrastructure, then the costs of implementing these requirements can be determined as the amount of the cost of meeting a specific requirement L_i:

$$L = \sum_{i=1}^{l} L_i \, . \tag{7}$$

It should be taken into account that if the amount of damage R_i from the implementation of the threat T_i is less than the cost L_i, it is advisable to use a compensating measure that will make the amount of costs less than the amount of damage. In the absence of such a compensating measure, it is necessary to justify the inapplicability of this requirement and to exclude it from the general set. After estimating the costs of implementing requirements and optimizing costs using compensating measures, and eliminating the not applicable, a new valuation of L is given.

A complex of such events, organizational and technical, is called measures to implement information security systems. Every measure will influence on the set of the treats. Let's compose the matrix of information security system's measures according to legislative requirements L.

TABLE III. THE MATRIX OF LEGISLATIVE REQUIREMENTS

	L_1	L_2	…	L_l
T_1	l_{11}	l_{12}	…	l_{1l}
T_2	l_{21}	l_{22}	…	l_{2l}
…	…	…	…	…
T_g	l_{g1}	l_{g2}	…	l_{gl}

According to the matrix of legislative requirements system's measures, the damage from the threat T_h can be defined as follows (on condition, that l measures were implemented):

$$T_h^{'} = \sum_{i=1}^{l} l_{hi} \times T_h \, , \tag{8}$$

in which l_{hi} – an impact of legislative requirements L_i on the threat T_h.

After implementing information security system, the probability of the threat T_h will be changed and will be defined as $p_h^{'}$. Thus, after implementing some measures from legislative requirements, an estimated value of risk will be changed $R_h^{'}$. Further it's necessary to develop some measures to protect automated system [11] based on the previously implemented measures taking into account the updated values from the threats $T_h^{'}$. Taking this into account the final matrix of information security system's measures will look as follows:

TABLE IV. THE MATRIX OF INFORMATION SECURITY SYSTEM'S MEASURES

	D_1	D_2	…	D_l
$T_1^{'}$	d_{11}	d_{12}	…	d_{1l}
$T_2^{'}$	d_{21}	d_{22}	…	d_{2l}
…	…	…	…	…
$T_g^{'}$	d_{g1}	d_{g2}	…	d_{gl}

According to the matrix of information security system's measures, the damage from the threat $T_h^{'}$ can be defined as follows (on condition, that l measures were implemented):

$$T_h^{''} = \sum_{i=1}^{l} d_{hi} \times T_h^{'} \, , \tag{9}$$

in which d_{hi} – an impact of information security system on the threat $T_h^{'}$.

The value of estimated risk $R_h^{''}$ is changed according to this.

To select a specific technology for modeling information security of automated control systems for technical processes, we will use the formalized structure of the components and interactions (1-3), a set of attributes for risks' assessment (4-9) and such criteria's as:

- the input data of the model should be simply defined (the model can use different data as input data, but the possibility of obtaining these data can be a task of varying complexity);
- the level of preparation and equipment of the intruder;
- the probability of different vulnerabilities; risks connected with this threatp; a possibility to estimate damage caused by the threat;
- the possibility to introduce heterogeneousness of components ad their interactions on different levels of automated control systems for technical processes;
- the possibility to introduce different legislative requirements according to existing laws;
- the possibility to estimate intrusion detection time according to existing information security system;

- it's important to estimate time from the beginning of the attack till it's preventing.

The analysis of criteria's above shows that the suitable mathematical model for information security of automated control systems for technical processes of a gas producing enterprise can be defined as follows:

$$M = \{C,S,A,T,V,P,D,R,L\}, \qquad (10)$$

in which C – a set of system's components;

S – a set of variable types of connections between components;

A – a set of value assets;

T – a set of threats;

$V_i = \{v_1, ..., v_h\}$ – a set of vulnerabilities for the threat T_i;

P – a set of threat's characteristic including probability characteristics;

D – a set of measures taken to reduce risks;

R – a set of estimated value of the risks;

L – a set of legislative requirements concerning automated control systems for technical processes.

III. Conclusion

Before implementing measures, it is important to calculate the cost of their implementation, based on the allocated budget for information security and the requirements of the law. If the cost of the activities exceeds the eligible costs, it is necessary to correct the risks: postpone the unlikely risks for the next cycle, and reduce the most dangerous risks within the current budget.

The process of risk management will occur until the value of the overall estimated risk (R) falls below the permissible level established in the organization and the cost of implementing such measures will not exceed allowable costs.

The proposed model (10) allows to perform analysis and assess the risks of information security. A decision for the need of introducing the information security system is made after establishing the permissible level of the overall estimated risk value. The process takes place until the estimated value of the risk takes a permissible level.

References

[1] Serdceva A.V. The evaluation of automated control systems for technical processes. UlGTU Newsletter. 2016, no. 3(75), pp. 58-61. (in Russian)

[2] Kirsanov S.V. The method for assessment of information security threats for APCS of the gas industry. Proceedings of Tomsk State University of Control Systems and Radioelectronics. 2013, no. 2(28), pp. 112-115. (in Russian)

[3] Krymsky V.G., Zhalbekov I.M., Imilbaev R.R., Yunusov A.R. Automation of technological process control in gas distribution networks: challenges, trends and perspectives. Electrical and data processing facilities and systems. 2013, no. 2, pp. 70-79. (in Russian)

[4] Baranova E.K. Methods of analysis and risk assessment Information security. Educational Resources and Technologies. 2015, no. 1(9), pp. 73-79. (in Russian)

[5] Churkin G.M., Velikanov A.M., Tyrin E.A. The problem of selecting automation for the automated process control system. Vestnik Saratov State Technical University. 2013, no. 1(70), pp. 151-158. (in Russian)

[6] Zakharov A.A., Rimsha A.S., Kharchenko A.M., Zulkarneev I.R. Analysis of information security of automated control systems for technical processes of a gas producing enterprise. UrFR Newsletter, Information Security. 2017, no. 3(25), pp. 24–33. (in Russian)

[7] Doukhvalov A.P. Cyber attacks on critical facilities - the probable cause of the accident. Cybersecurity issues. 2014, no. 3(4), pp. 50-53. (in Russian)

[8] Druzhinin E., Karpov I., Gnedin E., Boyko A., Simonova Y. Information security of automated control systems for technical processes in numbers. Moscow, Positive Technologies. 2016, pp. 1-9. (in Russian)

[9] Pishchik. B.N. Security of automated control systems for technological processes. Computational Technologies. 2013, no. 5, pp. 170-175. (in Russian)

[10] Baranova E.K., Maltseva A.N. Analysis of information security risks for small and medium businesses. Security Director. 2015, no. 9(69), pp. 58-63. (in Russian)

[11] Rimsha A.S. The problem of information security of automated control systems for technical processes of a gas producing enterprise. *Sbornik tezisov dokladov: Vtoraya Arkticheskaya sovmestnaya nauch.-prakt. konf.* [Proceedings of the Second Arctic joint scientific-practical conference]. Novy Urengoy. 2018, pp. 84-85. (in Russian)