IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Determination of the required degree of data protection in automated control systems

To cite this article: N V Davidyuk and V V Davidyuk 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **537** 052026

Determination of the required degree of data protection in automated control systems

N V Davidyuk[1] and V V Davidyuk[2]

[1] Department of Information Security, Astrakhan State Technical University, Tatishchev St. 16, Astrakhan, 414056, Russia
[2] Department of Technological Machines and Equipment, Astrakhan State Technical University, Tatishchev St. 16, Astrakhan, 414056, Russia

E-mail: davidyuknv@bk.ru

Abstract. The article considers the specifics of automated control systems for technological production and processes as objects of information security, proposed the approach to the decomposition of their components for further evaluation of the necessary degree of protection of the data they process. The method for obtaining the quantitative assessment of the grade of information resources security is presented. The proposed method allows taking into account the data value and the degree of criticality of violations of its integrity, accessibility and confidentiality for the functioning of the system. It can be used in practice at enterprises of various kinds of activity as an independent procedure, or as part of measures at the stages of preliminary analysis of automation systems before design or improving their data protection subsystems.

1. Introduction

The initial stage of measures for ensuring of information security of automation systems and, especially, automated control systems (ACSs) as their "central" component requires the preliminary analysis of these objects in order to identify and categorize the data to be protected and to further determine the degree of their security need to provide.

The solution of this task is critical for the whole object operation and underlies the follow-up measures for the design and implementation of a newly developed data protection system or improvement of one that is already in operation.

When analyzing the ACSs, the approach to the formation of information security requirements based on consideration and prioritization of its confidentiality (secrecy) (while the requirements for ensuring the information integrity and accessibility are among the general requirements for these data processing systems only indirectly) are not relevant. It is incorrect to assume that, in the case of limited access of a narrow circle of trusted proxies to the resources and components of the system, the probability of distortion, theft and destruction of data is insignificant.

Moreover, due to the specifics of automation systems and ACSs as protection objects, in practice, the priority of ensuring the properties of information security is reduced precisely to the reliability of data circulating in the system. Reliability of information in this context is closely correlated with the concept of integrity (accuracy, non-distortion) and accessibility.

Therefore, there is the task of forming the quantitative assessment of the degree of protection of ACSs information resources, which would be the reference value in estimation of the effectiveness of protective measures taken.

2. Approach to solving the problem

Let’s consider some ACS of any production or technological process as an protection object.

So, it is necessary to obtain the quantitative assessment P_o^{ACS} of the required degree of information resources protection within the framework of this ACS, taking into account the intermediate estimation of the grade of criticality of a violation of one or another information security property.

To solve this problem, the following method is proposed:

1. Preliminary analysis of the ACS and information resources (data) circulating in it, in order to obtain baseline data for assessment:

- the list of nodes and units *Zi* allocated in the ACS, i=1…s, s is the total number of ACS nodes;
- the list of data resources processed by the ACS (general and per-node).

2. Ranking of nodes and units of ACS by groups according to the value of the data processed by them.

3. Formation of the numerical assessment P_o^{ACS} of the protection degree for information resources of the ACS, taking into account their value and the degree of criticality of the data integrity, accessibility and confidentiality.

3. The method description

At the first stage, it is necessary to decompose the researching ACS into key nodes. The approximate list of nodes: workstations and terminals; information input / output devices, primary measurement information conversion and control; servers and network equipment; communication equipment, including communication lines; auxiliary devices that ensure the functioning of the ACS, including the main and backup power systems, ventilation, etc.

If necessary, the selected components of the ACS can be further elaborated. For example, group 2 can be refined by specific types of input / output devices, system sensors, types of their sensitive elements; group 3 - by the platforms on which the servers operate, etc.

The detailing of nodes for ACSs for technological production and processes should be carried out according to the hierarchical structure of the specific system. It is necessary to separate nodes of:

- lower (field) level (sensors, actuators, etc.);
- medium level (programmable logic controllers);
- top level (operator's terminal, servers, etc.).

The particularly important ACSs component is the information transmission channels, since the unauthorized impact on data is often associated with obtaining direct or contact access to them. The loss of data during transmission also depends on the reliability of these system components.

It should be borne in mind that not only data but also control commands are subject to transmission.

Often, the lower and middle levels of the ACS are combined by a “fieldbus”, which is a net-work with guaranteed packet delivery time, which allows creating the distributed control systems operating in real time. Applications at the top level of the ACS usually do not require work in the real time mode, therefore, workstations communicate via the Ethernet network, which allows the ACS to easily integrate with enterprise-level control systems by sending production data to the united enterprise databases [1].

Thus, the transmission channels differ from the rest of the selected ACSs nodes by a distributed property, which determines the specificity of ensuring the protection of information transmitted through them.

In order to take into account this specificity, the following way is proposed: on the basis of information about the geometric features of the protected object and the layout of ACS nodes on it, rep-resent the protected physical information channel by a set of linear sections, each of which is considered as the separate ACS unit. Thus, the provisions set forth below are also valid for the distributed units of the ACS [2-4].

At the next stage, there is the local task of distributing the identified information resources of the ACS, as well as the nodes involved in their processing, according to the degree of security importance depending on their value.

In practice, the value of any data is determined by the average value of potential damage in the event of an information security breach by a threat of a given type. The damage from the loss of information ultimately depends on its cost to the owner. The assessment of potential damage can be made using the risk analysis apparatus [5].

Let's distinguish the following types of data circulating within the framework of the ACSs:

- ACSs technological data - control commands, feedback signals, etc.;
- service information - is necessary for the functioning of the ACS and its protection system;
- other information - is processed, stored, transmitted in the ACS circuit and does not refer to the service or technological data.

One of the approaches to the classification of ACSs service and technological data is given in [6-7]:

- especially important data - irreplaceable information resources having high value and necessary for the ACS functioning;
- important data - information that can be replaced or restored in the event of loss, but the recovery process is time-consuming or is associated with large time or financial costs, also has a relatively high value;
- useful data - information that has an average level of value and is difficult to recover, but its theft, distortion will not be critical for the ACS functioning;
- non-essential data - information that does not represent special value for the effective ACS functioning.

Note that unauthorized modification or destruction of unclassified information (change of control commands, etc.) may entail serious consequences in the ACS functioning, therefore, considering the so-called, non-essential information resources is necessary while ensuring the security of the ACS.

Data processed by the ACS, but not related to the service, contains information of a secret or confidential nature, the list of which is defined in the relevant legislative acts.

For unification within the framework of the work, let's assume that on the basis of a preliminary assessment of potential damage from loss, modification, destruction, etc. the ACS information resources adopted their classification, similar to the service information of the ACS:

- especially important information;
- important information;
- information of medium importance;
- low importance information.

In order to rank the selected ACS nodes by the degree of importance of ensuring their safety, we introduce the value indicator Q_i^C of the data processed by the *i*-th ACS node. The assessment of this indicator is advisable to carry out informal methods with the assistance of an expert group. Further processing of the obtained expert information can be performed by any known methods [8].

Based on the list of ACS information resources and the given rating scale, experts should estimate the cost of the *j*-th information resource circulating in the system. In case of difficulties in obtaining a specific numerical assessment from an expert, it is possible to offer a certain value range and go to relative indicators:

$$C_j = \frac{C_j^{\min}\gamma_1 + C_j^{\max}\gamma_2}{(\gamma_1+\gamma_2)(C_j^{\min}+C_j^{\max})} \quad , \tag{1}$$

where γ_1 and γ_2 are empirical coefficients;

j = 1 ... m, m is the total number of information resources allocated to the ACS.

Then the indicator of the value of the *j*-th ACS information resource:

$$q_j^C = C_j / (\max_j C_j) \tag{2}$$

The indicator of the value of information resources for the specific *i*-th node ACS Z_i is defined as:

$$Q_i^C = \max_{j \in Z_i} q_j^C \quad , \tag{3}$$

where q_j^C - the value of the *j*-th ACS information resource.

As a result, the generalized matrix of indicators of the data value for all selected nodes *i* of the considered ACS is obtained:

$$Q^C \begin{array}{ccc} Z_1 & Z_i & Z_s \\ \end{array} \begin{pmatrix} Q_1^C & Q_i^C & Q_s^C \end{pmatrix} \tag{4}$$

The resulting matrix (4) allows to rank the nodes and units of the ACS according to the value of the data they process by groups: especially important, important, medium and low importance.

At the third stage, in order to assess the desired indicator P_o^{ACS} of the required degree of ACS data security, we introduce the concept of the criticality Q_i^K of the information resources of the *i*-th ACS node.

As already noted, in general, the information security of the ACS is provided by combination of such basic data characteristics being processed as confidentiality, integrity and accessibility [9], the indicator should take into account quantitative estimates of the degree of criticality of violations of each of these properties for each selected node and unit of the ACS.

As a result of the processing of expert information, we obtain the summary matrix of criticality estimates of such type:

$$\begin{array}{c|ccc} & Q_{conf}^K & Q_{acc}^K & Q_{in}^K \\ Z_1 & q_{cof}^1 & q_{acc}^1 & q_{in}^1 \\ Z_i & q_{conf}^i & q_{acc}^i & q_{in}^i \\ Z_s & q_{conf}^s & q_{acc}^s & q_{in}^s \end{array} , \tag{5}$$

where Z_i is the *i*-th node of the ACS; $q_{conf}^i = [0-1]$, $q_{acc}^i = [0-1]$, $q_{in}^i = [0-1]$ are the degree coefficients of violation of information security properties (confidentiality, accessibility and integrity, respectively) for Z_i, set on the range $[0-1]$ and obtained as a result of processing expert information based on a preliminary analysis of the ACS at the first stage of the method. At the same time, the degree of consistency of experts is evaluated by known methods, for example, confirmation of the statistical significance of the examination using the χ^2 distribution.

Due to the different importance of the ACS nodes by the information they process, the mechanisms for evaluating the indicators P_o^{ACS} for the selected groups of nodes will also differ.

For groups of important *Z_{im}* and especially important *Z_{eim}* nodes during the formation of indicators $P_o^{Z_{im}}$ and $P_o^{Z_{eim}}$, the multiplicative convolution of found indicators Q_{conf}^K, Q_{acc}^K, Q_{in}^K, should be used, since the contribution of each of them to the overall assessment is extremely critical:

$$P_o^{Z_{eim}} = \left(\prod_{i=1}^{s_{eim}} \frac{(q_{conf}^i + q_{acc}^i + q_{in}^i)}{3} \right)^{1/s_{eim}}, \tag{6}$$

$$P_o^{Z_{im}} = \left(\prod_{i=1}^{s_{im}} \left(\frac{(q_{conf}^i + q_{acc}^i + q_{in}^i)}{3} \right)^K \right)^{1/k}, \tag{7}$$

where s_{im}, s_{eim} - the number of ACS nodes in the groups of important and especially important, respectively;

k- is coefficient taking into account the degree of sensitivity of the overall assessment to the indicators of this group.

For estimating the indicators $P_o^{Z_{mim}}$ and $P_o^{Z_{\text{lim}}}$ for the ACS nodes, assigned to the groups of the medium Z_{mim} and low importance Z_{lim}, the additive convolution of the estimates is used:

$$P_o^{Z_{mim}} = \left(\frac{\sum_{i=1}^{s_{mim}} \left(\frac{(q_{conf}^i + q_{acc}^i + q_{in}^i)}{3} \right)^2}{s_{mim}} \right)^{1/2}, \tag{8}$$

$$P_o^{Z_{\text{lim}}} = \frac{\sum_{i=1}^{s_{\text{lim}}} \frac{(q_{conf}^i + q_{acc}^i + q_{in}^i)}{3}}{s_{\text{lim}}} \tag{9}$$

Then the generalized indicator P_o^{ACS} of the protection degree for ACS information resources, taking into account the weights W_{eim}, W_{im}, W_{mim}, W_{lim} of each group of indicators, is defined as:

$$P_o^{ACS} = W_{eim} P_o^{Z_{eim}} + W_{im} P_o^{Z_{im}} + W_{mim} P_o^{Z_{mim}} + W_{\text{lim}} P_o^{Z_{\text{lim}}}, \tag{10}$$

where $\sum_i W_i = 1$.

4. Conclusion

The paper deals with the features of ACSs as objects of data protection, suggests the approach to isolating its components as part of analyzing and assessing the protection grade that must be ensured for high-quality and efficient system operation.

The result of applying the described method is obtaining of quantitative indicators of the protection degree for especially important $P_o^{Z_{eim}}$, important $P_o^{Z_{im}}$, medium $P_o^{Z_{mim}}$ and low important $P_o^{Z_{\text{lim}}}$ ACSs nodes (equations (6) - (9)), taking into account the value and criticality of the integrity, accessibility and confidentiality of the data they process. On the basis of these indicators, a generalized indicator P_o^{ACS} (10) of the required degree of ACS information resources protection was obtained.

References

[1] Lunev R A 2008 Struct and composition of information systems in the automation of technological processes and productions *Journal of Orel state technical university. Series: information systems and technologies* **4-3** 56-9

[2] Davidyuk N V, Kosmacheva I M and Sibikina I V 2012 The procedure for assessing the indicators of the detectability of a security system for informatization objects *Information and Security* **4** 537-42

[3] Dakhnovich A D, Moskvin D A and Zegzhda D P 2018 Analysis of the Information Security Threats in the Digital Production Networks *Automatic control and computer sciences* **52** 1071-5

[4] Davidyuk N, Vybornova O and Gostyunin Y 2018 Improving reliability of electric power systems based on application of risk assessment model *IEEE Xplore Digital Library*

[5] Balanovskaya A N and Volkodayeva A V 2017 Information security of critically important objects in automatic technological process control systems *Bulletin of Samara municipal institute of management* **1** 74-81

[6] Voloshin B V and Zhukov V G 2015 Concerning creation of information security management system for automated system *Current problems of aviation and cosmonautics* **1** 485-7

[7] Tsirlov V L 2008 *Fundamentals of information security of automated* systems (Moscow: Phoenix)

[8] Popov G A, Popov A G, Shishkin N D and Rudenco M F 2017 The conceptual scheme of information security in the object protection model *Bulletin of Astrakhan state technical university. Series: managment, computer technology and informatics* **4** 45-53

[9] Egorov A V, Grishchenko A S and Laushkin D V 2016 Expert estimates of quality of automated systems of information processing and management *Science and world* **1** 51-3