Problems of collaborative work of the automated process control system (APCS) and the its information security and solutions.

E K Arakelyan, A V Andryushin, S V Mezin, A A Kosoy, Ya V Kalinina and I S Khokhlov.

National Research University "Moscow Power Engineering Institute"
Russia, 111250 Moscow, Krasnokazarmennaya, 14

Abstract. The principle of interaction of the specified systems of technological protections by the Automated process control system (APCS) and information safety in case of incorrect execution of the algorithm of technological protection is offered. - checking the correctness of the operation of technological protection in each specific situation using the functional relationship between the monitored parameters. The methodology for assessing the economic feasibility of developing and implementing an information security system.

1. Introduction.
Currently, information security problem of automated process control system (APCS) becomes more and more important and urgent. With the introduction of unauthorized access and interference with the operation of the Automated process control system (APCS) of third party, management acutely raises the question of the proper protection of Automated process control system (APCS) and information systems. Now are only the first steps in this direction, so inevitable some difficulties when trying to solve this problem: the lack of experience of execution of similar projects, limited normative and methodological framework, the difficulties of practical implementation and deployment. Despite certain steps taken by various organizations to create effective information security systems, many problems have not yet found its practical solution. One of these is the interaction between the two systems, information security and the existing Automated process control system (APCS) of technological process control systems and management.

Third-party intervention (for example, a virus attack) in the operation of large energy facilities, as a rule, has as its ultimate goal the violation of the technological process, which entails the disruption of both individual units in particular and the entire power unit as a whole [1–4]. To prevent the development of emergency protection technology used in Automated process control system (APCS). As one of the tasks of information security system proposed verification process to protect the reliability of action in any given situation with the use of a functional relationship between controllable parameters.

2. The proposed approach is collaborative Automated process control system (APCS) and information security
Automated process control system (APCS) of large facilities, including power plants, until recently remained to a certain extent-closed system. Access to the remote control had only authorized personnel, and control algorithms have been built in the non-programmable or programmable logic. The Automated process control system (APCS) was completely isolated from the non-operative control loop and the Internet network. With the advent of programmable controllers and the TCP/IP protocol stack, Automated process control system (APCS) became more functional, flexible, easy to manage and efficient. Control of the latest generation system integrated with non-operative control loop networks, enterprise networks and the Internet, faced with the problems of providing protection against intentional and unintentional dangerous actions aimed at the destruction of control systems, control and interception of control, etc. In this case, the solution of problems of information security Automated process control system (APCS) general its architecture can be divided into two parts - the part to which may be applicable standard approaches and solutions to ensure information security (mostly upper and partly middle levels of management), as well as part of the requiring individual approach - the lower and middle levels of Automated process control system (APCS).

It is obvious that the external intervention (e.g., virus attacks) to the work of the large energy facilities often has as its ultimate goal of creating an emergency situation that entails disabling both the individual units in particular, and the entire unit as a whole (and possibly and the entire station by malicious intruder’s impact on the general station equipment). To prevent the development of emergencies using technological protection. In the case of an incorrect execution of the technological protection algorithm, either its false triggering or non-triggering is possible.

In both cases, there are financial and economic losses, and in order to ensure a proper level of information security and at the same time meet the requirements of the order, the Federal Service for Technical and Export Control (FSTEC of Russia) No.31 proposes to divide the information processed in the Software-Technical complex, for each considered object into three categories in accordance with the object's security class and the level of importance (criticality) of the information [5,6]:

1. Information, requiring ongoing monitoring (protection) in the pace of technological process, which can be attributed to the parameters of the technological processes involved in the functions of the Automated process control system (APCS) of technological protections, the violation of which leads to an emergency shutdown of individual generating unit and as possible development of the emergency stations as a whole. This information is transmitted from the process control system in its entirety in the information security system, which runs continuously, in parallel with the control system online. When an emergency stop signal appears, the information security system must determine the nature of the threat—indeed a technological one or a consequence of unauthorized exposure.

2. Information requiring periodic control (protection) when required, which can be attributed to the process parameters involved in the control system of technological protection function, the violation of which leads to an emergency stop or emergency stop or unloading of individual units. In this case, the information security system is in standby in readiness and is connected to an information process control system only at the time the risk of the emergency stops.

3. Information that is not involved in technological protections due to complete absence or possibility of impact on it, or the absence of a risk of emergence of critical situations when it deviates from normal values. In this case, the priority of the work rests with the Automated process control system (APCS) and information security system is the operator of the need to confirm the correctness of his decision.

Information security work when validating technological protection action in each situation involves the use of a functional relationship between the controlled parameter and one or more other measured parameters.

3. Methods of assessing the cost-effectiveness of the proposed approach
Feasibility of developing and implementing protection and Automated process control system (APCS) information depends on two factors: the expected damage in the absence of information security and the necessary cost of funds for the development, commissioning and operation of such a system. Possible damage is a decrease in the marginal profit of electricity generating companies from the under-supply of electricity, because of the disruption of the process (reduction of power plants, emergency shutdowns of power units and equipment, etc.); damage from not provided capacity to the market; material and financial costs of restoration and ensuring the integrity of information, etc.

A set of threats present in the form of four blocks [2]:

1. Organizational (disclosure of information, unauthorized access to documents and resources of a critical facility (CF), blocking of authorized access, unauthorized actions to disrupt the normal mode of operation of a critical (CF), etc.);
2. Physical (negative natural and technical phenomena, failures, non-fatal accidents, false operation of technological protections and processes, targeted physical impact on the elements of critical facility (CF), the side electromagnetic radiation and crosstalk, the introduction of specific means of information reading, repeaters and eavesdropping, etc.);
3. Program-mathematical (implementation of software bookmarks and declared features in software for data retrieval or violating the normal functioning of the system, the introduction of malware and different viruses, etc.);
4. Information (violation of technology of removal, collection and processing of information and its transfer to the level of control, unauthorized access to information resources, manipulation and information theft, unauthorized exposure to the management system via the network system resources, or nodes, wireless communication, etc.).

Possible annual damage caused by incorrect operation of technological protections in the absence of process control in power system protection can be represented as:

\[
Y_r = Y_r\left(\mu \Delta \mathcal{E}_r\right) + S_N + S_F
\]

where \(\Delta \mathcal{E}_r\) is the mathematical expectation of damage from undersupply of electricity, as a result of violation of technological process (decrease in capacity of power plants, emergency shutdown of power units and equipment, etc.); emergency shutdowns of power units and equipment, etc.); \(S_N\) is damage from power is not supplied to the market; \(S_F\) is material and financial costs of restoration and ensuring the integrity of information.

The mathematical expectation of the annual damage from the under-supply of electricity is presented as:

\[
Y_r\left(\mu \Delta \mathcal{E}_r\right) = (C_\mathcal{E} - C_\mathcal{F}b_{C_{\mathcal{F}}}b) \mathcal{C}_r \sum_{i=1}^{4} (\mu \Delta q_i)
\]

where \(C_\mathcal{E}\) is total annual power generation at power plants, megawatt hour, \(\mu \Delta q_i\) is the mathematical expectation of an increase in underproduction of electricity according to the \(i\) block of possible damage \((i = 1, 2, 4)\); are calculated either on the basis of statistical analysis, or evaluated by expert experts; \(C_\mathcal{F}\) is the price of electricity in the electricity and capacity market, (\$/MWh); \(C_\mathcal{F}\) is conditional fuel price (Thousand rubles) \$/t; \(b_{C_{\mathcal{F}}}\) is the average specific consumption of equivalent fuel for electricity generation (CFS t./MWh).

Damage from power is not supplied to the market in the form (calculated monthly):

\[
S_N = \sum_{j=12}^{12} N_{\mathcal{M}_j} C_N \sum_{i=1}^{4} \mu \Delta q_i
\]
where $N_{M_{j,p}}$ is the average power provided by the power plant in the j-th month on electricity and capacity market.

Material and financial costs for the restoration and integrity of information depend on the specific conditions, and according to expert estimates, amount to 15% of the annual damages from lost electricity and unrepresented power.

Taking into account the above dependencies, the expression (1) will be presented in the form:

$$Y_F = 1.15 \left( C_5 - C_T b_{CPJ} \Delta F_T + C_T \sum_{j=1}^{12} N_{M_{j,p}} \right) \sum_{i=1}^{4} \left( \mu \Delta q_i \right).$$

(4)

The annual economic effect from the introduction of the system of protection of automated process control systems and information security in power plants is represented as:

$$S_F = \alpha Y_F$$

(5)

where $\alpha$ is the share threat prevention

The above methodology for assessing damage can also be used to assess the appropriateness of applying individual measures to protect information.

Reference

[1] Khaibulatov Rustam / Information Security of Automated process control system (APCS) for Energy Companies // Information Security .- №4, 2015;
[2] A. Lukatsky. Critical infrastructure safety and security: the international experience. [Information resource]: http://www.slideshare.net/lukatsky/ ss26553193
[3] Problems of information security of process control systems and control systems for critical objects. V.A. Artamonov / Proceedings of the Conference "Information Security of the APCS CF", 2016, p. 26-35.
[4] Information technology – Security techniques – Methodology for IT Security Evaluation – ISO/IEC 18045:2008.
[5] Arakelyan E.K. Information security automation systems: current status, problems and difficulties of its implementation // Arakelyan E.K., Kalinina Ya.V., Kosoy A.A., Khokhlov I.S. // New in the Russian Electric Power Industry 2017 №3
[6] Arakelyan, E. K. the Problem of information security of thermal power Plant (TPP) and Nuclear power plants (NPP) and possible ways of their solution // E. K. Arakelyan, A. V. Andryushin, A. S. Minnow, Sergey V. Mezin // New in Russian power 2015. No. 5.