Organization of Secure Communication between Programmable Logic Controllers Using the Open Platform Communications Protocol

F R Ametov¹, E A Bekirov¹ and M M Asanov¹

¹Electrical Energy and Electrical Engineering Department, V.I. Vernadsky Crimean Federal University, Academician Vernadsky Ave., 4, Simferopol, 295007, Russia

E-mail: ametov.ferat@gmail.com, bekirov.e.a@cfuv.ru, asanov.m.m@cfuv.ru

Abstract. Modern automated control systems in industrial and private enterprises are represented by a set of programmable logic devices and components from various manufacturers. They operate based on many of the most widely used protocols and interfaces. Some manufacturers have their own solutions that are mainly focused only on their product, without direct or indirect compatibility with third-party solutions. Many control systems used now operate on relatively old solutions that cannot be partially modernized due to lack of technical resources or financial unprofitability.

The paper considers the most popular industrial protocols Modbus and Profibus, analyzes their advantages, as well as features of the structure and functionality.

The study of the operation problems and information security of modern control systems is considered, solutions for their elimination are analyzed.

A solution for the control systems modernization was proposed based on the analysis. It can become effective and financially justified due to its technical features, allowing it to be adapted to existing solutions. Conclusions about the effectiveness of the proposed solution were formulated based on the data collected and the goals achieved.

1. Introduction

The principles of communication between devices within industrial networks, as well as the features of the information transfer over them, are defined in standardized specifications. Specifications are a set of protocols that are implemented by the system components.

A number of the specifications used have limitations related to multiplatform, security and modernization, that leads to problems with network configuration, its support, upgrades and security.

Thus, many automated control systems (ACS) of the components of energy, agro-industrial, agricultural and other complexes operating now are an integrated distributed computing system that was developed primarily to provide functional technological advantages and ease of use [1].

The architecture of such systems is a collection of components, systems and algorithms that work using open protocols, the main functionality of which is limited only to data processing and transmission.

The openness of these protocols is expressed in their accessibility from the outside. In other words, such interfaces do not have mechanisms for restricting access to data, their encryption and encapsulation.
As a result, communication over such open, but at the same time widespread, protocols is insecure and potentially vulnerable to cyber-attacks.

2. Actuality
The modern infrastructure of many business and economy sectors is closely related to the use of automated control systems, many of which have been in operation for quite a long time. Even the slightest errors and interruptions in these systems operation can entail large and unpleasant consequences.

These systems are based on components and interfaces from different manufacturers, and operate, perhaps, under different protocols and specifications. For a long time automated control systems were based on specifications, most of which rely on technologies that imply access to information, its recording, reading and processing, but are not designed to ensure its information security [2].

2.1. Scientific significance of the topic
Recently, the number of threats and cyber-attacks aimed specifically at energy and agro-industrial complexes has sharply increased. The probable cause and consequence of such attacks is the use of control systems or data transmission and processing protocols that have low or no information security requirements.

It became possible to provide remote access to the system with the development of information networks and program-logical controllers. However, the security requirements at the time of implementation and development were minimal because information security was not as relevant as it is now.

In this regard, an urgent task is the design and development of stable protocols, algorithms and devices for automated control systems components communication.

At the same time, it is worth noting that the solutions being developed should be able to be effectively implemented in both modern and long-standing systems, must have support for connecting to systems based on various components and interfaces, and be able to combine them into a single whole.

2.2. Brief overview of literature sources
The Kaspersky ICS CERT laboratory provides in their article [3] a detailed analysis of vulnerabilities and cyber threats for industrial enterprises. Specialist Evgeny Goncharov states that a special place among the majority of cyber threats is occupied by cyber espionage for various purposes, which becomes available due to the ineffective security system of control systems and problems with the delimitation of the access level to certain data and functions.

Another work [4], devoted to the issues of a unified communication solution in industrial controllers, includes a description of the Modbus network interaction with an open platform communications (OPC) UA server in an intelligent monitoring system for air conditioning equipment. The authors of the article Nguyen Thi, Thanh Tu and Huynh Quyet Thang review generally accepted standards and specifications and propose their own monitoring solutions based on the concatenation of Modbus and OPC, including for implementation in existing industrial networks.

However, the authors did not consider the subject of compliance with modern information security standards, which is key in the developed system. The critical data availability, its safety and confidentiality is an integral part of any control system.

3. Problem statement
The main requirement for the proposed solution is also financial and productive feasibility and efficiency, which follows from the massiveness of its possible application.

The aim of the study is to develop a modernized, safe and efficient process of interaction and communication between the control system components at electric power enterprises, as well as agro-industrial and agricultural complexes.

To achieve the goal, the following tasks have been set:
• Analyze the problems of existing approaches to the automated control systems design.
• Analyze the most widely used communication protocols of system components, identify their features and vulnerabilities.
• Analyze and propose a solution for the modernization of existing solutions for the components interaction.
• Build functional and structural diagrams of the proposed solution.
• Implement own solutions to ensure secure communication of control system components

4. Theoretical part
Following from the results of the problem analysis, it can be concluded that the generally accepted standards for the control systems design are gradually being modernized, acquiring a more unitary form. Expanding the standard specifications capabilities by using new, universal mechanisms, it becomes possible to use the data collected and processed by the control system components more efficiently. Using an OPC server for processing and storing data it is possible to organize multiple communication with various components, services and protocols for more efficient and informative processing.

However, the communication and information processing system is a critical component and the highest security requirements are imposed on it. As the analysis shows, most of the new approaches application examples, including OPC servers, do not include information security issues. A unitary solution is used for data collection and processing, modeling, forecasting and control, as well as for many other capabilities, access to which is often strictly confidential. The ability to remotely connect to the system, view and edit data are potential threats to the system, which can lead to serious consequences.

In this regard, there is an acute issue of organizing information security when implementing such a technical solution [5].

Currently, communication protocols and interfaces for data transmission and processing, such as Modbus, Profibus, Ethernet, CAN and others, are used for the industrial control networks organization. Many of them are based on the master-slave (M-S) architectural model, which involves communication between components in the form of polling and responding to software devices. The protocol also regulates the polling format, response format and functional features of data transmission between system devices [6].

From the results of the existing principles of switching the devices within the ACS analysis follows that the main existing solutions, which are widely used everywhere, have a number of their own functional and structural features and limitations.

Well-established multifunctional solutions without proper improvement are exposed to threats due to their peculiarities and ineffective solutions in the information security field. Improving such systems and protocols, in some cases, is not financially feasible, since the scale of their use entails significant financial costs for the modernization of such systems or their complete or partial replacement.

| Protocol     | Percentage of use |
|--------------|-------------------|
| Profinet     | 17%               |
| Modbus       | 10%               |
| EtherCAT     | 7%                |
| Profibus     | 8%                |
| EtherNet/IP  | 17%               |
| POWERLINK    | 4%                |
| Other        | 37%               |
The HMS industrial company report shows that the share of the systems based on Modbus is about 10% of all applied solutions [7]. The same analysis confirms the use of Profibus (Profinet) in 17% of cases, which confirms the massive use of these communication protocols.

Despite the partial structural identity of Modbus and Profibus, the concatenation of these interfaces into a single control system is not directly possible.

Within the framework of a scientific study on the information security organization in Modbus TCP interfaces between master and slave devices, a solution to improve and modernize algorithms for checking trust and encrypting messages is proposed in order to increase the efficiency of electric power enterprises communication systems information security [8].

The possibility of implementing a universal communication component, which is functionally able to satisfy simultaneously the set of the most commonly used communication protocols, implies the creation of a separate autonomous gateway in the program-logical device form. This approach will allow implementing this solution in the existing networks infrastructure effectively and with the lowest financial and technological costs.

Let's consider the functional similarity of Modbus and Profibus protocols. They have a common commutation principle - master-slave, which means that it is possible to introduce additional masters into such networks. This approach allows achieving the desired autonomy and versatility [9].

5. Practical relevance
The developed master-component (APLC - Autonomous program-logic controller) must meet the requirements for building an automated control system and have an external access setting, for example, from SCADA.

This module is designed to combine both master-slave devices and master-master, taking into account that the two master-components are capable to operate on different data transfer protocols. One of the most versatile solutions is the design of an APLC in the OPC UA server form.

![Figure 1. Schematic diagram of the algorithm operation.](image)

The schematic diagram (Figure 1) of the solution describes the minimum set of components and the ways of interconnection between them. In our case, there is an example of four modules that attempt to communicate in pairs. In the case of # Module1 - # Module2, according to the scenario, the exchange of session and keys is successful. In the case of # Module3 - # Module4, the connection is broken, initiated by one of the possible errors (including an attempt to connect untrusted persons).

The same sequence can be described more sequentially by presenting it graphically in the form of a sequential diagram (Figure 2).
Figure 2. A graph describing the process of connecting to a control device, taking into account the implementation of the developed algorithm.

The efficiency of the developed scheme can be expressed in terms of asymptotic complexity, since the circuit is an algorithm for the connected components operation. The main indicators affecting efficiency are execution time and data volume since the current principle is aimed at establishing communication and receiving / processing data.

One method is to find complexity in the worst case \( t(n) \):

\[
\max \left\{ t(R_1, \ldots, R_m) \sum_{i=1}^{m} \log_2 \left( |R_i| + 1 \right) \leq n \right\}
\]  
(1)

Suppose that \( t(n) \) is the program execution time that the algorithm can guarantee for a known total amount of data not exceeding \( n \).

In addition, each algorithm has optimal efficiency, i.e. these are the optimal indicators of time and resource costs for execution, and the actual efficiency, depending on the input factors, among which we can distinguish - the executing resources and the amount of data.

To determine, an approximate algorithm will be used:

\[
\frac{T^A}{T^*} \leq \frac{T_{\min}^A + t_{\max}}{T^*} \leq \frac{T^* + t_{\max}}{T^*} = 1 + \frac{t_{\max}}{T^*} = 2
\]
(2)

where \( T^* \) is the optimal running time of the algorithm; \( T^A \) is the running time of an arbitrary heuristic; \( T_{\min}^A \) is the sum of the running time on the least productive resources.

It follows from the ratio that the algorithm actual execution time at any resource capacity and a predetermined amount of data will not exceed the optimal operation time by more than 2 times.

6. Conclusions
The architectural and structural component of industrial control systems was considered during the study. The issue problematics related to their modernization is analyzed. Issues related to the use of
established and modern protocols for data transmission and processing, namely, the problems of their modification and compatibility, are considered.

The research analysis in the field of modern protocols application, as well as their design, development and modernization was carried out. The analysis is based on general issues of protocols communication problems and software components interfaces.

As a result of the analysis, it was concluded that at the moment there is a problem of information security support while ensuring communication between various components and protocols.

A review of past studies on this topic was carried out, their general conclusions were presented, and based on the problems analysis, the application of these results was proposed to solve the current problem.

The program-logic controller structure (PLC) and its main software component are considered, various parameters examples are given.

Based on the information collected during the analysis, as well as using the results of past research, a PLC program was built that implements an algorithm for ensuring secure communication between system various components. The program components structure is presented, the interaction process is described, built based on the functional and structural diagrams of the implemented algorithm.

The proposed program is built based on an OPC UA server, which makes it possible to apply the proposed solution to components with different protocols types.

7. References
[1] Ametov F R and Bekirov E A 2020 Formalization of secure communication of SCADA components according to the OPC specification (Moscow: Moscow State University of Technology Press)
[2] Niv G and Avishai W Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems Electronic materials vol 6 (Tel Aviv: School of Electrical Engineering) p 63
[3] Goncharov E 2021 Cyber attacks for industrial enterprises in 2021 Kaspersky ICS CERT
[4] Nguyen Thi Thanh Tu and Huynh Quyet Thang 2013 Design and Development of the Air Conditioning System by Using OPC UA Specifications and Modbus Protocol (Hanoi: ICIEA)
[5] Claudiu-Ionel N and Duta M 2018 SCADA Systems Architecture Based on OPC and Web Servers and Integration of Applications for Industrial Process Control (Craiova: International Journal of Control Science and Engineering)
[6] Manoj Manjunath R and Janaki Raman S 2011 Fuzzy Adaptive PID for Flow Control System based on OPC (Hebei: NCCSE)
[7] Hansson A 2020 Industrial network market shares 2020 according to HMS Networks HMS Industrial Networks
[8] Ametov F R, Bekirov E A, Asanov M M 2020 Organizing the information security in Modbus TCP interfaces for use in the energy complex (Belgorod: ICES 2020)
[9] Tovar E and Vasques F 2000 Real-time fieldbus communications using Profibus networks (Porto)