UDC 004.738.5:681.518
DOI: 10.15587/1729-4061.2025.348728

EXTENDING THE FUNCTIONALITY OF TOPOLOGIES OF WEB-ORIENTED CONTROL SYSTEMS FOR TECHNOLOGICAL OBJECTS BASED ON "OPEN USER COMMUNICATION"

Leonid Zamikhovskyi
Corresponding author
Doctor of Technical Sciences,
Professor, Head of Department*
E-mail: leozam@ukr.net
Mykola Nykolaychuk
PhD, Associate Professor*
Ivan Levytskyi
PhD, Associate Professor*
*Department of Information and
Telecommunication Technology and Systems
Ivano-Frankivsk National Technical
University of Oil and Gas
Karpatska str., 15, Ivano-Frankivsk, Ukraine, 76019

This study focuses on the information processes involved in the interaction between components of WEB-oriented control systems based on the "Open User Communication" (OUC) technology. The task addressed related to the violation of data consistency across different topology levels in process control systems during cyclic server requests, the need for batch transmission of heterogeneous data types, the unification of equipment, and the technical validation of solutions.

A system topology has been designed using a SCADA (Supervisory Control and Data Acquisition) system, a server PLC (Programmable Logic Controller), and four terminal PLCs with integrated OUC in the "TIA Portal" environment. This topology allows for data consistency between the server and terminal PLCs by transmitting heterogeneous data formats within a single frame using dynamic data-slice selection.

Hardware tools and application software were developed in the Function Block Diagram (FBD) language of the IEC 61131-3 standard to implement "Open User Communication" with transmission capacities of up to 8192 bytes per frame.

To study information processes, a simulation model of interaction between the server and terminal PLCs based on OUC was built and tested using virtual PLC simulators with dynamic data-slice adjustment. The transmission of 12 different data formats (a total of 332 bytes) was tested using the "TSEND_C" and "TRCV_C" instructions under a "monitoring-on" mode.

GRE tunneling protocol parameters were configured to enable simultaneous data exchange between the server and terminal PLCs via "Open User Communication", alongside PLC programming via "S7-Communication".

Based on the proposed solutions, a WEB-oriented data acquisition system for technological facilities of municipal water-supply enterprises was developed and validated under industrial conditions

Keywords: Open User Communication, OUC topology, SCADA, PLC Simatic-S7, OUC simulation model

Received 01.10.2025
Received in revised form 11.12.2025
Accepted 19.12.2025
Published 30.12.2025

***How to Cite:** Zamikhovskyi, L., Nykolaychuk, M., Levitskyi, I. (2025) Extending the functionality of topologies of Web-oriented control systems for technological objects based on "Open User Communication". Eastern-European Journal of Enterprise Technologies, 6 (2 (138)), 94–115. https://doi.org/10.15587/1729-4061.2025.348728*

1. Introduction

Developing automated control systems for technological objects (TO ACS) based on modern hardware and software tools and information technologies implies comprehensive solutions to the problems of design, modeling, implementation, testing, and support for such systems.

The Open User Communication (OUC) technology provides open, standardized, and unified access to information resources and services of control systems based on WEB technologies. This makes it possible to design TO ACS with a diverse topology – from centralized to distributed, cloud and hybrid [1].

The components of WEB-oriented TO ACS are standard and intelligent sensors and actuators, PLC (Programable Logic Controller), SCADA (Supervisory Control and Data Acquisition), operator HMI (Human Machine Interface), industrial communications (Industrial NET) and IT systems [2, 3].

Organizing a reliable and effective communication environment when implementing TO ACS is an integral task, especially when building territorially distributed control systems for technological facilities.

In addition, modern technological facilities and production systems are characterized by increasing complexity, a high degree of automation, and often special operating conditions. This leads to the formation of increased requirements for technological facility control systems, in particular in terms of functionality, optimization of communication traffic, and unification of hardware and software. In response to such requirements, WEB-oriented maintenance control systems are gaining significant popularity, which provide control and management of technological processes based on a multi-level network infrastructure with heterogeneous segments. However, existing approaches to building such systems are often limited by the functionality of topologies and insufficient flexibility in terms of coordination of hardware and software and the communication environment. The direction of expanding the functional capabilities of maintenance control system topologies in order to increase their efficiency, productivity, adaptability, consistency, and data security, which are key factors in building modern maintenance control systems, is particularly relevant.

In the context of ensuring the above requirements, the integration of the Open User Communication technology in the TO ACS topology for the implementation of standardized, unified, and open mechanisms of interaction between TO ACS components determines the relevance of research in this area. At the same time, the use of OUC in topologies of WEB-oriented TO ACS requires deeper theoretical and practical research to develop models, algorithms, and topologies that allow for the most effective realization of OUC potential.

In addition, special attention and appropriate solutions require approaches, methods, and means of building TO ACS for critical infrastructure (electric power, oil and gas facilities, water supply, etc.). In this regard, it is important that such systems function under conditions of power supply interruptions, communication traffic restrictions, as well as are unified and, accordingly, maintainable.

Thus, research aimed at expanding the functionality of topologies of WEB-oriented TO ACS based on "Open User Communication" is relevant and should improve the level of efficiency of such systems as a whole.

2. Literature review and problem statement

Paper [4] reports the results of research related to a new industrial direction – the combination of Industrial Internet of Things (IIoT) technologies with artificial intelligence, which gives rise to the concept of "Artificial Intelligence of Things" (AIoT). A systematic review of the main reference architectures intended for industrial AIoT applications was performed, their key characteristics, goals, advantages were analyzed, and examples of practical application were given. It was shown that existing architectures are a necessary tool for standardizing AIoT solutions, but their implementation in industry is still limited, and the need for further research for the practical implementation of such architectures was emphasized. The research methodology involves identifying several key factors for developing AIoT applications for the industrial environment (types, requirements, and needs of AIoT applications, goals of "Industry 4.0"). The cited paper is a review; therefore, special attention is required to the practical tasks of designing, modeling, developing, and operating TO ACS. This gives grounds to argue that it is advisable to conduct research related to the integration of modern information technologies into the reference architecture of IIoT and AIoT at the level of topologies, algorithms, models, and unified hardware and software.

Work [5] reports the results of research on increasing the resistance of the Simatic S7-1500 PLC to cyberattacks that can be applied by "offline injection" of malicious code, without direct interaction with the PLC network interfaces. It is indicated that the possibility of modifying the "TIA-Portal" project in such a way that malicious changes remain unnoticed by the operator until the project is loaded into the PLC. One of the main results of the work is the demonstration that even modern PLCs, which include advanced authentication and protection mechanisms, can be manipulated at the level of the design environment and the internal structure of the code. It is noted that the "offline injection" of malicious code bypasses most network monitoring tools, since the cyberattack is disguised as a regular engineering operation. For a real cyberattack scenario, an approach was implemented on the "Fischertechnik" training system based on the Simatic S7-1500 PLC using the latest version of the "S7CommPlus" protocol. The work can be especially valuable for researchers of Industrial Control Systems (ICS) components and emphasizes the relevance of increasing the protection of project files, control of the development environment and project procedures. Despite its relevance and volume, the cited work does not solve the task of increasing the level of cybersecurity of industrial communications based on the "Open User Communication" technology. The ways to solve the relevant problems can be the use of encrypting SSL certificates and the use of the "protocol tunneling" technology of communication by encapsulating them during data exchange between the components of the TO ACS. This gives reason to argue that it is advisable to conduct research related to the implementation of additional effective methods and means of protecting industrial communications from unauthorized access.

In [6], a broad overview of Networked Control Systems (NCSs) in which sensors, controllers, and actuators exchange data via communication networks is given. The evolution of NCSs is divided into three phases (before 2000, during 2001–2010, and since 2011). The paper considers the main problems of the functioning of such systems – communication delay, packet loss, synchronization and security, and also identifies promising directions for the development of NCSs taking into account current trends in the field of IIoT. The paper discusses some important practical applications that have been implemented using NCSs and identifies the main directions of future research on NCSs. However, from the standpoint of industrial communications, the paper does not solve the problem of organizing real network topologies, including those based on deterministic data transmission technology – Time-Sensitive Networking (TSN). The generalized reason for unsolved problems in the field of NCSs may be the lack of complexity of the approach based on the concept of "Control-Communication Co-design", which is a modern trend in the design and creation of maintenance automation systems. The approach to the implementation of "Control-Communication Co-design" may be the use of modern integrated environments for the design of maintenance automation systems – from the organization of topologies, communication environment, and hardware, to application software and simulation modeling. This gives grounds to argue that it is advisable to conduct research related to the integration of industrial communications into network topologies of maintenance automation systems and testing the operating modes of maintenance automation systems based on simulation modeling methods and tools.

In work [7], SCADA architectures are considered and a comparative analysis of communication protocols and modern methods and tools of cybersecurity is performed. It is shown that modern SCADA has evolved from autonomous systems to complex, integrated open systems based on the latest information WEB-oriented technologies. The paper highlights critical research problems that need to be solved to improve the security of SCADA and industrial communications – a key component in the management of critical infrastructure (electric power, oil and gas and chemical industries, water supply facilities, etc.). The paper considers the basic architecture of SCADA systems, including the HMI (Human Machine Interface), MTU (Maximum Transmission Unit), RTU (Remote Terminal Unit) levels and communication channels. Considerable attention is paid to the classification of cyberattacks, the description of historical incidents and the analysis of weaknesses in the SCADA infrastructure. The emphasis is on common causes of vulnerabilities – the use of open network protocols, the lack of encryption, insufficient access separation and the interaction between the OT (Operational Technology) and IT (Information Technology) environments. At the same time, there are risks of unauthorized access from the IT network to the OT level, vulnerability to cyberattacks of industrial protocols, not all PLCs and SCADAs have built-in authentication and encryption mechanisms. The consequences of improper integration of TO ACS components are disruption of control processes, accidents and production shutdowns, violation of personnel safety, etc. The methods for eliminating such critical consequences can be the use of proven technologies and unified hardware and software tools and communication protocols from global manufacturers (Siemens, Honeywell, Emerson, ABB, Phoenix Contact, etc.). At the same time, it is necessary to comprehensively solve interaction problems from the sensor, actuator, RTU/PLC levels to the communication environment, SCADA and IT levels.

In [8], a reference architecture of an engineering WEB platform combining microservices (MS) and AutomationML (Automation Markup Language) is proposed – an open data exchange standard for describing, storing, and exchanging engineering information in the ASC of M&E. It is shown that such a modular structure increases flexibility, data reuse, and integration between engineering environment tools. The work is practically oriented and meets the modern requirements of the "Industry 4.0" concept. In the context of such a WEB platform, data interoperability between different modules (configurators, simulation of control processes, planning, data exchange, etc.) is necessary. AML provides universality of the data exchange format, which allows individual providers and developers to provide their services independently, and the WEB platform coordinates them. This approach (WEB platform + AML) makes the solution more accessible to small and medium-sized enterprises, which often do not have the opportunity for complex and costly individual design. It is shown that the approach using MS and AML allows for flexible combination of modules from different manufacturers, which is advantageous in modular and customized design. At the same time, the study is limited mainly to a conceptual assessment without taking into account the heterogeneous data structure, some specific parameters of devices or processes may not have a standard description in AML. In addition, AML is not always integrated with streaming data and its dynamic sampling in the process of interaction between components of TO ACS. One of the directions for solving the above problems may be the use of the Open User Communication technology, which is optimized for cyclic and acyclic exchange of heterogeneous data (both for standard and specific formats).

In [9], the Open Platform Communications Unified Architecture (OPC UA) communication protocol is considered, which is a standard for industrial communication that provides interaction between equipment components from different manufacturers. OPC UA is designed for real-time data exchange and includes security functions (authorization and encryption). This standard is a key element for modern industrial automation systems based on "Industry 4.0", which, among other things, provides tools for semantic and simulation modeling. However, building OPC UA information models is a relatively labor-intensive task that requires a deep understanding of both the OPC UA metamodel and the application area. Therefore, methods and tools for automatically generating OPC UA information models (from relational databases, tools or programming languages, by integrating multiple models into a single system-level information model) are relevant. The work is relevant but limited only to structural and functional design without examples of practical solutions to the problems of building TO ACS based on industrial communications. Thus, research is advisable in the area of practical application of the "Open User Communication" technology, which has advantages over OPC UA for data exchange tasks between PLCs in topologies of WEB-oriented systems. These advantages include the built-in functionality of "Open User Communication" at the level of design tools, in particular based on the TIA Portal platform (Siemens, Germany).

In [10], approaches to building real-time systems for IoT data analytics deployed on Edge Computing are investigated. This is an approach in which data processing is not performed in a remote cloud, but as close as possible to the data source – on local RTU/PLC, gateways or routers. Two modern architectural models are studied – microservices and serverless-functions – by comparing their life cycle, performance and resource efficiency in streaming IoT data processing scenarios. The essence of the applied approach is to process data locally on terminal devices with minimal delays without transferring all traffic to the cloud. At the same time, Edge platforms make it possible to reduce traffic delay and unload the network, but impose restrictions on computing resources, which makes the issue of optimality of architectural solutions key. Parameters such as traffic delay, stability under overloaded traffic, scalability, computing resources are analyzed. It is shown that the microservices architecture demonstrates better performance and lower overhead, especially at high event rates, while serverless-functions is more convenient for distributed IoT scaling. It is emphasized that there is no universal architecture – microservices are suitable for stable real-time loads, while serverless-functions are more effective for irregular or variable data flows. A list of unresolved problems is identified, including life cycle optimization, standardization of resource management mechanisms, and increased predictability of communication delays for Edge Computing. However, the practical value of the conclusions may be partially limited due to the laboratory conditions of the experiments and dependence on specific technological parameters. Thus, the generalization of the research results depends on the conditions of the experiments – the availability of real hardware, the ability to manage the communication load, testing on heterogeneous Edge Computing topologies. For optimization and effective application of Edge Computing, resource allocation, local caching and data filtering, automatic scaling, prediction models, Edge-Cloud balancing can be applied.

In [11], an Edge-oriented architecture for analyzing communication traffic and detecting intrusions in Industrial IoT in combination with clustering and ML models is proposed. The results show high accuracy (especially Random Forest) and lower latency due to processing at the Edge Computing level. Methods for increasing the level of IIoT security are presented by transferring the filtering, classification and response processes closer to the data sources, which makes it possible to reduce latency, reduce the load on the network, and increase the autonomy of the systems. A multi-tier architecture is proposed, which includes modules for local IoT traffic collection, pre-processing on Edge nodes, machine learning for anomaly detection and centralized analysis in the cloud. The paper contains an experimental performance evaluation of the proposed IDS (Intrusion Detection System), which optimizes response time and computing resources compared to traditional "cloud" methods. Particular attention is paid to the fact that the Edge architecture provides faster detection of cyberattacks critical for Cyber-Physical Systems (CPS) (e.g., DoS, modification of control commands or unauthorized access to devices).

Despite its significant practical value, the paper has a number of methodological limitations. The proposed system is tested on a limited data set and mainly on simulated or laboratory test benches, which complicates the evaluation in real industrial environments with high noise and traffic variability. Despite the above limitations, the paper makes a valuable contribution to the study of CPS and IIoT security, demonstrating the advantages of the "Edge Computing" approach to network traffic analytics. The architecture proposed in [11] can be potentially suitable for real-world applications, provided that the issues of scalability, model security, and compliance with standards are addressed. The work forms the basis for further research on the integration of Edge Computing and IDS in real-time industrial systems.

In [12], a study of the integration of Cloud Manufacturing and Cyber-Physical Systems via OPC UA in the context of "Industry 4.0" is reported. A methodology for combining CPS and Cloud Manufacturing is proposed to increase the flexibility and efficiency of production processes. The use of the OPC UA standard as a data exchange protocol ensures the integration of different types of systems. Emphasis is on automation, real-time monitoring, and adaptive production control. Experimental and simulation results are described that confirm the feasibility of the applied approach. It is shown how a standardized data exchange platform can provide flexibility, scalability, and transparent communication in distributed production environments. At the same time, OPC UA is considered a key technology due to its support for information models, secure data exchange, compatibility between equipment from different manufacturers, and the ability to integrate different architecture models into a single information structure. The work systematizes the current state of technology, demonstrates the role of OPC UA as a universal data exchange platform, and provides a structured architectural model for combining CPS and Cloud production. However, work [12] does not solve the problem of technical validation of the proposed solutions, and the experimental part is limited to demonstration examples and does not cover real production processes and problems of scaling Cloud services. Ways to solve the problem of technical validation can be further research in the direction of improving architectural models, algorithms and hardware and software tools, which involve the construction and testing of simulation models in tool environments for developing real systems. Simulation models built in actual systems development environments provide the possibility of direct transfer of configurations, parameters, algorithms, and application programs, which brings them as close as possible to the designed TO ACS and ensures technical validation.

The results of [4–12] allow us to conclude that at the current stage of development of technologies for building TO ACS, in addition to "reference" topologies, various non-standard topologies and complex multi-level communication environments are effectively used. Analysis of modern scientific research in the field of industrial automation, IIoT, AIoT, Networked Control Systems, SCADA and Cyber-Physical Systems revealed that the main trend in the development of TO ACS is the transition to open distributed WEB-oriented architectures. At the same time, existing approaches, architectures, and standards need to be adapted to the growing requirements for such systems at the level of functionality of topologies and communication environment, provision of "Digital Twins" for modeling and unification of hardware and software. To do this, it is necessary to comprehensively solve the problem of expanding the functionality of TO ACS topologies simultaneously with the study of information processes and communication environment in TO ACS.

From our review of the literature [4, 7, 8], it can be concluded that the goal is to expand the functionality of the considered TO ACS architectures in the direction of ensuring data consistency and implementing methods of priority (by events) data transmission. In [5], most attention is paid to cyber protection of TO ACS at the local level, without interaction with PLC network interfaces, which requires additional cyber protection measures at the level of the global communication environment. In [10, 11], a solution for an Edge-oriented TO ACS architecture operating in real time with partial data processing at the level of terminal PLCs is considered. But for potential real-time application and scaling, such an approach requires preliminary testing at the level of simulation models that provide real-time mode. OPC UA technology considered in [9, 12] solves the problem of coordination between hardware and software from different manufacturers but is a separate software product and requires additional resources for integration and administration. As a result of our analysis of [4, 6, 7, 12], it seems appropriate to single out the problem of technical validation of the proposed solutions for information systems and network topologies, which requires further research and solution.

The individual aspects of the construction of TO ACS identified as a result of our review identify the following problem:

– with cyclic requests from SCADA, technological parameters from the terminal level are sent separately in time and from different objects, which violates data consistency at different levels of the topology (there are interconnected parameters for which simultaneous analysis and processing are critical);

– in the maintenance control system, it is necessary to implement effective methods for organizing packet transmission of heterogeneous data types in real time;

– in case of data loss at the communication level in the maintenance control system, it is necessary to restore them using timestamps for current indication and in SCADA archives;

– when designing, implementing, and operating the maintenance control system, modeling procedures and technical validation of decisions made on the basis of unified hardware and software tools are necessary.

Thus, expanding the functionality of WEB-oriented TO ACS topologies based on the "Open User Communication" technology complements and adapts the existing methodology for building TO ACS, especially for territorially distributed technological objects with limited communication traffic.

3. The aim and objectives of the study

The purpose of our research is to expand the functionality of topologies of WEB-oriented control systems for technological objects based on "Open User Communication". This will make it possible to ensure data consistency at different levels of TO ACS topologies, packet transmission of heterogeneous data types, optimize traffic between SCADA and terminal PLCs, as well as restore data lost at the communication level.

To achieve the goal, the following tasks have been formulated:

– to design a topology of WEB-oriented automated control systems based on "Open User Communication";

– to develop a data acquisition system based on PLC Simatic S7 with "Open User Communication";

– to build a simulation model and test data exchange algorithms based on "Open User Communication";

– to test solutions under industrial conditions for WEB-oriented data acquisition systems from technological objects.

4. The study materials and methods

The object of our study is the information processes of interaction between components of WEB-oriented automated control systems based on "Open User Communication".

The hypothesis of the study is as follows. It is proposed to apply a topology with server and terminal PLCs with integrated "Open User Communication" technology in WEB-oriented ASCs of maintenance and repair based on SCADA and PLC and to implement the transmission of heterogeneous data formats in one frame. This approach will ensure the consistency of heterogeneous data types at the corresponding levels of the TO ACS topology of maintenance and repair, optimize communication traffic and provide the possibility of recovering lost data at the communication level. Additionally, this will make it possible to effectively combine the exchange of technological data and programming of terminal PLCs of territorially distributed technological objects in a single network infrastructure.

The following assumptions are adopted: the information processes of interaction between the virtual components of the simulation model "Open User Communication" may have some limitations compared to the real ones (the number of simultaneously used PLC simulators is limited by computing resources).

The following simplifications are accepted in the work: the constructed simulation model "Open User Communication" is single-channel with unidirectional traffic, which, if necessary, can be scaled to an allowable number of channels with bidirectional traffic.

The complex solution to the formulated tasks involves the use of a set of methods for designing topologies, constructing simulation models, configuring and parameterizing hardware, developing algorithms and application software for TO ACS [13, 14].

To implement the tasks of integrating "Open User Communication" in the topology of WEB-oriented automated control systems, the following hardware and software tools were used:

– Server work station (PC-System_1 "SIMATIC PC Station");

– PLC_5 (Programmable Logic Controller Simatic S7-1212C) [15];

– Switch_1 "SCALANCE X208" [16];

– PLC_PLC_4 (Programmable Logic Controller Simatic S7-1214C);

– CP_1–CP_5 (Communication Processor CP 1243-7 LTE) [17];

– Communication Network (PROFINET/Industrial Ethernet) [18];

– MS OS Windows Windows 11 IoT Enterprise LTSC 24H2 (build 26100.6584);

– Software tool platform TIA Portal V20 [19];

– Virtual Simulator (PLCSIM V20) [20].

The TIA Portal V20 software tool platform provides the following functionality:

– management of projects under development;

– configuration of project hardware;

– parameterization of project hardware;

– parameterization of the project communication environment;

– development of PLC-based TO ACS application software;

– integration of SCADA into technological object management systems;

– simulation of PLC and SCADA operation for tasks of simulation modeling and testing of TO ACS components.

5. Integration of "Open User Communication" in the topology of WEB-oriented automated control systems

5. 1. Development of the topology of WEB-oriented automated control systems based on "Open User Communication"

The paper proposes a distributed client-server topology of a WEB-oriented automated control system of the middle level based on the concept of "Open User Communication" (Siemens, Germany) [21]. A feature of the developed topology is the use of SCADA at the server level with a server PLC (hardware or software) with support for "Open User Communication". In addition, the topology provides for terminal PLCs with support for "Open User Communication" directly on technological control objects. Examples of such technological objects are, first of all, objects of critical infrastructure (energy supply, water supply, etc.) with a distributed architecture. For such objects, additional requirements are formed regarding the uninterrupted operation, protection functions of technological equipment, unification and maintainability, maximum automation of control and management processes, optimization of communication traffic and data processing at the terminal level.

The proposed topology is based on a comprehensive analysis [4–12], a formulated scientific and technical problem that needs to be solved, and unified hardware and software tools optimized for the implementation of the specified research tasks. Thus, it is the inclusion of the server PLC in the topology and the integration of the Open User Communication technology that allow a qualitative expansion of the functionality of the TO ACS topologies. Such an expansion of functionality includes:

– the developer can define the structure of data types and formats (for the Simatic S7-1200 PLC, 66 standard and specific data types are available) for exchange between components of the ACS based on the Open User Communication protocols (Fig. 1);

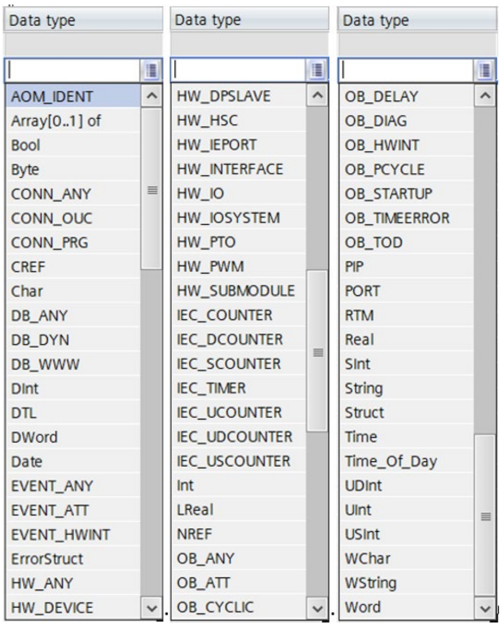
– proprietary "S7-Communication", which provides the possibility of remote programming of terminal PLCs via global networks in parallel with the Open User Communication traffic by "tunneling" communication protocols;

– the possibility of using cyclic and acyclic (by events) packet data transmission with dynamic sampling of the volume of data being transmitted;

– the possibility of additional processing on the server PLC of data coming from distributed terminal PLCs for their analysis and coordination with SCADA;

– the possibility of optimizing the load on the communication network and PLC due to a smaller number of transactions, compared to cyclic (polling) requests from SCADA;

– unification of design procedures and hardware and software tools (all design stages, including simulation modeling and design of the TO ACS dispatcher interface) are performed in a single tool environment with cross-references.



Data type
AOM_IDENT
Array[0..1] of
Bool
Byte
CONN_ANY
CONN_OUC
CONN_PRG
CREF
Char
DB_ANY
DB_DYN
DB_WWW
DInt
DTL
DWord
Date
EVENT_ANY
EVENT_ATT
EVENT_HWINT
ErrorStruct
HW_ANY
HW_DEVICE

Data type
HW_DPSLAVE
HW_HSC
HW_IEPORT
HW_INTERFACE
HW_IO
HW_IOSYSTEM
HW_PTO
HW_PWM
HW_SUBMODULE
IEC_COUNTER
IEC_DCOUNTER
IEC_SCOUNTER
IEC_TIMER
IEC_UCOUNTER
IEC_UDCOUNTER
IEC_USCOUNTER
Int
LReal
NREF
OB_ANY
OB_ATT
OB_CYCLIC

Data type
OB_DELAY
OB_DIAG
OB_HWINT
OB_PCYCLE
OB_STARTUP
OB_TIMEERROR
OB_TOD
PIP
PORT
RTM
Real
SInt
String
Struct
Time
Time_Of_Day
UDInt
UInt
USInt
WChar
WString
Word

Fig. 1. Standard and specific data types supported by Simatic S7-1200 Programmable Logic Controllers, which can be transferred via "Open User Communication"

Fig. 2 shows the developed topology of a WEB-oriented automated control system based on SCADA, server and terminal PLCs with support for "Open User Communication".

The topology for a server workstation and 4 terminal PLCs includes:

– PC-System_1 "SIMATIC PC Station" (server workstation with SCADA WinCC RT Prof and communication processor CP/IE on the PN/IE_5 network);

– PLC_5 "CPU 1212C" (server PLC with LTE router and "Open User Communication" functionality on the PN/IE_5 network);

– Switch_1 "SCALANCE X208" (IE switch on the PN/IE_5 network);

– PLC_1–PLC_4 "CPU 1214C" (terminal PLCs with LTE router and "Open User Communication" functionality on the PN/IE_1–PN/IE_4 networks.

The interaction between the server and terminal levels can be based on wired, optical, or mobile radio networks with the functionality of "Open User Communication". The developed topology provides all the advantages of the "Open User Communication" concept and can be scaled up to 8 terminal PLC S7-1200 with support for 8 signal modules each (in configuration with an intermediate PLC of the S7-1200 type). In configuration with an intermediate PLC of the S7-1500 type – from 78 to 310 "Open User Communication" connections (depending on the type of PLC S7-1500) [22].

5. 2. Design of a data acquisition system based on PLC Simatic S7 with "Open User Communication"

5. 2. 1. Configuration and parameterization of system hardware

The design of the system involves the following stages:

– initiating a project in the "TIA Portal" environment;

– configuration and parameterization of system hardware;

– development and debugging of the system communication environment;

– development of system application software at the PLC level;

– testing of interaction processes between server and terminal PLCs based on the developed simulation model "Open User Communication";

– development of a system of tags and technological mnemonics for SCADA at the server level;

– parameterization of industrial routers with support for "tunnel" protocols;

– testing of solutions under industrial conditions for WEB-oriented data acquisition systems from technological objects.

Fig. 3 shows the hardware configuration of the system at the server level with SCADA (WinCC RT Prof) and server PLC (PLC_1 CPU 1212C). In this case, the server robot station is transformed into an object "NMJ-PC [Simatic PC station]". The hardware configuration is a representation of the system components in the "TIA Portal" design environment, from which all configuration data and application programs are directly downloaded to real hardware PLCs and SCADA working files.

For interaction between SCADA and server PLC, a tag system has been devised (Project tree → SERVER OUC_171225 → → NMJ-PC [Simatic PC station] → HMI_RT_1_[WinCC RT Professional] → HMI tags), through which objects of technological mnemonics read data from the server PLC (Fig. 2).

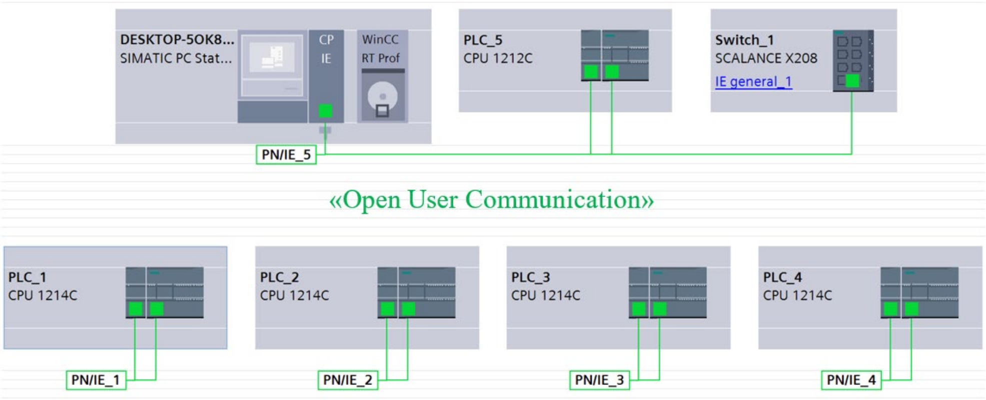


Fig. 2. Topology of a WEB-oriented automated control system based on Supervisory Control and Data Acquisition, server and 4 terminal Programmable Logic Controllers with support for "Open User Communication"

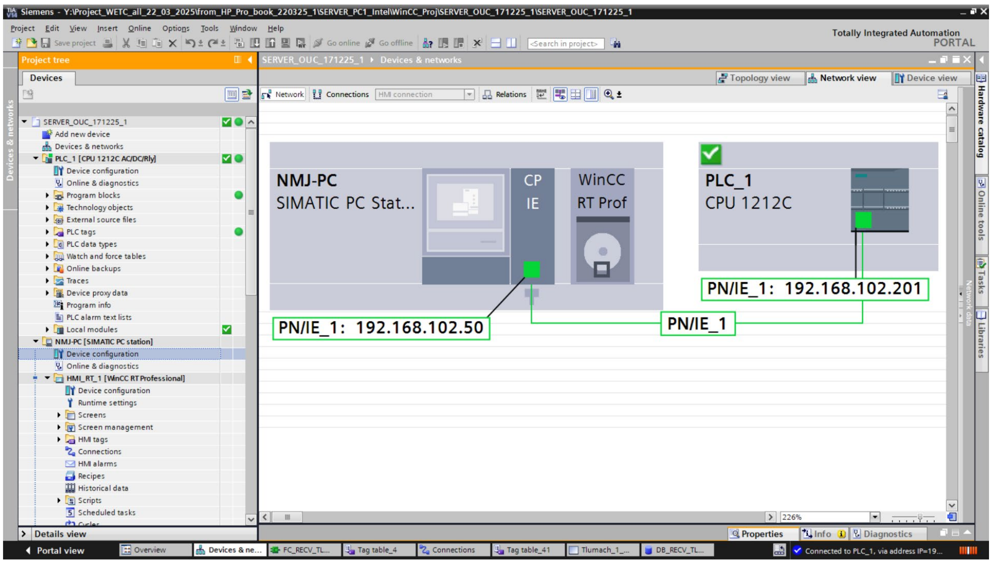
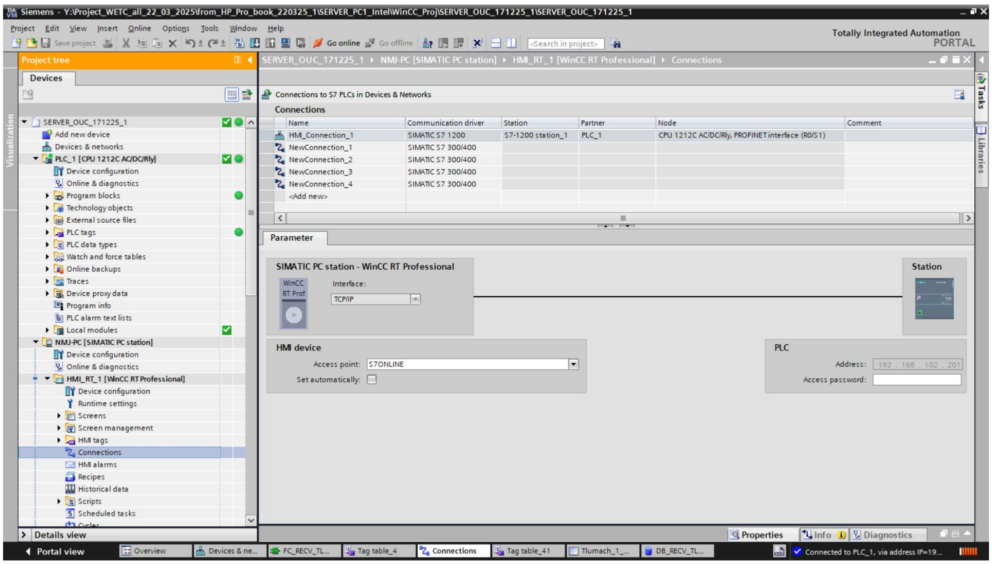

Siemens - Y:\Project_WETC_all_22_03_2025\from_HP_Pro_book_220325_1\SERVER_PC1_Intel\WinCC_Proj\SERVER_OUC_171225_1\SERVER_OUC_171225_1
Totally Integrated Automation PORTAL
Project tree
SERVER_OUC_171225_1 ▸ Devices & networks
Topology view
Network view
Device view
NMJ-PC
SIMATIC PC Stat...
CP IE
WinCC RT Prof
PLC_1
CPU 1212C
PN/IE_1: 192.168.102.50
PN/IE_1: 192.168.102.201
PN/IE_1
226%
Portal view
Connected to PLC_1, via address IP=19...

Fig. 3. Configuration of the system hardware at the server level with Supervisory Control And Data Acquisition "WinCC RT Prof" and server Programmable Logic Controller "PLC_1 CPU 1212C"

Fig. 4 shows the procedure for parameterizing TCP/IP communication between SCADA and server PLC (Project tree → SERVER OUC_171225 → NMJ-PC [Simatic PC station] → HMI_RT_1_[WinCC RT Professional] → Connections). In the section "Connections to S7 PLCs in Devices & Networks → "HMI_Connection_1" was created for data communication with a separate terminal "PLC_1 CPU 1212C AC/DC/Rly, PROFINET interface (R0/S1)" via the Communication driver "SIMATIC S7 1200". Thus, for each technological object, a "Connection" is created with separate parameters and PLC types (or via OPC UA), which solves the problem of unification and coordination of hardware parameters from different manufacturers.

The application software of the server PLC_1 includes the "Organization Block [OB1]", which cyclically executes the program instructions entered in it (including calling and executing FC functions as subroutines). Fig. 5 shows the function "FC_RECV_TLUMACH_1 [FC1]", which implements the reception of a data frame from a technological object based on the "Open User Communication" technology. The data is received simultaneously by the array "P#DB1.DBX0.0 REAL 31" in the floating-point format "REAL" (mode – Monitoring-on).

Fig. 6 shows the hardware configuration of the terminal PLC "PLC_1 CPU 1212C AC/DC/Rly" from the technological object. The application software of the server PLC_1 includes the "Organization Block [OB1]", which cyclically executes the program instructions entered into it (including calling and executing FC functions as subroutines). "Organization Block [OB100]" is executed once before restarting PLC_1 to enter certain constants, counter states and timers into the PLC. The used PLC provides 2 AI (Analog Input) 8 DI (Digital Input), 6 DQ (Digital Quit) and supports PROFINET/Industrial Ethernet communication. The CPU 1212C AC/DC/Rly can be expanded (up to three communication modules and up to two signal modules for processing input and output signals).


Siemens - Y:\Project_WETC_all_22_03_2025\from_HP_Pro_book_220325_1\SERVER_PC1_Intel\WinCC_Proj\SERVER_OUC_171225_1\SERVER_OUC_171225_1
Totally Integrated Automation PORTAL
Project tree
Portal view
Connected to PLC_1, via address IP=19...

SERVER_OUC_171225_1 ▸ NMJ-PC [SIMATIC PC station] ▸ HMI_RT_1 [WinCC RT Professional] ▸ Connections

Connections to S7 PLCs in Devices & Networks

Connections

Name	Communication driver	Station	Partner	Node	Comment
HMI_Connection_1	SIMATIC S7 1200	S7-1200 station_1	PLC_1	CPU 1212C AC/DC/Rly, PROFINET interface (R0/S1)	
NewConnection_1	SIMATIC S7 300/400				
NewConnection_2	SIMATIC S7 300/400				
NewConnection_3	SIMATIC S7 300/400				
NewConnection_4	SIMATIC S7 300/400				
<Add new>					

Parameter

SIMATIC PC station - WinCC RT Professional

Interface: TCP/IP

Station

HMI device

Access point: S7ONLINE

Set automatically: □

PLC

Address: 192 . 168 . 102 . 201

Access password:

Fig. 4. Procedure for parameterizing communication between Supervisory Control And Data Acquisition "WinCC RT Prof" and server Programmable Logic Controller "PLC_1 CPU 1212C"

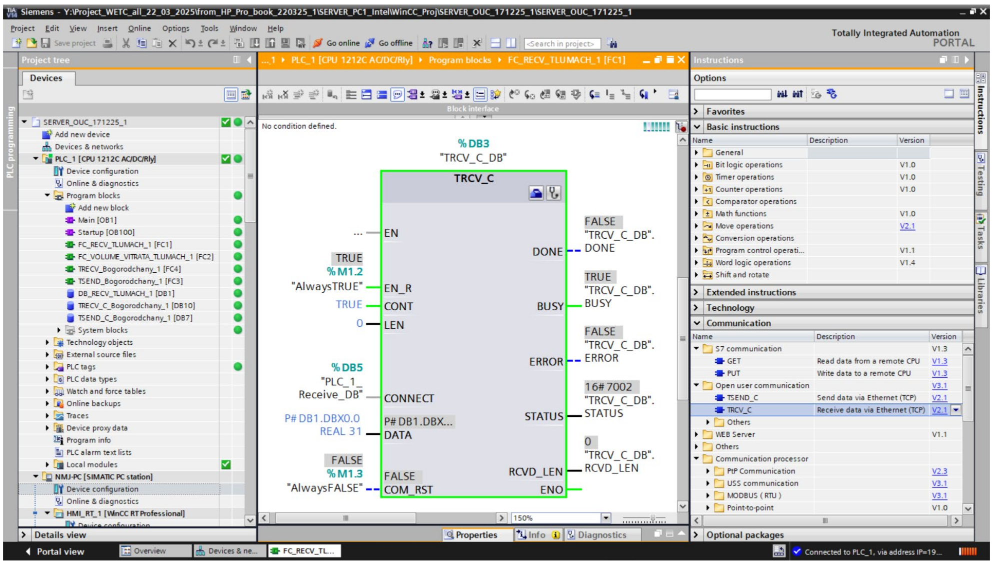


Fig. 5. Function "FC_RECV_TLUMACH_1 [FC1]", which implements the reception of a data frame from a technological object based on the "Open User Communication" technology (mode — Monitoring-on)

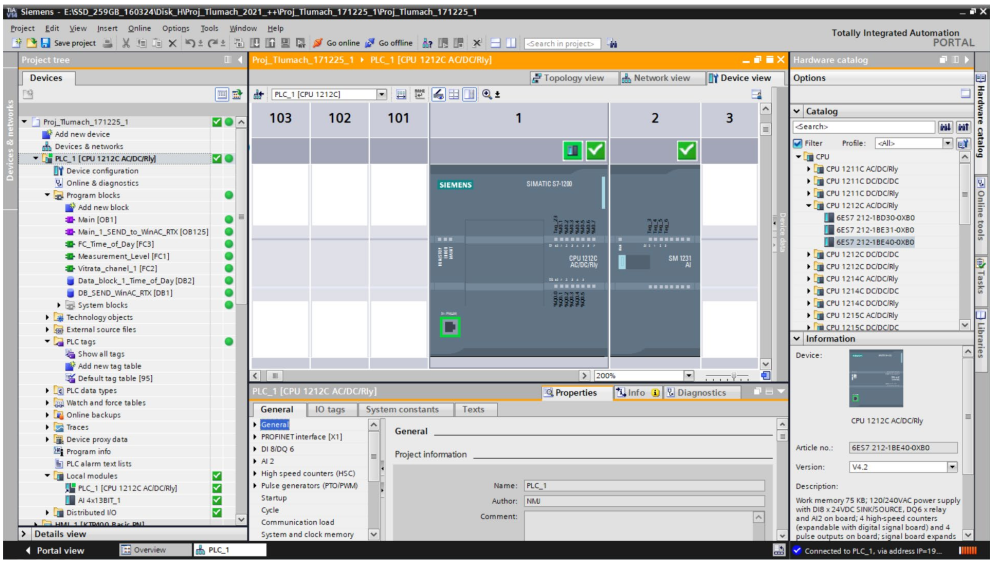
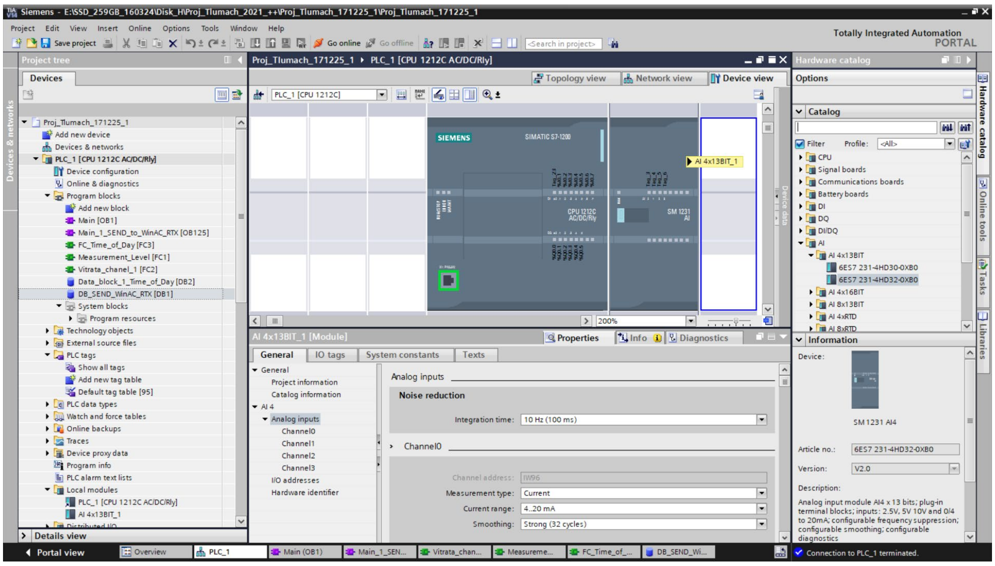

Siemens - E:\SSD_259GB_160324\Disk_H\Proj_Tlumach_2021_++\Proj_Tlumach_171225_1\Proj_Tlumach_171225_1
Totally Integrated Automation PORTAL
Project tree
Devices
Proj_Tlumach_171225_1
PLC_1 [CPU 1212C AC/DC/Rly]
Main [OB1]
Main_1_SEND_to_WinAC_RTX [OB125]
FC_Time_of_Day [FC3]
Measurement_Level [FC1]
Vitrata_chanel_1 [FC2]
Data_block_1_Time_of_Day [DB2]
DB_SEND_WinAC_RTX [DB1]
Local modules
PLC_1 [CPU 1212C AC/DC/Rly]
AI 4x13BIT_1
Proj_Tlumach_171225_1 ▸ PLC_1 [CPU 1212C AC/DC/Rly]
Topology view
Network view
Device view
103
102
101
1
2
3
SIEMENS
SIMATIC S7-1200
CPU 1212C AC/DC/Rly
SM 1231 AI
Hardware catalog
CPU 1212C AC/DC/Rly
6ES7 212-1BE40-0XB0
Article no.: 6ES7 212-1BE40-0XB0
Version: V4.2
Name: PLC_1
Author: NMJ
Portal view
Connected to PLC_1, via address IP=19...

Fig. 6. Hardware configuration of the terminal Programmable Logic Controller "PLC_1 CPU 1212C AC/DC/Rly" from a technological object (mode — Monitoring-on)

In the designed data acquisition system at one technological facility, it is necessary to obtain technological data from two hydrostatic sensors (calibrated for 0–5 m) of the water level in the tanks and a water flow meter with a pulse output (calibrated for 1.5 liters per output pulse). To process unified output signals from primary hydrostatic level transducers (4–20 mA), the parameterization of the 4-channel signal module SM 1221 AI4 with an analog-to-digital converter (ADC) with a bit depth of 13 bit (12 bit + sign) (Fig. 7) was performed. The module allows parameterization both by measurement type (Voltage or Current) and by the main measurement ranges of unified signals.

Fig. 8 shows a fragment of the application program structured into the function "Measurement_Level [FC1]" in the FBD language for processing measurement signals from hydrostatic water level transducers (mode – Monitoring-on). The output signal from the hydrostatic level transducer (4–20 mA) is digitized by SM 1221 AI4, entered into the register "IW96" and fed to the input "VALUE" of the normalization program instruction "NORM_X". The format is "Int-Integer" in the range of relative units (from "MIN" 0 to "MAX" 27648). At the output "OUT" of the normalization program instruction "NORM_X" a floating-point value in the format "REAL" in the range (from 0 to 1) proportional to the measured water level value in meters is formed. The output "MD104" is fed to the input "VALUE" of the scaling program instruction "SCALE_X", which scales the measured water level value in meters in absolute units according to the measuring range of the primary transducer (from 0.0 to 5.0 m). Additionally, the algebraic summation program instruction "ADD" corrects the linear offset of the zero point of the water tank, taking into account the design features of the tank.

Considering that the full main cycle "Main [OB1]" of the terminal PLC is fixed at the level (from 1 to 5 ms) "Online tools → Cycle time" (Fig. 9), processing of pulse signals from the flowmeter through the standard "Digital Input" mode is possible at a level of up to 200 Hz.



AI 4x13BIT_1 [Module]

General | IO tags | System constants | Texts

General: Project information, Catalog information; AI 4: Analog inputs (Channel0, Channel1, Channel2, Channel3), I/O addresses, Hardware identifier

Analog inputs

Noise reduction

Integration time: 10 Hz (100 ms)

Channel0

Channel address: IW96

Measurement type: Current

Current range: 4..20 mA

Smoothing: Strong (32 cycles)

Information

Device: SM 1231 AI4

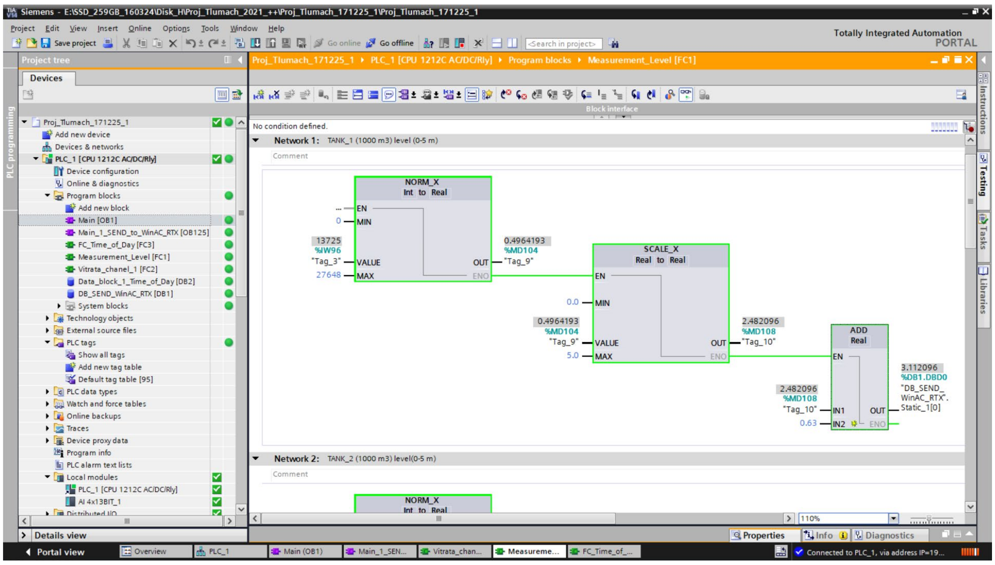
Article no.: 6ES7 231-4HD32-0XB0

Version: V2.0

Description: Analog input module AI4 x 13 bits; plug-in terminal blocks; inputs: 2.5V, 5V 10V and 0/4 to 20mA; configurable frequency suppression; configurable smoothing; configurable diagnostics

Connection to PLC_1 terminated.

Fig. 7. Procedure for parameterizing the SM 1221 AI4 signal module with 13 bit analog-digital bit depth


Siemens - E:\SSD_259GB_160324\Disk_H\Proj_Tlumach_2021_++\Proj_Tlumach_171225_1\Proj_Tlumach_171225_1
Totally Integrated Automation PORTAL
Project tree
Devices
Proj_Tlumach_171225_1 ▸ PLC_1 [CPU 1212C AC/DC/Rly] ▸ Program blocks ▸ Measurement_Level [FC1]
Block interface
NORM_X
Int to Real
EN
MIN
VALUE
MAX
OUT
ENO
SCALE_X
Real to Real
ADD
Real
IN1
IN2
110%
Properties
Info
Diagnostics
Portal view

No condition defined.

Network 1: TANK_1 (1000 m3) level (0-5 m)

NORM_X Int to Real: MIN = 0; VALUE = 13725 %IW96 "Tag_3"; MAX = 27648; OUT = 0.4964193 %MD104 "Tag_9"

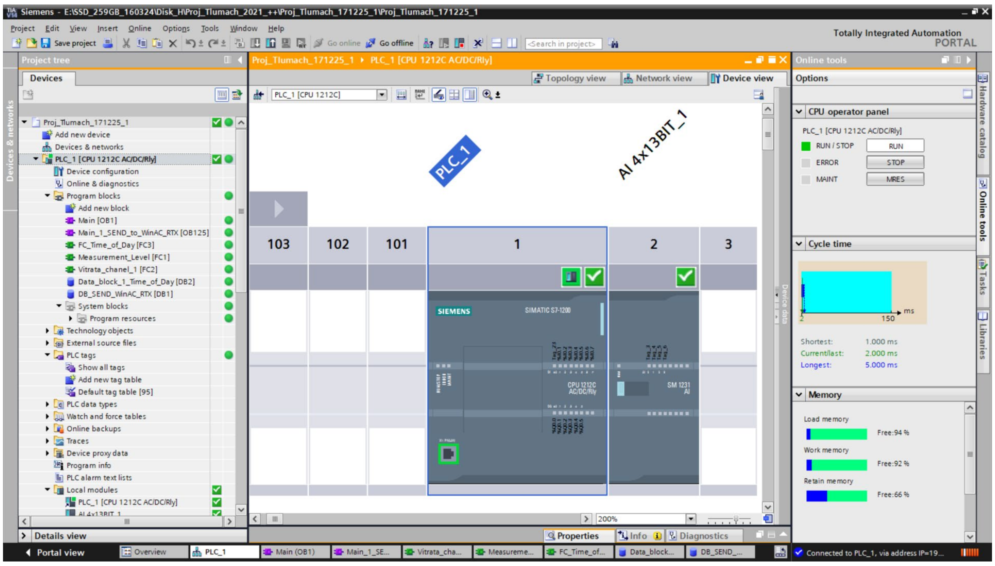
SCALE_X Real to Real: MIN = 0.0; VALUE = 0.4964193 %MD104 "Tag_9"; MAX = 5.0; OUT = 2.482096 %MD108 "Tag_10"

ADD Real: IN1 = 2.482096 %MD108 "Tag_10"; IN2 = 0.63; OUT = 3.112096 %DB1.DBD0 "DB_SEND_WinAC_RTX".Static_1[0]

Network 2: TANK_2 (1000 m3) level(0-5 m)

Connected to PLC_1, via address IP=19...

Fig. 8. Fragment of an application program structured into the function "Measurement_Level [FC1]" for processing measurement signals from hydrostatic water level transducers (mode – Monitoring-on)


Siemens - E:\SSD_259GB_160324\Disk_H\Proj_Tlumach_2021_++\Proj_Tlumach_171225_1\Proj_Tlumach_171225_1
Totally Integrated Automation PORTAL
Project tree
Devices
Proj_Tlumach_171225_1 ▸ PLC_1 [CPU 1212C AC/DC/Rly]
Topology view
Network view
Device view
PLC_1
AI 4x13BIT_1
103
102
101
1
2
3
SIEMENS
SIMATIC S7-1200
CPU 1212C AC/DC/Rly
SM 1231 AI
Online tools
Options
RUN
STOP
MRES
2
150
ms
Portal view

CPU operator panel

PLC_1 [CPU 1212C AC/DC/Rly]

RUN / STOP; ERROR; MAINT

Cycle time

Shortest: 1.000 ms

Current/last: 2.000 ms

Longest: 5.000 ms

Memory

Load memory Free:94 %

Work memory Free:92 %

Retain memory Free:66 %

Connected to PLC_1, via address IP=19...

Fig. 9. Complete main cycle "Main [OB1]" of the terminal PLC at the level (from 1 to 5 ms) "Online tools → Cycle time"

Therefore, to solve the above limitation, the software instruction "CTR_HSC" (Control Speed Counter) from the "Technology" section (Fig. 10) was used, which provides processing of input pulse signals with a frequency of up to 100 kHz due to combined functionality. PLC hardware counters operate at a frequency of up to 100 kHz, and the software instruction "CTR_HSC" controls their operation by implementing hardware interrupts outside the PLC program cycle and periodically reading the results of processing the input signal.

Fig. 11 shows a fragment of the application program for calculating the average current water flow rate (in m^3/h) based on the program instruction "CTR_HSC". The input "IN" of the program instruction for converting data formats "CONV" is fed with the value of the counted pulses from the register "ID1000" of the "CTR_HSC" instruction in the format "UDInt-Unsigned Double Integer" to the format "REAL". From the output "OUT → MD192" the value is fed to the input "IN" of the program instruction for algebraic division "DIV" by 1500 to convert the flow rate in 1.5 liters per pulse to m^3 per pulse. The output of the program instruction "DIV" is multiplied by 3600 to convert the flow rate in m^3/h.

In a similar way, an algorithm for processing and calculating hourly and similar water consumption at a water supply technological facility is built.

Fig. 12 shows the data block "DB_SEND_WinAC_RTX [DB1]" in the structure of the terminal PLC_1, which contains a formed frame for data transmission from a technological facility using the "Open User Communication" technology (mode – Monitoring-on).

The data is formed into an array "Arrey[0..30] of Real" and includes the following technological parameters:

– TLUMACH_RChV_Level_1;
– TLUMACH_RChV_Level_2;
– TLUMACH_RESERV_1;
– TLUMACH_RESERV_2;
– TLUMACH_RESERV_2;
– TLUMACH_za_sec_mitteva_(potochna);
– TLUMACH_za_hour;
– TLUMACH_za_god_0;
– …
– TLUMACH_za_god_23.

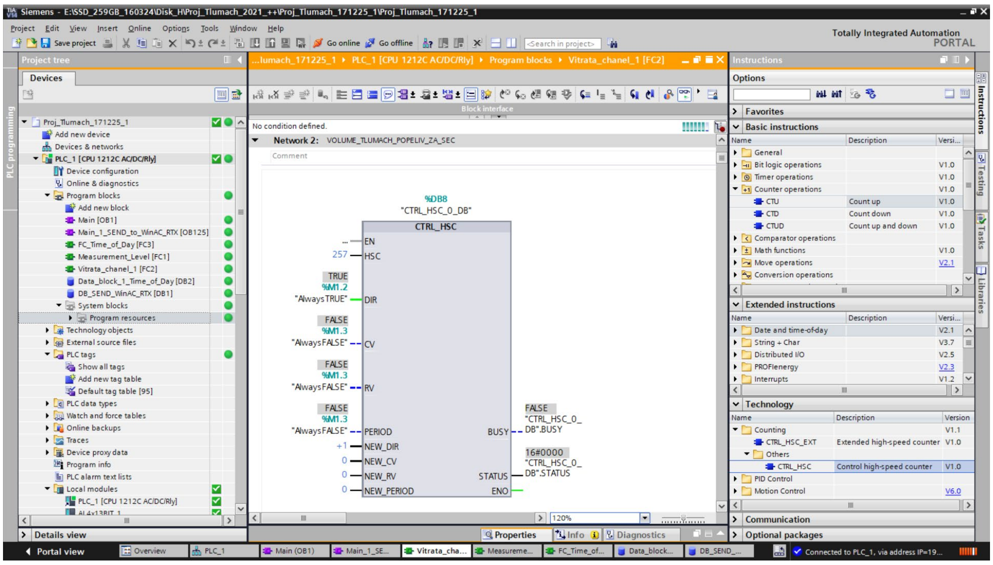
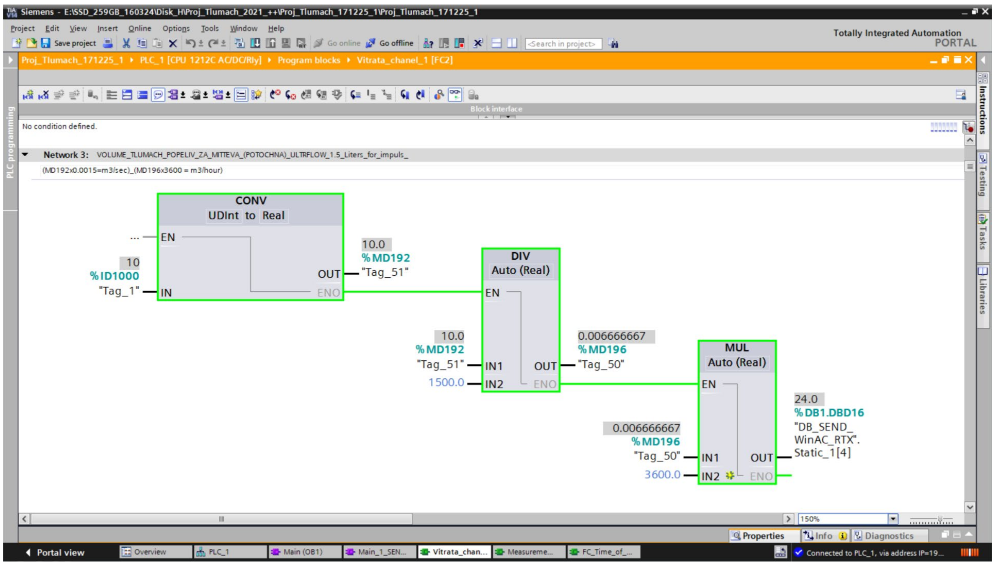


Fig. 10. Program instruction "CTR_HSC" (Control Speed Counter) from the "Technology" section to provide processing of input pulse signals with a frequency of up to 100 kHz



Siemens - E:\SSD_259GB_160324\Disk_H\Proj_Tlumach_2021_++\Proj_Tlumach_171225_1\Proj_Tlumach_171225_1
Project Edit View Insert Online Options Tools Window Help
Save project
Go online
Go offline
Totally Integrated Automation PORTAL
Proj_Tlumach_171225_1 ▸ PLC_1 [CPU 1212C AC/DC/Rly] ▸ Program blocks ▸ Vitrata_chanel_1 [FC2]
Block interface
No condition defined.
Network 3: VOLUME_TLUMACH_POPELIV_ZA_MITTEVA_(POTOCHNA)_ULTRFLOW_1.5_Liters_for_impuls_
(MD192x0.0015=m3/sec)_(MD196x3600 = m3/hour)
CONV
UDInt to Real
EN
10 %ID1000 "Tag_1" IN
OUT
10.0 %MD192 "Tag_51"
ENO
DIV
Auto (Real)
EN
10.0 %MD192 "Tag_51" IN1
1500.0 IN2
OUT
0.006666667 %MD196 "Tag_50"
ENO
MUL
Auto (Real)
EN
0.006666667 %MD196 "Tag_50" IN1
3600.0 IN2
OUT
24.0 %DB1.DBD16 "DB_SEND_WinAC_RTX". Static_1[4]
ENO
150%
Properties Info Diagnostics
Instructions Testing Tasks Libraries
Portal view Overview PLC_1 Main (OB1) Main_1_SEN... Vitrata_chan... Measureme... FC_Time_of...
Connected to PLC_1, via address IP=19...

Fig. 11. Fragment of an application program for calculating the average current water flow rate (in m^3/h) based on the program instruction "CTR_HSC"

Fig. 13 shows the program instruction "TSEND_C", which implements asynchronous transmission (by events) of data in one frame from a technological object to the server level based on the "Open User Communication" technology.

Thus, the completed configuration and parameterization of hardware is the basis for performing the next stages of designing a data acquisition system based on the developed topology and Open User Communication technology.

5. 2. 2. Formation of a data set for simulation modeling

For simulation modeling tasks, a global data block PLC_5_TRCV_C [DB4] was created to store data received from the data block PLC_1_TSEND_C [DB3] of one of the terminal PLC_1 [CPU1214C AC/DC/Rly]. Both data blocks [DB4] and [DB3] must have the same structure and data formats. For simulation modeling "Open User Communication", a test set of basic data formats transferred from [DB4] of the terminal PLC_1 to [DB3] of the server PLC_5 was formed (Fig. 14):

– Static_1 – Int (Integer) with the value read from the incremental counter IEC_Counter_0_DB1;

– Static_2 – Byte (Byte) with the value (2#10101010);

– Static_3 – DInt (Double Integer) with the value (-0123456789);

– Static_4 – UInt (Unsigned Integer) with the value (0123456789);

– Static_5 – UDInt (Unsigned Double Integer) with the value (01234567890);

– Static_6 – Word (Word) with the value (16#AB);

– Static_7 – DWord (Double Word) with the value (16#A1F9);

– Static_8 – Real (Floating Point) with the value (1.234568E+08);

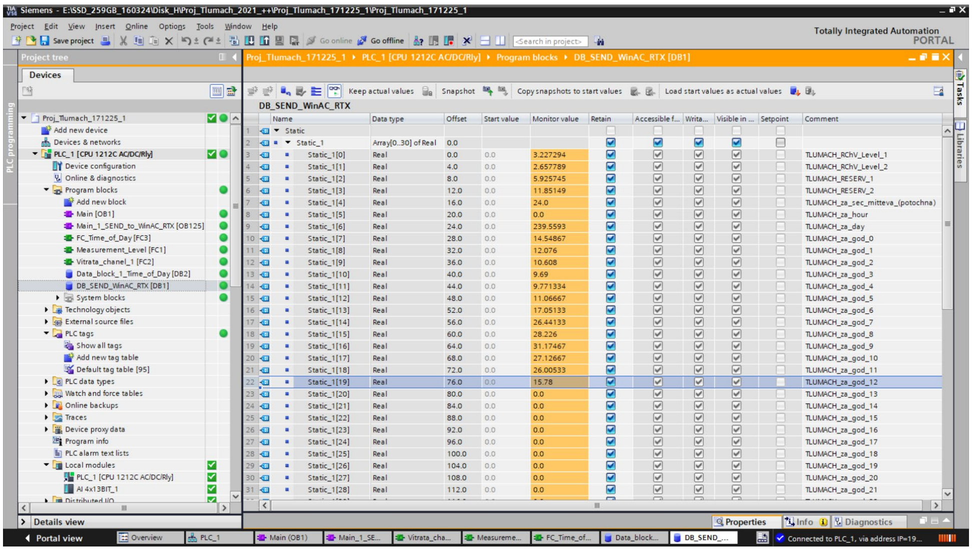
– Static_9 – Array[0..7] of Real (Array) with the value (-1.123, -2.123, -3.123, -4.123, -0.123, 5.123, 6.123, 7.123);

– Static_10 – DTL (Date and Time Long) with the value (current date and time);

– Static_11 – String (String) with the value (‘#Open_User_Communication#’);

– Static_12 – LReal (Long Real) with the value (332.0).

The result of simulation modeling should be the consistency of the data transmitted from [DB4] PLC_1 and received in [DB3] PLC_5 in the corresponding formats.



Siemens - E:\SSD_259GB_160324\Disk_H\Proj_Tlumach_2021_++\Proj_Tlumach_171225_1\Proj_Tlumach_171225_1

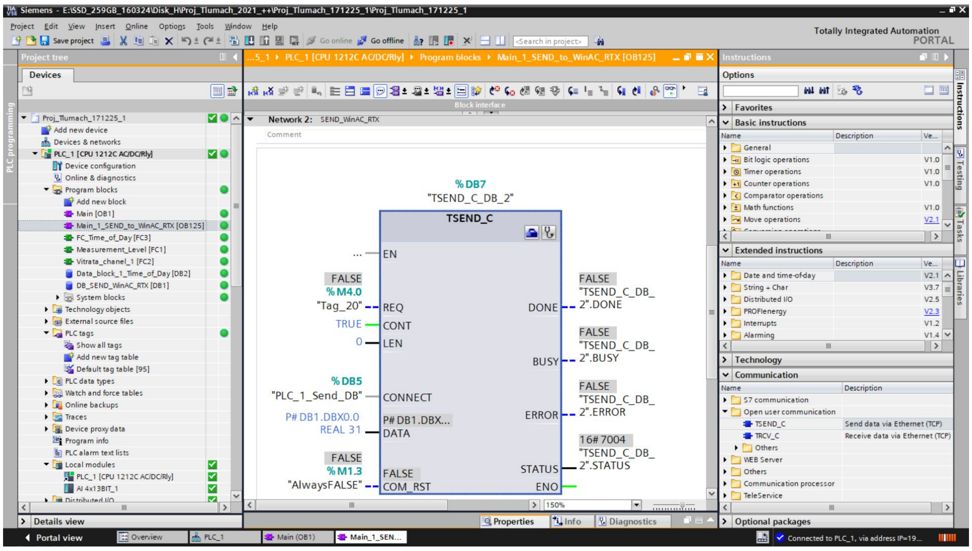
Proj_Tlumach_171225_1 ▸ PLC_1 [CPU 1212C AC/DC/Rly] ▸ Program blocks ▸ DB_SEND_WinAC_RTX [DB1]

DB_SEND_WinAC_RTX

	Name	Data type	Offset	Start value	Monitor value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Comment
1	▼ Static					☐	☐	☐	☐	☐	
2	▼ Static_1	Array[0..30] of Real	0.0			☑	☑	☑	☑	☐	
3	Static_1[0]	Real	0.0	0.0	3.227294	☑	☑	☑	☑	☐	TLUMACH_RChV_Level_1
4	Static_1[1]	Real	4.0	0.0	2.657789	☑	☑	☑	☑	☐	TLUMACH_RChV_Level_2
5	Static_1[2]	Real	8.0	0.0	5.925745	☑	☑	☑	☑	☐	TLUMACH_RESERV_1
6	Static_1[3]	Real	12.0	0.0	11.85149	☑	☑	☑	☑	☐	TLUMACH_RESERV_2
7	Static_1[4]	Real	16.0	0.0	24.0	☑	☑	☑	☑	☐	TLUMACH_za_sec_mitteva_(potochna)
8	Static_1[5]	Real	20.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_hour
9	Static_1[6]	Real	24.0	0.0	239.5593	☑	☑	☑	☑	☐	TLUMACH_za_day
10	Static_1[7]	Real	28.0	0.0	14.54867	☑	☑	☑	☑	☐	TLUMACH_za_god_0
11	Static_1[8]	Real	32.0	0.0	12.076	☑	☑	☑	☑	☐	TLUMACH_za_god_1
12	Static_1[9]	Real	36.0	0.0	10.608	☑	☑	☑	☑	☐	TLUMACH_za_god_2
13	Static_1[10]	Real	40.0	0.0	9.69	☑	☑	☑	☑	☐	TLUMACH_za_god_3
14	Static_1[11]	Real	44.0	0.0	9.771334	☑	☑	☑	☑	☐	TLUMACH_za_god_4
15	Static_1[12]	Real	48.0	0.0	11.06667	☑	☑	☑	☑	☐	TLUMACH_za_god_5
16	Static_1[13]	Real	52.0	0.0	17.05133	☑	☑	☑	☑	☐	TLUMACH_za_god_6
17	Static_1[14]	Real	56.0	0.0	26.44133	☑	☑	☑	☑	☐	TLUMACH_za_god_7
18	Static_1[15]	Real	60.0	0.0	28.226	☑	☑	☑	☑	☐	TLUMACH_za_god_8
19	Static_1[16]	Real	64.0	0.0	31.17467	☑	☑	☑	☑	☐	TLUMACH_za_god_9
20	Static_1[17]	Real	68.0	0.0	27.12667	☑	☑	☑	☑	☐	TLUMACH_za_god_10
21	Static_1[18]	Real	72.0	0.0	26.00533	☑	☑	☑	☑	☐	TLUMACH_za_god_11
22	Static_1[19]	Real	76.0	0.0	15.78	☑	☑	☑	☑	☐	TLUMACH_za_god_12
23	Static_1[20]	Real	80.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_13
24	Static_1[21]	Real	84.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_14
25	Static_1[22]	Real	88.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_15
26	Static_1[23]	Real	92.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_16
27	Static_1[24]	Real	96.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_17
28	Static_1[25]	Real	100.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_18
29	Static_1[26]	Real	104.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_19
30	Static_1[27]	Real	108.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_20
31	Static_1[28]	Real	112.0	0.0	0.0	☑	☑	☑	☑	☐	TLUMACH_za_god_21

Connected to PLC_1, via address IP=19...

Fig. 12. Data block "DB_SEND_WinAC_RTX [DB1]" in the structure of the terminal PLC_1, which contains a formed frame for data transmission from a technological object using the "Open User Communication" technology (mode – Monitoring-on)

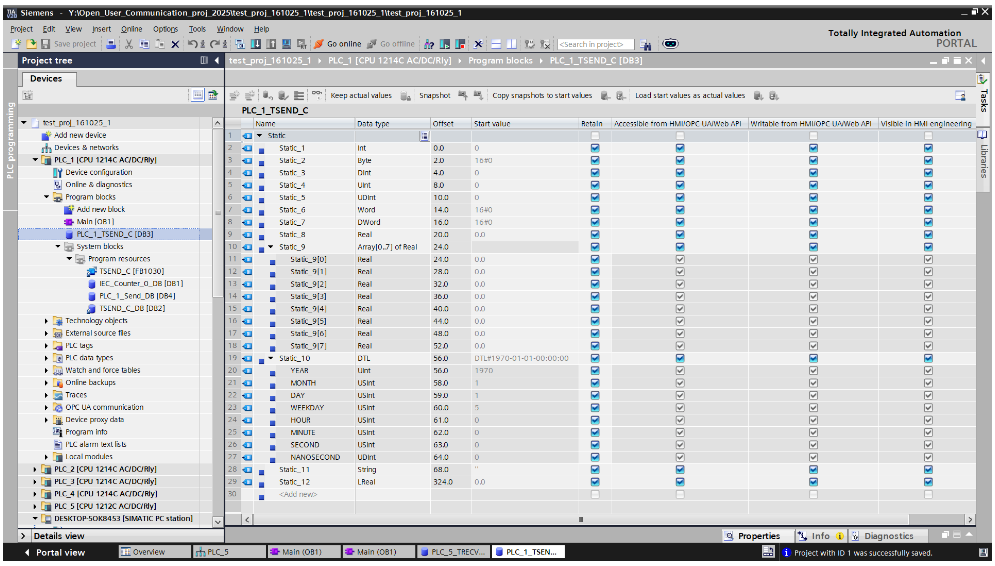


Siemens - E:\SSD_259GB_160324\Disk_H\Proj_Tlumach_2021_++\Proj_Tlumach_171225_1\Proj_Tlumach_171225_1

Network 2: SEND_WinAC_RTX

Connected to PLC_1, via address IP=19...

Fig. 13. Program instruction "TSEND_C", which implements asynchronous transmission (by events) of data in one frame from a technological object based on the "Open User Communication" technology


Siemens - Y:\Open_User_Communication_proj_2025\test_proj_161025_1\test_proj_161025_1\test_proj_161025_1
Totally Integrated Automation PORTAL
Project tree
Devices
test_proj_161025_1 ▸ PLC_1 [CPU 1214C AC/DC/Rly] ▸ Program blocks ▸ PLC_1_TSEND_C [DB3]
Keep actual values
Snapshot
Copy snapshots to start values
Load start values as actual values
Details view
Portal view
Properties
Info
Diagnostics

PLC_1_TSEND_C

	Name	Data type	Offset	Start value	Retain	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API	Visible in HMI engineering
1	▼ Static				□	□	□	□
2	Static_1	Int	0.0	0	☑	☑	☑	☑
3	Static_2	Byte	2.0	16#0	☑	☑	☑	☑
4	Static_3	DInt	4.0	0	☑	☑	☑	☑
5	Static_4	UInt	8.0	0	☑	☑	☑	☑
6	Static_5	UDInt	10.0	0	☑	☑	☑	☑
7	Static_6	Word	14.0	16#0	☑	☑	☑	☑
8	Static_7	DWord	16.0	16#0	☑	☑	☑	☑
9	Static_8	Real	20.0	0.0	☑	☑	☑	☑
10	▼ Static_9	Array[0..7] of Real	24.0		☑	☑	☑	☑
11	Static_9[0]	Real	24.0	0.0	☑	☑	☑	☑
12	Static_9[1]	Real	28.0	0.0	☑	☑	☑	☑
13	Static_9[2]	Real	32.0	0.0	☑	☑	☑	☑
14	Static_9[3]	Real	36.0	0.0	☑	☑	☑	☑
15	Static_9[4]	Real	40.0	0.0	☑	☑	☑	☑
16	Static_9[5]	Real	44.0	0.0	☑	☑	☑	☑
17	Static_9[6]	Real	48.0	0.0	☑	☑	☑	☑
18	Static_9[7]	Real	52.0	0.0	☑	☑	☑	☑
19	▼ Static_10	DTL	56.0	DTL#1970-01-01-00:00:00	☑	☑	☑	☑
20	YEAR	UInt	56.0	1970	☑	☑	☑	☑
21	MONTH	USInt	58.0	1	☑	☑	☑	☑
22	DAY	USInt	59.0	1	☑	☑	☑	☑
23	WEEKDAY	USInt	60.0	5	☑	☑	☑	☑
24	HOUR	USInt	61.0	0	☑	☑	☑	☑
25	MINUTE	USInt	62.0	0	☑	☑	☑	☑
26	SECOND	USInt	63.0	0	☑	☑	☑	☑
27	NANOSECOND	UDInt	64.0	0	☑	☑	☑	☑
28	Static_11	String	68.0	''	☑	☑	☑	☑
29	Static_12	LReal	324.0	0.0	☑	☑	☑	☑
30	<Add new>				□	□	□	□

Project with ID 1 was successfully saved.

Fig. 14. Test set of basic data formats transferred from Data Block [DB4] of the terminal Programmable Logic Controller "PLC_1" to Data Block [DB3] of the server Programmable Logic Controller "PLC_5" with support for "Open User Communication"

5. 2. 3. Development of the application program "Open User Communication"

The application program for the implementation of "Open User Communication" is developed in the FBD (Function Block Diagram) language [23]. The communication program instruction "TSEND_C" from the "Communication" → "Open user communication" section is integrated into the block of the main program cycle "Main [OB1]" of PLC_1 (Fig. 15).

The program instruction "TSEND_C" includes the following inputs and outputs:

– EN – Enable (input: of Enable);

– REQ – (input: Starts the send job on a rising edge);

– CONT – (input: Controls the communication connection);

– LEN – (input: Maximum number of bytes to be sent with the job (Optional parameter (hidden));

– CONNECT – (input: Pointer to the structure of the connection description);

– DATA – (input: Pointer to the send area containing the address and the length of the data to be sent);

– ADDR – (input: In this case it contains a pointer to the system data type TADDR_Para (hidden));

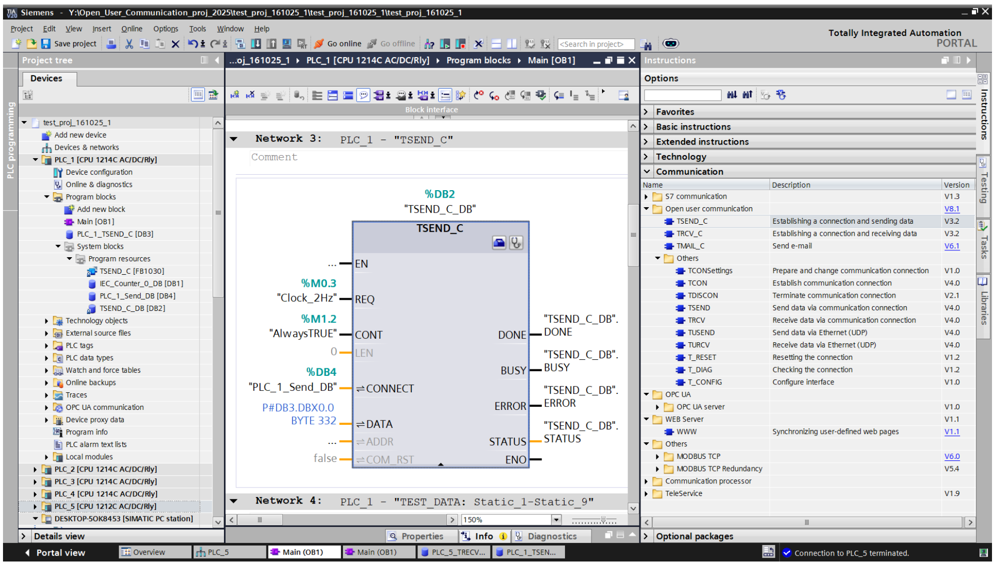
– COM_RST – (input: Resets the connection (Optional parameter (hidden));

– DONE – (output: Status parameter with the following values ("0" – Send job not yet started or still in progress, "1" – Send job executed without error. This state is only displayed for one cycle CPU of PLC);

– BUSY – (output: Status parameter with the following values ("0" – Send job not yet started or already completed, "1" – Send job not yet completed. A new send job cannot be started);

– ERROR – (output: Status parameter with the following values ("0" – No error, "1" – Error occurred during connection establishment, data transfer or connection termination);

– STATUS – (output: Status of instruction).



Network 3: PLC_1 - "TSEND_C"

Network 4: PLC_1 - "TEST_DATA: Static_1-Static_9"

Name	Description	Version
S7 communication		V1.3
Open user communication		V8.1
TSEND_C	Establishing a connection and sending data	V3.2
TRCV_C	Establishing a connection and receiving data	V3.2
TMAIL_C	Send e-mail	V6.1
Others		
TCONSettings	Prepare and change communication connection	V1.0
TCON	Establish communication connection	V4.0
TDISCON	Terminate communication connection	V2.1
TSEND	Send data via communication connection	V4.0
TRCV	Receive data via communication connection	V4.0
TUSEND	Send data via Ethernet (UDP)	V4.0
TURCV	Receive data via Ethernet (UDP)	V4.0
T_RESET	Resetting the connection	V1.2
T_DIAG	Checking the connection	V1.2
T_CONFIG	Configure interface	V1.0
OPC UA		
OPC UA server		V1.0
WEB Server		V1.1
WWW	Synchronizing user-defined web pages	V1.1
Others		
MODBUS TCP		V6.0
MODBUS TCP Redundancy		V5.4
Communication processor		
TeleService		V1.9

Connection to PLC_5 terminated.

Fig. 15. The procedure for integrating the communication program instruction "TSEND_C" from the "Communication" → "Open user communication" section into the "Main [OB1]" Organization Block of the Programmable Logic Controller "PLC_1"

The "CONNECT" input is automatically parameterized after defining the parameters of the data transfer program instruction "TSEND_C" for PLC_1 in the "Connection data" parameter (PLC_1_Send_DB) (Fig. 16).

The "DATA" input is parameterized with the syntax P#DB3.DBX0.0 BYTE 332:

– P# – prefix of the corresponding syntax;

– DB3 – source of data to be transferred;

– DBX0.0 – start address of the data to be transferred;

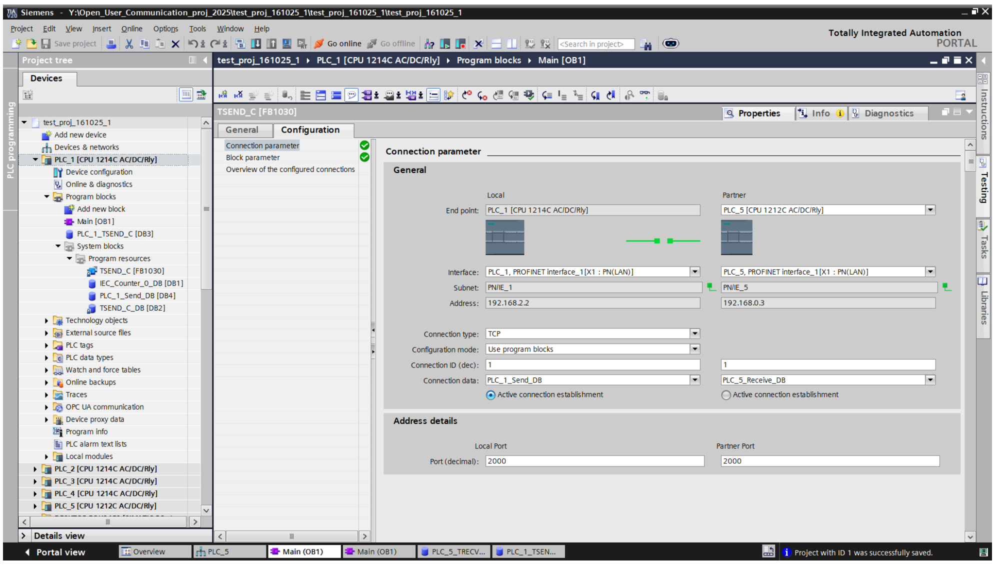
– BYTE – data format for calculating the total volume of data to be transferred;

– 332 – volume of data of the corresponding format to be transferred.

Similar parameterization is performed for the data reception program instruction "TRCV_C" for PLC_5 (Fig. 17). Thus, the syntax used for parameterizing the input "DATA" of the program instruction "TSEND_C" can provide a dynamic change in the sample of transmitted data based on the event-dependent control algorithm (Event). Accordingly, the task of optimizing traffic between the server PLC_5 and the terminal PLC_1–PLC_1 is solved, especially with a significant communication load and with significant volumes of transmitted data. "Open user communication" provides dynamic selective transmission and reception of up to 8192 Byte in one frame, which is an advantage compared to uncontrolled cyclic requests from SCADA to terminal PLCs.

5. 3. Simulation model and results of testing the data exchange algorithm based on "Open User Communication"

The simulation model "Open User Communication" was developed based on a test project in the TIA Portal V20 environment and PLC simulators (PLCSIM V20). The purpose of simulation modeling is to verify the correctness of the developed project of the control system and data collection from technological objects based on "Open User Communication". The main criterion when testing the project using the simulation model is to verify the functionality of the project as a whole and the consistency of the transmitted and received data. For simulation modeling, a simplified system configuration was used, which includes a server (PLC_5) that communicates with SCADA and simultaneously receives data from one of the terminal PLCs (PLC_1) based on "Open User Communication" [24].


Siemens - Y:\Open_User_Communication_proj_2025\test_proj_161025_1\test_proj_161025_1\test_proj_161025_1
Totally Integrated Automation PORTAL
test_proj_161025_1 ▸ PLC_1 [CPU 1214C AC/DC/Rly] ▸ Program blocks ▸ Main [OB1]
TSEND_C [FB1030]
Properties
Info
Diagnostics
General
Configuration
Connection parameter
Block parameter
Overview of the configured connections
Portal view
Project with ID 1 was successfully saved.

Connection parameter

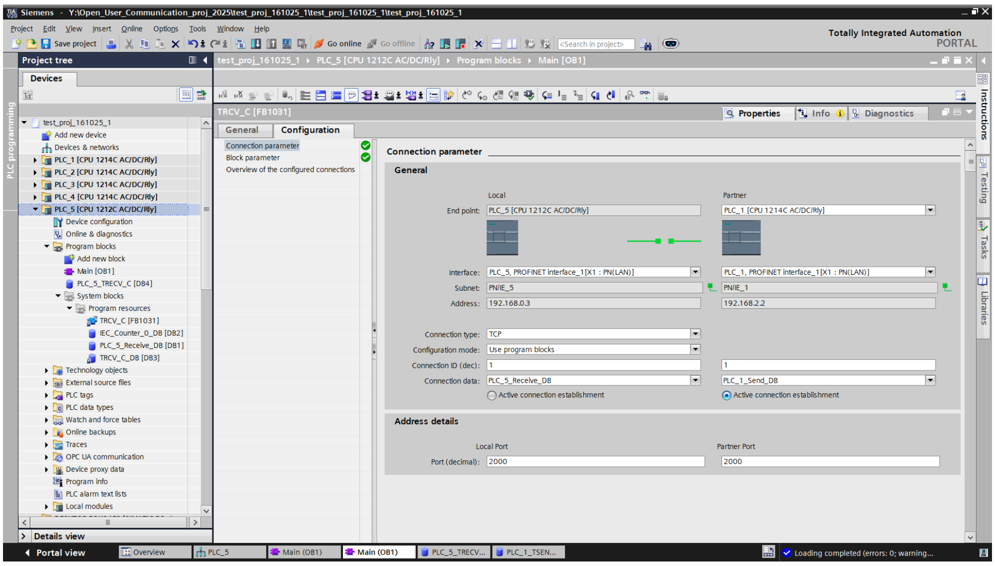
General

	Local	Partner
End point:	PLC_1 [CPU 1214C AC/DC/Rly]	PLC_5 [CPU 1212C AC/DC/Rly]
Interface:	PLC_1, PROFINET interface_1[X1 : PN(LAN)]	PLC_5, PROFINET interface_1[X1 : PN(LAN)]
Subnet:	PN/IE_1	PN/IE_5
Address:	192.168.2.2	192.168.0.3
Connection type:	TCP	
Configuration mode:	Use program blocks	
Connection ID (dec):	1	1
Connection data:	PLC_1_Send_DB	PLC_5_Receive_DB
	● Active connection establishment	○ Active connection establishment

Address details

	Local Port	Partner Port
Port (decimal):	2000	2000

Fig. 16. Procedure for parameterizing the data transfer program instruction "TSEND_C"


Siemens - Y:\Open_User_Communication_proj_2025\test_proj_161025_1\test_proj_161025_1\test_proj_161025_1
Totally Integrated Automation PORTAL
test_proj_161025_1 ▸ PLC_5 [CPU 1212C AC/DC/Rly] ▸ Program blocks ▸ Main [OB1]
TRCV_C [FB1031]
Properties
Info
Diagnostics
General
Configuration
Connection parameter
Block parameter
Overview of the configured connections
Portal view
Loading completed (errors: 0; warning...

Connection parameter

General

	Local	Partner
End point:	PLC_5 [CPU 1212C AC/DC/Rly]	PLC_1 [CPU 1214C AC/DC/Rly]
Interface:	PLC_5, PROFINET interface_1[X1 : PN(LAN)]	PLC_1, PROFINET interface_1[X1 : PN(LAN)]
Subnet:	PN/IE_5	PN/IE_1
Address:	192.168.0.3	192.168.2.2
Connection type:	TCP	
Configuration mode:	Use program blocks	
Connection ID (dec):	1	1
Connection data:	PLC_5_Receive_DB	PLC_1_Send_DB
	○ Active connection establishment	● Active connection establishment

Address details

	Local Port	Partner Port
Port (decimal):	2000	2000

Fig. 17. Procedure for parameterizing the data reception program instruction "TRCV_C"

Fig. 18 shows a simulation model for testing "Open User Communication". The simulation model includes:

- software simulator of server PLC_5 "Instance_2";
- software simulator of terminal PLC_1 "Instance_1";
- software block of data transmission of terminal PLC "TSEND_C";
- software block of data reception of server PLC "TRCV_C";
- communication environment based on technology "Open User Communication".

Terminal PLC_1 and server PLC_5 are launched as separate instances (Instance_1 and Instance_2, respectively) of the PLCSIM V20 software simulator and interact with each other through the program blocks "TSEND_C" and "TRCV_C".

After transferring individual instances of the PLCSIM V20 simulator from the "STOP" mode to the "RUN" mode, the configuration, parameters, and algorithms are simulated based on "Open User Communication" similarly to information processes in real systems (Fig. 19).

Fig. 20, 21 show the results of simulation modeling of terminal PLC_1 and server PLC_5 projects under the "monitor-on" mode.

Analysis of the simulation results indicates the correct functioning of the system as a whole and the consistency of the transmitted and received data formats (except for the DTL (Date and Time Long) format, due to the time offset when copying the corresponding "skreenshorts").

The simulation model also makes it possible to analyze the states of the diagnostic outputs of the sending data "TSEND_C" and receive data "TRCV_C" program instructions. The corresponding states for the "TSEND_C" and "TRCV_C" program instructions under the "Monitoring-on" mode are shown in Fig. 22, 23.

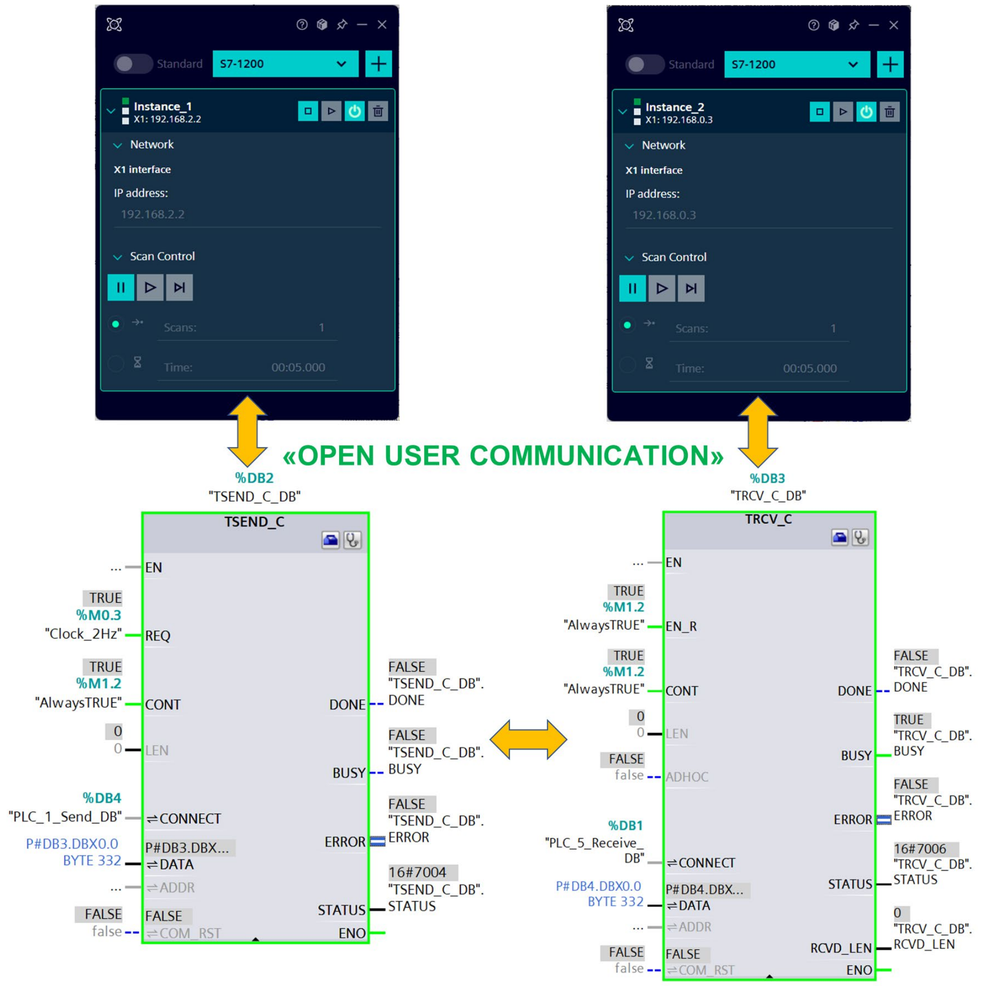
Diagnostic output states of the data transfer program instruction TSEND_C:

- output "DONE" (TRUE: Send job executed without error);
- output "BUSY" (FALSE: Send job not yet started or already completed);
- output "ERROR" (FALSE: No error);
- output "STATUS" (16#0000: Send job was executed without error).

Diagnostic output states of the TRCV_C data reception program instruction:

- output "DONE" (TRUE: Send job executed without error);
- output "BUSY" (FALSE: Send job not yet started or already completed);
- output "ERROR" (FALSE: No error);
- output "STATUS" (16#0000: Send job was executed without error);
- output "RCVD_LEN" (332: Amount of data actually received in bytes).

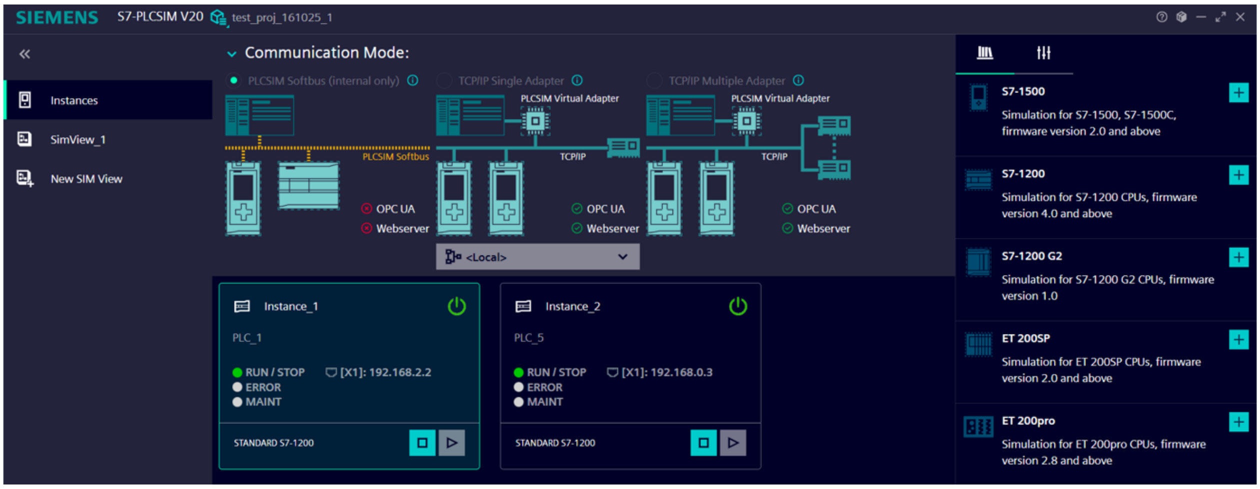
Thus, the operability and correctness of the functioning of the developed topology and data exchange algorithms between the server and terminal PLC based on "Open User Communication" were recorded.



Standard S7-1200
Instance_1 X1: 192.168.2.2
Network
X1 interface
IP address: 192.168.2.2
Scan Control
Scans: 1
Time: 00:05.000

Standard S7-1200
Instance_2 X1: 192.168.0.3
Network
X1 interface
IP address: 192.168.0.3
Scan Control
Scans: 1
Time: 00:05.000

Fig. 18. Simulation model for testing "Open User Communication"



Instance_1
PLC_1
RUN / STOP [X1]: 192.168.2.2
ERROR
MAINT
STANDARD S7-1200

Instance_2
PLC_5
RUN / STOP [X1]: 192.168.0.3
ERROR
MAINT
STANDARD S7-1200

S7-1500 – Simulation for S7-1500, S7-1500C, firmware version 2.0 and above

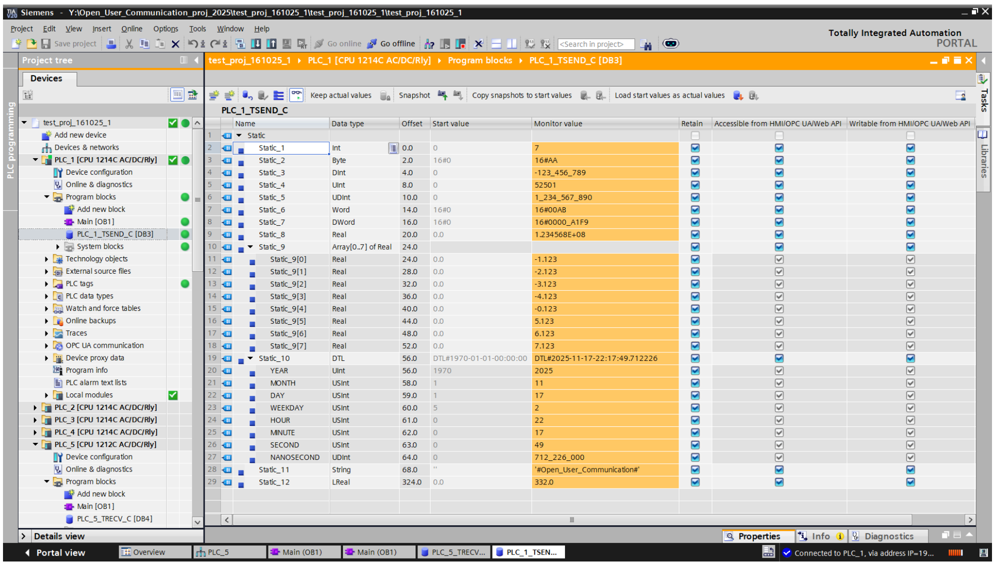
S7-1200 – Simulation for S7-1200 CPUs, firmware version 4.0 and above

S7-1200 G2 – Simulation for S7-1200 G2 CPUs, firmware version 1.0

ET 200SP – Simulation for ET 200SP CPUs, firmware version 2.0 and above

ET 200pro – Simulation for ET 200pro CPUs, firmware version 2.8 and above

Fig. 19. The simulator panel "S7-PLCSIM V20" with instances Programmable Logic Controller "PLC_1" and Programmable Logic Controller "PLC_5" (Instance_1 and Instance_2) under a "RUN" mode

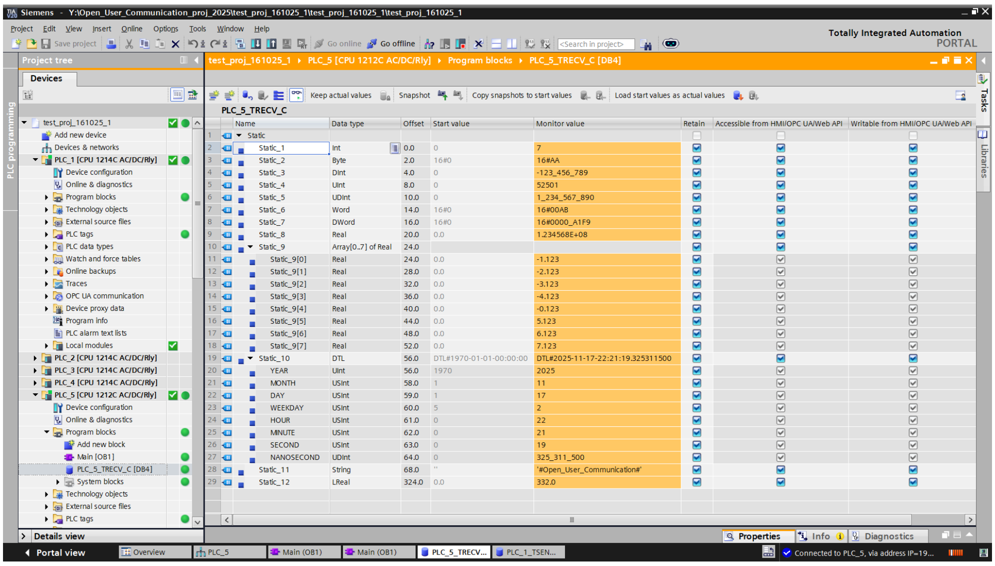

Siemens - Y:\Open_User_Communication_proj_2025\test_proj_161025_1\test_proj_161025_1\test_proj_161025_1
Project Edit View Insert Online Options Tools Window Help
Go online
Go offline
Totally Integrated Automation PORTAL
Project tree
Devices
Keep actual values
Snapshot
Copy snapshots to start values
Load start values as actual values
Details view
Portal view
Overview
PLC_5
Main (OB1)
Main (OB1)
PLC_5_TRECV...
PLC_1_TSEN...
Properties
Info
Diagnostics
Connected to PLC_1, via address IP=19...

test_proj_161025_1 ▸ PLC_1 [CPU 1214C AC/DC/Rly] ▸ Program blocks ▸ PLC_1_TSEND_C [DB3]

PLC_1_TSEND_C

	Name	Data type	Offset	Start value	Monitor value	Retain	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API
1	Static					☐	☐	☐
2	Static_1	Int	0.0	0	7	☑	☑	☑
3	Static_2	Byte	2.0	16#0	16#AA	☑	☑	☑
4	Static_3	DInt	4.0	0	-123_456_789	☑	☑	☑
5	Static_4	UInt	8.0	0	52501	☑	☑	☑
6	Static_5	UDInt	10.0	0	1_234_567_890	☑	☑	☑
7	Static_6	Word	14.0	16#0	16#00AB	☑	☑	☑
8	Static_7	DWord	16.0	16#0	16#0000_A1F9	☑	☑	☑
9	Static_8	Real	20.0	0.0	1.234568E+08	☑	☑	☑
10	Static_9	Array[0..7] of Real	24.0			☑	☑	☑
11	Static_9[0]	Real	24.0	0.0	-1.123	☑	☑	☑
12	Static_9[1]	Real	28.0	0.0	-2.123	☑	☑	☑
13	Static_9[2]	Real	32.0	0.0	-3.123	☑	☑	☑
14	Static_9[3]	Real	36.0	0.0	-4.123	☑	☑	☑
15	Static_9[4]	Real	40.0	0.0	-0.123	☑	☑	☑
16	Static_9[5]	Real	44.0	0.0	5.123	☑	☑	☑
17	Static_9[6]	Real	48.0	0.0	6.123	☑	☑	☑
18	Static_9[7]	Real	52.0	0.0	7.123	☑	☑	☑
19	Static_10	DTL	56.0	DTL#1970-01-01-00:00:00	DTL#2025-11-17-22:17:49.712226	☑	☑	☑
20	YEAR	UInt	56.0	1970	2025	☑	☑	☑
21	MONTH	USInt	58.0	1	11	☑	☑	☑
22	DAY	USInt	59.0	1	17	☑	☑	☑
23	WEEKDAY	USInt	60.0	5	2	☑	☑	☑
24	HOUR	USInt	61.0	0	22	☑	☑	☑
25	MINUTE	USInt	62.0	0	17	☑	☑	☑
26	SECOND	USInt	63.0	0	49	☑	☑	☑
27	NANOSECOND	UDInt	64.0	0	712_226_000	☑	☑	☑
28	Static_11	String	68.0	''	'#Open_User_Communication#'	☑	☑	☑
29	Static_12	LReal	324.0	0.0	332.0	☑	☑	☑

Fig. 20. Result of simulation of the terminal Programmable Logic Controller "PLC_1" under the "Monitoring-on" mode (Data Block for transmission – [DB4])

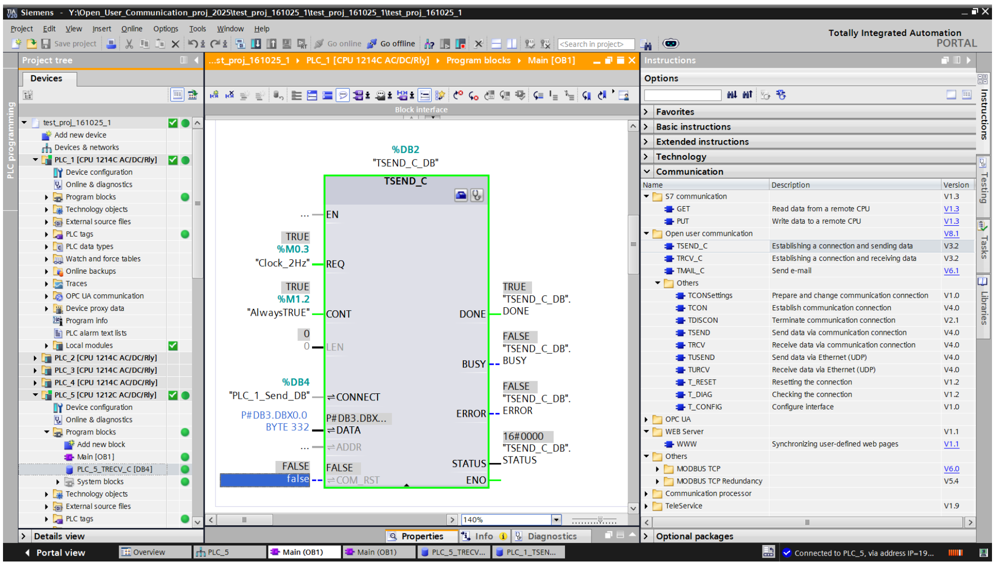

Siemens - Y:\Open_User_Communication_proj_2025\test_proj_161025_1\test_proj_161025_1\test_proj_161025_1
Project Edit View Insert Online Options Tools Window Help
Go online
Go offline
Totally Integrated Automation PORTAL
Project tree
Devices
Keep actual values
Snapshot
Copy snapshots to start values
Load start values as actual values
Details view
Portal view
Overview
PLC_5
Main (OB1)
Main (OB1)
PLC_5_TRECV...
PLC_1_TSEN...
Properties
Info
Diagnostics
Connected to PLC_5, via address IP=19...

test_proj_161025_1 ▸ PLC_5 [CPU 1212C AC/DC/Rly] ▸ Program blocks ▸ PLC_5_TRECV_C [DB4]

PLC_5_TRECV_C

	Name	Data type	Offset	Start value	Monitor value	Retain	Accessible from HMI/OPC UA/Web API	Writable from HMI/OPC UA/Web API
1	Static					☐	☐	☐
2	Static_1	Int	0.0	0	7	☑	☑	☑
3	Static_2	Byte	2.0	16#0	16#AA	☑	☑	☑
4	Static_3	DInt	4.0	0	-123_456_789	☑	☑	☑
5	Static_4	UInt	8.0	0	52501	☑	☑	☑
6	Static_5	UDInt	10.0	0	1_234_567_890	☑	☑	☑
7	Static_6	Word	14.0	16#0	16#00AB	☑	☑	☑
8	Static_7	DWord	16.0	16#0	16#0000_A1F9	☑	☑	☑
9	Static_8	Real	20.0	0.0	1.234568E+08	☑	☑	☑
10	Static_9	Array[0..7] of Real	24.0			☑	☑	☑
11	Static_9[0]	Real	24.0	0.0	-1.123	☑	☑	☑
12	Static_9[1]	Real	28.0	0.0	-2.123	☑	☑	☑
13	Static_9[2]	Real	32.0	0.0	-3.123	☑	☑	☑
14	Static_9[3]	Real	36.0	0.0	-4.123	☑	☑	☑
15	Static_9[4]	Real	40.0	0.0	-0.123	☑	☑	☑
16	Static_9[5]	Real	44.0	0.0	5.123	☑	☑	☑
17	Static_9[6]	Real	48.0	0.0	6.123	☑	☑	☑
18	Static_9[7]	Real	52.0	0.0	7.123	☑	☑	☑
19	Static_10	DTL	56.0	DTL#1970-01-01-00:00:00	DTL#2025-11-17-22:21:19.325311500	☑	☑	☑
20	YEAR	UInt	56.0	1970	2025	☑	☑	☑
21	MONTH	USInt	58.0	1	11	☑	☑	☑
22	DAY	USInt	59.0	1	17	☑	☑	☑
23	WEEKDAY	USInt	60.0	5	2	☑	☑	☑
24	HOUR	USInt	61.0	0	22	☑	☑	☑
25	MINUTE	USInt	62.0	0	21	☑	☑	☑
26	SECOND	USInt	63.0	0	19	☑	☑	☑
27	NANOSECOND	UDInt	64.0	0	325_311_500	☑	☑	☑
28	Static_11	String	68.0	''	'#Open_User_Communication#'	☑	☑	☑
29	Static_12	LReal	324.0	0.0	332.0	☑	☑	☑

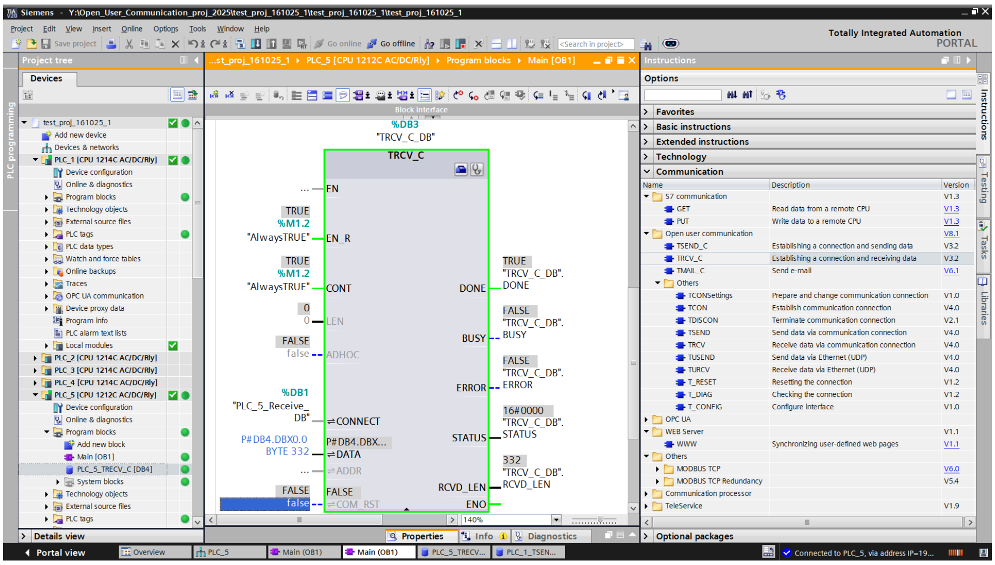
Fig. 21. Result of simulation of the server Programmable Logic Controller "PLC_5" under the "Monitoring-on" mode (Data Block for reception – [DB3])



Name	Description	Version
S7 communication		V1.3
GET	Read data from a remote CPU	V1.3
PUT	Write data to a remote CPU	V1.3
Open user communication		V8.1
TSEND_C	Establishing a connection and sending data	V3.2
TRCV_C	Establishing a connection and receiving data	V3.2
TMAIL_C	Send e-mail	V6.1
Others		
TCONSettings	Prepare and change communication connection	V1.0
TCON	Establish communication connection	V4.0
TDISCON	Terminate communication connection	V2.1
TSEND	Send data via communication connection	V4.0
TRCV	Receive data via communication connection	V4.0
TUSEND	Send data via Ethernet (UDP)	V4.0
TURCV	Receive data via Ethernet (UDP)	V4.0
T_RESET	Resetting the connection	V1.2
T_DIAG	Checking the connection	V1.2
T_CONFIG	Configure interface	V1.0
OPC UA		
WEB Server		V1.1
WWW	Synchronizing user-defined web pages	V1.1
Others		
MODBUS TCP		V6.0
MODBUS TCP Redundancy		V5.4
Communication processor		
TeleService		V1.9

Connected to PLC_5, via address IP=19...

Fig. 22. Diagnostic output states of the sending data program instruction "TSEND_C" under the "Monitoring-on" mode



Name	Description	Version
S7 communication		V1.3
GET	Read data from a remote CPU	V1.3
PUT	Write data to a remote CPU	V1.3
Open user communication		V8.1
TSEND_C	Establishing a connection and sending data	V3.2
TRCV_C	Establishing a connection and receiving data	V3.2
TMAIL_C	Send e-mail	V6.1
Others		
TCONSettings	Prepare and change communication connection	V1.0
TCON	Establish communication connection	V4.0
TDISCON	Terminate communication connection	V2.1
TSEND	Send data via communication connection	V4.0
TRCV	Receive data via communication connection	V4.0
TUSEND	Send data via Ethernet (UDP)	V4.0
TURCV	Receive data via Ethernet (UDP)	V4.0
T_RESET	Resetting the connection	V1.2
T_DIAG	Checking the connection	V1.2
T_CONFIG	Configure interface	V1.0
OPC UA		
WEB Server		V1.1
WWW	Synchronizing user-defined web pages	V1.1
Others		
MODBUS TCP		V6.0
MODBUS TCP Redundancy		V5.4
Communication processor		
TeleService		V1.9

Connected to PLC_5, via address IP=19...

Fig. 23. Diagnostic output states of the receiving data program instruction "TRCV_C" under a "monitoring-on" mode

5. 4. Testing solutions under industrial conditions for WEB-oriented data collection systems from technological facilities

Based on the proposed topology, simulation modeling results and "Open User Communication", a WEB-oriented automated data collection system from technological facilities of water supply at municipal enterprises was developed and tested under industrial conditions.

The system makes it possible to organize local and central dispatching points and operates in real time.

The subsystem for monitoring house cold water flow meters monitors and documents water consumption in apartment buildings.

The automated system includes the following components:

– PC-Server server workstation;

– Simatic S7-1200 server PLC with GSM LTE industrial router;

– Simatic S7-1200 terminal PLCs with GSM LTE industrial routers;

– communication equipment (SCALANCE X208 Ethernet switches);

– SCADA (WinCC Professional).

The system performs tasks of collecting, primary processing, transmitting, and storing technological parameters in accordance with the operating algorithm and production regulations.

The system operates with water flow meters with pulse output from different manufacturers. Pulse outputs of flow meters form groups of up to 128 in a radius of up to 1200 m and are combined on terminal PLCs.

The communication network between the server and terminal PLCs is organized on the basis of VPN (Virtual Private Network) of the mobile operator "Kyivstar" of the GSM LTE standard and is protected from unauthorized access.

Fig. 24 shows the current parameters of an industrial router based on the 4G module "QUECTEL EC25" (Quectel Wireless Solutions, China):

– GRE L2 tunnel (gre1) – the tunnel encapsulation protocol provides the possibility of simultaneous data exchange between the server and terminal PLCs based on "Open User Communication" and servicing terminal PLCs via "S7 Communication";

– Local Network (lan) – local network parameters ("Status", "Type", "Address", "Uptime", "MAC", "Rx/Tx");

– Mobile Internet (sim1) – mobile 4G network parameters (including indication of "Signal quality" and "Rx/Tx" traffic);

– Routing table – provides static and dynamic data transmission routes.

For the controller and workstation, application software has been developed that adapts to the equipment configuration of a specific facility. The dispatcher's dialog with the system is implemented in the form of mnemonics in SCADA [25]. Archiving and documentation of technological parameters are provided.

The system provides the ability to control additional technological parameters (level, pressure, temperature, etc.), as well as control actuators (electric pumps, electric shut-off valves, lighting subsystems, signaling, etc.).

In the dispatcher interface, when activating the house number, a mnemonic diagram of the parameters of the corresponding cold water flow meter "SENSUS" WP Dynamic 50/50 (as of 12/25/2017) is displayed (Fig. 25).

The mnemonic diagram of the parameters of the activated flow meter includes the following data:

– current (instantaneous flow);

– hourly flow (from 0 to 23 hours);

– daily flow (for 24 hours);

– total flow (corresponds to the flow meter reading);

– monthly flow (for one year);

– graphical representation of water flow (by 4 parameters):

– current flow (blue trend and scale);

– daily flow (green trend and scale);

– monthly flow (purple trend and scale);

– total flow (red trend and scale).

The system archives 4 graphic parameters for a given period (for example, for 1 year).

The WEB-oriented automated data collection system from technological water supply facilities (Municipal Enterprise – "TLUMACH" Water Supply) has been modernized and expanded (as of November 15, 2025) (Fig. 26, 27).

Fig. 25 shows a schematic diagram of the level control and calculated volume of water in tanks from the technological water supply facility (Municipal Enterprise – "TLUMACH" Water Supply) as of 11/15/2025.

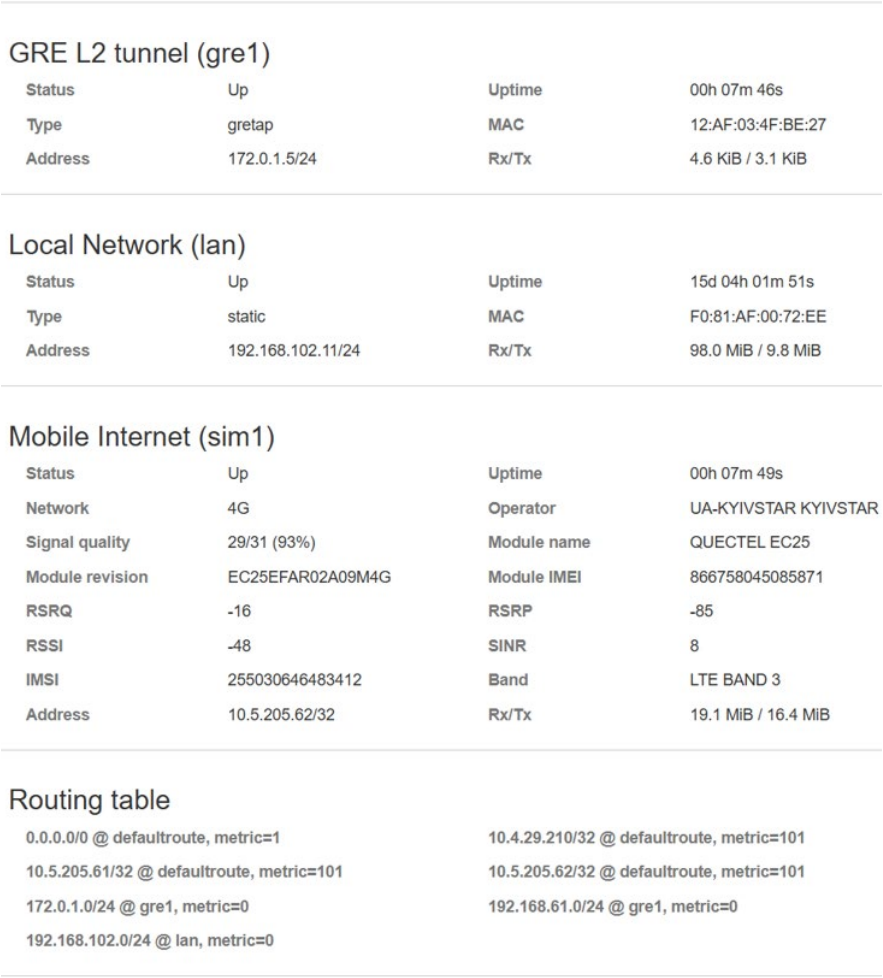
Graphical representation of the level and calculated volume of water in tanks (No. 1, 2) (Fig. 27):

– archives of water level (m) in tanks No. 1, 2 (blue trend and scale);

– current value of water level (m) in tanks No. 1, 2 with dynamic color indication (according to defined markers of the lower and upper water levels);

– current calculated value of water volume (m^3) in tanks No. 1, 2.

Thus, positive experience has been gained in designing, testing, servicing, and supporting WEB-oriented automated data collection systems from technological objects based on "Open User Communication" and modern unified hardware and software.



GRE L2 tunnel (gre1)

Status	Up	Uptime	00h 07m 46s
Type	gretap	MAC	12:AF:03:4F:BE:27
Address	172.0.1.5/24	Rx/Tx	4.6 KiB / 3.1 KiB

Local Network (lan)

Status	Up	Uptime	15d 04h 01m 51s
Type	static	MAC	F0:81:AF:00:72:EE
Address	192.168.102.11/24	Rx/Tx	98.0 MiB / 9.8 MiB

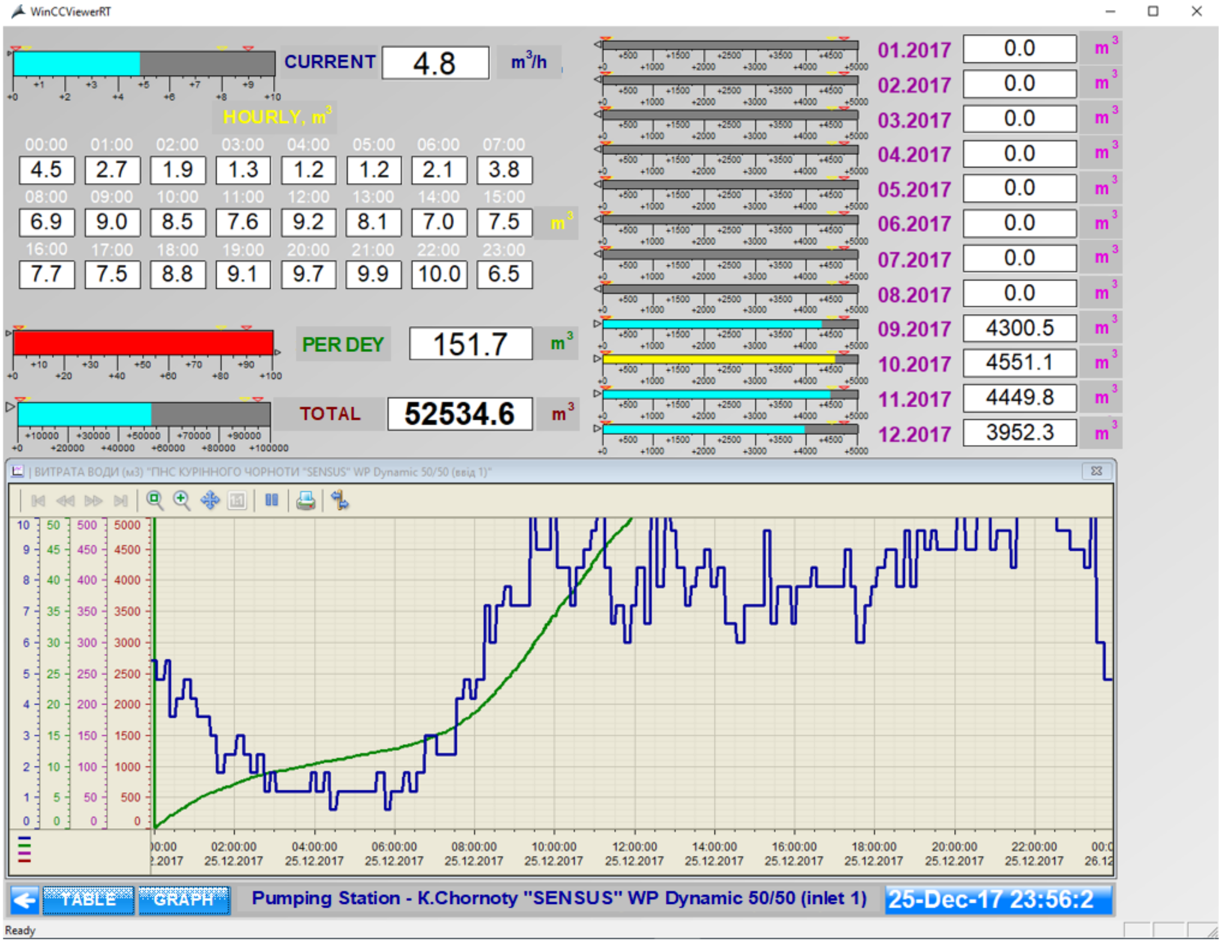
Mobile Internet (sim1)

Status	Up	Uptime	00h 07m 49s
Network	4G	Operator	UA-KYIVSTAR KYIVSTAR
Signal quality	29/31 (93%)	Module name	QUECTEL EC25
Module revision	EC25EFAR02A09M4G	Module IMEI	866758045085871
RSRQ	-16	RSRP	-85
RSSI	-48	SINR	8
IMSI	255030646483412	Band	LTE BAND 3
Address	10.5.205.62/32	Rx/Tx	19.1 MiB / 16.4 MiB

Routing table

0.0.0.0/0 @ defaultroute, metric=1	10.4.29.210/32 @ defaultroute, metric=101
10.5.205.61/32 @ defaultroute, metric=101	10.5.205.62/32 @ defaultroute, metric=101
172.0.1.0/24 @ gre1, metric=0	192.168.61.0/24 @ gre1, metric=0
192.168.102.0/24 @ lan, metric=0	

Fig. 24. Current parameters of the industrial router based on the 4G module "QUECTEL EC25"



WinCCViewerRT

CURRENT 4.8 m³/h

HOURLY, m³

00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00
4.5	2.7	1.9	1.3	1.2	1.2	2.1	3.8
08:00	**09:00**	**10:00**	**11:00**	**12:00**	**13:00**	**14:00**	**15:00**
6.9	9.0	8.5	7.6	9.2	8.1	7.0	7.5
16:00	**17:00**	**18:00**	**19:00**	**20:00**	**21:00**	**22:00**	**23:00**
7.7	7.5	8.8	9.1	9.7	9.9	10.0	6.5

PER DEY 151.7 m³

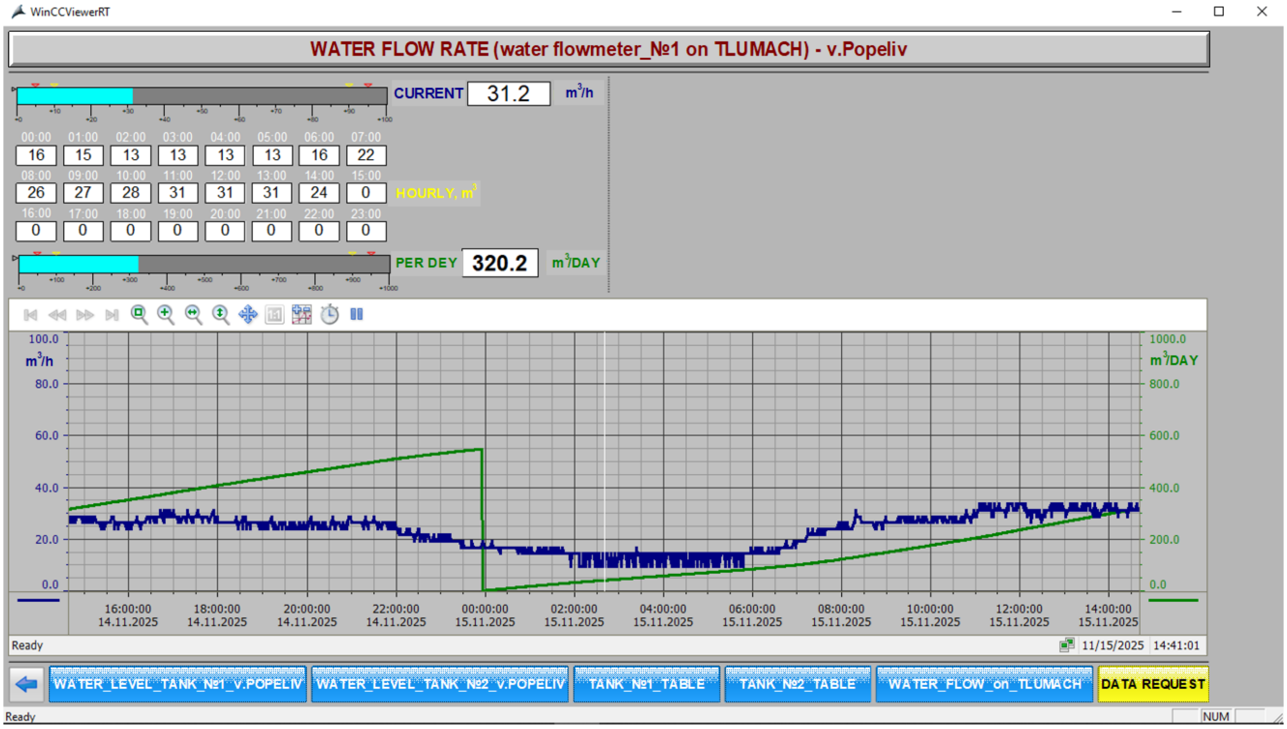
TOTAL 52534.6 m³

01.2017	0.0	m³
02.2017	0.0	m³
03.2017	0.0	m³
04.2017	0.0	m³
05.2017	0.0	m³
06.2017	0.0	m³
07.2017	0.0	m³
08.2017	0.0	m³
09.2017	4300.5	m³
10.2017	4551.1	m³
11.2017	4449.8	m³
12.2017	3952.3	m³

TABLE GRAPH Pumping Station - K.Chornoty "SENSUS" WP Dynamic 50/50 (inlet 1) 25-Dec-17 23:56:2

Ready

Fig. 25. Mnemonic diagram of parameters of the cold water flow meter "SENSUS" WP Dynamic 50/50 as of 12/25/2017



WinCCViewerRT

WATER FLOW RATE (water flowmeter_№1 on TLUMACH) - v.Popeliv

CURRENT 31.2 m³/h

HOURLY, m³

00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00
16	15	13	13	13	13	16	22
08:00	**09:00**	**10:00**	**11:00**	**12:00**	**13:00**	**14:00**	**15:00**
26	27	28	31	31	31	24	0
16:00	**17:00**	**18:00**	**19:00**	**20:00**	**21:00**	**22:00**	**23:00**
0	0	0	0	0	0	0	0

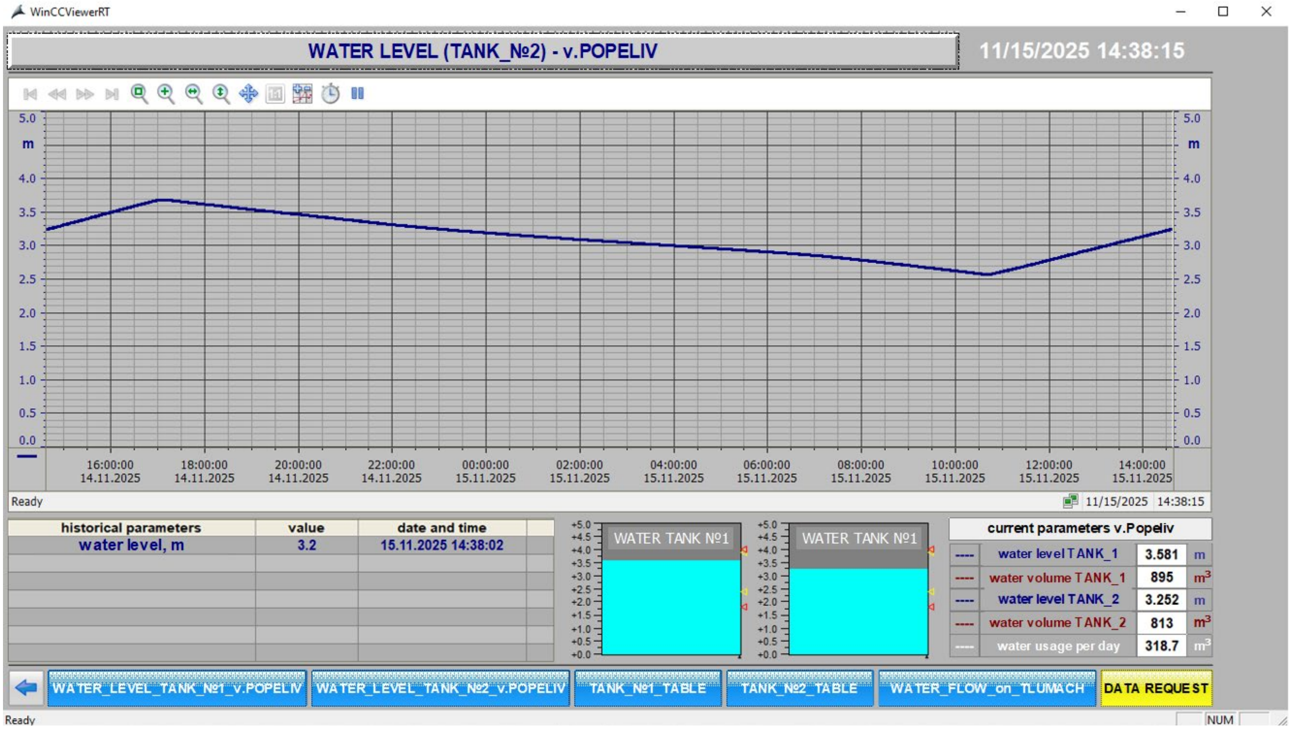
PER DEY 320.2 m³/DAY

Ready 11/15/2025 14:41:01

WATER_LEVEL_TANK_№1_v.POPELIV WATER_LEVEL_TANK_№2_v.POPELIV TANK_№1_TABLE TANK_№2_TABLE WATER_FLOW_on_TLUMACH DATA REQUEST

Ready NUM

Fig. 26. Mnemonic diagram of parameters of flowmeter No. 1 from the technological object of water supply (Municipal Enterprise — "TLUMACH" Water Supply) as of 11/15/2025



historical parameters	value	date and time
water level, m	3.2	15.11.2025 14:38:02

current parameters v.Popeliv			
----	water level TANK_1	3.581	m
----	water volume TANK_1	895	m³
----	water level TANK_2	3.252	m
----	water volume TANK_2	813	m³
----	water usage per day	318.7	m³

Fig. 27. Mnemonic diagram of level control parameters and calculated volume of water in tanks from a technological water supply facility (Municipal Enterprise – "TLUMACH" Water Supply) as of 11/15/2025

6. Discussion of the results of integration of "Open User Communication" in the topology of WEB-oriented automated control systems

The main result of our work is designing and testing under industrial conditions of a WEB-oriented automated data collection system from technological objects with integrated "Open User Communication" based on the proposed client-server topology (Fig. 2). A feature of the developed system is the presence of a server PLC on the SCADA side and terminal PLCs with "Open User Communication" functionality.

The use of such a topology has additional advantages and solves the following engineering and technical tasks:

– the developer has the ability to determine the structure and format of data for exchange between control system components based on TCP, UDP, ISO-on-TCP protocols;

– the ability to organize cyclic and acyclic (on request) communication;

– the ability to organize communication between different PLC manufacturers;

– the ability to transmit custom (non-standard) data packets;

– the ability to devise your own industrial communication protocols;

– the ability to transmit data by events (event-based), and not cyclically;

– optimization of the load on the communication network and PLC due to a smaller number of transactions, compared to cyclic (polling) requests from SCADA;

– scaling of PLC and data volume without changing the communication mechanism (with insignificant loss of performance) compared to direct communication with SCADA;

– data consistency and state synchronization (simultaneity of formation, transmission and processing) due to packet transmission in one frame.

The developed topology of the WEB-oriented control and data collection system based on "Open User Communication" complements and expands the functionality of the IIoT described in [4–6] at the level of topologies, algorithms, models, and unified hardware and software. In addition, the implemented procedure of "tunneling" of communication protocols by encapsulation over VPN additionally increases the protection of the TO ACS components from unauthorized access and cyberattacks at the communication level.

In [7, 8], emphasis is on the problems associated with disruption of control processes, production stops, personnel safety violations, etc., which are a consequence of improper integration and interaction of TO ACS components. The methods for eliminating such critical consequences are the comprehensive use of proven technologies and unified hardware and software and communication protocols from world manufacturers. To solve the above-mentioned problems, the TIA Portal was used in the work, which made it possible to organize in one environment (Fig. 3, 4, 6, 7) compatible hardware and software tools Simatic S7 (Siemens, Germany), including communication components [15–19]. At the same time, the problem of interaction from the levels of sensors, actuators, RTU/PLC to the levels of the communication environment, SCADA and IT was comprehensively solved.

In [9], the OPC UA protocol is considered, which is a standard for industrial communication and provides interaction between equipment from different manufacturers, but is a separate product and requires additional resources for integration and administration. The integration of "Open User Communication" in the topology of the TO ACS makes it possible to solve the specified problem due to direct communication between the server and terminal PLCs without an additional software add-on.

According to the results of research [10, 11], the problems in the direction of data processing at the terminal level "Edge

Computing" were identified. With this approach, data processing is performed as close as possible to the data source – on local RTUs/PLCs. Thus, the current tasks that need to be solved are the tasks of modeling and testing information processes in the TO ACS at the PLC level, which perform data processing and support communications.

For simulation modeling tasks, a global data block PLC_5_TRCV_C [DB4] was created to store data received from the data block PLC_1_TSEND_C [DB3] of one of the terminal PLC_1 [CPU1214C AC/DC/Rly] (Fig. 13). Communication program instructions "TSEND_C" and "TRCV_C" with support for "Open user communication" and state diagnostics (Fig. 18) [21] were used.

The terminal PLC_1 and server PLC_5 projects are recorded in separate instances (Instance_1 and Instance_2, respectively) of the PLCSIM V20 simulator and simulation modeling based on "Open User Communication" was performed (Fig. 19) [20]. When performing simulation modeling, the "Monitoring-on" mode was activated to visualize the modes of operation of the "Open User Communication" communication algorithm (Fig. 22, 23). The consistency of the transmitted and received data from the terminal to the server PLC was recorded in the "Monitoring-on" mode (Fig. 20, 21) [23]. In the work, based on th e proposed topology, the results of simulation modeling and "Open User Communication", a WEB-oriented automated data collection system from technological objects of water supply of municipal enterprises was developed and tested under industrial conditions [24]. This, in comparison with study [12], solves the problem of technical validation for testing solutions on real production processes.

The communication network between the server and terminal PLCs of the system is organized on the basis of the VPN of the mobile operator "Kyivstar" of the GSM 4G standard with the parameters shown in Fig. 24. The GRE L2 tunnel protocol is organized, which provides simultaneous data exchange between the server and terminal PLCs based on "Open User Communication" and servicing of terminal PLCs via "S7 Communication" (Fig. 24).

The dialog of the dispatcher with the system is implemented in the form of mnemonics in SCADA and provides archiving and documentation of technological parameters of the data collection system (Fig. 25–27) [25].

Positive experience has been gained in designing, testing, servicing, and supporting WEB-oriented automated data collection systems from technological objects based on modern unified hardware and software tools and information technologies.

The limitations of the study include the single-channel unidirectional mode of operation of the simulation model, which for other topological configurations can be scaled within certain limits.

The disadvantages of the work include undefined quantitative indicators of communication traffic with "Open User Communication" in the event-based data exchange mode, compared to the cyclic data request mode from the SCADA side.

The study can be continued to build new improved simulation models with extended functionality and WEB-oriented TO ACSs for maintenance under special operating conditions.

7. Conclusions

1. A topology of the TO ACS with extended functionality based on SCADA, server and terminal PLCs and integration of the "Open User Communication" technology has been designed. The peculiarity and distinctive properties of the proposed topology are the presence of a separate server PLC and integrated into the "Open User Communication" topology for asynchronous communication (based on events) compared to cyclic requests from SCADA. At the same time, data consistency is ensured due to packet transmission in one frame and the ability to choose the structure, different types and formats of data for communication between TO ACS components.

2. A data collection system based on "Open User Communication" has been designed in the TIA Portal toolkit based on Simatic S7 hardware and software. During the development process, hardware configuration and parameterization, communication environment setup, and application software development in the FBD language of the IEC 61131-3 standard were performed. The communication program instructions "TSEND_C" and "TRCV_C" have been parameterized, through which "Open User Communication" directly functions. The specific syntax "P#DB3.DBX0.0 BYTE 332" at the "DATA" inputs of the communication program instructions allowed dynamic data sampling with different starting addresses and different volumes (for PLC S7-1200 up to 8192 bytes).

3. A simulation model has been built for testing information processes of interaction between the server and terminal PLC based on "Open User Communication", the peculiarity of which is that it can use configuration data, parameters, and algorithms directly from the development environment and, accordingly, be as close as possible to information processes in real TO ACS. Based on the simulation model built, "Open User Communication" testing was performed and the states of the diagnostic outputs of the TSEND_C and TRCV_C program blocks under the "Monitoring-on" mode were analyzed. The correctness of the simulation model functioning and the consistency of the data exchange process based on "Open User Communication" were recorded.

4. The designed system was implemented at a water supply utility based on the proposed topology with integrated "Open User Communication". The following technological parameters are monitored at the terminal level and transmitted to the server: current water flow, hourly water flow, daily water flow, water level and volume in tanks (0–5 m, and 1000 m^3, respectively), from which archives lasting 1 year are formed in SCADA.

Parameterization of the tunnel GRE protocol over VPN ensured simultaneous data exchange between the server and terminal PLCs based on "Open User Communication" and programming of terminal PLCs via "S7 Communication". A feature of our system is optimized traffic at the level of 1 GB per month for a corporate data transfer package based on the 4G standard from the mobile operator "Kyivstar".

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available, either in numerical or graphical form, in the main text of the manuscript.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

Acknowledgments

The authors are grateful to the Subsidiary Enterprise with 100% Foreign Investment "Siemens Ukraine" for the support provided within the framework of agreement No. 01-01/KTSU-08 dated February 22, 2008, on cooperation with the Ivano-Frankivsk National Technical University of Oil and Gas (based on agreement No. 81102477 dated May 16, 2005, between SE "Siemens Ukraine" and the German Society for Technical Cooperation (GTZ)).

Authors' contributions

Leonid Zamikhovskyi: Conceptualization, Methodology, Validation, Writing – review & editing, Project Administration; **Mykola Nykolaychuk**: Methodology, Software, Validation, Formal analysis, Writing – original draft; **Ivan Levitskyi**: Methodology, Software, Validation, Writing – original draft, Visualization.

References

1. Basics of Open User Communication: S7-1200, S7-1500, S7-1500T (TIA Portal V20) (2024). Siemens. Available at: https://docs.tia.siemens.cloud/r/en-us/v20/editing-devices-and-networks/configure-networks/communication-via-connections/working-with-connections/using-open-user-communication-s7-1200-s7-1500-s7-1500t/basics-of-open-user-communication-s7-1200-s7-1500-s7-1500t
2. Products for Totally Integrated Automation: Catalog ST 70 (Catalog No. E86060-K4770-A101-C2-7600) (2025). Siemens. Available at: https://support.industry.siemens.com/cs/attachments/109744167/simatic-st70-complete-english-2025_1.pdf
3. Reyes Domínguez, D., Infante Abreu, M. B., Parv, A. L. (2024). Main Trend Topics on Industry 4.0 in the Manufacturing Sector: A Bibliometric Review. Applied Sciences, 14 (15), 6450. https://doi.org/10.3390/app14156450
4. Villar, E., Martín Toral, I., Calvo, I., Barambones, O., Fernández-Bustamante, P. (2024). Architectures for Industrial AIoT Applications. Sensors, 24 (15), 4929. https://doi.org/10.3390/s24154929
5. Alsabbagh, W., Langendöerfer, P. (2022). A New Injection Threat on S7-1500 PLCs – Disrupting the Physical Process Offline. IEEE Open Journal of the Industrial Electronics Society, 3, 146–162. https://doi.org/10.1109/ojies.2022.3151528
6. Gautam, M. K., Pati, A., Mishra, S. K., Appasani, B., Kabalci, E., Bizon, N., Thounthong, P. (2021). A Comprehensive Review of the Evolution of Networked Control System Technology and Its Future Potentials. Sustainability, 13 (5), 2962. https://doi.org/10.3390/su13052962
7. Yadav, G., Paul, K. (2021). Architecture and security of SCADA systems: A review. International Journal of Critical Infrastructure Protection, 34, 100433. https://doi.org/10.1016/j.ijcip.2021.100433
8. Schäffer, E., Penczek, L. N., Bartelt, M., Brossog, M., Kuhlenkötter, B., Franke, J. (2021). A Microservice- and AutomationML-based Reference Architecture for an Engineering Configurator Web Platform. Procedia CIRP, 103, 274–279. https://doi.org/10.1016/j.procir.2021.10.044
9. Busboom, A. (2024). Automated generation of OPC UA information models – A review and outlook. Journal of Industrial Information Integration, 39, 100602. https://doi.org/10.1016/j.jii.2024.100602
10. Tusa, F., Clayman, S., Buzachis, A., Fazio, M. (2024). Microservices and serverless functions-lifecycle, performance, and resource utilisation of edge based real-time IoT analytics. Future Generation Computer Systems, 155, 204–218. https://doi.org/10.1016/j.future.2024.02.006
11. Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., Abdildayeva, A. (2025). An Edge-Computing-Based Integrated Framework for Network Traffic Analysis and Intrusion Detection to Enhance Cyber-Physical System Security in Industrial IoT. Sensors, 25 (8), 2395. https://doi.org/10.3390/s25082395
12. Ji, T., Xu, X. (2025). Exploring the Integration of cloud manufacturing and cyber-physical systems in the era of industry 4.0 – An OPC UA approach. Robotics and Computer-Integrated Manufacturing, 93, 102927. https://doi.org/10.1016/j.rcim.2024.102927
13. Nazarenko, I. V., Nikolaychuk, M. Ya., Ferenets, V. D., Sukhanov, D. Ye. (2014). Construction and modeling of unified control systems of actuating mechanisms for objects of gas-transport system. Eastern-European Journal of Enterprise Technologies, 1 (2 (67)), 41–48. https://doi.org/10.15587/1729-4061.2014.21204
14. Zamikhovskiy, L., Levytskyi, I., Nykolaychuk, M. (2021). Designing a system that removes metallic inclusions from bulk raw materials on the belt conveyor. Eastern-European Journal of Enterprise Technologies, 3 (2 (111)), 79–87. https://doi.org/10.15587/1729-4061.2021.234235
15. S7-1200 Programmable controller: System manual (V4.7, A5E02486680-AQ) (2024). Siemens. Available at: https://support.industry.siemens.com/cs/document/109977302/s7-1200-programmable-controller?dti=0&lc=en-US
16. SCALANCE X-200: Operating instructions (BA_SCALANCE-X-200_76) (2024). Siemens. Available at: https://cache.industry.siemens.com/dl/files/056/109955056/att_1266072/v1/BA_SCALANCE-X-200-2023_76_en-US.pdf
17. SIMATIC NET S7-1200 telecontrol / SIMATIC CP 1243-7 LTE (2025). Siemens. Available at: https://support.industry.siemens.com/cs/document/109995459/simatic-net-s7-1200-telecontrol-simatic-cp-1243-7-lte?dti=0&lc=en-US
18. Industrial Ethernet / PROFINET: Networking manual. System Manual, 07, C79000-G8900-C242 (Doc. No. SYH_IE-Net_76) (2019). Siemens. Available at: https://support.industry.siemens.com/cs/attachments/27069465/SYH_IE-Net_76.pdf

19. SIMATIC STEP 7 Basic/Professional V20 and SIMATIC WinCC V20 (2024). Siemens. Available at: https://support.industry.siemens.com/cs/document/109977280/simatic-step-7-basic-professional-v20-und-simatic-wincc-v20?dti=0&lc=en-US
20. S7-PLCSIM online help (Version 21, Doc. No. A5E46238743-AJ) (2025). Siemens. Available at: https://support.industry.siemens.com/cs/document/109997161/s7-plcsim-online-help
21. Basic examples for Open User Communication (OUC): ISO-on-TCP, TCP, UDP (2021). Siemens. Available at: https://support.industry.siemens.com/cs/document/109747710/basic-examples-for-open-user-communication-%28ouc%29?lc=en-cy
22. S7-1500 / S7-1500T motion control overview: Function manual (Version 7.0, Doc. No. A5E03879256-AH) (2022). Siemens. Available at: https://support.industry.siemens.com/cs/attachments/109812056/s71500_s71500t_motion_control_overview_function_manual_en-US_en-US.pdf
23. Open User Communication with TSEND_C and TRCV_C: SIMATIC S7-1200 CPU (Version 2.1) (2018). Siemens. https://support.industry.siemens.com/cs/attachments/67196808/net_s7-1200_isoontcp_en.pdf
24. Zamikhovskyi, L., Nykolaychuk, M., Levytskyi, I. (2024). Organizing the automated system of dispatch control over pump units at water pumping stations. Eastern-European Journal of Enterprise Technologies, 5 (2 (131)), 61–75. https://doi.org/10.15587/1729-4061.2024.313531
25. Zamikhovskyi, L., Zamikhovska, O., Ivanyuk, N., Mirzoieva, O., Nykolaychuk, M. (2025). Development of an anti-surge protection system for gas pumping units based on hardware and software vibration monitoring tools. Eastern-European Journal of Enterprise Technologies, 4 (2 (136)), 117–132. https://doi.org/10.15587/1729-4061.2025.337736