International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-15 Issue-1, December 2025

Analysis of ISO on TCP, UDP, PROFINET IO, and S7 Communication Protocols

Monika Rybczak, Andrzej Januszewski

***Abstract**: This article is based on an analysis of communication protocols used in industrial solutions. It presents a brief description of Ethernet communication protocols, specifically ISO on TCP (described as a mechanism that enables ISO applications to be ported to the TCP/IP network), UDP (User Datagram Protocol), Profinet IO, and S7-connection. Based on these characteristics, four industrial network models were configured, and individual protocols were implemented in the controller. The publication presents several Ethernet protocols that were configured on Siemens S7-1200 family controllers in the TIA Portal environment. The purpose of this publication is to present and analyse commonly used industrial Ethernet networks. The possibility of data exchange between individual controllers has been verified, with relevant instructions provided. Detailed differences between the industrial networks in question have been highlighted. Profinet IO is the most versatile network in terms of control process selection, integration with other networks, and ease of configuration. On the other hand, the cheapest solution is to choose the S7-connection protocol. In addition, the authors presented the types of instructions introduced for bit and byte exchange, such as TCON, TSEND, PUT, and TDISCON. Chapter 4 provides a descriptive analysis of the advantages and disadvantages of the communication protocols discussed, as well as a table summarising the topology and integration of each protocol. There are many different protocols to choose from in industrial automation. It should be noted that the selection of individual devices depends not only on data transfer speed but also on hardware and software configuration. After analysis, the authors pointed out that the choice is often driven by selecting an easier data exchange application.*

***Keywords**: Transmission Protocols, ISO on TCP, S7-Connection, Profinet IO, S7-1200.*

Nomenclature:
IT: Information Technology
IP: Internet Protocol
TSAP: Transport Service Access Point

I. INTRODUCTION

Automation manufacturers make extensive use of TCP (Transport Control Protocol), ISO on TCP, and UDP (User Datagram Protocol), which are generally available and free of charge and are commonly used in Internet networks. Protocols [1]. Based on them, they have created their own applications to facilitate the configuration of Ethernet module communication. Increasing automation, quality control requirements, global coordination, and the management of factories working together to manufacture a single product are driving the rapid development of industrial Ethernet networks [2], [3]. The standardisation of communication at the production level, using existing technical infrastructure for management and monitoring, is becoming the norm. The connection of the industrial network to the office or even corporate network enabled simpler, more reliable, and cheaper remote access to the former, which quickly proved a great convenience for production planning, resource management, and faster response times in the event of problems requiring specialist intervention. Configuration options, diagnostics, and remote service were expanded. The development of today's automation is primarily driven by information technology (IT) and the standards adopted within it, such as TCP/IP.

The trend mentioned above has led to an increase in the amount of data transmitted and the number of devices exchanging data via Ethernet networks, as well as in the number of communication protocols supporting industrial Ethernet networks [4],[5].

Major automation manufacturers and their associations are trying to create or co-create and promote their own network communication, primarily to meet the requirements of network determinism, i.e., to guarantee a minimum, constant time for information to reach from one network user to another. Different solutions have significant impacts on network properties, including performance, stability, integration with other networks, and security. The paper focuses on industrial network communication solutions, including a controller from the Siemens family.

II. ETHERNET NETWORK

The publication presents several Ethernet protocols configured on Siemens S7-1200 controllers in the TIA Portal environment. Below is a brief presentation of the individual configurations of the ISO on TCP, Profinet IO, S7 connection, and UDP protocols [6].

A. Characteristics of the ISO on the TCP protocol

The TCP protocol uses the Internet Protocol (IP), which is why it is often referred to as the "TCP/IP protocol." It is in layer 4 of the ISO-OSI reference model. Despite the use of various upgrades to meet the requirements of network determinism, all of them fall within the scope of the standards describing this technology. Mutual parameterization of communication at the sender and receiver is required. The advantage of the ISO transport protocol is

Manuscript received on 01 December 2025 | First Revised Manuscript received on 04 December 2025 | Second Revised Manuscript received on 07 December 2025 | Manuscript Accepted on 15 December 2025 | Manuscript published on 30 December 2025.

*Correspondence Author(s)
Monika Rybczak*, Department of Autonomous Systems, Gdynia Maritime University, Gdynia, Poland. Email ID: m.rybczak@wi.umg.edu.pl, ORCID ID: 0000-0002-8518-865X
Andrzej Januszewski, Department of Faculty of Computer Science, Gdynia Maritime University, Gdynia, Poland. Email ID: a.januszewski@we.umg.edu.pl

packet-oriented data transmission. However, as the number of networks increased, the lack of routing functionality became a growing disadvantage. As the routing-compatible TCP/IP protocol became dominant due to the Internet, an attempt was made to combine the advantages of both protocols. The ISO on TCP protocol is a mechanism that allows ISO applications to be introduced into TCP/IP networks. Therefore, the ISO on the TCP protocol is connection-oriented but transmits data in packets, allowing data to be transported as messages. Data packets reach the recipient in the same form in which they were sent from the sender. It should be added that in the RFC1006 (Request for Comments) extension, also known as ISO on TCP, the image of the ISO transport protocol properties is defined in the TCP protocol.

B. Characteristics of the UDP Protocol

Unlike TCP, UDP transmission remains packet-oriented, i.e., each data packet is sent separately without confirmation of receipt. When recovering from a timeout and reinitialising the connection, UDP is preferable to TCP for time-critical connections. Data blocking and connection control in UDP for applications can be done via RPC (Remote Procedure Call). The UDP protocol was introduced for fast and simple data transfer. It is located in the transport layer (layer 4) of the ISO-OSI reference model. It uses the IP layer (layer 3) for addressing. Only minimal administrative information is added to the transmitted data packet, resulting in higher data throughput than TCP and ISO over TCP. The UDP protocol eliminates the security mechanisms found in TCP and ISO TCP protocols. The UDP protocol is connectionless and meets real-time requirements, but it is unreliable because there is no guarantee of correct data transfer.

C. Characteristics of the Profinet IO Communication Protocol

In industrial automation, the basic function of an industrial network is to transmit data between a PLC controller and input/output modules [7], [8]. Each Profinet device, regardless of manufacturer, can be integrated into the project by importing a GSDML file that describes the device into the engineering software. This makes it possible to set up communication between the IO Controller device (e.g., a PLC) and the IO Devices (e.g., a distributed I/O station). Input and output signals are exchanged between the controller and the IO Device as cyclic data – the controller sets the refresh time, which can be individual for each device. Profinet IO is used to connect distributed I/O devices directly via an Industrial Ethernet network. Using TIA Portal or STEP 7 tools, IO Device devices – distributed input/output islands – are connected to a central controller – the IO Controller. Each Profinet device is uniquely identified by:

i. MAC address (factory set)
ii. IP address
iii. Device name

A number is automatically added to the device name. For Siemens devices, this is done programmatically by selecting the Generate PROFINET device name automatically option.

D. Characteristics of the S7 Communication Protocol - Connection

This protocol is used only in Siemens controllers. PLC network communication via an Ethernet connection in accordance with the S7 Connection protocol requires hardware and communication configuration of at least one network node [9]. It works based on the IP addresses of individual devices connected to the network and the TSAP (Transport Service Access Point) access point, specified in both ASCII and hexadecimal. TSAP addresses characterize the connection and location of the communication module on the controller bus.

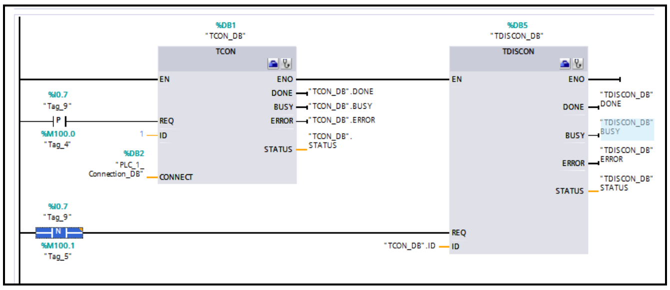
III. HARDWARE CONFIGURATION OF PROTOCOLS

A. PLC Configuration in the ISO on TCP Model

The ISO protocol for TCP is located in layer 4 of the ISO-OSI reference model and defines port 102 as the default port for data transmission. The ISO-on-TCP communication protocol enables data exchange between two applications. Higher-layer applications are addressed via TSAPs (similar to port numbers in a TCP connection) [9], [10].

Addressing is based on MAC and TSAP addresses. Different TSAP pairs are used for each connection between communicating partners. Thanks to these parameters, the connection between two stations is uniquely defined. TSAPs are between 2 and 16 bytes long. TSAP addresses characterize the connection and the location of the communication module on the controller bus. The first two digits indicate the connection number, starting with 10. The last two digits indicate the module's location in the controller. Using TSAP (Transport Service Access Point) access points, the TCP protocol allows multiple connections to be established with a single IP address (up to 64k connections).

For Open User Communications protocols, the manufacturer provides separate blocks for configuring TCON and TDISCON. When using these instructions, a single connection can be used for both sending and receiving data [Fig. 1].



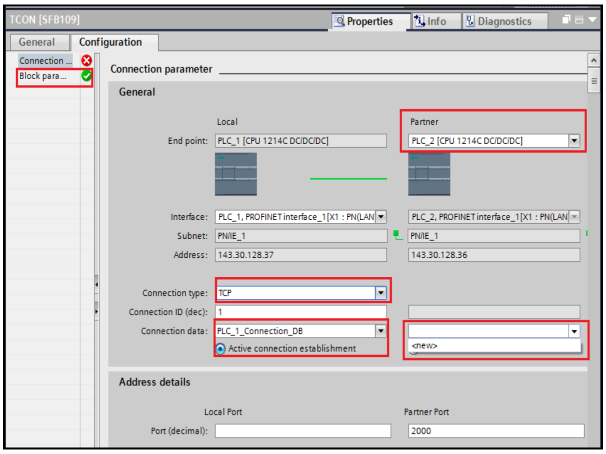
[Fig.1: Data Exchange Instructions in the ISO on TCP Protocol TCON and TDISCON]

TCON is a connection establishment instruction triggered by a rising edge on the REQ input [Fig. 2]. TDISCON instruction – applies to communication disconnection. These are universal blocks in terms of their properties. In the Connection tab, you need to specify the partner, protocol type, and block that supports this instruction. After selecting the connection type, the following appear in the window: the detailed address and additional parameters

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-15 Issue-1, December 2025

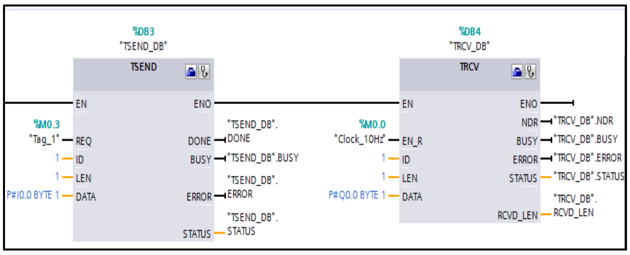
describing the network's properties. Memory for communication and diagnostic data control is allocated in the Block Parameter tab. Communication is not configured in the TDICON instruction; you must specify the number of the connection that you want to disconnect and that you have declared in the TCON block. The remaining parameters are completed in the same way as in the TCON block.



[Fig.2: ISO on TCP Protocol Configuration]

B. PLC Configuration in the UDP Model

Given the need for fast data transfer, the UDP protocol provides only basic functionality and does not require network feedback [11]. The TUSEND and TURCV instructions are used to declare data exchange. Note that the TSEND and TRCV commands are executed asynchronously via the REQ or EN_R input. [Fig.3]. The transmission process is performed by the positive edge of the REQ signal; TRCV block readiness is not required because the data is buffered. This data can be received later upon permission (EN_R=1 setting).

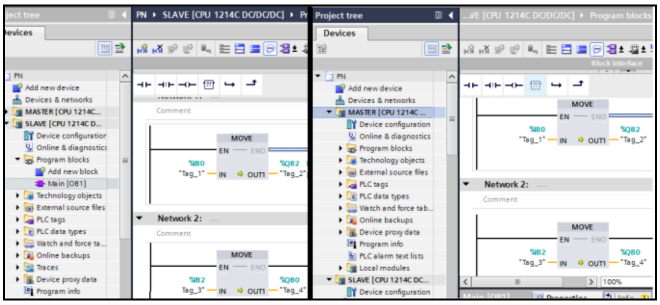


[Fig.3: Data Exchange Instructions in the UDP Protocol TSEND and TRCV]

C. PLC Configuration in the PROFINET IO Model

Profinet IO is used for direct connection of distributed IO devices via an Industrial Ethernet network. Using TIA Portal or STEP 7 tools, IO devices – distributed islands of inputs and outputs – are connected to a central controller, the IO Controller.

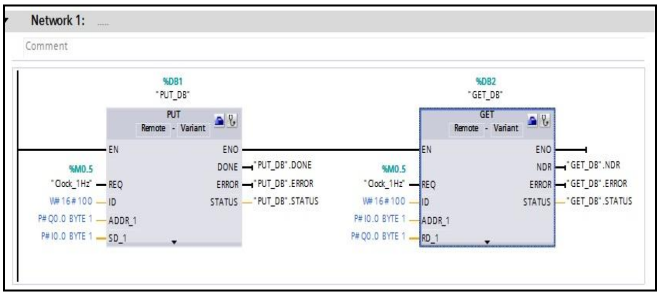
For Profinet IO configuration, all communication is configured in the IO Controller in the Network view of the new project. After configuring the controller in the project, the remaining IO devices and their input/output modules are placed in the Network view configuration editing window. Next, the Ethernet modules of all devices are configured, i.e., unique IP addresses and a standard subnet mask are assigned. The name and Profinet addresses of distributed stations should also be added. Devices operating in the Profinet IO standard in the TIA Portal environment from manufacturers other than Siemens have library files that can be imported using the GSD extension [Fig. 4]. A number is automatically added to the device name. For Siemens devices, this is done programmatically: select the option to automatically generate the PROFINET device name. For other manufacturers of IO devices, switches for entering the station number (1-127) are provided on the housing; the option for automatic name assignment should then be unchecked.



[Fig.4: Profinet IO Protocol Instructions, MOVE Instructions]

D. PLC Configuration in the S7-Connection Model

The protocol mentioned is an internal standard proposed by Siemens. An Ethernet connection is configured on the controller, and the program contains instructions to activate communication. Communication modules integrated in the PLC have the number 02. For communication nodes with unknown hardware configuration, declared as "Unspecified," the TSAP value is assumed to be 03.00. Dedicated data transfer instructions (GET/PUT) have also been created [Fig. 4]. When entering the properties of the PUT instruction, communication is configured on the Connection parameter tab, and the area for sent data is on the Block Parameter tab. When transferring data, you can use absolute addresses such as IB0, QW0, MD10, or symbolic addresses. After connecting to the partner's network in the Network View tab, the communication configuration is carried out almost automatically; all you need to do is select the partner in the instructions. In the case of the data reception block – GET, the procedure is similar. You need to declare the communication partner, then the bit that triggers the instruction, the connection number, the area read from the partner's memory, and where it is to be saved. On the right side of the block, you assign a memory address to the diagnostic parameters.



[Fig.5: Data Exchange Instructions in the S7-Connection PUT and GET Protocol]

Note!

In S71200 controllers, versions above V4, the

GET/PUT instruction must be enabled manually in the controller hardware. This is done via the "Device configuration" option in the "Properties" tab, "Protection" level. In older versions, this option is not available, and the blocks are permanently active.

IV. RESULT AND DISCUSSION

According to the author, it appears that TCP is the protocol most commonly used by various manufacturers to build their applications. It is used to transfer large data packets. It integrates easily with office networks and the Internet. It has excellent diagnostic properties; each data packet is checked for correctness and monitored to ensure correct transmission. If the station does not confirm receipt, the packets are sent again. Due to the transmission of fixed-length data and the combination of data packets, it is not suitable for controlling fast or cyclical processes. The protocol itself does not provide time determinism. In industry, however, it is very often used to collect and transfer production data, to communicate and transfer data between controllers or panels, and to connect to the office network.

Compared with TCP, UDP is a simpler and less efficient protocol. Addressing is based on port numbers. UDP is a protocol that provides fast data exchange without security measures to detect datagram loss and incorrect datagram order. Data transfer is packet-oriented, which makes it much faster. It is suitable for use in control processes requiring a response time of 10 ms.

The ISO on TCP protocol combines the advantages of both protocols, but is limited to devices from a single manufacturer, Siemens.

The same applies to the S7 protocol, but its advantage over the protocols above is the ease of configuring the communication interface. It is based on the client/server communication model. This means that after configuring the device ports to operate in a single network, communication configuration is performed only on the client side, and the client decides when the data exchange should take place. It ensures network determinism.

The most versatile and best-performing protocol is Profinet. It includes various communication configuration options available depending on the requirements of the production process. Thanks to a modernised frame with a controlled time slot in the Layer 2 protocol and partner synchronisation, it can transmit data in a cycle of less than 1 ms and with deviations of less than 1 µs. This requires the use of special switching circuits in the switch. Profinet also uses the master/slave method for establishing communication. Generally speaking, its telegram has a higher priority than TCP and UDP and higher signal security. This is defined in the IEEE 802.1Q standard, while the PCP (Priority Code Point) field is described in the Ethernet frame header. This ensures that the data reaches the correct recipient within an acceptable time frame. It therefore maintains time determinism, is suitable for drive control and large data transfer, and has excellent diagnostic properties. Additional advantages include the communication interface, ease of configuration, and integration with other industrial networks (Table I).

When cooperation between controllers is necessary, standard TCP, ISO TCP, or UDP protocols can be used to exchange data. With the development of Profinet in controllers from the S7-1500, S7-1200, and S7-300 families, starting with version v4.0, it became possible to share the functionality of the IO Controller and IO Device. This functionality is called an I Device (Intelligent CPU as an I/O Device). In this case, data exchange between controllers boils down to a configuration similar to that of peripheral devices.

Table I: Analysis of the Topology and Integration of Individual Communication Protocols

Model	ISO-on-TCP	UDP	Profinet IO	S7-Connection
Topology	Bus; tree; star; ring	Bus;	Redundancy Bus; tree; star; ring	Redundancy Bus; tree; star; ring
Integration with third-party networks	Can be used primarily in homogeneous SIMATIC structures	Flexible, can be implemen ted with third-part y systems	Flexible, can be implemente d with other manufacture rs' systems	It can mainly be used in homogeneo us SIMATIC structures
Instructions	TCON, TDISCON,	TSEN_C, TRCV_C	Built-in instructions (MOVE)	GET, PUT
Network expansion	A separate configuration of the connection with the partner and the data exchange area is required.	A separate configurat ion of the connectio n with the partner and the data exchange area is required.	Connection configuratio n: Data exchange takes place automaticall y	Connection and PLC memory area exchange area configuratio n required

V. CONCLUSION

The ability to select protocols for specific tasks, integrate network devices from different manufacturers, and provide remote service is becoming a challenge for automation engineers and an increasingly essential skill.

This publication aimed to present and compare commonly used industrial Ethernet networks and detail the differences among them. Profinet IO is the most universal network in terms of selection for control processes, integration with other networks, and ease of configuration. There are two levels of improvement available in the Profinet layer. Optimised (in terms of performance) data exchange is called Real-Time communication and is used to exchange standard process data between the PLC controller and the Inputs/Outputs device. The second level is deterministic, time-synchronized IRT communication. A good example of this type of performance management is process data, such as electrical motor variables (current, voltage, power, etc.), which, when processed in real time by the controller, are not considered the most crucial element. However, safety-critical functions, such as emergency shutdown, which must be performed very quickly, will be transmitted using the IRT protocol. Major automation manufacturers and their associations are trying to create or co-create and promote their own network communication, primarily to meet the requirements of network determinism, i.e., to guarantee a minimum, constant time for information to reach from one network user to another. Different solutions have significant impacts on network properties, including

Retrieval Number: 100.1/ijitee.B120615020126
DOI: 10.35940/ijitee.B1206.15011225
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

performance, stability, integration with other networks, and security.

APPENDIX

It is optional. Appendices, if any, appear before the acknowledgement.

ACKNOWLEDGMENT

This research was funded as part of a research project in the Faculty of Computer Science, Gdynia Maritime University, Poland, No. WI/2025/PI/01.

DECLARATION STATEMENT

Authors of review-type articles are required to include a declaration of accountability in the article that stipulates each author's involvement. The level of detail differs; Some subjects yield articles that consist of isolated efforts that are easily voiced in detail, while other areas function as group efforts at all stages. It should be after the conclusion and before the references.

As the article's author, I must verify the accuracy of the following information after aggregating input from all authors.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and without external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. IEC 61158 standard: https://webstore.iec.ch/publication/59890 - accessed on 20.05.2019
2. Bartoň, Martin, et al. "Industry Communication Based on TCP/IP Protocol." Vedecké Práce Materiálovotechnologickej Fakulty Slovenskej Technickej Univerzity v Bratislave so Sídlom v Trnave 29.49 (2021): 59-66. DOI: http://doi.org/10.2478/rput-2021-0025
3. Folgado, F. J., Calderón, D., González, I., Calderón, A. J. (2024). Review of Industry 4.0 from the perspective of automation and supervision systems: Definitions, architectures and recent trends. Electronics, 13(4), 782. DOI: https://doi.org/10.3390/electronics13040782
4. Bansal, R., Dubey, A. K. (2024). Communication protocols used for industrial automation. In Computational Intelligence in the Industry 4.0 (pp. 73-94). CRC Press. DOI: https://doi.org/10.1201/9781003479031
5. Shaikh, M., Shah, P., Sekhar, R. (2023, September). Communication Protocols in Industry 4.0. In 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET) (pp. 709-714). IEEE. https://ieeexplore.ieee.org/document/10303397
6. Hartley W.," Siemens Basic PLC programming S7-1200 TIA Portal v17",2022, ISBN-13:979-8355257743
7. Yun-Hai, C., Dong-Ying, Z., Ji, J., & Chen, X. (2023, August). Design of PROFINET I/O Real-time Communication System between PLC Based on S7-1200. In Journal of Physics: Conference Series (Vol. 2569, No. 1, p. 012013). IOP Publishing. DOI: http://doi.org/10.1088/1742-6596/2569/1/012013
8. Rybczak, M., Radzimski, D., Popowniak, N. (2021). Watertight Door Control System on A Ship using Profinet IO. International Journal of Innovative Technology and Exploring Engineering, 10, 84-89. DOI: https://doi.org/10.35940/ijitee.K9469.09101121
9. Elizabeth, S. J., Wilson, S. O., Rolando, S. P., & Stalin, M. C. (2024, January). Distributed systems and communication protocols connected to the Internet of Things (IoT). In International Conference on Information Technology and Systems (pp. 446-456). Cham: Springer Nature Switzerland. DOI: http://doi.org/10.15866/ireaco.v12i5.17687
10. Environment Siemens TIA Portal, Availed: ttps://www.siemens.com/nl/nl/products/automation/systems/industrial/plc/s7-1200.html
11. Mahmoodi Khaniabadi, S., Javadpour, A., Gheisari, M., Zhang, W., Liu, Y., Sangaiah, A. K. (2023). An intelligent, sustainable, efficient transmission internet protocol to switch between User Datagram Protocol and Transmission Control Protocol in IoT computing. Expert Systems, 40(5), e13129. DOI: https://doi.org/10.1111/exsy.13129

AUTHOR'S PROFILE

Monika Rybczak is a graduate of the Faculty of Electrical Engineering at the Gdynia Maritime University, majoring in Computer Control Systems. She obtained her doctoral degree in 2016. She was the deputy head of the Department of Ship Automation at the Faculty of Electrical Engineering of the Maritime University of Gdynia from 2020 to 2024 and is currently employed in the Department of Systems and Autonomous at the Faculty of Computer Science. Conducts research in the field of autonomous systems. The study focuses on absolute ship control using linear matrix inequalities and reinforcement learning. A second research area is the performance analysis of control algorithms based on artificial intelligence and Industry 4.0.

Andrzej Januszewski has been working at Gdynia Maritime University for thirty years. He deals with issues related to Industry 4.0, including industrial networks and programmable controllers, such as the Siemens S7-300, S7-1200, and S7-1500 families.