Journal of Scientific Perspectives

Volume **4,** Issue **2,** Year **2020**, pp. **99-110**
E - ISSN: **2587-3008**
URL: https://ratingacademy.com.tr/ojs/index.php/jsp
DOİ: https://doi.org/10.26900/jsp.4.008
Research Article

TEACHING AND LEARNING OF INDUSTRIAL CYBER SECURITY TECHNOLOGIES BASED ON PHOENIX CONTACT COMPANY WIRELESS EQUIPMENT

Vladlen SHAPO* & Maksym LEVINSKYI** & Valeriy VOLOVSHCHYKOV***

** NatIonal UnIversIty "Odessa MarItIme Academy",*
UKRAINE, e-maIl: vladlen.shapo@gmaIl.com
ORCID: https://orcid.org/0000-0002-3921-4159

*** NatIonal UnIversIty "Odessa MarItIme Academy",*
UKRAINE, e-maIl: maxlevInskyI@gmaIl.com
ORCID: https://orcid.org/0000-0002-6544-5110

**** National Technical University "Kharkiv Polytechnic Institute",*
UKRAINE, e-maIl: valvol98@gmail.com
ORCID: https://orcid.org/0000-0003-4454-2314

ReceIved: 6 January 2020, Accepted: 29 April 2020

ABSTRACT

Nowadays occurs a jump in approaches to maritime technical systems developing with implementation of Industry 4.0, IIoT, Shipping 4.0 concepts. Progress in wireless technologies allows to perform absolutely new engineering tasks. Maritime branch realizes digital transformation steps, which envisage creation of unmanned, autonomous and remote controlled ships. But such systems are vulnerable for external malicious intrusion. Thus it's necessary to deepen information technologies learning in maritime education in the following directions: IIoT, industrial wired and wireless data transfer technologies and hardware; satellite systems; big data, artificial intelligence, virtual and augmented reality; remote control; cyber security technologies. National University "Odessa Maritime Academy" participates in Trainings in Automation Technologies for Ukraine project. Obtained mobile equipment allows to study PcWorx and CoDeSys software for automation systems development (based on PLCs) and Profibus, ProfiNet, EtherCAT and wireless technologies. This base equipment may be supplemented by security firewalls.

Ways of modern technologies implementing in maritime branch are analyzed. Directions of deep studying are shown. Actuality and possibilities of cyber security technologies studying are highlighted. Approaches and technologies, successfully realized in education process and planned for future, are described.

***Keywords**: Industry 4.0, IIoT, Shipping 4.0, digital transformation, e-learning, industrial cyber security.*

1. CONTEXT

Nowadays took place true jump in approaches to developing, control and exploitation of complex technical systems in maritime field with implementation of Industry 4.0, IIoT, Shipping 4.0, Ports 4.0 concepts. Thanks to progress in wireless and satellite technologies and mass appearance of embedded computer systems it's became possible to perform absolutely new engineering tasks and to create fully unmanned ships. Thus Unmanned Cargo Ship Development Alliance, Advanced Autonomous Waterborne Applications Initiative autonomous ship research project, Maritime Autonomous Surface Ships direction, Distributed Intelligent Vessel Components software, Digital, Internet, Materials & Engineering Co-Creation technical ecosystem, One Sea Ecosystem Alliance, Safer Vessel with Autonomous Navigation project are created. Currently maritime branch realizes digital transformation steps, which envisage creation of unmanned, autonomous and remote controlled ships by 2025 - 2035. But such complex systems are very vulnerable for external malicious intrusion. As a result huge financial losses, accidents and technological catastrophes are possible and already happened.

2. PURPOSE

Thus, on one side it's necessary to improve and deepen information technologies learning in maritime education institutions in the following directions: IIoT, industrial data transfer technologies, networks and protocols; wireless data transfer technologies; wide class computer control systems hardware; satellite data transfer systems, technologies and protocols; big data, artificial intellect, virtual and augmented reality technologies; remote control technologies and protocols; English language learning enhancement in general and IT terms particularly. On the other side, it's necessary to learn cyber security aspects, technologies and protocols. For realization of both these tasks it's necessary to use specific hardware facilities and e-learning technologies.

3. APPROACH

Theory of Automatic Control and Computing Machinery (TACCM) department of National University "Odessa Maritime Academy" (NUOMA) participates in EduNet (Education Network) program from 2011 (this program has unlimited duration) and participated in TATU (Trainings in Automation Technologies for Ukraine) project in 2013-2017. Formally TATU project had to last till December 2016 but because of unexpected bureaucratic problems at shipping of equipment from European Union to Ukraine was extended to the June 2017. Goals and some obtained results of TATU project are described in paper [1]. During TATU project realization learning books [2-4] in English and Russian languages are created by efforts of TACCM department of NUOMA collaborators, which have taken part in TATU project [2, 3], including participants from European and another Ukrainian universities [4]. Some specificities of maritime engineers education and training are touched on in papers [5, 6]. Some ways of enhancement of English language studying for maritime engineers are considered in paper [7]. Existing EduNet and TATU equipment allows to study the following software and technologies.

1. PcWorx (developer is Phoenix Contact company) and CODESYS (manufacturer independent software, developer is 3S-Smart Software Solutions company) are complex software integrated development environments (IDE) for development of automation and control systems based on programmable logic controllers.
2. Profibus, Profinet, EtherCAT and some another technologies/protocols.
3. Wireless data transfer technologies: IEEE 802.11 b/g/n and GSM standards.

During TATU project TACCM department of NUOMA obtained 4 sets of TATU Smart Lab (TSL) equipment. This is a flexibly configurable mobile set of devices for teaching modern automation technologies. It contains devices from Phoenix Contact, Siemens and Berghof manufacturers and was developed within the framework of Industry 4.0 (the fourth stage of industrial revolution). There are 3 hardware modules (independent portable boxes) in each TSL set: Profibus hardware module (HM), Profinet HM and EtherCAT and Process Modeling HM. Appearance and internal structure of Profibus HM presented in Figures 1, 2 accordingly.

Fig. 1. Appearance of TSL PROFIBUS hardware module

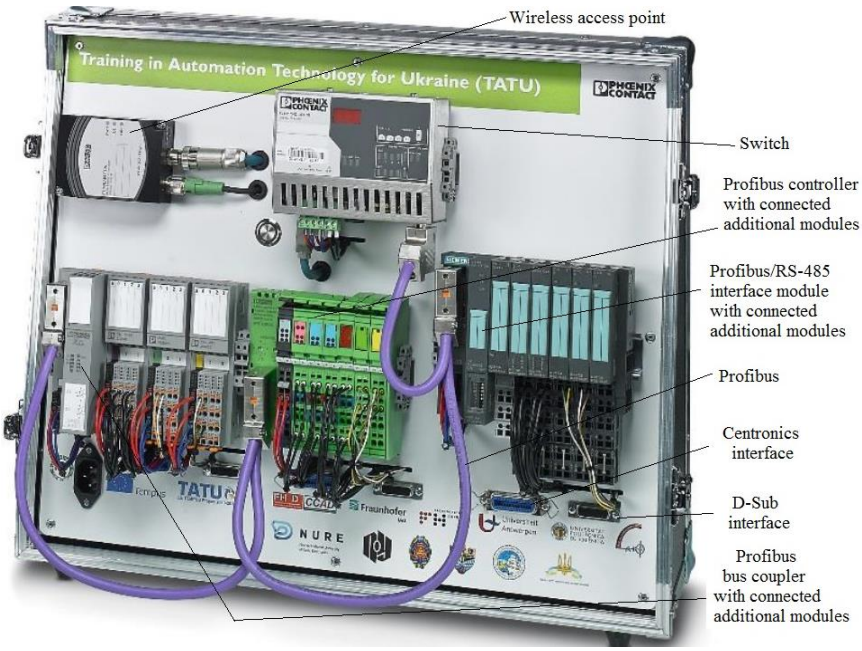
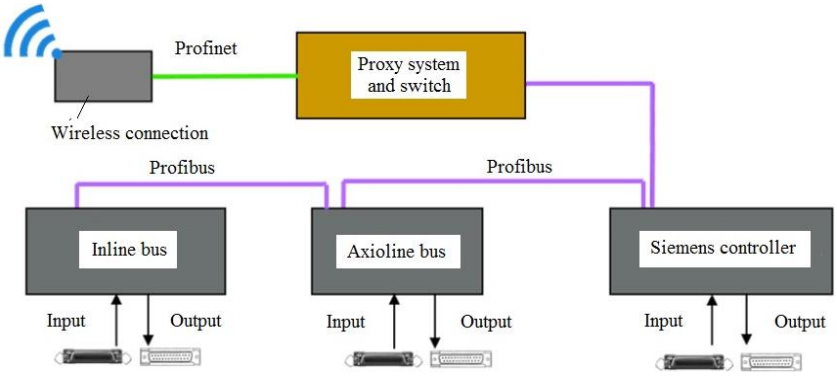


Fig. 2. Internal structure and external connections in TSL PROFIBUS hardware module



Profibus technology was created in 1989. At present time about 12.3 millions Profibus devices are installed (near 20% of the total quantity) in different automation systems [8]. Increasing of Profibus devices number is quite stable (for example, 0.8 million in 2018, but less than in 2017). In general it's possible to say that Profibus protocol/technology step by step will become relatively obsolete for strategic development and big projects, but will be used many years in future to realize compatibility between different generations of devices, appliances and equipment. That's why it's necessary to study this technology mainly for maintenance of installed devices and systems. But for future development it's recommended to shift attention to modern protocols/technologies where addressing is based on IP addresses and devices may

be reached using IP network directly without any additional proxy system like Profinet and EtherCAT which are also supported in TSL equipment.

In the same time about 26 millions Profinet devices are working in different industrial automation systems nowadays. More than 5.1 million devices were added in different projects in 2018 (12 % more than in 2017). Appearance and internal structure of Profinet hardware module presented in Figures 3, 4 accordingly.

Fig. 3. Appearance of TSL PROFINET hardware module

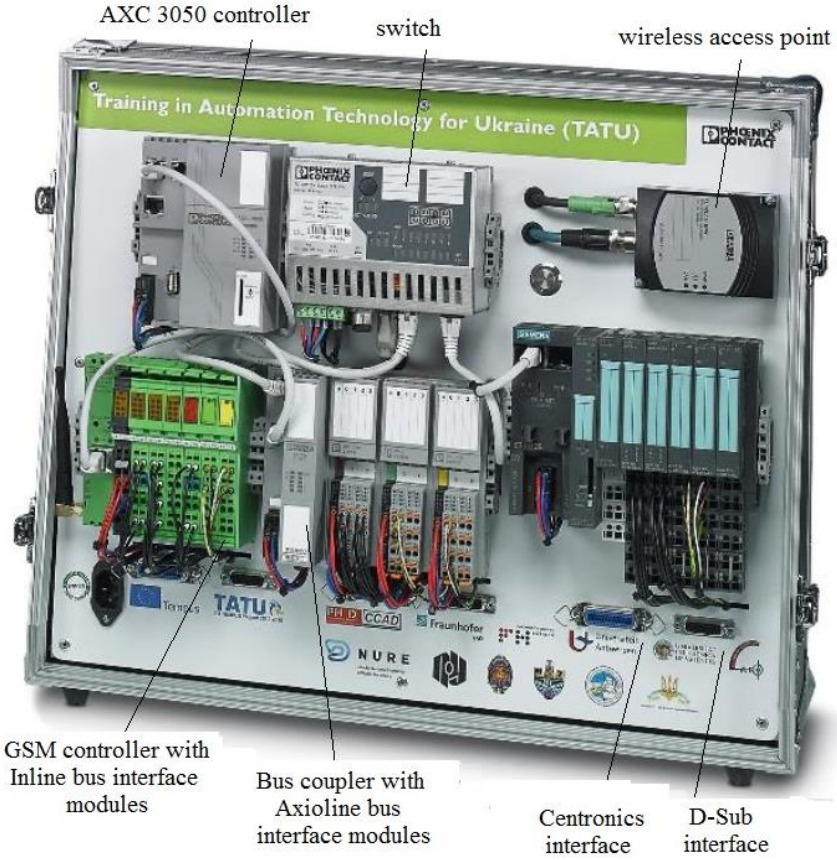
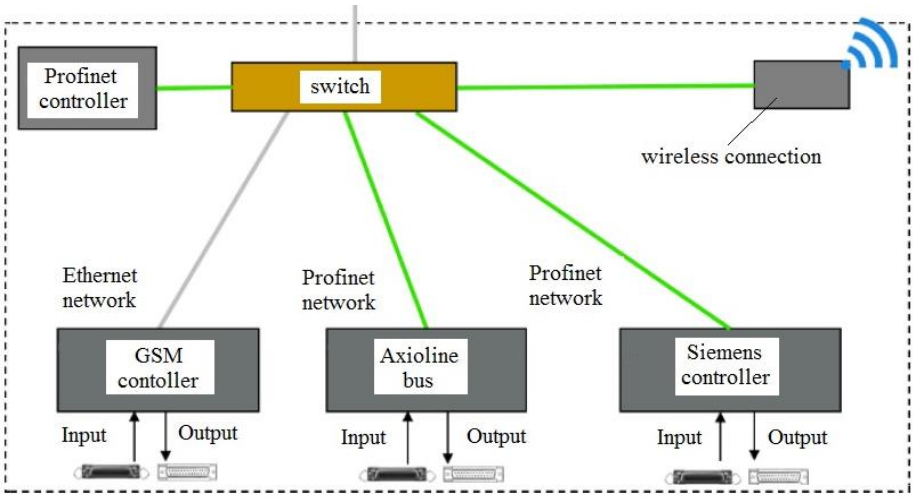
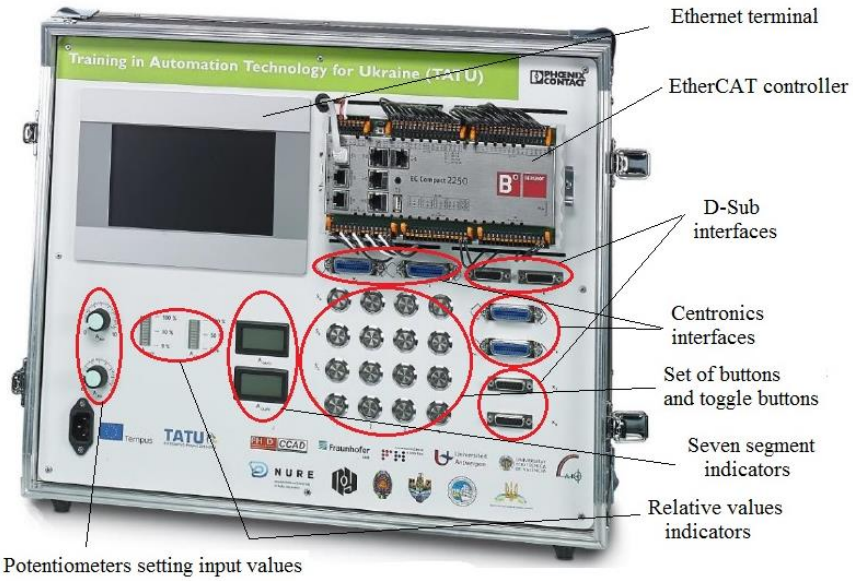


Fig. 4. Internal structure and external connections in TSL PROFINET hardware module



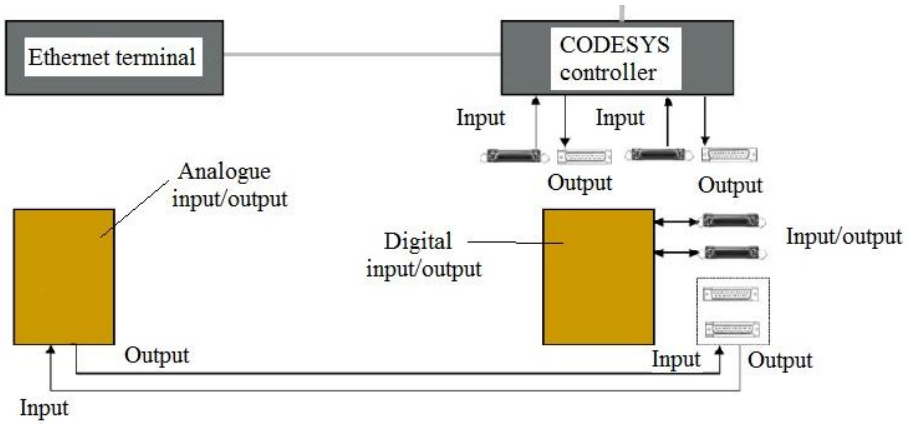
Appearance and internal structure of EtherCAT and Process Modeling HM presented in Figures 5, 6 accordingly. The third HM (Figure 5) is intended for modeling of technological processes. Models should be developed in CODESYS of 3.x versions (last accessible version is CODESYS V3.5 SP14 Patch 2) and loaded into the EtherCAT EC2250 controller. The graphical interface can be seen in the browser by entering the link http://xxx.xxx.xxx.xxx:8080/webvisu.htm, where xxx.xxx.xxx.xxx is the IP address of the EtherCAT EC2250 controller.

Fig. 5. Appearance of TSL EtherCAT and Process Modeling hardware module



For visualization it is possible to use the built-in graphic terminal Ethernet ET1007 WT. This module also allows to study the programming of controllers in CODESYS of 3.x versions. The third HM has various analog and digital inputs and outputs, as well as buttons that can be used for testing and simulating the operation of a highly complex control system. Each button has a built-in LED that is connected to the digital output. There are eight non locking and eight locking buttons as well.

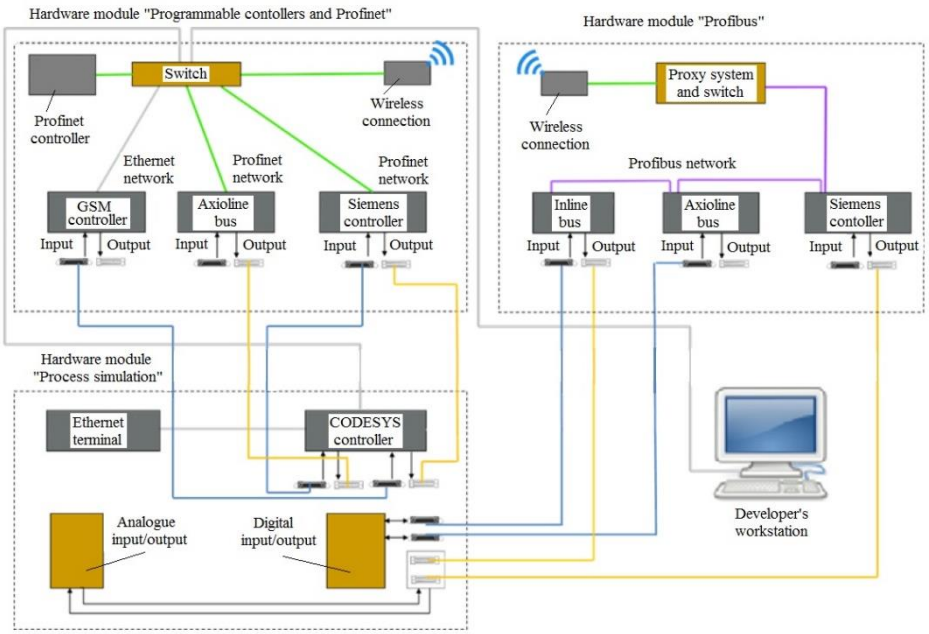
Fig. 6. Internal structure and external connections in TSL EtherCAT and Process Modeling HM



To provide physical connections between hardware modules, Centronics IEEE 488 connector with 24 pins and a 15-pin D-Sub connector are used. Up to 6 analog signals are connected to the D-Sub connector. The analog-to-digital conversion is performed at resolution capacity of 12 bits. The sample rate is 0.5 kHz. Only the third HM can be connected to other modules by standard cables, as their inputs and outputs are mounted symmetrically. All HMs may be connected to each other using standard cables as shown in Figure 7. These cables may also be used for connecting other external devices that do not have IP addresses. Devices that have IP addresses are connected to RJ-45 ports of Ethernet switches using a standard Cat. 5 twisted-pair cable. After the modules are switched, the control elements located in the EtherCAT and Process Modeling hardware module become available. Wireless possibilities of different types of modern equipment are very significant for a variety of tasks solution. That's why TATU TSL is equipped with two wireless access points (WAP), integrated in TSL Profibus HM and TSL Profinet HM. Structure of entire laboratory created for maritime engineers studying and retraining is shown in Fig. 8.

Modules and equipment which allow to explore different possibilities of modern cybersecurity hardware and protocols are absent in TATU equipment shipping. But as mentioned before, this field is very actual in modern conditions. Fortunately it's possible to add auxiliary modules or devices using standard DIN (Deutsches Institut für Normung; the German Institute for Standardization in English) rail and to connect them to base devices of TATU project or to another devices connected to the network by standard Ethernet technology.

Fig. 7. The structure of TSL hardware modules and their connection to computer



Majority of separate devices like PLCs, switches, bus couplers and so on, installed in TATU project, produced by Phoenix Contact company. That's why it was decided to explore devices with cyber security functions, created by exactly this company. Corresponding product line consist of following devices: FL mGuard RS2000, FL mGuard RS2005, TC mGuard RS2000, FL mGuard RS4000, FL mGuard RS4004, TC mGuard RS4000, FL mGuard GT/GT, TC mGuard PCI. In general these devices may work as LAN switches with different number of LAN ports, Internet routers, hardware firewalls (full stateful firewall), support cellular and Global Positioning System (GPS) capability, Virtual Private Network (VPN) hub capability, demilitarized zone (DMZ, protected network located between an untrusted and trusted

networks) capability, compatible with mGuard Secure Cloud (Industrial VPN for secure remote access) and may combine these functions and modes.

The following abbreviations are used in Figure 8: PLC – Programmable Logic Controller; BK – Bus Coupler (Bus Kupler in German language); SW – Switch.

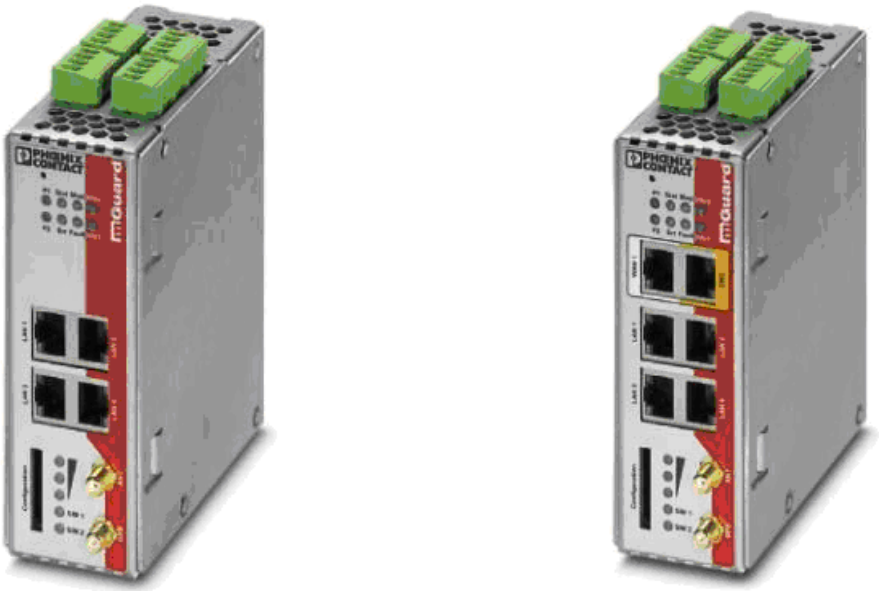
Wired and wireless data exchange have certain strengths and weaknesses both. Wireless data exchange and corresponding devices allow to organize much more flexible remote control of complex industrial objects, unmanned or autonomous ships, aircrafts, cars, etc. Some of such projects are already realized at the present time and are planned for pretty close future. Such approach allows to solve such complex technical problems and tasks which were impossible to solve using wired data transfer systems.

There are two devices in mentioned product line which support wireless communications presented in Fig. .

1. Router TC MGUARD RS2000 3G VPN is security device with mobile phone interface. It is equipped with any SD memory card slot, supports two fixed VPN tunnels, has easy configurable firewall, router with NAT/1:1 NAT, four port Fast Ethernet switch, two slots for SIM cards and GPS receiver.
2. Router TC MGUARD RS4000 3G VPN is security device with mobile phone interface as well. It has NAT/1:1 NAT, 4-port managed switch. This is router with intelligent firewall with full scope of functions and VPN for 10 tunnels by default (up to 250 supported), CIFS integrity monitoring as an option, slot for SD memory card, slots for two SIM cards and GPS receiver.

Both devices use 50 Ω impedance SMA antenna socket. Supported satellite protocols are GPS and GLONASS.

Figure 8. Routers TC MGUARD RS2000 3G VPN and TC MGUARD RS4000 3G VPN



Wireless interfaces for both routers are described and presented in Table 1.

Table 1. Wireless interfaces for TC MGUARD RS2000 3G VPN and TC MGUARD RS4000 3G VPN routers

Supported wireless data transfer technologies	Frequencies, power, substandard	Data transfer rate	GPRS	EDGE	UMTS
GSM, GPRS, EDGE, UMTS, CDMA2000	850/900 MHz (2 W, EGSM); 1800/1900 MHz (1 W, EGSM); 800 MHz UMTS/HSPA B6; 850 MHz UMTS/HSPA B5; 900 MHz UMTS/HSPA B8; 1900 MHz UMTS/HSPA B2; 2100 MHz UMTS/HSPA B1; 800/1900 MHz CDMA2000 EVDO	14.4 Mbps and less (HSDPA) 5.7 Mbps and less (HSUPA) 3.1 Mbps and less (DL CDMA2000) 1.8 Mbps and less (UL CDMA2000)	Class 12, Class B CS1...CS4	Multislot Class 12	HSPA 3GPP R6

The following abbreviations are used in the Table 1: GSM – Global System for Mobile communications, GPRS – General Packet Radio Service, EDGE – Enhanced Data rates for GSM Evolution, EVDO – EVolution-Data Optimized, GPS – Global Positioning System; GLONASS – GLObal NAvigation Satellite System; EGSM – Extended Global System for Mobile communications), UMTS – Universal Mobile Telecommunications System, HSPA – High Speed Packet Access, CDMA – Code Division Multiple Access, HSDPA – High Speed Downlink Packet Access, HSUPA – High-Speed Uplink Packet Access, DL – DownLink, UL – UpLink, 3GPP – 3rd Generation Partnership Project, CS – Coding Schemes.

Both devices support the same network functions: 4 time slots for receiving data, 4 time slots for transmitting data. The PIN is saved in the modem. After a voltage interruption, there is automatic redialing into the network. Integrated TCP/IP stack, firewall and VPN support, independent connection establishment. Web-based management by SNMP is supported as well.

Table 2. Wired interfaces for TC MGUARD RS2000 3G VPN and TC MGUARD RS4000 3G VPN routers

	Interface type	Number and type of ports	Cable segment length, m	Supported protocols or data flow control	File format and coding	Data transfer rate, kbps
TC MGUARD RS2000 3G VPN	Ethernet, 10/100Base-T(X) IEEE 802.3u	4 RJ45	100 (STP)	TCP/IP, UDP/IP, FTP, HTTP; ARP, DHCP, PING (ICMP), SNMP, SMTP		
	V.24 (RS-232) interface in acc. with ITU-T V.28, EIA/TIA-232, DIN 66259-1	1 D-SUB 9 plug	15	Software handshake, Xon/Xoff or hardware handshake RTS/CTS	UART/NRZ: 8 Data, 1/2 Stop, None/Even/ Odd Parity	9.6; 19.2; 38.4; 57.6; 115.2
TC MGUARD RS4000 3G VPN	Ethernet, 10/100Base-T(X) in acc. with IEEE 802.3u	6 RJ45	100 (STP)	TCP/IP, UDP/IP, FTP, HTTP; ARP, DHCP, PING (ICMP), SNMP, SMTP		
	V.24 (RS-232) interface in acc. with ITU-T V.28, EIA/TIA-232, DIN 66259-1	1 D-SUB 9 plug	15	Software handshake, Xon/Xoff or hardware handshake RTS/CTS	UART/NRZ: 8 Data, 1/2 Stop, None/Even/ Odd Parity	9.6; 19.2; 38.4; 57.6; 115.2

The following abbreviations are used in the Table 2: STP – shielded twisted pair; ITU-T – International Telecommunication Union Telecommunication Standardization Sector; IEEE – Institute of Electrical and Electronics Engineers; RTS – Request To Send; CTS – Clear To Send; UART – Universal Asynchronous Receiver-Transmitter; NRZ – Non Return to Zero; RS – Recommended Standard; DHCP – Dynamic Host Configuration Protocol; HTTP – Hyper Text Transfer Protocol; SNMP – Simple Network Management Protocol; NAT – Network Address Translation; FTP – File Transfer Protocol; IP – Internet Protocol; TCP – Transmission Control Protocol; UDP – User Datagram Protocol; ARP – Address Resolution Protocol; ICMP – Internet Control Message Protocol; EIA/TIA – Electronic Industries Alliance/Telecommunication Industries Association.

It is meaningful and recommended to connect devices of mGuard product line to AXC 3050 controller because it is most productive PLC among another devices implemented in TATU project. By another words, it is the best way to connect any mGuard device to TSL PROFINET hardware module. PLC AXC 3050 can work with Ethernet family networks and the Axioline F local bus, which supports any Ethernet-based data transfer protocols. The Axioline station can be created by connecting Axioline modules to the controller. The Axioline F local bus can be used for the sequential installation of various modules (devices) one closely to the other. The AXC 3050 controller can be fully configured and programmed in one of five programming languages in accordance with IEC 61131-3 standard with PC Worx when connected over Ethernet network. It has built-in interfaces for connecting devices over Ethernet

network. It allows to configure the controller using TCP/IP or UDP (User Datagram Protocol) protocols. The controller has three integrated Ethernet ports X1, X2, X3.

Using function blocks IP_USEND (sending user data via TCP/IP protocol) and IP_URCV (receiving user data via TCP/IP protocol) in PC Worx, it's possible to organize data exchange (i.e., values of variables corresponding to the measured process parameters and physical quantities) between the PLCs. This approach allows implementing distributed and configurable automation solutions. By using the AX OPC server (Object Linking and Embedding for Process Control, a collection of software technologies that provide a single interface for managing automation objects and technological processes), the controller is accessible over Ethernet network and can be used in software visualization packages.

The PROFINET technology can be implemented by connecting to the Ethernet interfaces of the AXC 3050 PLC. The PROFINET controller is always available when connected via the eight-pin RJ45 connector of the X3 interface. Modbus TCP technology can also be implemented by connecting to the Ethernet interfaces of the AXC 3050 controller. This controller can act as a Modbus client, and can be configured as a MODBUS TCP server when using its corresponding function blocks.

AXC 3050 PLC has communication interface with the local Axioline F bus for connecting various modules. Up to 63 devices can be connected to this PLC. The actual number of devices depends on the total current consumption of all devices, which should not exceed the maximum current that the controller provides to the local bus. Due to the Web-based management interface integrated into the PLC, the user can visualize the status and diagnostic information from the controller in the browser. The AXC 3050 PLC is equipped with two USB interfaces and has internal memory. It can be used for storing programs and configurations for a custom project. If the internal memory is insufficient for the created application, the AXC 3050 can work with external memory in the form of SD format flash memory (Secure Digital) or USB drive. Also AXC 3050 has 4 MB internal memory for program storage, and 8 MB memory for data storage; 128 kB is used for storing data after power off. The minimum controller cycle time is 1 ms, the number of control tasks performed simultaneously is 16. It is also possible to create complex multi segment industrial networks using this PLC model [9].

It is obviously that protocols and technologies of cybersecurity mentioned and briefly described above can not be learned in brief term especially together with wide spectrum of wired and wireless industrial data transfer protocols and technologies. That's why it is proposed to use multi level approach which consist of the following stages as partly mentioned above.

1. Basics of PLCs programming using PcWorx and CODESYS IDEs and corresponding IDEs of another developers if necessary (like very popular Siemens Simatic Step 7, Mitsubishi GX Developer, Schneider Unity Pro and so on).
2. Studying classic industrial technologies/protocols like ProfiBus, ModBus, ASI, HART, etc.
3. Studying of modern perspective industrial technologies/protocols like Profinet, ModBus TCP, HART IP, EtherCAT, etc.
4. Studying of wireless data transfer technologies based on IEEE 802.11 family, GSM standards, Bluetooth, Zigbee and so on.
5. Cybersecurity protocols and technologies.

4. ACTUAL OR ANTICIPATED OUTCOMES

Equipment obtained at European Tempus TATU project performing allows to learn PcWorx and CODESYS integrated development environments for programmable logic controllers programming and to study the following network devices: switches, wireless access points, different types of programmable logic controllers and some another equipment as well. Full time actively working laboratory "Means of industrial automation and network technologies" is created. In general it allows to learn studying disciplines, connected with mentioned above areas. E-learning system based on MOODLE platform is actively used for students' remote access to corresponding teaching materials and is constantly updated. Learning books in Russian, Ukrainian and English languages are created and successfully integrated in the education process. At least 200 students of "Ships' power plants operation", "Ships' power and refrigerating plants operation", "Automated Control of Ships' Power Plants", "Operation and Maintenance of Ship's Automated Systems" specialties pass corresponding lessons every year. Also there are a lot of potential consumers of such education and trainings because there are 187 crewing and shipping companies in Odessa region. Ukraine has 69000 seafarers (39000 officers) and keeps 6th place in the world on this indicator as well.

Author has some experience with industrial cyber security devices adjustment and different manufacturers devices integration in the same network. Bundled with PLCs, network switches, wireless access points it allows to learn studying disciplines, connected with most mentioned above areas.

5. CONCLUSIONS

Ways of modern concepts and technologies implementing in maritime field are analyzed. Concrete directions of deep studying are shown. Possibilities and technologies, successfully realized in education process, are described. Possibilities of existing equipment may be expanded by additional modules installation. Actuality and possibilities of cyber security technologies studying are highlighted. Approaches and technologies, successfully realized in education process and planned for future, are described.

REFERENCES

[1]LANGMANN R. "Workshop: The TATU Lab & smart education" [Text] /R. Langmann, Y.Makarova, L. Rojas-Peña, P. Galkin, I. Klyuchnik, V. Voropaeva, V. Pozepaev, L. Zinyuk, R. Skrypyuk, E. Shaporina, V. Shaporin, V. Shapo, S. Gorb// 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV).– Madrid, 2016.–P. 400-402.

[2] GORB S. I., NIKOLSKII V. V., SHAPO V. F., KHNIUNIN S. G. Programmirivanie controllerov v instrumentalnoi srede: uchebnoe posobie. – Kharkov: Izdatel' FLP Panov A.N., 2017. – 172 s. In Russian.

Горб С. И., Никольский В. В., Шапо В. Ф., Хнюнин С. Г. Программирование контроллеров в инструментальной среде: учебное пособие. – Харьков: Издатель ФЛП Панов А.Н., 2017. – 172 с.

[3] GORB S.I., NIKOLSKYI V.V., SHAPO V.F., KHNIUNIN S.H. Programming controllers in the integrated development environment: training manual. Practice. – Odessa: National University "Odessa Maritime Academy", 2017. – 164 p.

[4] TATU study book. Trainings in Automation Technology for Ukraine. Editors: C. Madritsch, W.Werth. – Villach: Carinthia University of Applied Sciences, 2017. – 211 p.

[5] GORB S. I., NIKOLSKII V. V., KHNIUNIN S. G., SHAPO V. F. Tekhnicheskoe obespechenie podgotovki sudovykh ingenerov po sistemam avtomatizatsii s programmiruemymi controllerami. // Avtomatizatsiia sudovykh tekhnicheskikh sredstv: nauch.-tekhn. sb. – 2016. – Vyp. 22. – Odessa: ONMA. – S. 39 – 46. In Russian.

Горб С.И., Никольский В.В., Хнюнин С.Г., Шапо В.Ф. Техническое обеспечение подготовки судовых инженеров по системам автоматизации с программируемыми контроллерами // Автоматизация судовых технических средств: науч.-техн. сб. – 2016. – Вып. 22. – Одесса: ОНМА. – С. 39 – 46.

[6] GORB S. I., NIKOLSKII V. V., KHNIUNIN S. G., SHAPO V. F. Metodicheskoe obespechenie tekhnologii avtomatizatsii na baze programmiruemykh controllerov // Avtomatizatsiia sudovykh tekhnicheskikh sredstv: nauch.-tekhn. sb. – 2017. – Vyp. 23. – Odessa: NU "OMA". – S. 30 – 36. In Russian.

Горб С.И., Никольский В.В., Хнюнин С.Г., Шапо В.Ф. Методическое обеспечение технологий автоматизации на базе программируемых контроллеров // Автоматизация судовых технических средств: науч.-техн. сб. – 2017. – Вып. 23. – Одесса: НУ "ОМА". – С. 30 – 36.

[7] IVASIUK N., SHAPO V. Unified English Language Communication as Service for Seafarers // 30th International Maritime English Conference IMEC 30. – Maritime Academy of Asia and the Pacific. – Manila, 2018.

[8] PROFIBUS and PROFINET International. PROFIsafe and IO-Link pass the 10 million mark. – https://www.Profibus.com/newsroom/news/profisafe-and-io-link-pass-the-10-million-mark/

[9] SHAPO V. Programmable Logic Controllers Applying for Multi Segment Industrial Data Transfer Networks Developing. International Robotics & Automation Journal. – Volume 3, Issue 4. – 2017. [Electronic resource]: http://medcraveonline.com/IRATJ/IRATJ-03-00060.php