

**EUROPEAN TEMPUS TATU PROJECT AND WIRESHARK SOFTWARE
IN INDUSTRIAL NETWORKS DATA TRANSFER PROTOCOLS
STUDYING AND ANALYZING***

Assoc. Prof. Dr. Vladlen SHAPO

National University "Odessa Maritime Academy", Ukraine,

E-mail: vladlen.shapo@gmail.com

ARTICLE INFO	ABSTRACT
<p>Article History: Received: 19 June 2018 Accepted: 25 July 2018</p>	<p><i>Industrial data transfer technologies are implementing in industry, transport, energetic together with Industry 4.0 and IIoT concepts. Compatible with previous generations TCP/IP based protocols ProfiNet, ModBus/TCP, Ethernet/IP, EtherCAT were created to perform com-plex technical systems remote control.</i></p>
<p>Keywords: European Tempus TATU Project, Wireshark network analyzer, industrial networks data transfer protocols, industrial networks data transfer protocols studying and analyzing</p>	<p><i>In 2013 – 2017 European TEMPUS TATU (Trainings in Automation Technologies for Ukraine) project was realized and TATU Smart Lab (TSL) equipment was obtained.</i></p> <p><i>TSL is a set of devices for modern automation technologies studying. It matches to Industry 4.0 and IIoT concepts. It contains programmable logic controllers, I/O devices, switches, wireless access points and can be used for studying of Ethernet based data transfer technologies, wireless data transfer, TCP/IP technologies, hard real-time systems, EtherCAT, CAN, RS232/485, PROFINET, Modbus TCP interfaces.</i></p>
<p>DOI: 10.26900/jsp.2018342247</p>	<p><i>WIRESHARK software allows to analyze network traffic and supports capturing of long network protocols list. It helps to understand the reason of network problems, simplifies industrial and corporate networks exploitation.</i></p>

1. INTRODUCTION

During last 5-7 years in industry, at the different kinds of transport, in energetic field, etc. are very actively implementing data exchange technologies between separate devices, device groups and networks. These technologies based on Industry 4.0 (4th industrial revolution), IoT (Internet of Things), IIoT (Industrial Internet of Things) concepts. In accordance with these concepts a lot of different devices became smart, possessing of own CPUs, memory and different wired and wireless interfaces for external data exchange. Some of them (like complex PLCs) allow to unite different industrial network segments, having sufficient productivity and much lower cost compared to computers (Shapo, URL-1, 2017).

* This study is the revised version of the same name paper presented in the "2nd International Rating Academy Congress: Hope" held in Kepez / Çanakkale on April 19-21, 2018.

From the beginning of 90th years of 20th century in industry are very popular some protocols and data transfer technologies, most known are ASI, ProfiBus, FieldBus, HART, ModBus, CAN family, BAC, etc. But in connection with Internet development and forthcoming of absolutely new challenges were created some TCP/IP based protocols, which allow to perform remote control of complex technical systems for enhancement of control quality, decreasing response time for force majeure situations and cost for control and exploitation of such systems. Protocols ProfiNet, ModBus/TCP, Ethernet/IP, EtherCAT became well known; they are compatible with previous generations, but allow to solve fundamentally new tasks. But in some situations by cost/productivity ratio win protocols and technologies, which don't have wide spread, but firmly hold theirs niche. Some of them are described below.

2. MAIN TEXT

ACN (Architecture for Control Networks) is network control protocol, initially destined for entertainment industry (URL-2, 2017). It has open source code and maintains some subordinate protocols (table 1).

AYIYA (Anything In Anything) is network protocol for tunneling between IP-networks and controlling there (URL-3, 2017). Very often it's used for IPv6 packets transit through the networks based on IPv4 protocol. Network security is provided with absence of addresses and content of tunneled packets falsification possibility. At least one of two tunnel endpoints allows mobile devices connecting.

Table 1. ACN protocols family and corresponding standards

Protocol	Standard
Root Layer, Session Data Transport and Device Management Protocols, Device Description Language	ANSI E1.17
Service Location Protocol (SLP)	RFC 2609
Simple Network Time Protocol (SNTP)	RFC 2030, ANSI E1.30-3-2009
Trivial File Transfer Protocol (TFTP)	RFC 1350
Streaming ACN (sACN)	ANSI E1.31
RDM Extension (RDMNet)	ANSI E1.33
Remote Device Management (RDM)	ANSI E1.20

CIP (Common Industrial Protocol) is the set of standards (URL-4, 2017), which are maintained by Open DeviceNet Vendors Association (ODVA). CIP extensions are CIP safety, CIP Sync and CIP Motion protocols. CIP contains full set of requirements and possibilities for complex automation systems and their subsystems development from following sides: control, information security, motion organizing, informing. Some most important protocols and industrial data transfer technologies are based on CIP as well and briefly described below.

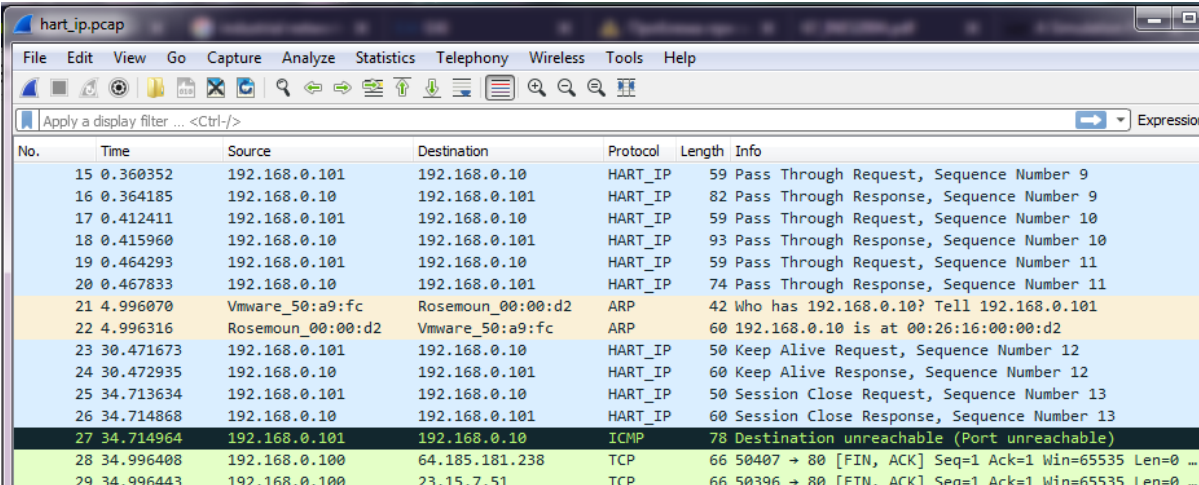
EtherNet/IP is open industry protocol, which uses standard Ethernet chips and cable systems, based on IEEE 802.3 standard, and serve for input/output real time data exchange and information messages in DeviceNet and ControlNet industrial networks. CIP provides common application level between networks, which doesn't depend on media (cable system). It allows to perform direct routing CIP messages in EtherNet/IP, ControlNet and DeviceNet. Depending on application requirements EtherNet/IP network may be stand-alone or combined with DeviceNet or ControlNet networks for additional flexible information and control services realization. EtherNet/IP transfers big user, configuration and input/output data volumes in the same high-speed network; tightly associates technological and corporate operations; facilitates technical maintenance expenses decreasing thanks to existing network

resources and technical facilities using; allows to commercial and industrial technological levels to coexist in the same network; works with TCP/IP and HTTP protocols.

DNP3 (Distributed Network Protocol, version 3) is a set of communication protocols (URL-5, 2017), which are used for data transfer between components in automation systems like different types of equipment for data acquisition and control and described in IEEE 1815 standard. In SCADA systems DNP3 is used by SCADA master stations (control centers), Remote Terminal Units (RTU) and different Intelligent Electronic Devices (IED). It uses 3 levels of OSI model (data link, transport, application) and contains Secure Authentication v5 mechanism, which allows to master or remote DNP3-system uniquely determine, that connection is established with legitimate user or host, but not with malicious user.

HART-IP (Highway Addressable Remote Transducer) protocol (URL-6, 2017) based on standard Ethernet IEEE 802.3 hardware and cable systems and with Wi-Fi IEEE 802.11 equipment, that's why it's possible to use it with standard network switches, routers, access points. It may be used in redundant mesh or ring topologies and with PoE (Power over Ethernet) power supply standard by twisted pair. Possible data transfer rates are 10 or 100 Mbps and 1 Gbps. HART network, including devices working with Wireless HART protocol, is compatible with office and industrial LAN-switches, fiber optics media converters, Wi-Fi access points and another equipment. Compatibility with classic HART protocol allows to put corresponding gateways into action and to work with classic analogue 4-20 mA technologies. Using IP as base interaction protocol allows HART-IP to work in the same network together with multiplicity of protocols, based on IP and Ethernet. More than 60 millions devices with HART protocol supporting are installed in the world. HART over Ethernet or HART-IP widen HART accessibility in local internal industrial networks with interconnection with corporate networks and ERP (Enterprise Resource Planning) software. Variables and diagnostic data in HART are encapsulated in HART-IP packets. It allows to realize real time processes in existing corporate networks and to use corporate VPN (Virtual Private Networks).

Figure 1. Viewing HART IP protocol packets in Wireshark network analyzer



No.	Time	Source	Destination	Protocol	Length	Info
15	0.360352	192.168.0.101	192.168.0.10	HART_IP	59	Pass Through Request, Sequence Number 9
16	0.364185	192.168.0.10	192.168.0.101	HART_IP	82	Pass Through Response, Sequence Number 9
17	0.412411	192.168.0.101	192.168.0.10	HART_IP	59	Pass Through Request, Sequence Number 10
18	0.415960	192.168.0.10	192.168.0.101	HART_IP	93	Pass Through Response, Sequence Number 10
19	0.464293	192.168.0.101	192.168.0.10	HART_IP	59	Pass Through Request, Sequence Number 11
20	0.467833	192.168.0.10	192.168.0.101	HART_IP	74	Pass Through Response, Sequence Number 11
21	4.996070	Vmware_50:a9:fc	Rosemoun_00:00:d2	ARP	42	Who has 192.168.0.10? Tell 192.168.0.101
22	4.996316	Rosemoun_00:00:d2	Vmware_50:a9:fc	ARP	60	192.168.0.10 is at 00:26:16:00:00:d2
23	30.471673	192.168.0.101	192.168.0.10	HART_IP	50	Keep Alive Request, Sequence Number 12
24	30.472935	192.168.0.10	192.168.0.101	HART_IP	60	Keep Alive Response, Sequence Number 12
25	34.713634	192.168.0.101	192.168.0.10	HART_IP	50	Session Close Request, Sequence Number 13
26	34.714868	192.168.0.10	192.168.0.101	HART_IP	60	Session Close Response, Sequence Number 13
27	34.714964	192.168.0.101	192.168.0.10	ICMP	78	Destination unreachable (Port unreachable)
28	34.996408	192.168.0.100	64.185.181.238	TCP	66	50407 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0 ...
29	34.996443	192.168.0.100	23.15.7.51	TCP	66	50396 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0 ...

During December 2013 – June 2017 European TEMPUS TATU (Trainings in Automation Technologies for Ukraine) project was realized (URL-7, 2018). Within the framework of this project TATU Smart Lab (TSL) equipment was obtained (Gorb et al, 2017a, 2017b). TSL is a flexibly configurable mobile set of devices for teaching modern automation technologies and its application in real projects. It contains devices from different European manufacturers and matches to goals of Industry 4.0, IoT and IIoT concepts (2 hardware modules (HM) of 3) where individual devices and their nodes can

communicate with each other and consumers using wireless data transmission technologies or IP technologies.

The first HM (Fig. 2) contains two programmable controllers (AXC 3050 and ILC 151 GSM/GPRS), PROFINET I/O devices, managed network switch and wireless access point for wireless LAN (Gorb et al, 2017a, 2017b). This HM can be used for studying a wide range of topics including working with data transfer technologies based on Ethernet, wireless data transmission and IP technologies. Two programmable controllers can communicate using TCP/IP or Modbus TCP data transfer protocols. Possible complex industrial IP network structure based on multi interface AXC 3050 smart controller shown at Fig. 3.

Controller EC2250 EtherCAT (Fig. 4), installed in second HM and working with IP-based protocols, has a short cycle time and designed for hard real-time systems [8, 9]. The controller uses a high-performance Cortex A9 800 MHz ARM processor. EtherCAT is an Ethernet based bus standardized by SEMI (Semiconductor Equipment and Materials International), IEC and ISO. EtherCAT is much faster than traditional buses and industrial Ethernet based solutions. The typical EtherCAT cycle time is 50-250 μ s, while in traditional buses 5-15 ms are required for each update. The device integrates communication interfaces Ethernet, EtherCAT, CAN, CAN Open, RS232/485, PROFINET, BACnet, Modbus TCP, TCP/IP.

Figure 2. PROFINET hardware module

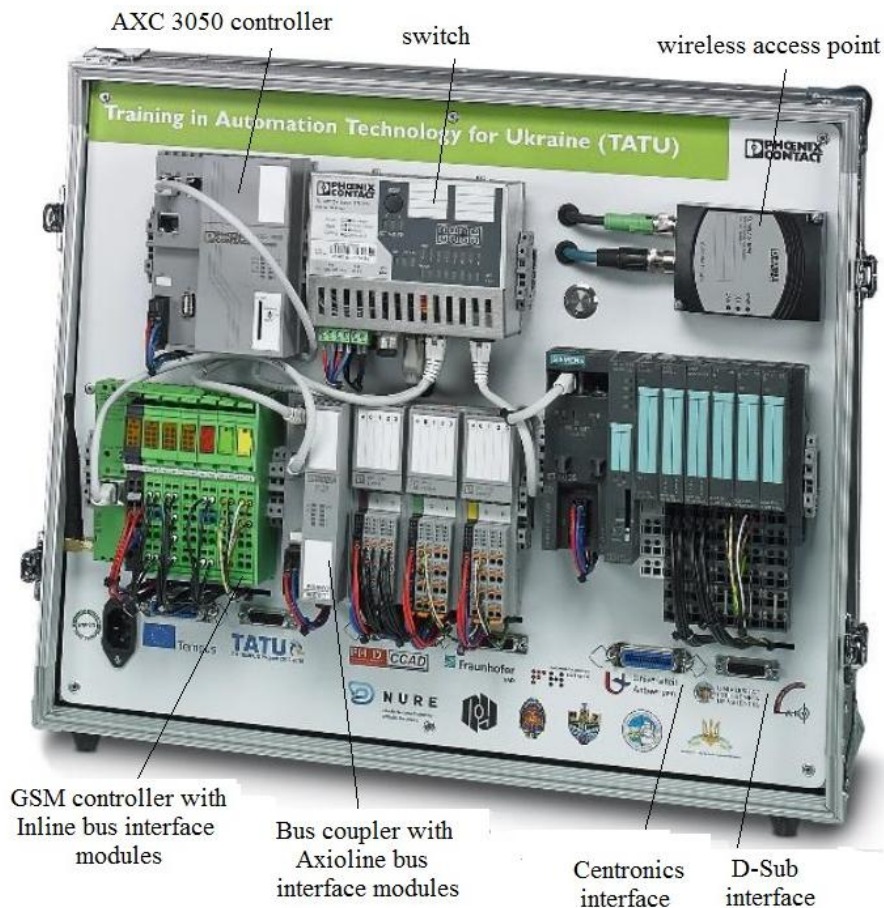


Figure 3. Complex industrial IP network structure based on multi interface controller

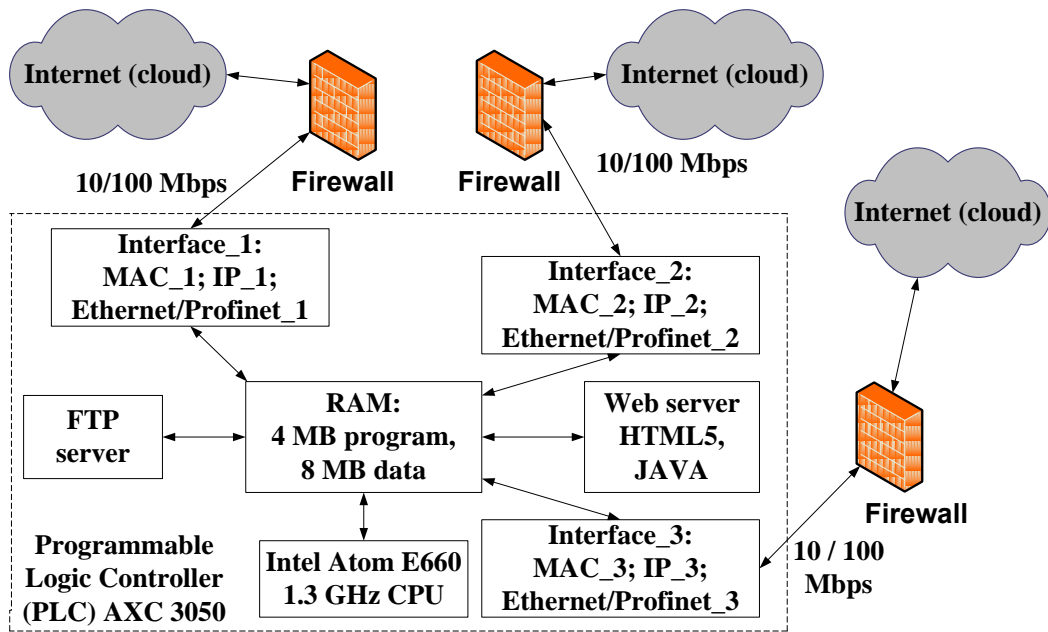
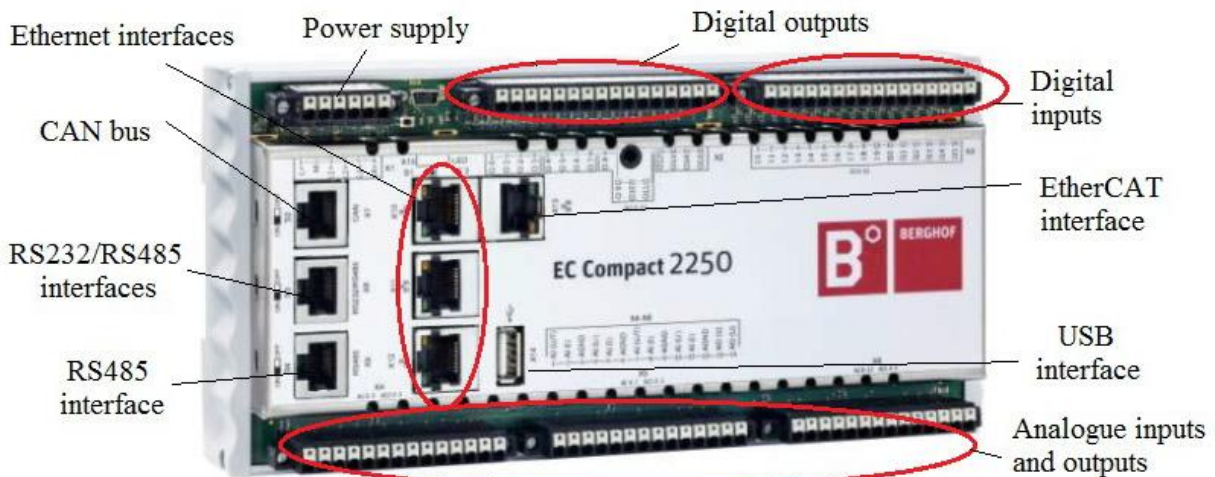


Figure 4. Multi interface industrial IP network controller



WIRESHARK software allows to analyze network traffic in industrial networks based on protocols and technologies described above. Also Wireshark supports capturing of long list of different network protocols. It significantly helps to understand the reason of unobvious network problems, to simplify complex industrial and corporate networks exploitation and making interconnection between different network technologies and protocols using corresponding hardware and software gateways.

REFERENCES

- ARCHITECTURE FOR CONTROL NETWORKS [Electronic resource]:
<https://acn.codeplex.com> [Date Accessed: 2 December 2017].
- DISTRIBUTED NETWORK PROTOCOL [Electronic resource]:
<https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf> [Date Accessed: 2 December 2017].
- EUROPEAN TEMPUS TATU PROJECT [Electronic resource]: <https://tatu.org.ua> [Date Accessed: 2 March 2018].
- GORB, S.I., NIKOLSKYI, V.V., SHAPO, V.F., KHNIUNIN, S.H., 2017, Programming controllers in the integrated development environment: training manual. Practice, Odessa: National University "Odessa Maritime Academy", 978-966-7591-73-1.
- GORB, S.I., NIKOLSKYI, V.V., SHAPO, V.F., Khniunin, S.H., 2017, TATU study book. Trainings in Automation Technology for Ukraine, Villach: Carinthia University of Applied Sciences, 978-3-9504443-0-8.
- INSTRUMENTATION TOOLS [Electronic resource]: <http://instrumentationtools.com/what-is-hart-ip/#.WibYR3lx1aQ> [Date Accessed: 2 December 2017].
- SHAPO, Vladlen, 2017, Programmable Logic Controllers Applying for Multi Segment Industrial Data Transfer Networks Developing [online]: <http://medcraveonline.com/IRATJ/IRATJ-03-00060.php> [Date Accessed: 2 December 2017].
- SixXS – IPv6 Deployment & Tunnel Broker [Electronic resource]: <https://www.sixxs.net/tools/ayiya/> [Date Accessed: 2 December 2017].
- THE FUTURE OF INDUSTRIAL AUTOMATION [Electronic resource]: <https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP> [Date Accessed: 2 December 2017].

