ANNALS of Faculty Engineering Hunedoara – International Journal of Engineering
Tome XX [2022] | Fascicule 1 [February]

[1.] László GÖCS, [1.] Attila PÁSZTOR, [1.] Zsolt Csaba JOHANYÁK

COMPUTER NETWORK SOLUTIONS IN MODERN INDUSTRIAL ENVIRONMENT

[1.] John von Neumann University, GAMF Faculty of Engineering and Computer Science, Department of Information Technologies, Kecskemét, HUNGARY

Abstract: Nowadays manufacturing systems are strongly dependent on data transfer and network connection. Therefore, information technology systems serving modern industrial environments have to provide a high level of reliability, redundancy, maintainability as well as a centralized monitoring. In order to meet these requirements, one should carefully design the topology, select the cabling solutions, different devices and computers as well as protocols and redundancy technologies. This paper presents a review of these concepts and gives an insight to some solutions that can be considered as best practice.
Keywords: Industry 4.0, reliable network, IT security, Turbo Ring, Turbo Chain

1. INTRODUCTION

The functioning of an industrial information technology (IT) system can be considered as reliable if the functionality of the software system (user programs and data) is provided to the user with a level of availability that meets the requirements of the given security class. Here availability means the probability that the system is usable by the user within a defined time interval, according to the level of functionality defined at design time. An application or resource is available when it is able to perform its function, to receive tasks, and to operate. Its value is expressed as a percentage. In case of servers, availability is the time when they are able to serve clients.

$$\text{Availability (R)} = \frac{T_{upt} - \sum_{upt} T_{dpo}}{T_{upt}} \times 100\%$$

where T_{upt} is the uptime period for which the availability is evaluated and T_{dpo} is the downtime per occasion. In an industrial environment, outages are not allowed and therefore the factors affecting the downtime must be taken seriously. Such factors are:

- capability to restart,
- error correction process,
- efficient management of system configuration.

The availability management also deals with the following features.

- *Reliability*: the ability of an information technology component to perform a required function under specified conditions for a specified period of time.
- *Maintainability*: the ability of a IT system component or service to be maintained in a state or restored to a state in which it can perform the required function.
- *Serviceability*: a contractual clause that defines the availability of an IT component as agreed with the external organisation providing and maintaining the components.
- *Security*: the ability to access IT components or services under secure conditions.

IT systems and services must be designed to be reliable, fault-tolerant and maintainable throughout their lifecycle, from design to decommissioning. Effective and efficient availability management results in the following benefits: improved quality of IT services, cost-effective delivery of new and existing IT services, improved manageability of IT infrastructure, improved planning capability, more secure delivery of IT services. Figure 1 illustrates the different time components relate to an incident and the associated recovery.

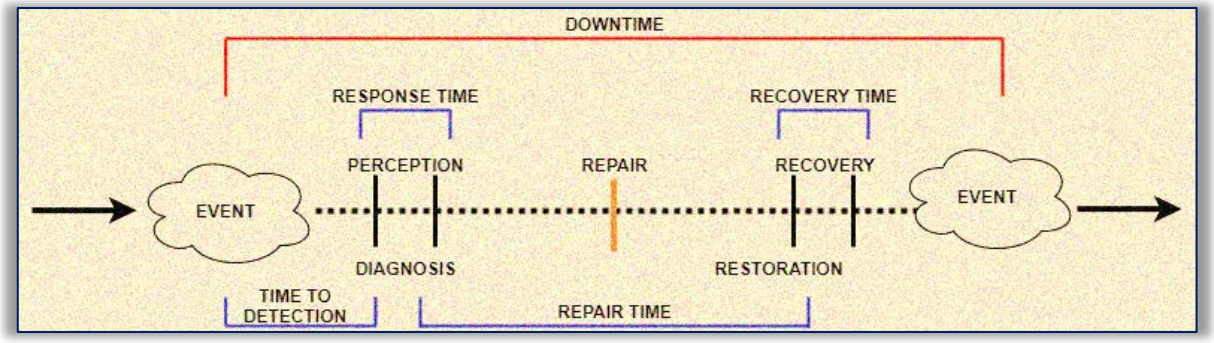

Figure 1. Time components

This paper tries to summarise the areas that are important to keep in mind in order to develop a reliable and well-functioning industrial IT system. The paper covers several areas of network layers. In case of the physical deployment, the cabling specifications and options will be discussed. In case of communication devices, the standards that are beneficial in an industrial environment are presented. Besides the proper selection of equipment at the endpoints, the possibility of secure data transmission, data storage, as well as the importance of user authentication are also discussed.

2. STRUCTURED NETWORK

The physical layer is the cornerstone of network communication. It provides the foundation for the entire IT infrastructure, so it must be built with great care. It is essential that the continuity and stability of communication between industrial systems are as reliable as possible [11]. A communication failure can be fatal to an industrial process, resulting in serious downtime or a defective product in production. When designing a structured network, the environment of the manufacturing system and the possible disturbances must be taken into account. Here the "MICE" classification can be a good starting point for planning. The four environmental elements that make up the acronym are:

- *M*: mechanical (impact, vibration, breakage, traction, bending, etc.)
- *I*: intrusion (e.g. water, dust in the form of liquids and particles)
- *C*: climatic/chemical (temperature, UV radiation, humidity, exposure to contaminants such as oil or gas, etc.)
- *E*: electromagnetic (surges, EMI/RFI interference, magnetic fields, transients, etc.)

In the MICE classification, a number appears after each of the four letters. The number indicates the "severity" of exposure to the environmental factor:

1: low severity (usually found in a commercial office environment)
2: medium severity (usually found in light industrial environments)
3: high severity (usually found in heavy industrial environments)

It is important to build the right topology that is transparent and maintainable. In an industrial environment, physical layer deployment is mainly based on wiring technology. Use of reliable and high quality materials is a primary consideration in the design of the cabling. Double shielding ensures (see Figure 2) transmission reliability in areas with electromagnetic interference, which is more prevalent in an industrial environment than in an office network. Another important aspect is that they can operate at temperatures from -30°C to 80°C and at data transmission rates of 2.5 or 5Gbit/sec.

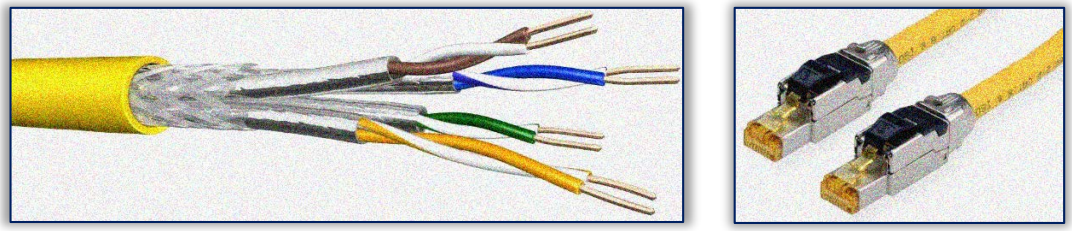

Figure 2. Special Ethernet cable and connectors [2] [21]

The special outer sheath is resistant to mineral oils and abrasion, but more importantly, it must be free of compounds containing halogenated additives for fire safety reasons, so halogen-free [22] cables must be used. Compliance with the ISO/IEC 11801:2017 [10] - Structured cabling standard is a prerequisite and a guarantee for the operability of all transmission protocols in information technologies. Part 3 of the standard is dedicated to industrial environments, where the performance categories of cabling, the structure and hierarchy of networks for use in the environment specified in the titles of each part (standard) are defined.

Another possible method of network interconnection is SPE (Single Pair Ethernet – in Figure 3), which transmits Ethernet over only one pair of copper wire and allows both data transmission over Ethernet and simultaneous power supply (PoDL). This technology can result in a 25% reduction in cable diameter compared to traditional Ethernet cable. The standardised SPE interfaces are ideally suited for efficient data transmission in factory and process automation according to IEC 63171-2:2021 (IP20) [6] and IEC 63171-5 (IP67) [3].

Figure 3. Single Pair Ethernet Connections [24]

In particular, industrial environments use of fibre optic cables (see Figure 4.) is becoming more and more prevalent, as they have high transmission speeds, can be used to bridge long distances (e.g. between separate production lines), provide low attenuation and are insensitive to electromagnetic interference.

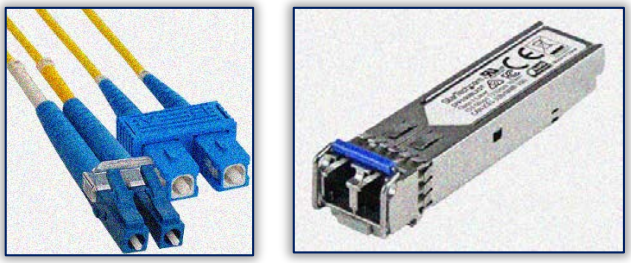

Figure 4. Optical connection and SFP module [13] [1]

3. NETWORK DEVICES

In an industrial environment, only dedicated network equipment should be used. Devices manufactured for home and office use are not suitable for this purpose. Such industrial switches can be DIN-rail mounted for easy integration into the industrial environment thanks to their modular design (Figure 5).

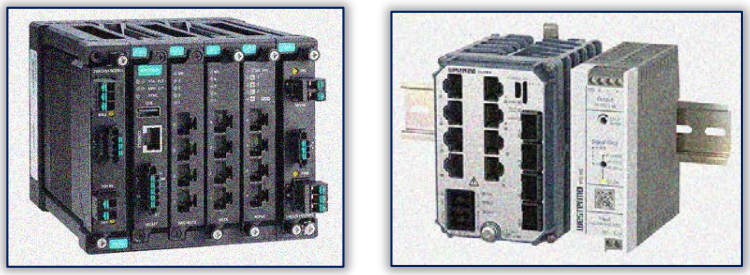

Figure 5. Layer 2 Managed Switches [12]

— Timing

It is very important that the equipment in a deployed system must be in sync, so high accuracy timing and time measurement is required. For this purpose, the NTP (Network Time Protocol) has been replaced by the high precision IEEE 1588-2019 v2.1 PTP (Precision Time Protocol) [7] clock synchronisation protocol. Devices used in industrial environment have to support this protocol.

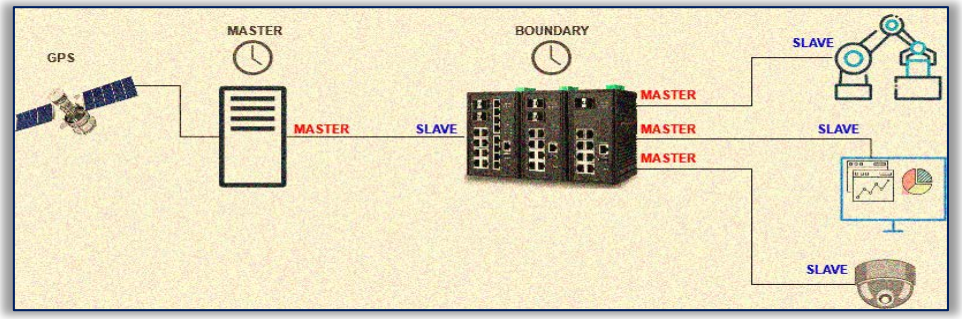

Figure 6. How time protocol works [20]

PTP has two types of clocks, the master and the slave (Figure 6). The clock in the endpoint device is the slave. The master is ideally controlled by an external radio clock, or a GPS receiver synchronises the corresponding slave clocks connected to it. There will also be transmission nodes in the network, e.g. an Ethernet switch with a control clock. This regulator clock will act as a slave clock relative to the master clock, then switch to act as a master clock relative to the endpoint slave devices. Each slave clock is synchronized to the master clock in time, frequency and phase, and synchronized to all other slave nodes.

Use of this network protocol has been common for a long time, e.g. for devices communicating on bluetooth [5]. Here, master-slave type networks are called piconet networks and networks used as a set of these are called scatternets. This model is also used, among others, as a communication protocol for robot swarms [17][18].

— Connection security

One of the main categories of Ethernet switches used in networks is the managed switch. This type is not only capable of basic switch operation (forwarding packets), but also has multiple security configuration options across the entire device, or even on individual ports.

≡ Port locking

In the case of a switch integrated into a system, it is not guaranteed that all ports will be actively involved in the operation during commissioning. Therefore, a simple but effective security setting should be made, which consists of disabling ports that are not in use. This way, if any new device is connected to one of these ports, it cannot establish any communication with the network until the system administrator activates the port (after having verified that the device is secure). Example of disabling the ports 10-24 on a 24 port switch:

Switch>enable
Switch#configure terminal
Switch(config)#interface range f0/10-24
Switch(config-if-range)#shutdown

≡ Port security

For each port of a switch one can specify one or more MAC addresses, so that the switch will accept incoming traffic only from the given MAC addresses. If a device with a MAC address not specified in the list is connected the port will be disabled. The sample configuration below shows the case when only one MAC address is specified for the port.

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 1234.5678.9ABC
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security
```

— Virtual LANs

For large corporate networks, the separation of certain traffic could be essential for performance and security purposes. Here separation means that although there is a common physical network one can define individual logical networks whose traffic is not visible for the others (Figure 7). These networks are called virtual local area networks (VLANs). The advantage of this solution is that the endpoints and equipment that are far apart can be consolidated into one logical network. For example in an industrial network, usually devices related to the production are separated from the office network. There is also a security reason for this solution, since a malicious software that could cause a network attack cannot damage the whole system.

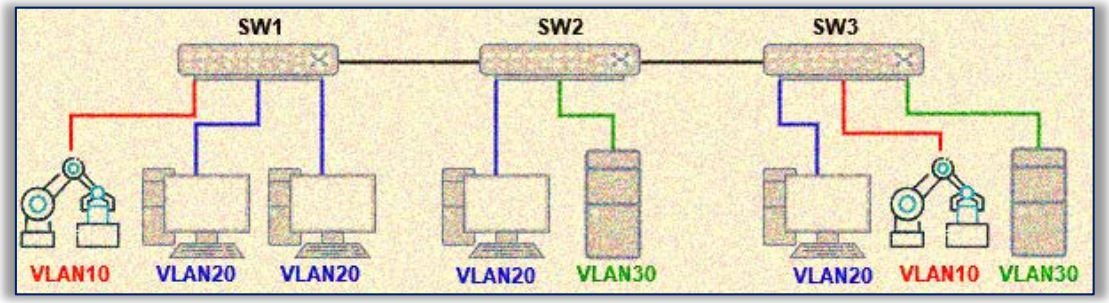

Figure 7. Virtual subnets

— Redundant communication

Ring topology is a very popular and cost-effective method for network deployment, and is considered one of the most efficient solutions in the industry for avoiding network downtime [14]. In this section four ring topology based solutions are presented that can ensure a high redundancy level for industrial networks.

Turbo Ring (Figure 8) is a technology developed by Moxa in 2007 that provides network redundancy for system redundancy. Turbo Ring connects all switches in a ring topology. Typically, if this is done with unmanaged switches, an infinite loop is created, causing a network failure. However, by using Moxa's managed switches, the infinite loop can be eliminated by setting an Ethernet port on the managed switch to disable it and only enable it when an error is detected [3]. Moxa's Turbo Ring technology allows networks to be recovered within 20 ms (10G/1G Ethernet recovery time <50 ms) on networks with up to 250 nodes.

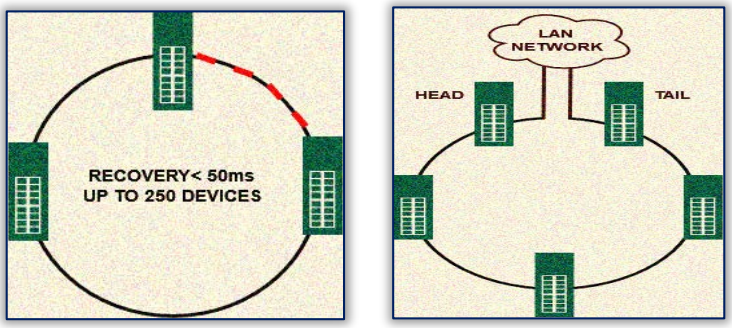

Figure 8. Moxa Turbo Ring (left) and Turbo Chain (right) concept [15]

Turbo Chain (Figure 8) is a highly flexible redundancy technology that offers unlimited redundant network expansion and is designed for use on widely deployed networks. Turbo Chain outperforms traditional ring topologies by providing superior flexibility, unlimited expansion and simplified configuration, allowing network operators to reduce deployment costs by connecting separate redundant rings together [15].

V-ON (Figure 9) ensures that simple and complex networks can be restored within milliseconds in the case of a connection failure. V-ON is designed for multicast network applications such as industrial automation PLCs and video surveillance systems. When combined with Turbo Ring or Turbo Chain chains, this technology can provide redundancy for the entire network. Its main features are:

≡ Layer 2 transmission recovery <50 ms for unicast and multicast networks
≡ Layer 3 transmission recovery <300 ms for unicast and multicast routing networks
≡ Millisecond level router redundancy

Parallel Redundancy Protocol (PRP) and High Availability Seamless Redundancy (HSR) (Figure 9) are two technologies that ensure seamless transmission even if part of the network fails. PRP achieves active network redundancy by duplicating packets over two independent networks operating in parallel, while HSR is primarily designed for ring topologies [15].

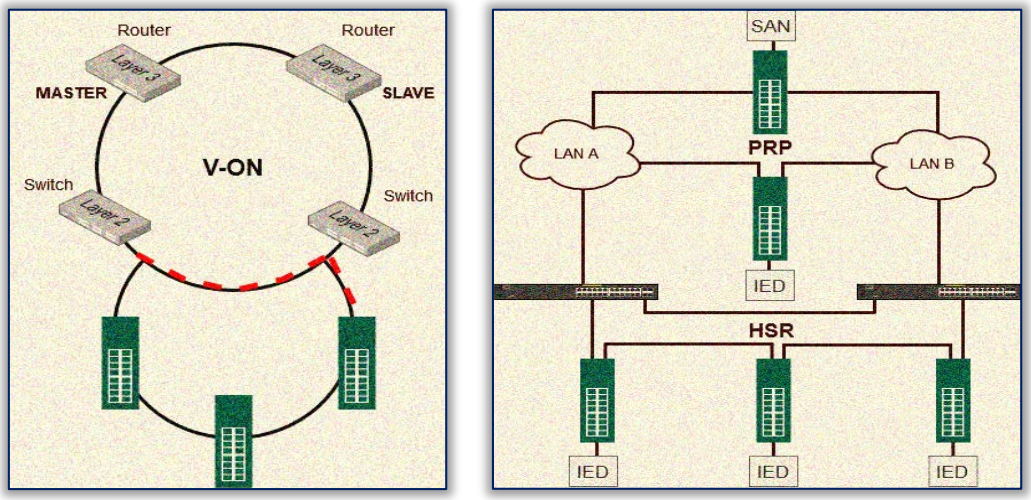

Figure 9. V-ON and PRP HSR [15]

4. INDUSTRIAL COMPUTERS

Usual workstations used in office applications are not suitable for industrial environments (presence of oil, gas, and extreme temperature). Like network devices, computers are exposed to various interfering signals and their DIN-rail mounting is a great advantage due to their ease of installation. Thus, industrial environments also prefer special workstations (e.g. Figure 10), which can be panel PCs with a display.

Figure 10. Industrial computers [9][8]

5. MANAGING USERS

In an environment where the number of users exceeds 20 and the use of the equipment is not limited to one location, i.e. a user needs to log in to different locations for work, central authentication is the best solution. The key idea of a server-based solution is that the credentials of the user are sent to a server at login. The use of an authentication server is also essential for managing a large number of network devices. A protocol providing the so called AAA functionality is the right solution for this purpose. The acronym refers to the following three tasks.

≡ Authentication – ensure the identification of the user.
≡ Authorization – ensure the permission management.
≡ Accounting – ensure the logging of the activities.

The most commonly used AAA protocols are Terminal Access Controller Access-Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and Diameter [16]. The AAA configuration of a router for a RADIUS protocol is presented below.

R1(config)#aaa new-model
R1(config)#radius-server host 192.168.1.3
R1(config)#radius-server key Radius12345
R1(config)#aaa authentication login default group radius

The user database can be on the authentication server, or the server can be connected to a Lightweight Directory Access Protocol (LDAP) service or Windows Active Directory service (Figure 11). Thus one can use a database to provide authentication for network devices, office workstations, and industrial equipment.

6. SUMMARY

This article gives a broad picture of what is possible in today's industrial environment. It is important to consider all areas when designing IT systems. Different technologies need to form a common unit to ensure proper and safe operation. IT components and tools integrated into industrial systems are not the building blocks of traditional market segments, so their cost may be higher, but it pays off more than a production system to build a well-functioning, reliable and secure IT system [23].

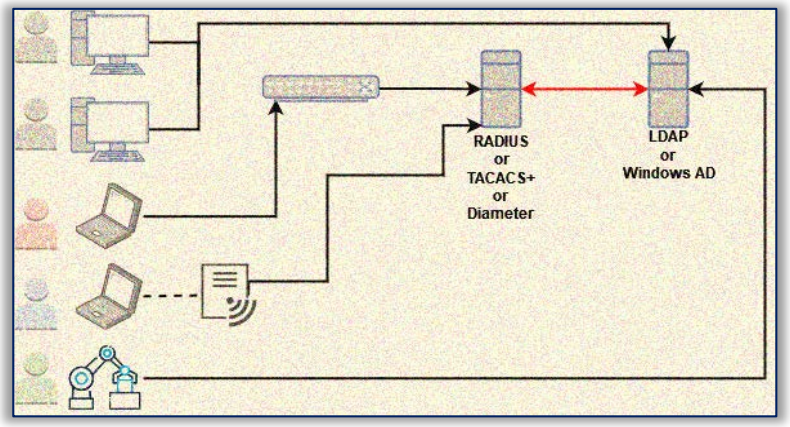

Figure 11. Centralized user management

Acknowledgements

Authors would like to thank the staff members of the institutions involved in the project - Nádor Rendszerház Kft., Controlsoft Automatika Szolgáltató Kft., GAMF Faculty of Engineering and Computer Science of the John von Neumann University. We are grateful for the support of the research, which was carried out within the framework of the grant 2020-1.1.2-PIACI-KFI-2020-00062 "Development of an industrial packaging machine with modular design for Industry 4.0 by integrated data analysis and artificial intelligence-based optimization, error analysis". Project is implemented with the support of the Hungarian State and the European Union, co-financed by the European Social Fund, in the framework of the Széchenyi 2020 programme.

References

[1] A Brief Introduction to Cisco Single-Mode SFP Modules, https://www.fiber-optic-components.com/cisco-1g-single-mode-sfp.html
[2] Cat8.2 Copper Cable, Draka, https://www.commscentre.com/cat82.html
[3] M. Cuaresma: Turbo Ring and Turbo Chain, Quantum Automation, https://www.quantumautomation.com/
[4] E DIN EN IEC 63171-5 VDE 0627-171-5:2020-05: Connectors for electrical and electronic equipment – Product requirements
[5] J. C. Haartsen: The Bluetooth radio system, IEEE Personal Communications 7, 2000, pp. 28-36
[6] IEC 63171-2:2021 Connectors for electrical and electronic equipment - Part 2: Detail specification for 2-way, shielded or unshielded, free and fixed connectors: mechanical mating information, pin assignment and additional requirements for type 2.
[7] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Std. 1588-2019 (Revision of IEEE Std 1588-2008), pp.1-499, 2020
[8] Industrial Panel PC, https://www.anxinpc.com/Industrial_panel_PC_with_D525/.
[9] Industrial PC COMPACT C7, https://www.syslogic.de/eng/industrial-pc-compact-c7-core-i-7th-generation-85598.shtml
[10] ISO/IEC 11801-1:2017, Information technology — Generic cabling for customer premises — Part 1: General requirements
[11] D. Jiang, Y. Wang, Z. Lv, S. Qi, S. Singh: Big Data Analysis-based Network Behavior Insight of Cellular Networks for Industry 4.0 Applications
[12] Layer 2 Managed Switches, https://www.moxa.com/en/products/industrial-network-infrastructure/ethernet-switches/
[13] LC-SC Duplex Singlemode 9/125 (OS2) Fiber Optic Patch Cable, https://icc.com/product/lc-sc-duplex-singlemode
[14] K.S. Kiangala, Z. Wang: An Effective Communication Prototype for Time-Critical IIoT Manufacturing Factories Using Zero-Loss Redundancy Protocols, Time-Sensitive Networking, and Edge-Computing in an Industry 4.0 Environment
[15] Moxa Redundancy Technologies, https://www.moxa.com/en/spotlight/industrial-ethernet/redundancy-technology/technologies
[16] C. Paquet: Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide, Cisco Press, 2013.
[17] A. Pásztor, T. Kovács, Z. Istenes: Piconet and Scatternet Communication Networks in Swarm Intelligence Simulation with Mobile Robots, Buletinul Stiintific al Universitatii Politehnica din Timisoara Romania, Seria Automatica si Calculatorae / Scientific Bulletin of Politechnica University of Timisoara Transactions on Automatic Control and Computer Science 54(68):(3) pp. 131-136. (2009)
[18] Pásztor, T. Kovács, Z. Istenes: Swarm intelligence simulation with NXT robots using Piconet and Scatternet, 5th International Symposium on Applied Computational Intelligence and Informatics, SACI 2009. Timisoara, Romania, 2009.05.28-2009.05.29.IEEE Hungary Section, pp. 199-204
[19] Perle Systems Technical Notes - PTP - Precision Time Protocol IEEE 1588 V1 and V2 PTP Boundary clock capabilities in Industrial Managed Switches https://www.perle.com/supportfiles/precision-time-protocol.shtml
[20] PTP - Precision Time Protocol, IEEE 1588 V1 and V2 PTP Boundary clock capabilities in Industrial Managed Switches, Perle Systems Technical Notes https://www.perle.com/supportfiles/precision-time-protocol.shtml
[21] ROLINE S/FTP Patch Cord Cat.8 (Class I), https://www.secomp-international.com/
[22] Test on gases evolved during combustion of materials from cables. Part 1: Determination of the halogen acid gas content (IEC 60754-1:2011 + corrigendum Nov. 2013)
[23] S. Saniuk, A. Saniuk, D. Caganova: Cyber Industry Networks as an environment of the Industry 4.0 implementation Big Data Analysis-based Network Behavior Insight of Cellular Networks for Industry 4.0 Applications
[24] S.Seereiner: Die Steckerfrage ist bei Single Pair Ethernet noch nicht entschieden, https://www.all-electronics.de/

copyright © University POLITEHNICA Timisoara, Faculty of Engineering Hunedoara,
5, Revolutiei, 331128, Hunedoara, ROMANIA
http://annals.fih.upt.ro