International Journal of Innovative
Computing, Information and Control
Volume **12**, Number **5**, October **2016**

 ISSN 1349-4198
pp. 1505–1522

INDUSTRIAL ETHERNET NETWORKS AND APPLICATIONS

Alexandre Baratella Lugli, Jonas Eduardo Moreira Souza
Leandro de Oliveira Pessoa, Ramon Lucano Ribeiro Rodrigues
and Thomás Henrique Moreno Tarifa

Department of Industrial Automation
National Institute of Telecommunications
CEP 37.540-000, Santa Rita do Sapucaí, MG, Brazil
baratella@inatel.br

Received April 2016; revised August 2016

Abstract. *The Industrial Ethernet Networks began with the objective to simplify the communication through the industrial area, aiming a cheaper implementation cost and a bigger flexibility of the system than common Ethernet Networks. This article is a study of the main Ethernet IP Networks, PROFINET, ETHERNET/IP and HSE, presenting the major features and application. It also counts with a comparison between the similar characteristics of these standards, and next to the study, a real application will be introduced.*
Keywords: Industrial application, Industrial Ethernet, Case study

1. **Introduction.** The TCP/IP model, formulated by Vinton G. Cerf and Robert E. Khan, is a union of two communication protocols between network computers: TCP (Transmission Control Protocol) and IP (Internet Protocol). It came in order to make the connection between different types of network, providing services such as voice, data and image [1].

The Ethernet protocol, developed by Robert M. Metcalfe, operates at the data link layer of the TCP/IP model (Transmission Control Protocol/Internet Protocol) and aims to realize the communication of local networks, also known as LAN (Local Area Network) [2,13,14].

With the association of digital controls and smart sensors developed in the 80s, there arose the idea of creating innovative digital networks, called fieldbuses, which came to replace the 4-20mA standards. These new networks promised simplification and flexibility of the system, where the exchange of information between the factory floor and administrative levels would be made by a single physical mean [3,13,14].

There are a lot of (many) fieldbuses in the industrial area, such as DeviceNet, PROFIBUS, Foundation Fieldbus e Interbus. Over time, communication and interaction between these different fieldbuses became necessary, so they had to be adapted to the Ethernet technology. However, each manufacturer developed its own standard for Industrial Ethernet, each of which (each one of them) differed in the use of TCP/IP layers and application for each user. These differences did not meet (attend or answer) the interconnectivity between the various standards [4,13].

Altogether there are fourteen protocols that use the Industrial Ethernet: PROFINET, Ethernet/IP, HSE, Modbus/TCP, EPA, EPL, EtherCAT, IEC 61850, JetSync, PNET, Sercos III, SynqNet, TCnet and Vnet/IP [1,14].

This article aims to conduct the study of the most used on the market: PROFINET, Ethernet/IP and HSE, and intends to present a comparison between them and conduct a

study of a real case of industrial use. The comparison study includes a lot of parameters, such as: logical, physical layers, topology, redundancy, interoperability and safety applications. The comparison objective is shown several different parameters about industrial networks.

2. Industrial Ethernet Networks.

2.1. **PROFINET.** The PROFINET standard, regulated by PROFIBUS and PROFINET International (PI), uses the Ethernet protocol for industrial networks. First, the standard was created in order to work in the automotive industry. However, with its high flexibility, reliability and full integration of the whole industrial area, from the factory floor to administrative and management levels, the protocol has expanded to other sectors of the industry, reducing costs and engineering risks in the industrial environment [3,5].

It also resulted in the migration of automation systems centralized to distributed systems, just modifying its layers in the TCP/IP architecture [4]. One of the PROFINET advantages is that it supports the integration of a single field device to real-time applications. The PROFINET protocol consists basically of three devices, as follows [3,5]:

- IO Controller: Master, where the control program is executed;
- IO Device: remote field device that maintains communication with a controller;
- IO Supervisor: programmable graphics device where the network analysis is made.

There is no kind of hierarchy between these devices, which means every IO has the same importance in a PROFINET network. These devices are illustrated in Figure 1 [5,15].

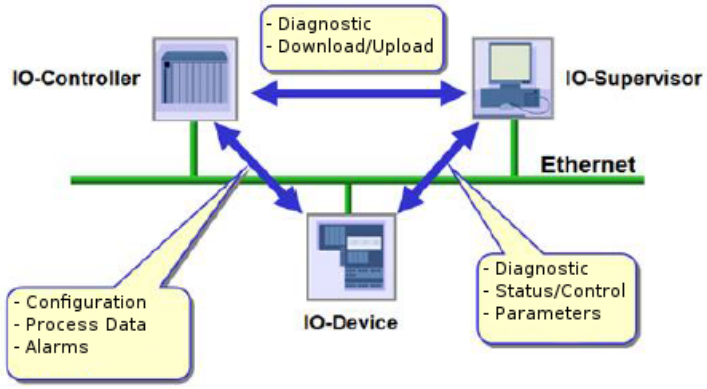

FIGURE 1. IO devices of PROFINET [5,15]

There are two kinds of PROFINET networks, which are [3,5]:

- PROFINET I/O (Input/Output): used in real-time applications where the information should be transmitted in a quick way at a very critical time interval;
- PROFINET CBA (Component Bases Automation): used in applications where there is no need for concern about the critical time, for example, the connection between the PROFINET protocol CBA and PROBUS DP protocol.

PROFINET is a very flexible protocol, where multiple topologies can be implemented together. Due to the extensive use of switches in PROFINET networks, the most widely used topology is star. This topology is based on communication of various IO Devices in a single switch. If any failure happens on a node, the other nodes will operate normally. However, if the switch fails, the communication between elements will be compromised. Figure 2 shows the Star topology [5,15].

The Tree topology is another kind of topologies used on PROFINET. It is a combination of several star topologies, interconnected by a single switch that works as a signal

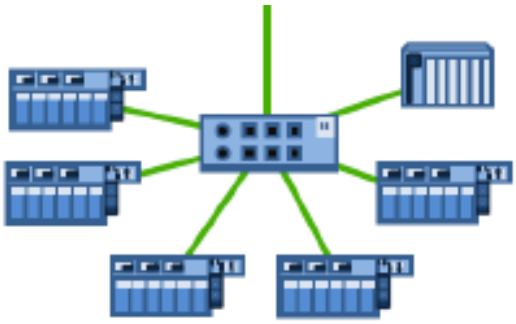

FIGURE 2. Star topology [5,15]

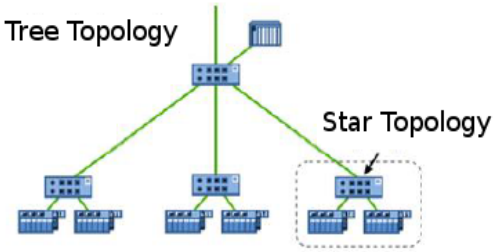

FIGURE 3. Tree topology [5,15]

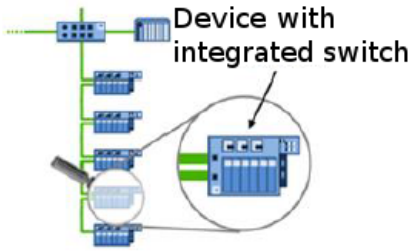

FIGURE 4. Bus topology [5,15]

distributor for star ends. This kind of topology can be used for example on an industrial plant, as shown in Figure 3 with the Tree topology [5,15].

The most known topology in the industrial area is the Bus topology, where each IO device contains an integrated switch that facilitates its implementation. Therefore, it is not a necessary centralized switch on the network. The problem with this topology is that if one element fails, the other elements will also be compromised. The Bus topology is shown in Figure 4 [5,15].

To solve the problem of Bus topology, the ring topology was created. It consists on the interconnection of bus topologies, creating a network redundancy. It is being carried out the study of a new topology, called "*butterfly*". This topology is an interconnection of one or more ring topologies creating connection points distributed across the rings on network.

Figure 5 shows the basic structure of the PROFINET standard, detailing the protocol types.

There are basically three different ways to perform the communication in PROFINET protocol: NRT (NonReal Time), SRT (Soft Real Time) and IRT (Isochronous Real Time) [3,12].

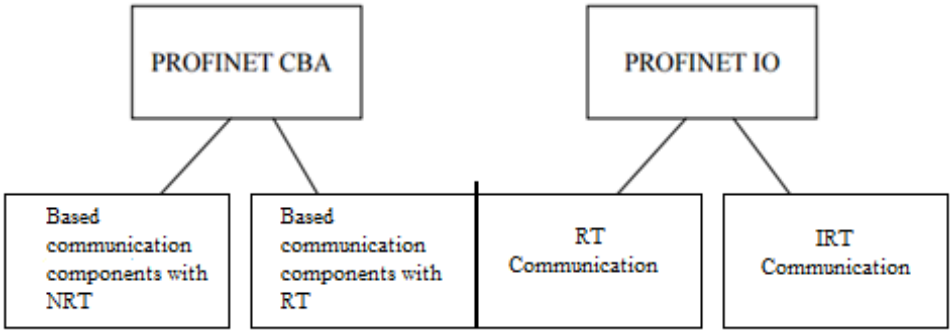

FIGURE 5. The basic structure of PROFINET [4]

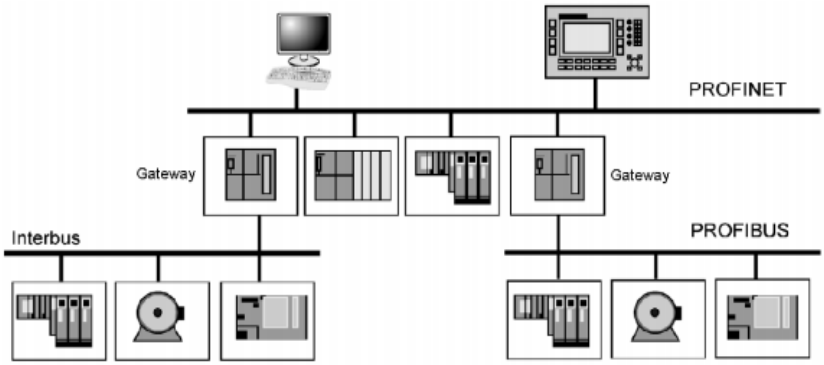

FIGURE 6. Interconnectivity between PROFINET/PROFIBUS and PROFINET/Interbus [3]

The first type, NRT, is based on the TCP/IP pure architecture and processing is approximately 100ms. It is used to perform the interconnectivity of PROFINET CBA PROFIBUS to PROFINET CBA Interbus, via gateways (also known as proxies). Figure 6 illustrates this interconnectivity [3,12].

The second type, called SRT establishes a direct communication Ethernet physical layer to the application layer. Because of this "shortcut" of communication, the lengths of the messages decrease, requiring less transmission time, being approximately 10ms. It is applied both in the network PROFINET I/O as in PROFINET CBA [3].

Finally, the form called IRT also establishes a direct communication Ethernet physical layer to the application layer. A major application of this communication is the motion control of robots, where the information response time is critical, being less than 1ms. It is only used with PROFINET I/O [3,12]. Figure 7 illustrates the way of an application for each type of PROFINET communication.

Figure 8 illustrates the layers of the three types of PROFINET communication.

PROFINET IO network is an extension of the PROFIBUS DP protocol. It operates directly on the field elements, making the sensor readings and updates of the output signals [3,12]. The network communication board PROFINET IO is shown in Figure 9 and follows the same standard Ethernet IEEE 802.3 model. The main difference is in the field Frame ID field, which has the function of identifying the type of network communication. The PROFINET IO frame has at least 72 bytes, adding a header, information and error checking [3,12].

The Preamble field is comprised of 7 bytes, each containing a sequence 10101010. It has the function of performing the synchronization of the network element [3,12].

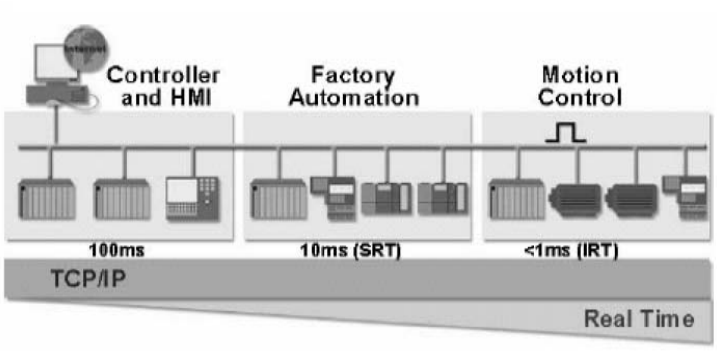

FIGURE 7. Types of communication and network time [5]

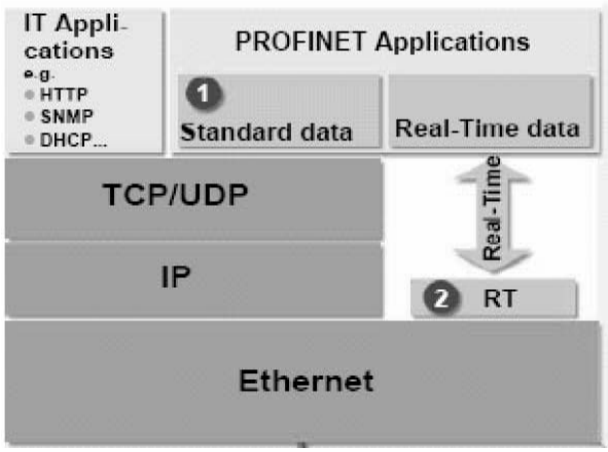

FIGURE 8. Types of communication and layers [3,5]

	Ethernet Frame											
InterFrame Gap 12 Byte	Pre-amble 7 Byte	Sync 1 Byte	MAC 6 Byte	MAC 6 Byte	VLAN 2 Byte	Ether-type 2 Byte	Frame ID 2 Byte	PROFINET Data 40*...1440 Bytes	Cycle Counter 2 Byte	Data-Status 1 Byte	Trans Status 1 Byte	FCS 4 Byte

FIGURE 9. PROFINET IO framework [8,12]

Sync field is 1 byte long and is responsible for defining the frame through the sequence 10101011 [3,12].

The MAC fields address tells the physical address of the target element and origin of the transmitted message. Each MAC field has 6 bytes [3,12].

The Ether-type field has 2 bytes and identifies whether there was a cyclic data exchange between the provider and the consumer. This exchange may be performed by elements such as switches and controllers [3,12].

The VLAN field is added in the frame for the cyclic data have priority in switches. It contains 2 bytes.

Field ID Frame has 2 bytes and performs the identification of the PROFINET communication type being used, IRT or SRT [3,12].

The DATA field can be formed 40-1440 bytes.

The FCS field (Frame Check Sequence) has 4 bytes. It performs the check for errors in communication through a CRC algorithm (Cyclic Redundancy Check) [3,12].

The PROFINET network elements are based on reliability and communication in real time. The usability is another system's important fact; hence the security mechanisms must be developed in a way to work with usability, aiming the improvement of PROFINET operations. The main objective of these mechanisms is to improve the reliability and availability of production units. One of its characteristics is the robustness of the devices against an overload of traffic on the network. However, these devices do not have intrinsic safety; in other words, attacks destined to them should be prevented or identified by external measures.

The PROFINET provides a security protocol called PROFIsafe. This protocol supports secure communication network for devices that target security with security controls. Therefore, the field devices can be used in safe automation activities until SIL3 (Safety Integrity Level 3). The PROFIsafe also performs other functions, for example, security functions EM 954-1 as STO (Safe Torque Off) or SLS (Safely Limited Speed). These functions enable (allow) you to reduce downtime of the components also allow (permit) the realization of assemblies while the parts are moving, without compromising the workers to mechanical hazards [5].

In order to work properly and safely, the PROFINET has to respect some conditions:

- Security in systems without their own security features – The security architecture of PROFINET must provide safety for any system;
- Real-time operation – The security mechanisms should not interfere on real-time transmission capacity of the system. Another condition is that these mechanisms should not delay the Human Machine performances, which often have a low processing time;
- Transparent integration with effective cost – A great cost-benefit ratio can be achieved through the integration of security measures that also provide security for groups/area.

The first step in the exchange of data between an IO controller and IO device is to create a logical connection between these elements, called Application Relationship (AR). With the establishment of this connection, some channels are created with the function to set alarms and process data. These channels are called Communication Relationship (CR). The AR and CR are shown in Figure 10.

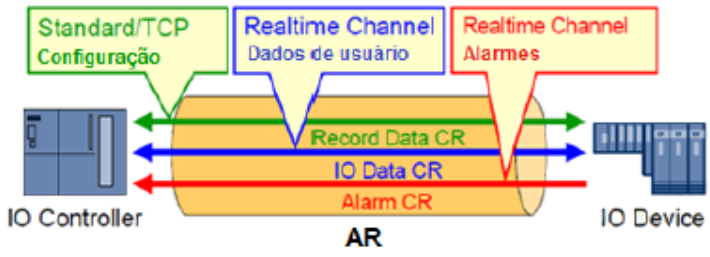

FIGURE 10. AR and CR [15]

Each device can have more than one AR. Therefore, an IO device can be controlled by one or more IO controllers, making flexible the use of IO device against various applications.

2.2. **Ethernet/IP.** The Ethernet/IP (Ethernet Industrial Protocol) was standardized by the ODVA (Open DeviceNet Vendor Association) and is a protocol that is based on the application layer TCP/IP [4].

The Ethernet/IP has only one type of communication, based on TCP/IP model. However, this communication has two modes of transmission that depends largely on the user

TABLE 1. Comparison between the Ethernet/IP transmissions [6]

Transmissions	Messages	Description
Explicit	Information	Transfer of non-critical data
Implicit	Data I/O	Real-time data
Implicit	Real-time synchronization	Real-time synchronization

application. Table 1 shows a comparison between the messages, transmission modes and applications. Thus, the transmissions are [6]:

- Explicit: this form of transmission uses the TCP (Transmission Control Protocol). It is applied in activities that are not considered critical, i.e., they do not require a low processing time. An example would be the exchange of information between controllers and HMIs (Human Machine Interface), where the cycle of a temple can be equal to or greater than 100ms;
- Implicit: this form of transmission uses the UDP (User Datagram Protocol). It is applied in activities which must be cyclical, requiring low processing time. An example would be the communication between I/Os, where the response time has to be around 10ms.

The Ethernet/IP application layer is modeled by the CIP protocol (Commom Industrial Protocol) which was developed by ODVA. The CIP provides a set of standards and services to control devices via network messages. It has the function of providing the information generated by the system. CIP is encapsulated in the TCP and UDP protocols being transmitted (is transmitted) according to the message type. Figure 11 shows the architecture of standard Ethernet/IP [6].

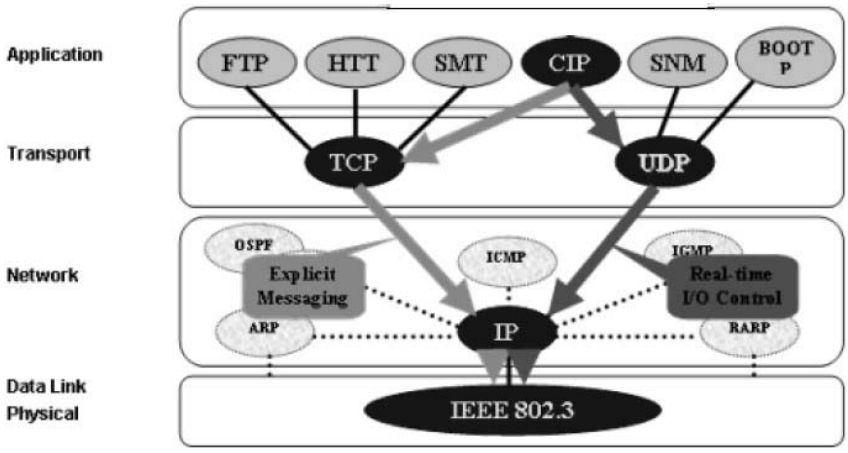

FIGURE 11. Types of transmissions of Ethernet/IP [1]

The CIP can perform communication between elements based on the DeviceNet protocol, also developed by ODVA, with its own Ethernet/IP network. This application is shown in Figure 12. However, the CIP does not communicate with the application layer protocols regulated by other organizations, for example, PROFINET. Therefore, there is no interconnectivity between the various Ethernet networks [6].

The frame of the Ethernet/IP protocol data link layer is illustrated in Figure 13 and follows the same standard IEEE 802.3.

The Preamble field consists of 7 bytes of a sequence of 10101010. Its purpose is to synchronize the network element [6].

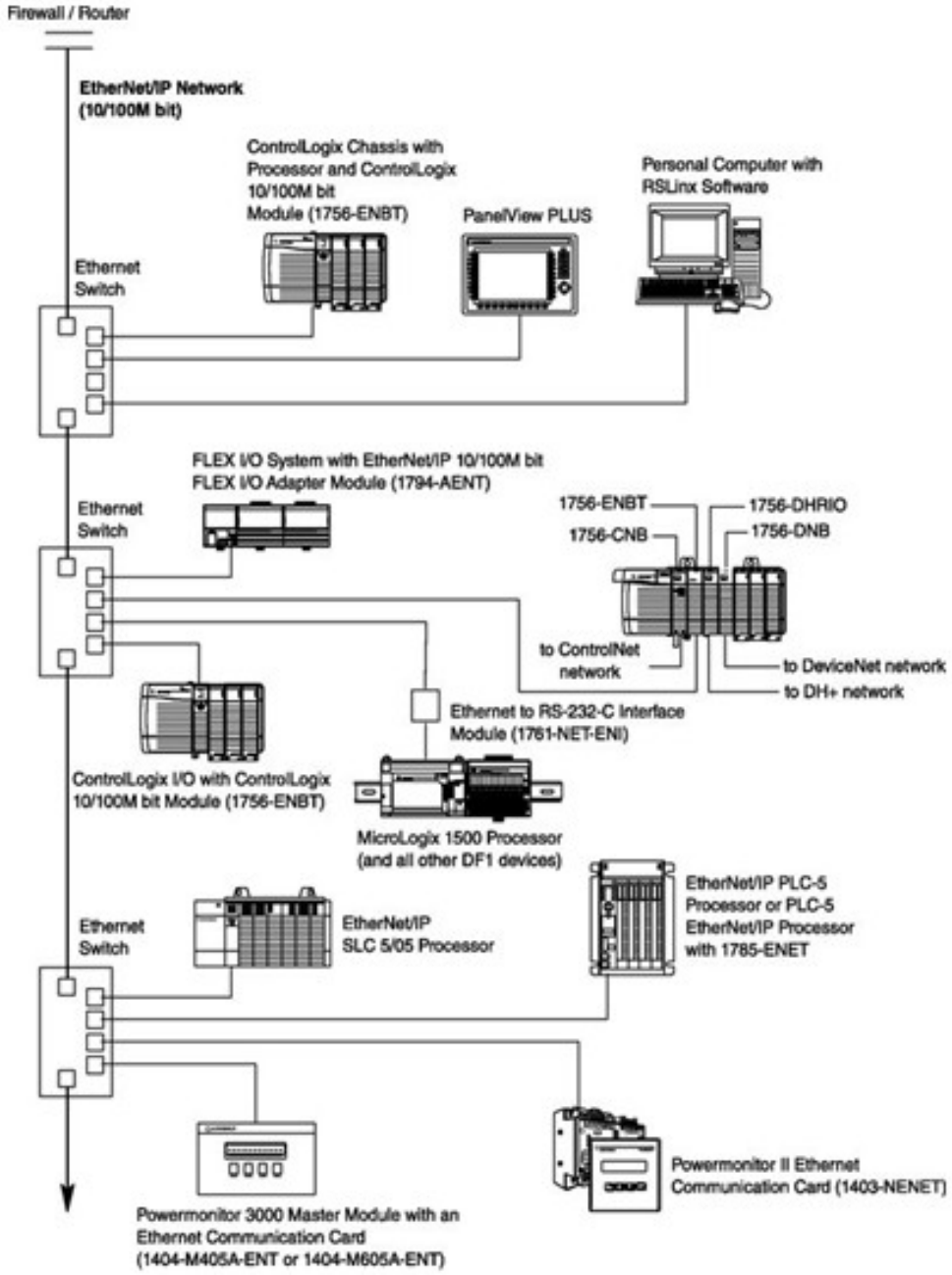

FIGURE 12. Applications of an Ethernet/IP network [6]

Preamble	SFD	MAC	MAC	Type	Data	FCS
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

FIGURE 13. Framework Ethernet/IP of the link layer [8]

The SFD field has one byte and is responsible for marking the end of the frame through the sequence 10101011 [6].

MAC field tells the physical address of the target element and origin of the transmitted message. Each MAC field has 6 bytes [6].

The type field consists of 2 bytes and identifies the protocol used and what the priority of each transmission message is [6].

The data field may be formed between 40 and 1500 bytes [6].

The FCS field (Frame Check Sequence) is 4 bytes. It has the function to check errors in communication through a CRC algorithm (Cyclic Redundancy Check) [6].

The frame of the Ethernet/IP network layer illustrated in Figure 14 shows as the main protocol, the IP (Internet Protocol). The IP is a service not connection-oriented and its objective is to provide, in an efficient way, the data transport from the source to destination, without worrying about the confirmation of receipt. The upper layers hold this guarantee delivery of messages.

Preamble	SFD	MAC	MAC	Type	IP	Data	FCS
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	24 bytes	22-1476 bytes	4 bytes

FIGURE 14. Framework Ethernet/IP of a network layer [8]

Figure 15 shows in detail the IP header structure.

+	0-3	4-7	8-15	16-18	19-31
0	Version	Overhead	Service type	Total length	
32	Identifier			Flags	Offset
64	TTL		Protocol	Checksum	
96	Source Address				
128	Destination Address				
160	Options				
192	Data				

FIGURE 15. IP framework [6]

The transport layer has two protocols, the TCP (connection-oriented) and UDP (not connection-oriented). The main purpose of this layer is to establish the connection between the two ports that will exchange information [6].

In the industrial area, both TCP and UDP can be used depending on the application and transmission requirements [6].

The TCP protocol, shown in Figure 16, is responsible for the configuration and parameterization of the network elements, consisting of 24 bytes [6].

Source Port		Destination Port	
Sequence Number			
Acknowledge Number			
Offset	Reserved	Flags	Window
Checksum		Urgent pointer	
Options			Padding

FIGURE 16. TCP framework [8]

Source Port	Destination Port
Length	Checksum

FIGURE 17. UDP framework [8]

The UDP protocol illustrated in Figure 17 is responsible for the exchange of information between network elements, because it has greater speed in the transport of messages, being formed by 8 bytes [6].

2.3. **HSE.** The solution HSE (High-Speed Ethernet) was developed by the Fieldbus Foundation and is based on the Ethernet protocols, IP and TCP/UDP. It is designed to achieve interoperability between the Foundation Fieldbus H1 networks to existing surveillance systems, shown in Figure 18. Table 2 shows the differences between the H1 network and the HSE.

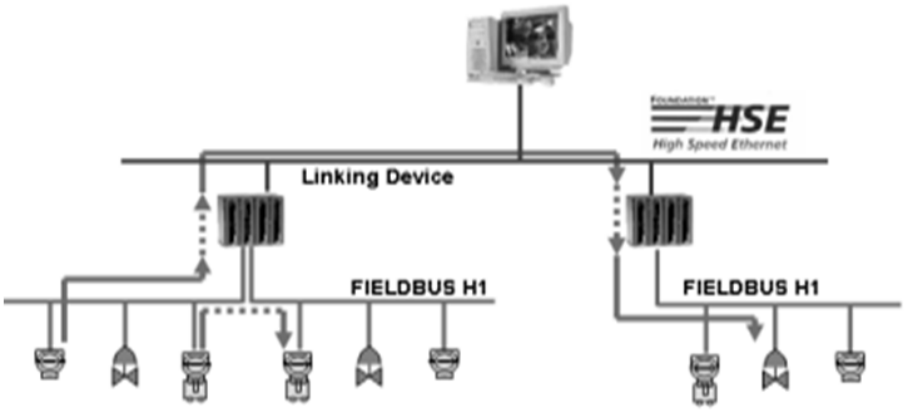

FIGURE 18. Interoperability between H1 and HSE [3]

TABLE 2. Comparison between the H1 network and the HSE [3]

	H1	HSE
Rate of transmission	31.2kbps	100Mbps
Distance	1900 meters	100 meters
Two wires	Yes	No
Multidrop	Yes	No
Intrinsic safety	Yes	No
Feeding by bus	Yes	No
Redundancy	No	Yes
Deterministic	Yes	Yes

The HSE network has four types of devices, as shown in Figure 19, as follows [3]:

- *Host Device* (HD): it is a station where the job settings are performed;
- *Link Device* (LD): it is the device that realizes the interoperability of the H1 networks to HSE;
- *Gateway Device* (GD): it is the device that performs the interconnectivity of HSE with one or more external networks;
- *Ethernet Device* (ED): it is the device that connects directly the control and measurement applications.

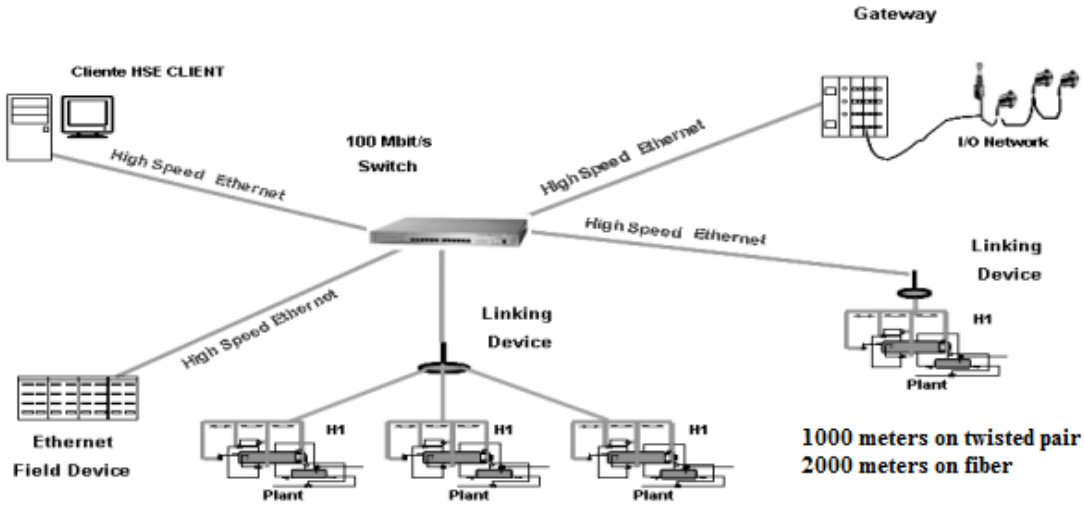

FIGURE 19. HSE devices [3]

The UDP protocol illustrated in Figure 17 is used in the client/server by the HSE. The reliable delivery of information is managed by the application layer instead of the transport layer. If the application layer is not getting the desired information, it will try again, and if it fails, the system enters a safe action to ensure the correct performance of the HSE network [3].

The information will become obsolete as they are updated several times per second. So it is not mandatory relay with guarantee of delivery provided by TCP. Therefore, it uses UDP, which transmits a new value on the sensor instead of trying to relay obsolete values that will be discarded anyway [3]. UDP is multicast, or in a single communication, it may be used by various receptors. This case type is most widely used for automation where a reading sensor is used most often in more than one location [3].

The table of HSE network data link layer is shown in Figure 13 and follows the same pattern model IEEE 802.3 [3].

2.4. **Network security.** It has been shown that the Ethernet protocol has become critical when it comes to the industrial area, because it can make the integration of various technologies. However, risk of breaches has increased, as virus attacks and other malicious programs. So it is necessary to analyze the potential risks to the network and thus implement appropriate security concepts [15].

In industrial automation systems, an operational disturbance caused intentionally, causing failures to the system, can be considered a security problem. There are many important factors to be considered when it comes to security. A major one is the strength or ability of a device to withstand an excessive volume of data traffic. Another important factor is the ID of those who access the system and when they access it. In other words, the access device must be limited [15].

There are some rules for an effective architecture, which are:

- As simple as possible, but not too simple. A good system should be understood by the whole group involved, not only the safety technicians;
- As uniform as possible, if a rule is applied at some time, it must also be applied in other similar applications;
- Understood and supported by all involved parts. If the team is aware of everything about the system, surely it will be more effective on implementation;
- Discussed by all members of staff.

The main purpose of the security measures in automation is to achieve a reliable network that meets all the needs, considering an important point, that automation networks are designed for maximum performance and not for maximum security. Thus, the challenge was to fulfill all these needs ensuring confidentiality, integrity and availability of systems, even though they are under attack [15].

With the increase of the I.T in Industrial Systems, it was suggested that I.T solutions could meet the needs of Industrial Plants. However, there are some significant differences between these two areas, which are:

- Functional Requirements and Performance – It can be mentioned that the delay and jitter in data transmission, may be tolerable; however, on an Industrial Automation System the delay and jitter may be a great problem;
- Man-Machine Interaction – Whereby the Automation Systems must always remain available, even in delicate situations, a reliable operation and control, could be done any time;
- Reliability and availability – Sudden failure of the production system is not acceptable. So to ensure high availability, several intensive tests are done during the devices installation;
- Risks and safety requirements – These factors differ significantly in an industrial area compared to a business area. Risk assessments are not transferable, taking more stringent safety measures;
- Differences in security architecture – Due to reasons of cost, redundancy mechanisms are implemented in an industrial automation system, typically on a device that could cause serious problems to the plant;
- Security Objectives – At I.T. (Information Technology) area, the priority order is:
  1. Confidentiality;
  2. Integrity;
  3. Availability;
- Although in automation systems, the priority order is:
  1. Availability;
  2. Integrity;
  3. Confidentiality.

3. **Comparison between Protocols.** Table 3 shows the comparison between similar features of Industrial Ethernet networks discussed here.

4. **Real Case Practical Study.** The case study conducted at the University of São Paulo (USP) by students Afonso Celso Turcato, Rogerio Andrade Flauzino, Guilherme Serpa Sestito, André Luiz Dias and guided by prof. Dennis Brandão, aims to make a diagnosis and solutions for DoS attacks in PROFINET networks [7].

4.1. **Attack on networks.** The network attacks may be anomalies that are displayed in a normal performance expected traffic network. There are several signs that indicate the attacks, such as misuse of a network, failure events, and infrastructure problems in data collection, among others. Therefore, not every abnormality can be considered an attack, but still must be examined as a precaution. Regarding the operation, the anomalies include the network failure events. These events may pause the operation of devices, equipment addition or misconfiguration of the network devices. The following events are considered anomalies.

- Anomalies flash crowd consist of a rapid increase in network traffic. This traffic decreases gradually with time.

- Measurement anomalies represent failures in the diagnostic system and collection of data that results in distorted receipt of network status information.

TABLE 3. Comparison between the PROFINET network, Ethernet/IP and HSE [5,9-11]

	PROFINET	Ethernet/IP	HSE
Physical environment	- twisted pair - fiber	- twisted pair - fiber	- twisted pair - fiber
Distance	- up to 100 meters of the twisted pair without a repeater - up to 2000 meters of fiber without a repeater	- up to 100 meters of the twisted pair without a repeater - up to 2000 meters of fiber without a repeater	- up to 100 meters of the twisted pair without a repeater - up to 2000 meters of fiber without a repeater
Maximun number of nodes	256	256	256
Voltage applied to the nodes	24 Vdc	24 Vdc	24/48 Vdc
Types of communication	- NRT (*NonReal Time*) - SRT (*Soft Real Time*) - IRT (*Isochronous Real Time*)	Follows exactly the model TCP IP, with two modes of operation	Based on protocols Ethernet, IP and TCP/UDP
Interoperability	Functional interoperability between network elements is certified through the transposition of the existing application profiles.	Full interoperability with other Ethernet/IP products, certified by the ODVA	Interoperability is performed from the Link Device, which makes the communication between various segments Fieldbus H1 with HSE.
Interconnectivity From Proxies, PROFINET offers a transparent communication with PROFIBUS, Interbus, ASI, and other protocols based on Industrial Ethernet	From a transparent routing with DeviceNet and ControlNet.	From the GD device (gateway device), communication is made from an HSE network with the network H1.	
Network topology	- star - ring - tree - bus - star - ring - tree - bus	- star - ring - tree - bus	
Rate of transmission	up to 1 Gbps	up to 1 Gbps	up to 1 Gbps
Intrinsic safety	Implemented transparently through proxies	Through bridge with transparent routing	No
Redundancy	Yes, with a ring topology to the physical medium with MRP technologies (Media Redundancy Protocol) and MRPD (Media Redundancy with Planned Duplication). It has the possibility of another kind of redundancy, the system with two controllers (PN I/O controllers) synchronized.	Yes, one built-in switch technology in ring topology	Yes, several levels of redundancy, such as field sources, signal conditioners, controllers and interface cards, communication master (LAS) and Ethernet networks
Distributed intelligence	Yes, with smart devices is allowed direct communication Controller/Controller.	Yes, with smart devices is allowed distributed control with an exchange of messages such as Producer/Consumer.	Yes, is performed by means of functional blocks, providing a uniform configuration throughout the system
Types of traffic	Is a cyclic data exchange between Producer/Consumer, QoS priority layer 2 based on the IEEE 802.1p	Unicast, Multicast and Broadcast Priority according to IEEE 802.1Q/p	Uses the data link layer of the Ethernet protocol, with CSMA-CD protocol (Carrier Sense Multiple Access with Collision Detection)

to be continued

continued

Advantages	- Real-time communication - I/O connection distributed - Motion Control - IT standards for diagnosis and safety - Provides security protocol (PROFIsafe) - Integration of multiple protocols	- Uses the Ethernet protocol transport layer - Lower cost system - High-performance system - Flexibility in topology - Web service	- Open architecture - All features of the TCP/IP model - Low cost of hardware - Simplifies network architecture - Uses standard network equipment
Disadvantages	- As the environment is a hostile industrial environment, the development of an industrial dedicated switch was required.	- As the environment is a hostile industrial environment, the development of an industrial dedicated switch was required. - Overloading the network with UDP messages even if the network is properly configured.	- As the environment is a hostile industrial environment, the development of an industrial dedicated switch was required. - Does not provide security protocol - Restrictions for cabling are more severe

- The attacks anomalies can be identified from the data traffic flow. These attacks can undermine the reliability of the system and they are due to weakness or errors that exist in network devices.

The types of attacks are based on criteria such as the source, target and objectives. As for the origin, they are identified in:

- External: It is an attack that is sent outside the network, where the attacker tries to get secret information or leave essential devices to the system off;
- Internal: It is an attack sent from within the local network, which crucial objective is to get the system resources.

Concerning the target, there are two types:

- Network attacks: In the case, the attacks are aimed at preventing the use of network resources or make that service unavailable;
- System attacks: In the case, the attack is to undermine the whole system, modifying passwords or changing important settings improperly in the equipment.

As objectives, the attacks can be divided into four types.

- DoS (Denial of Service): It is the attack that aims to overload the computing resources or the memory ones, and then the system may not meet the network's needs. Thus, the equipment becomes unavailable because it cannot be accessed. The DoS attack takes advantage of the vulnerability of protocols or programs to leave equipment or the network itself down. Smurf and Neptune are some examples of this attack.
- Probing: This attack aims to conduct a network general scanning, with the purpose of identifying vulnerabilities or weaknesses that could harm the system. It also identifies the features of each element connected to the network or the network's itself.
- R2L (Remote to Local Attacks): It is a penetration attack that uses a foreign network to send packages to any equipment in order to expose its vulnerabilities.
- U2R (User to Root Attacks): It is a penetrating attack that uses the own local network to send packets to a device, in order to expose their weaknesses.

4.2. **Attack accomplishment.** The attack carried out in this case study is a combination of a Probing attack followed by a DoS attack with an internal source, and with the main objective to stop the cyclical communication between the controller and the field module.

TABLE 4. Used equipments [7]

Equipment	Function
CPU 317-2 DP/PN	IO Controller
IM 11-3PN	IO Device
Switch Scalance X208	Switch
Computer	HMI Station
Packet/Traffic Generator and Analyzer	Attack

TABLE 5. Original system configuration [7]

IP Address	MAC Address	Equipment	Name
192.168.1.1	00-16-41-56-17-76	IO Controller	Controller
192.168.1.2	00-0E-8C-F6-13-42	IO Device	Device1

The PROFINET network system for this application consists of an IO controller, IO device and switch, which will be displayed in Table 4. The computer has a function of a remote viewing station (IHM).

The initial system configuration is shown in Table 5.

The topology in the system used was the star topology shown in Figure 20. The devices are interconnected via an industrial switch that supports a transmission rate of up to 100Mbps.

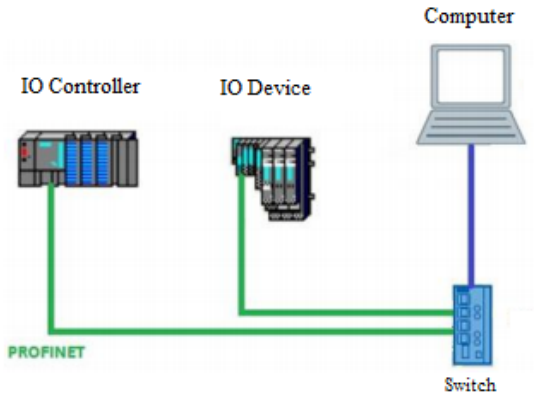

FIGURE 20. PROFINET system used in attack [7]

The objective of this attack is to change the field module name in a sudden and inappropriately way, making this equipment unrecognized by the controller. Even at the time of information exchange between IO controller and IO device, it is possible to perform this name change through the DCP-Set command, sent from a computer connected to the network. Thus, there is an interruption made of sudden form on the cyclic communication between IO controller and IO device. The attacks applied to the system are:

- *Probing*: when using the DCP protocol it is possible to collect critical information about the devices connected to the network, such as machine name, IP and MAC addresses;
- DoS: with the information collected by the first attack, a command to perform the name change of the field module is sent. This name will be unknown to the network and like this, will pause the cyclical communication with the IO controller.

There are four steps to accomplish these two attacks successfully, as follows:

- Send a DCP-Identify-All command (multicast) on the network to get information about the equipment;
- Do the filtering of the received data, identifying which equipments are field modules;
- Create random names for each field identified the module;
- Send DCP-Set command (unicast) for each IO device, changing their names with new names generated.

After the attack made by the DCP-Identify-All command, we found that the system had only one IO device. So to stop the cyclic communication of this device with the controller, just change its name, for example, device2. The configuration after the attack is shown in Table 6.

TABLE 6. System configuration after the attack [7]

IP Address	MAC Address	Equipment	Name
192.168.1.1	00-16-41-56-17-76	IO Controller	Controller
192.168.1.2	00-0E-8C-F6-13-42	IO Device	Device2

The sequence of commands to perform an attack on an IO device is shown in Figure 21. These DCP protocol commands are sent by the computer using the computer application Ostinato, like in Figure 22.

It is noticed that after carrying out the attack, as there is no more cyclical data exchange between controller and field module (restored manually), the outputs of all devices are required to take a default value.

4.3. **Defense perimeter.** The perimeter defense is the solution most widely used in industrial automation systems, where each network is a trusted zone and thus all the elements belonging to it can communicate with each other without any restrictions.

About DoS attacks, there are two possible solutions which are the prevention and detection of the attack. The first option limits the access to system resources to the maximum, causing the attacker to have no access to the network. An example of prevention is to prevent physical access to network elements. In the Ethernet standard, this can be accomplished by isolating the cables and equipment in a secure and locked position (physical

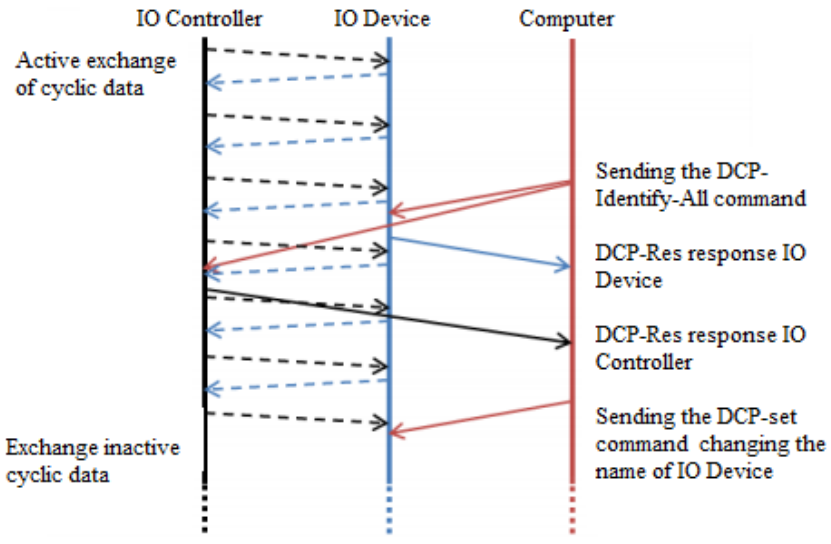

FIGURE 21. Commands to perform the attack successfully [7]

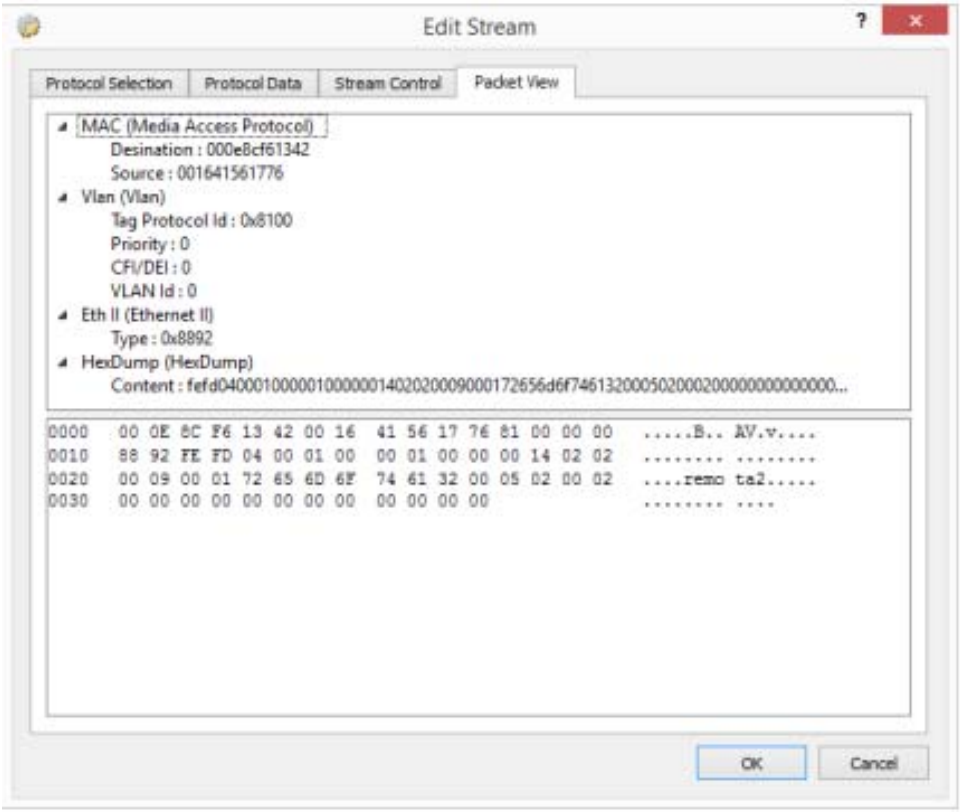

FIGURE 22. Computer application Ostinato [7]

security). However, not all cases use prevention. In this case, the DoS attack should be at least detected. Thus, the detection techniques attempt to identify any anomalies in the network and define whether this situation can be a DoS attack. If the attack is proven, some measures should be taken in order to minimize the consequences and try to prevent other parts of the network to be affected.

For industrial automation systems, it is proposed of a hybrid solution with these two cases presented.

5. **Conclusion.** The industrial Ethernet protocol has shown an essential technology when implemented in an industrial automation system. This protocol can satisfy the major needs in industry, for example, determinism, interconnectivity and flexibility of the network. The importance of industrial networks called deterministic networks that they have exact times to carry traffic information. Regarding interconnectivity, industrial networks perform the communication between various industrial protocols through gateways, for example, performing the interconnectivity between PROFIBUS and PROFINET. Even so, the industrial Ethernet protocol still has to grow in its negative aspects, especially in network security environment. This development and other improvements aim a better system performance, expanding its range of applications and simplifying the implementation.

REFERENCES

[1] A. B. Lugli, *Uma Arquitetura Distribuída Flexível para Aplicações Industrias Baseada no Padrão Ethernet*, Ph.D. Thesis, Itajubá/MG, Brazil, 2013.

[2] A. S. Tanenbaum, *Redes de Computadores*, 3rd Edition, São Paulo/SP, Brazil, Editora Campus, 1997.

[3] A. B. Lugli and M. M. D. Santos, *Redes Industriais Para Automação Industrial: ASI, Profibus e PROFINET*, 1st Edition, São Paulo/SP, Brazil, Editora Érica, 2010.
[4] P. Ferrari, A. Flammini, F. Venturini and A. Augelli, Large profinet IO RT networks for factory automation: A case study, *IEEE ETFA Conference (Conference on Emerging Technologies & Factory Automation)*, France, 2011.
[5] M. Popp and C. Webber, *The Rapid Way to PROFINET*, PROFIBUS Organization, 2004.
[6] A. B. Lugli and M. M. D. Santos, *Sistemas Fieldbus para Automação Industrial: DeviceNet, CANOpen, SDS e Ethernet*, 1st Edition, São Paulo/SP, Brazil, Editora Érica, 2009.
[7] D. Brandao et al., *Ataque Denial of Service em Redes PROFINET: Estudo de Caso*, Simpósio Brasileiro de Automação Inteligente (SBAI), Natal/RN, Brazil, 2015.
[8] L. F. Guedes, *Ethernet Industrial*, http://www.dca.ufrn.br/∼affonso/DCA0447/aulas/Eth_Industrial.pdf, 2016.
[9] *Profibus Aasociation*, http://www.profibus.org.br/artigos_tecnicos, 2016.
[10] A. B. Lugli, *Uma Ferramenta Computacional Para Análise de Topologia e Tráfego Aplicada as Redes Ethernet Industriais*, Master Thesis, Itajubá/MG, Brazil, 2007.
[11] F. M. Ribeiro, T. S. Costa, A. Baratella, M. M. Santos and S. Stevan Jr, Comparative analysis of industrial ethernet networks: Profinet, Ethernet/IP and HSE, *International Journal of Innovative Computing, Information and Control*, vol.10, no.5, pp.1931-1948, 2014.
[12] Y. Ming and L. Guang, Analysis of PROFINET IO communication protocol, *IEEE International Conference on Instrumentation and Measurement, Computer, Communication and Control*, China, 2014.
[13] T. Sauter, The three generations of field-level networks – Evolution and compability issues, *IEEE Trans. Industrial Electronics*, vol.57, no.11, pp.3585-3595, 2010.
[14] M. Felser and T. Sauter, The fieldbus war: History or short break between battles? *The 4th IEEE International Workshop on Factory Communication System*, Sweden, pp.73-80, 2002.
[15] A. C. Turcato, *Desenvolvimento de Uma Metodologia Baseada em Redes Neurais Artificiais Para Identificação de Anomalias em Redes de Comunicação Profinet*, Master Thesis, São Carolos/SP, Brazil, 2015.