Real Time Industrial Network Analysis through Data Monitoring

M. A. S. Birchal and V. S. Birchal

***Abstract*—The use of Ethernet/IP technology in automation networks brought innovation only comparable to the appearance of the field buses themselves. This work presents an analysis of the behavior of a network through data monitoring. This is accomplished by the scanning of Ethernet frames in real time using sniffer software, in the search of communication patterns among the industrial devices over the network. This allows the comprehension of the normal operation of the network aiming the detection of security issues and performance analysis.**

***Index Terms*—Real time network, industrial network, protocol analysis.**

I. Introduction

The advent of real time Ethernet networks brought automation whole new dimension of possibilities and is characterized as the greatest innovation in distributed communication in automation, since the advent of industrial field bus buses.

If this reality is classic in conventional networks, Ethernet employment combined with the IP (Internet Protocol) is something totally different and new in industrial automation.

The growing employment of Industrial Ethernet brings advantages over other industrial protocols since it is compatible with corporate networks, which facilitates the migration of data from the plant to the rest of the company and promotes effective integration between the factory floor and the corporate network.

On the other hand, security issues are shown to be the main concern of today's networks, and certainly greater integration is also a greater openness to the invader.

This new scenario brings complex challenges and concerns that can only be overcome through a systematic study of the new industrial environment of data communication that comes through the inclusion of Ethernet as an industrial network [1].

Analysis of the data that travels between the elements belonging to the industrial environment can bring information about the performance and behavior of the network, promoting a greater understanding of the mechanisms underlying the normal operation and enabling the detection of possible abnormalities. Therefore, one can employ frame capture software (sniffer) in search of communication patterns that occur during communication among industrial network devices. In this paper, a PROFINET network was monitored in real time via a computer connected to the network running a sniffer software capturing Ethernet frames.

II. PROFINET

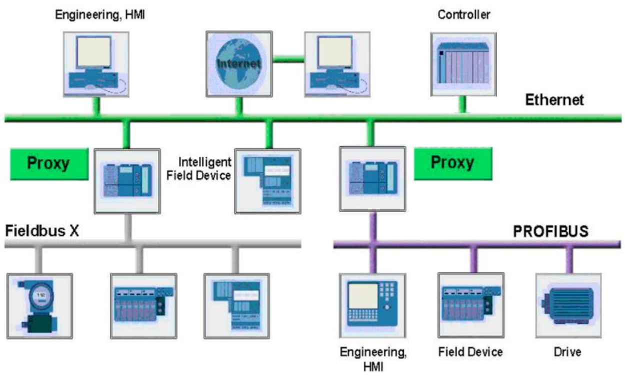
There are many industrial automation protocols, each supported by a respective standards organization. The PROFINET is a network open standard specified and maintained by the PROFIBUS & PROFINET International (PI), which also supports the PROFIBUS standard.

The IEC 61158 (Digital data communication for measurement and control – Field bus for use in industrial control systems) is the standard that specifies the various types of field bus automation protocols in terms of physical layer, data link layer and application layer, according to the classification ISO/OSI [1].

PROFINET IO is integrated in the standard in a similar way to the PROFIBUS, being its Ethernet infrastructure version. The PROFINET is also defined as the type 10 of IEC 61158.

The IEC 61784 (Profile sets for continuous and discrete manufacturing relative to field bus use in industrial control systems), an IEC 61158 companion that describes what services subsets specified by other standards (eg, IEC 61158) a certain field bus uses in its communication, sets PROFINET as their CPF Family 2 (Communication profile families) [2].

PROFINET is, thus, a standard automation network based on IEEE 802.3 Ethernet specification that uses TCP/IP (Transmission Control Protocol/Internet Protocol) and IT standards (information technology). This allows the protocol to reach a wide spectrum of use, at the same time communicating with real-time and high-level devices in the pyramid of automation. Fig. 1 shows the scope of the PROFINET, illustrating its compatibility with both field and Internet devices [2].



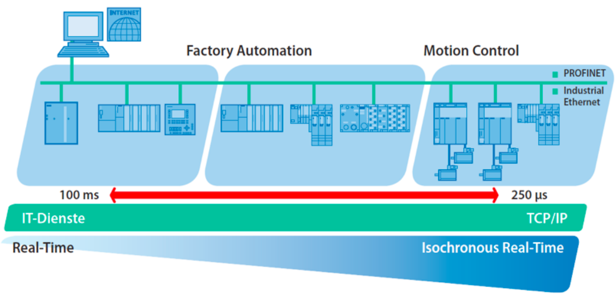
Source: PROFINET System Description — Technology and Application
Fig. 1. PROFINET scope.

Manuscript received May 7, 2015; revised November 17, 2015.
M. A. S. Birchal and V. S. Birchal are with Pontifícia Universidade Católica de Minas Gerais, Control and Automation Engineering Department, Av. Dom José Gaspar, 500, Coração Eucarístico, Belo Horizonte, Minas Gerais, 30535-901, Brazil (e-mail: birchal@pucminas.br, vsbirchal@gmail.com).

To make this possible, PROFINET is divided into two parts or perspectives: PROFINET CBA (Component Based Automation) and the PROFINET IO (Input/Output) [2], [3].

The PROFINET CBA is a component-based communication over TCP/IP used to establish communication between PLCs (Programmable Logic Controllers) in a modular way. PROFINET IO, in turn, describes communication from the standpoint of distributed or decentral periphery I/Os. It allows real time communication and isochronous real time communication (IRT), which takes into account data processing cycles and is based on a real time system cascade. The PROFINET IO is designed for a rapid exchange of data between Ethernet-based field devices, possessing, on master/slave fashion way.

PROFINET CBA is non real time communication at 50 ms to 100 ms bus cycle time. PROFINET IO is real-time communication on the order of a few ms and isochronous real time, on the order of a few hundred microseconds. Fig. 2 illustrates the different response time of PROFINET and their applications [3].



Source: PROFINET System Description — Technology and Application
Fig. 2. PROFINET real time response.

As an Ethernet based protocol, PROFINET uses Ethernet frame structure to send data [4], [5].

Ethernet is specified as an IEEE 802 protocol, and defined as a LAN network. In accordance with the IEEE 802.3 standard it is a CSMA/CD bus (Carrier Sense Multiple Access/Collision Detection) [5] . Indeed, one of the most important features of an Ethernet network and the one that defines it is its frame format, as shown in Fig. 3 [6].

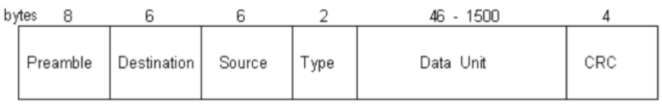


Fig. 3. The Ethernet frame.

The frame, in addition to having the MAC addresses (Medium Access Control) source and destination, has a field type (Type) that specifies content of the frame. The type is essential to identify the traffic.

In a typical PROFINET network may be found both, PROFINET and TCP/IP frames, travelling on the same bus. The distinction between them is essential to understanding the operation of the communication mechanism and may be done by observing the TYPE field. Table I summarizes the major types found in a PROFINET session [6].

III. Testbed and Procedure

Tests were developed using two Siemens PLC S7-1200, a 3COM switch and a computer running Wireshark sniffer software [7] to frame capture. Fig. 4 illustrates the testing platform.

TABLE I: PROFINET/Ethernet Type Frames

Protocol	Description	Ethernet Type
PROFINET/CBA	distributed automation	0x8892
PROFINET/DCP	discovery and basic configuration	0x8892
PROFINET/IO	decentralized periphery	0x8892
PROFINET/MRP	media redundancy protocol	0x88E3
PROFINET/MRRT	media redundancy for PROFINET/RT	0xFF60
PROFINET/PTCP	precision time control protocol	0x8892
PROFINET/RT	real time data transfer	0x8892
UDP/IP	IEEE 802.3 – IP datagram	0x0800
ARP	Addres Resolution Protocol	0x0806
UDP	UDP_SrcPort	0x8894
UDP	UDP_DstPort	0x8894

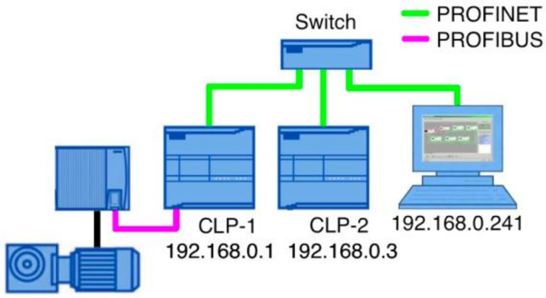


Fig. 4. Testbed.

To create a typical plant communication, PLCs were programmed to send and receive data to each other [8]. This is illustrated in Fig. 5.

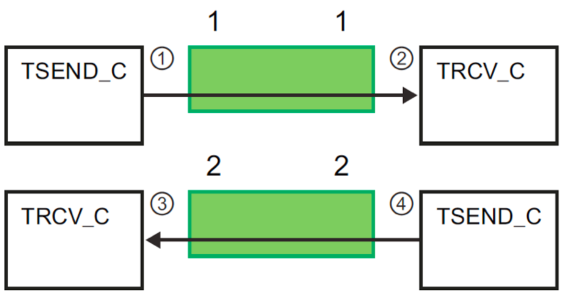


Fig. 5. Send and receive between CLPs.

Several different data types were sent, such as integers, characters and words. The traffic frame was captured and the TYPE field analyzed to figure out the network behavior.

Although only data between PLCs were explicitly sent, it was noted the appearance of several other types of Ethernet frames, arising from the normal operation of the PROFINET protocol itself or external to the automation network, from the Windows operating system.

IV. Results

In each test session, capture files were generated by Wireshark software and, applying the appropriate filters, frames were separated by nature. Fig. 6 illustrates a PLC communication test output before the filter use.

It can be noticed that there is traffic from several different types of frames. The LLDP frames (Link Layer Discovery

Protocol) are used by PROFINET to the topology discovery. LLDP promotes an exchange of address and physical location identification information of devices so it can do an automatic neighbor discovery. The data exchange via LLDP allows communication between devices without prior configuration.

After the discovery topology, communication is carried between the PLCs. The CLP 1 (IP 192.168.0.1) sends data through the TSEND_C command to the CLP 2 (IP 192.168.0.3), which receives, using the TRCV_C command. As this routine is a loop, these sequences will repeat itself over time.

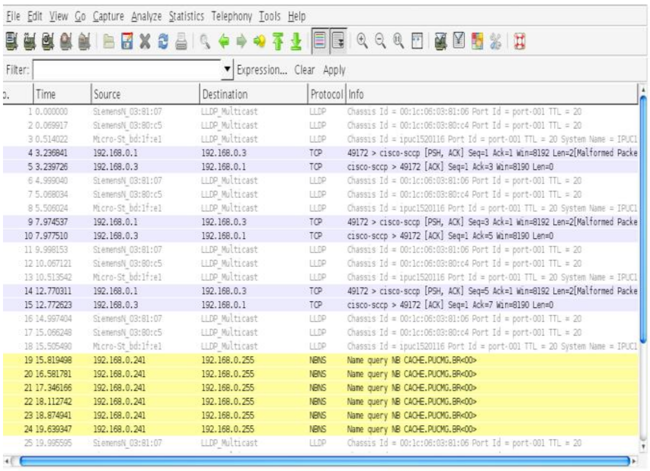


Fig. 6. Frame capture.

However, were observed inserts of NBNS (NetBIOS Name Service) frames. These events stem from the fact that computer is running Windows operating system, which has a native WINS service (Windows Name Service). WINS generates NBNS requests, similar to the DNS (Domain Name Service), though more restricted, since only operate in the Windows environment, for name resolution.

This shows that there is general traffic - such as NBNS - competing with the specific traffic PROFINET on the same Ethernet network. This is important because, when detect suspicious or unexpected traffic, one can stand before an attack generated by the TCP/IP environment.

Fig. 7 illustrates the sending of integer values ABh and CDh from PLC 1 to PLC 2 via the Ethernet frame number 4.

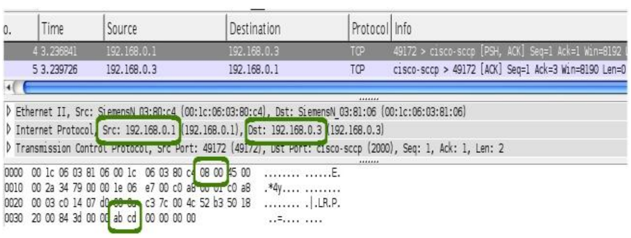


Fig. 7. CLP 1 sends integers to CLP 2.

In the above figure, the source and destination address fields have been deployed, the type field (0800h) which is a TCP/IP communication between devices in the standard high level PROFINET CBA and, finally, the trafficked content in the data field Ethernet frame, ABh CDh. One can therefore see that a sniffer is actually able to capture the trafficked PROFINET data on an Ethernet network. Fig. 8, which shows the Ethernet frame in sequence, frame number 5, brings the response of the PLC 2 to the PLC 1. This closes the communication cycle via a data reception acknowledge by the sent frame number 4.

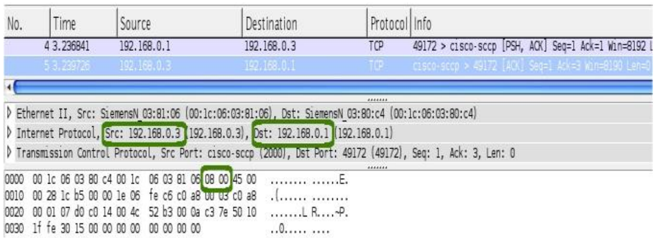


Fig. 8. Acknowledge sent by CLP 2.

Adding up new elements to the network, such as a supervisory system on a second computer, one can see the increasing complexity of communications among the elements and the emergence of new protocols, such as ARP (Address resolution protocol) and DHCP (Dynamic Host configuration Protocol), since the TCP/IP requires no configuration of their new hosts. Fig. 9 depicts these new elements in the network.

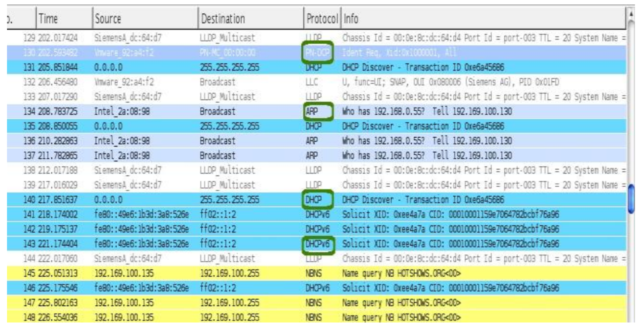


Fig. 9. The increasing complexity of communications.

V. Conclusion

The use of networks based on Ethernet and TCP/IP in automation brings new and powerful possibilities once facilitates the communication among the various pyramid levels of automation to a new range of possibilities. The use of classical IT solutions such as databases or web servers on the network automation, as well as direct interfacing to the corporative network, brings great benefits to the productive system.

However, this open access to other services than the intrinsic plant ones that, if not properly observed and monitored, can degrade network performance or even turn into threats to the automation system. The correct interpretation of traffic over the network now has a huge importance in maintaining continuity of service and ensuring that it is operating safely.

Using a known architecture and a controlled access among devices - like PLCs and Supervisory Systems – provides a way to observe the resulting traffic. From there, the data communication model becomes known, predictable and abnormal flows of data can be detected. One can even evaluate the quality of the bus by detection repetitions, loss of data and system timeouts.

The study of Ethernet-based industrial networks is extremely relevant since this protocol has proven to be a key of adoption in the current automation projects.

Knowledge of hardware and software architecture also contributes to the good specification and maintenance of infrastructure, avoiding the use of devices not designed for real time operation in later replacements to the project, either by faulty parts, either undue expansion. It is extremely important not to let enter new unskilled devices that could compromise the deterministic behavior of the automation network.

REFERENCES

[1] M. A. S. Birchal and V. S. Birchal, "Protocolos de redes industriais e o padrão ISO/OSI," *SSPI — Seminário Nacional de Sistemas de Produção e de Informação*, Belo Horizonte, 2008.

[2] M. Popp and K. Weber, *The Rapid Way to PROFINET*, PROFIBUS Mutzerorganisation, 2004.

[3] Information. [Online]. Available: http://www.profibus.com/technology/profinet/

[4] A. S. Tanenbaum, D. J. Wetherall, *Computer Networks*, 5th ed., Boston, U.S.: Pearson, 2011, ch. 4.

[5] W. Stallings, *Data and Computer Communications*, 8th ed., Upper Saddle River, U.S.: Pearson Prentice Hall, 2007, ch. 16, pp. 490-492.

[6] M. Popp, *Industrial Communication with PROFINET*, PROFIBUS Mutzerorganisation, 2007.

[7] U. Lamping, R. Shape, and E. Warnicke, *Wireshark User's Guide for Wireshark 1.9*, Free Software Foundation, 2012.

[8] *S7-1200 Programmable Controller — System Manual*, SIEMENS, 2009.

M. A. S. Birchal was born in Belo Horizonte, Minas Gerais, Brazil, on October 6, 1968. He got his electrical engineering degree at Pontificia Universidade Católica de Minas Gerais, in the city of Belo Horizonte, Minas Gerais, Brazil in 1994, and his master (1999) and the doctor (2005) degree on electrical engineering at Universidade Federal de Minas Gerais, in the city of Belo Horizonte, Brazil. His major field of study is real time network systems.

He is a professor of the Electronics Engineering Department of the Universidade Federal de Minas gerais and the chief of the Automation and Control Engineering Department of the Pontificia Universidade católica de Minas Gerais.

Dr. Birchal was the president of the ISA Section of Belo Horizonte from 2011 to 2015.

V. S. Birchal was born in Belo Horizonte, Minas Gerais, Brazil, on November 27, 1971. She got her chemical engineering degree at Universidade Federal de Minas Gerais, in the city of Belo Horizonte, Minas Gerais, Brazil in 1996, and her master (1999) and the doctor (2003) degree on chemical engineering at Universidade Federal de Minas Gerais, in the city of Belo Horizonte, Brazil. Her major field of study is drying systems optimization. She is a coordinator of the chemical engineering undergraduate course of the Universidade Federal de Minas Gerais.