# 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

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). 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

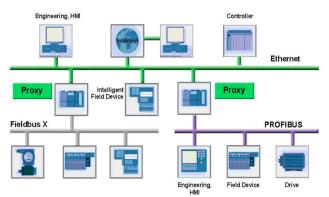
There are many industrial automation protocols, each supported by a respective standards organization. The PROFINET is a network open standard specified and maintained by the PROFIBUS & PROFINET International (PI), which also supports the PROFIBUS standard.

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].

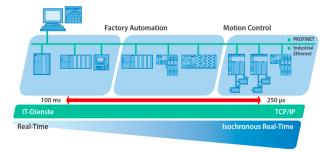


Source: PROFINET System Description — Technology and Application Fig. 1. PROFINET scope.

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 а 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].

by <u>tes 8 6 6 2 46-1500 4</u>								
	Pream	ble	Destination	Source	Туре	Data Unit	CRC	
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.

Protocol         Description         Ethernet Type           PROFINET/CBA         distributed automation         0x8892           PROFINET/DCP         discovery and basic         0x8892           configuration         configuration         0x8892           PROFINET/IO         decentralized periphery         0x8892           PROFINET/MRP         media redundancy protocol         0x88E3           PROFINET/MRPT         media redundancy for         0xEE60	TABLE I: PROFINET/ETHERNET TYPE FRAMES						
PROFINET/CBA         distributed automation         0x8892           PROFINET/DCP         discovery and basic         0x8892           configuration         configuration           PROFINET/IO         decentralized periphery         0x8892           PROFINET/MRP         media redundancy protocol         0x8893	Protocol	Description	Ethernet				
PROFINET/DCP     discovery and basic     0x8892       configuration     configuration       PROFINET/IO     decentralized periphery     0x8892       PROFINET/MRP     media redundancy protocol     0x8823			Туре				
configurationPROFINET/IOdecentralized periphery0x8892PROFINET/MRPmedia redundancy protocol0x88E3	PROFINET/CBA	distributed automation	0x8892				
PROFINET/IOdecentralized periphery0x8892PROFINET/MRPmedia redundancy protocol0x88E3	PROFINET/DCP	discovery and basic	0x8892				
PROFINET/MRP media redundancy protocol 0x88E3		configuration					
	PROFINET/IO	decentralized periphery	0x8892				
PROFINET/MPPT media redundancy for 0xFE60	PROFINET/MRP	media redundancy protocol	0x88E3				
I KOFINE I/WIKKI IIICula ledullualicy loi 0XITO0	PROFINET/MRRT	media redundancy for	0xFF60				
PROFINET/RT		PROFINET/RT					
PROFINET/PTCP precision time control 0x8892	PROFINET/PTCP	precision time control	0x8892				
protocol		protocol					
PROFINET/RT real time data transfer 0x8892	PROFINET/RT	real time data transfer	0x8892				
UDP/IP IEEE 802.3 – IP datagram 0x0800	UDP/IP	IEEE 802.3 – IP datagram	0x0800				
ARP Addres Resolution Protocol 0x0806	ARP	Addres Resolution Protocol	0x0806				
UDP UDP_SrcPort 0x8894	UDP	UDP_SrcPort	0x8894				
UDP UDP_DstPort 0x8894	UDP	UDP_DstPort	0x8894				

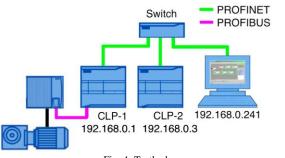
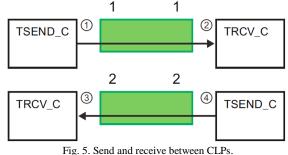


Fig. 4. Testbed.

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



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.

ilter:			<ul> <li>Expression</li> </ul>	tr.	
Time	1	Source	Destination	Protocol	Info
1 0.000		SLemensN_03:81:07	LLDP_Multicast	LLSP	Chassis Id = 00:1c:06:03:81:06 Port Id = port-001 TTL = 20
2 0.069	9917	StemensN 03:80:c5	LLDP_Multicast	LLOP	Chassis Id = 00:1c:06:03:80:c4 Port Id = port-001 TTL = 20
3 0.514	4022	Micro-St bd:lf:el	LLDP_Multicast	LLOP	Chassis Id = ipuc1520116 Port Id = port-001 TTL = 20 System Name = IPU
4 3.236	5841	192.168.0.1	192.168.0.3	TCP	49172 > cisco-sccp [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=2[Malformed Pac
5 3.239	9726	192.168.0.3	192.168.0.1	TCP	cisco-sccp > 49172 [ACK] Seq=1 Ack=3 Win=8190 Len=0
6 4.999	9040	SienensN_03:81:07	LLDP_Multicast	LLOP	Chassis Id = 00:1c:06:03:81:06 Port Id = port-001 TTL = 20
7 5.068	8034	SLemensN_03:80:c5	LLDP_Multicast	LLDP	Chassis Id = 00:1c:06:03:80:c4 Port Id = port-001 TTL = 20
8 5.506	5024	Micro-St bd:lf:el	LLDP_Multicast	LLDP	Chassis Id = ipuc1520116 Port Id = port-001 TTL = 20 System Name = IPU
9 7.974	4537	192.168.0.1	192.168.0.3	TOP	49172 > cisco-sccp [PSH, ACK] Seq=3 Ack=1 Win=8192 Len=2[Malformed Pac
10 7.977	7510	192.168.0.3	192.168.0.1	TOP	cisco-sccp > 49172 [ACK] Seq=1 Ack=5 Win=8190 Len=0
11 9.998	3153	SienensN_03:81:07	LLDP_Multicast	LLEP	Chassis Id = 00:1c:06:03:81:06 Port Id = port-001 TTL = 20
12 10.08	57121	SienensN 03:80:c5	LLDP_Multicast	LUSP	Chassis Id = 00:10:06:03:80:04 Port Id = port-001 TTL = 20
13 10.51	3542	Micro-St bd:1f:el	LLDP Multicast	LLDP	Chassis Id = ipuc1520116 Port Id = port-001 TTL = 20 System Name = IPU
14 12.77	70311	192.168.0.1	192.168.0.3	TOP	49172 > cisco-sccp [PSH, ACK] Seq=5 Ack=1 Win=8192 Len=2[Malformed Pac
15 12.77	72623	192.168.0.3	192.168.0.1	TCP	cisco-sccp > 49172 [ACK] Seq=1 Ack=7 Win=8190 Len=0
16 14.99	97404	SienensN 03:81:07	LLDP Multicast	LLDP	Chassis Id = 00:1c:06:03:81:06 Port Id = port-001 TTL = 20
17 15.08	56248	SLenensN 03:80:c5	LLDP Multicast	LLDP	Chassis Id = 00:1c:06:03:80:c4 Port Id = port-001 TTL = 20
18 15.50	05490	Micro-St bd:1f:e1	LLDP Multicast	LLDP	Chassis Id = ipuc1520116 Port Id = port-001 TTL = 20 System Name = IPU
19 15.81	19498	192.168.0.241	192.168.0.255	NBNS	Name query NB CACHE.PUCMG.BR<00>
20 16.58	81781	192.168.0.241	192.168.0.255	NBNS	Name query NB CACHE.PUCMG.BR<00>
21 17.34	46166	192.168.0.241	192.168.0.255	NBNS	Name query NB CACHE.PUCMG.BR<00>
22 18.11	2742	192.168.0.241	192.168.0.255	NBNS	Name query NB CACHE.PUCMG.BR<00>
23 18.87	74941	192.168.0.241	192.168.0.255	NBNS	Name query NB CACHE.PUCMG.BR<00>
24 19.63	39347	192.168.0.241	192.168.0.255	NBNS	Name query NB CACHE. PUCMG. BR<00>
25 19.99	5595	SienensN 03:81:07	LLDP Multicast	LLDP	Chassis Id = 00:1c:06:03:81:06 Port Id = port-001 TTL = 20

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.

0.	Time	Source	Destination	Protocol	Info
	4 3.236841	192.168.0.1	192.168.0.3	TCP	49172 > cisco-sccp [PSH, ACK] Seq=1 Ack=1 Win=8192
	5 3.239726	192.168.0.3	192.168.0.1	TCP	cisco-sccp > 49172 [ACK] Seq=1 Ack=3 Win=8190 Len=0
) Ir	nternet Protocol	Src: 192.168.0.1 (19	:lc:06:03:80:c4), Dst: Sie 2.168.0.1), Dst: 192.168.0 : 49172 (49172), Dst Port:	.3 (192.168.0.3)	
0000	00 1c 06 03 8 00 2a 34 79 0	1 06 00 1c 06 03 80 c 0 00 1e 06 e7 00 c0 a	08 00 5 00	E.	() and i a land of must be
0030	20 00 84 3d 0	0 00 ab cd 00 00 00 00	=		

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.

No.	Time	Source	Destinat	ion Protoci	al Info
	4 3.236841	192.168.0.1	192.168.0	0.3 TCP	49172 > cisco-sccp [PSH, ACK] Seq=1 Ack=1 Win=8192
•					
Eth	ernet II. Src: !	SiemensN 03:81:06 (0	1:1c:06:03:81:06), [	Dst: SiemensN 03:80:c4 (00	1:1c:06:03:80:c4)
				92.168.0.1 (192.168.0.1)	
) Int	ernet Protocol,	Src: 192.168.0.3 1	92.168.0.3), Dst: 19		
) Int ) Tra	ernet Protocol, nomission Contro	Src: 192.168.0.3 1 ol Protocol, Src Por	92.168.0.3), Dst: 19 t: cisco-sccp (2000)	92.168.0.1) (192.168.0.1) J, Dst Port: 49172 (49172)	
) Int ) Tra	ernet Protocol, nomission Contro 00 lc 06 03 80	Src: 192.168.0.3 1	92.168.0.3), Dst: 19 t: cisco-sccp (2000) 6 08 00,45 00	92.168.0.1 (192.168.0.1) ), Dst Port: 49172 (49172)	
∲ Int ∲ Tra 0000 0010	ernet Protocol, nsmission Contro 00 lc 06 03 80 00 28 lc b5 00	Src: 192.168.0.3 1 ol Protocol, Src Por c4 00 1c 06 03 81 0	92.168.0.3), Dst: 19 t: cisco-sccp (2000) 6 08 00 45 00 8 00 03 c0 a8 .(.	92.168.0.1 (192.168.0.1) J, Dst Port: 49172 (49172)	
≬ Int ≬ Tra 0000 0010 0020	ernet Protocol, nsmission Contro 00 lc 06 03 80 00 28 lc b5 00 00 01 07 d0 c0	Src: 192.168.0.3 1 ol Protocol, Src Por c4 00 1c 06 03 81 0 00 1e 06 fe c6 c0 a	92.168.0.3), Dst: 19 t: cisco-sccp (2000) 6 08 00 45 00 8 00 03 c0 a8 .(. a c3 7e 50 10	92.168.0.1 (192.168.0.1) J, Dst Port: 49172 (49172)	

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.

	Time	Source	Destination	Protocol	Info
1	29 202.017424	SierensA_dc:64:d7	LLDP_Multicast	LIDP	Chassis Id = 00:0e:8c:dc:64:d4 Port Id = port-003 TTL = 20 System Name
				PI-DP	
1	31 205.851844	0.0.0.0	255.255.255.255	UHOP	DHCP Discover - Transaction ID Dxe6a45686
-1	32 206.456480	Viware_92:a4:f2	Broadcast	LLC	U, func=UI; SNAP, OUI 0x080006 (Siemens AG), PID 0x01FD
1	33 207.017290	SiemensA_dc:64:d7	LLOP_Multicast	LLDP	Chassis Id = 00:0e:8c:dc:64:d4 Port Id = port-003 TTL = 20 System Name
1	34 208.783725	Intel_2a:08:98	Broadcast	ARP	Who has 192.168.0.55? Tell 192.169.100.130
1	35 208.850055	0.0.0.0	255.255.255.255	DHOP	DHCP Discover - Transaction ID Oxe6a45686
1	36 210. 282863	Intel 2a:08:98	Broadcast	ARP	Who has 192.168.0.55? Tell 192.169.100.130
1	37 211.782965	Intel_2a:08:98	Broadcast	ARP	Who has 192.168.0.55? Tell 192.169.100.130
1	38 212.017188	SiemensA_dc:64:d7	LLDP_Multicast	LLDP	Chassis Id = 00:0e:8c:dc:64:d4 Port Id = port-003 TTL = 20 System Name
1	39 217.016029	SiemensA_dc:64:d7	LLOP Multicast	LLDP	Chassis Id = 00:0e:8c:dc:64:d4 Port Id = port-003 TTL = 20 System Name
1	43 217.851637	0.0.0.0	255.255.255.255	DHOP	DHCP Discover - Transaction ID 0xe6a45686
1	41 218.174002	fe80::49e6:1b3d:3a8:526e	ff02::1:2	DHCPv6	Solicit XID: 0xee4a7a CID: 00010001159e7064782bcbf76a96
1	42 219.175137	fe80::49e6:1b3d:3a8:526e	ff02::1:2	DHOPv6	Solicit XID: 0xee4a7a CID: 00010001159e7064782bcbf76a96
1	43 221.174404	fe80::49e6:1b3d:3a8:526e	ff02::1:2	DHOPV6	Solicit XID: 0xee4a7a CID: 00010001159e7064782bcbf76a96
1	44 222.017060	SiemensA_dc:64:d7	LLOP_Multicast	LUP	Chassis Id = 00:0e:8c:dc:64:d4 Port Id = port-003 TTL = 20 System Name
1	45 225.051313	192.169.100.135	192.169.100.255	NBNS	Name query NB HOTSHOWS.ORG<00>
1	46 225.175546	fe80::49e6:1b3d:3a8:526e	ff02::1:2	DHOPv6	Solicit XID: 0xee4a7a CID: 00010001159e7064782bcbf76a96
1	47 225.802163	192.169.100.135	192.169.100.255	NENS	Name query NB HOTSHOWS.ORG<00>
1	48 226.554036	192,169,100,135	192.169.100.255	NBNS	Name query NB HOTSHOWS.ORG<00>

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

- 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.