A Study on Communication Protocol Analyzers for PROFINET Network.

Prof. PhD. Alexandre Baratella Lugli.
Control and Automation Department.
INATEL National Telecommunication Institute.
Santa Rita do Sapucai/MG – Brazil.
baratella@inatel.br
linkedin.com/in/alexandre-baratella-lugli-a0543b247
https://inatel.br/home/

SUMMARY

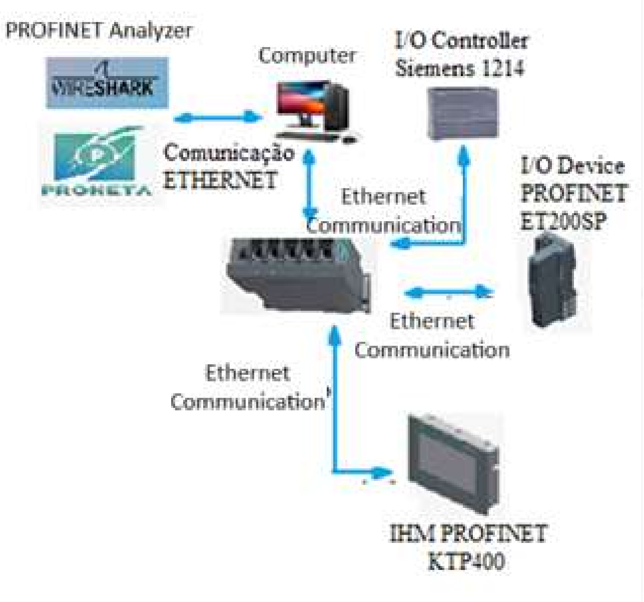
1. INTRODUCTION
2. CONCEPTS AND DEFINITIONS
3. PRACTICAL APPLICATION AND RESULTS
4. CONCLUSION

INTRODUCTION

1. PROFINET network;

2. Network analyzers;

3. The analysis of a real network will be done, containing the communication characteristics to be analyzed and determined in each scenario proposed in the tests on the proposed PROFINET network. In order to analyze networks faults and problems, the paper structured a study about main analyzers used in the market.



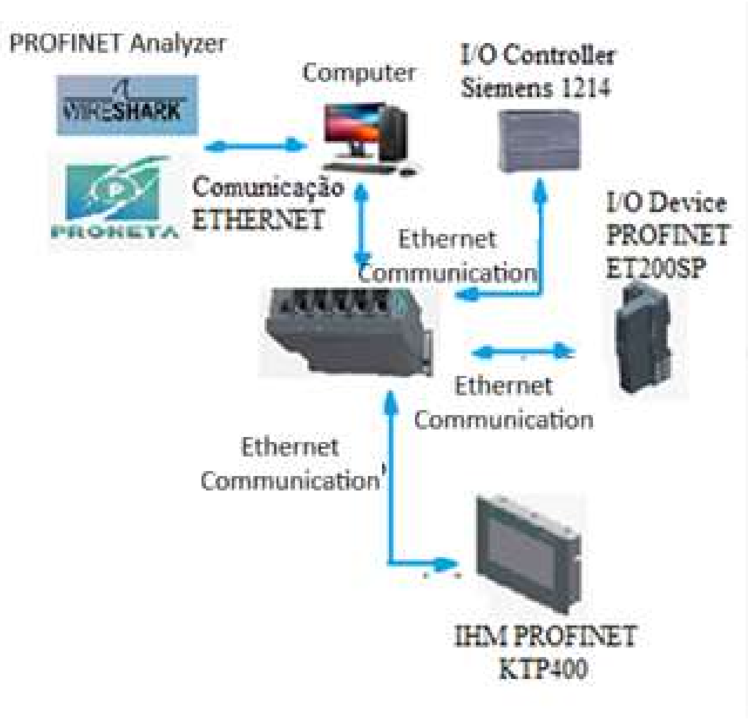
CONCEPTS AND DEFINITONS

A. PROFINET Network;
    A. 100Mbps;
    B. RT, IRT, Non-RT;
    C. IO Controller, IO Devices and IO Supervisor.
    D. Consolidated Industrial Ethernet Network.

B. PLC – Programmable Logic Controller;
    A. IO Controller;
    B. 5 standard programing languages: LADDER, STL, FBD, Assembly and Structured text.

C. PROFINET Network Analyzer;
    A. Monitoring networks;
    B. Important to check errors, diagnoses and parameters from networks.

PRACTICAL APPLICATION AND RESULTS



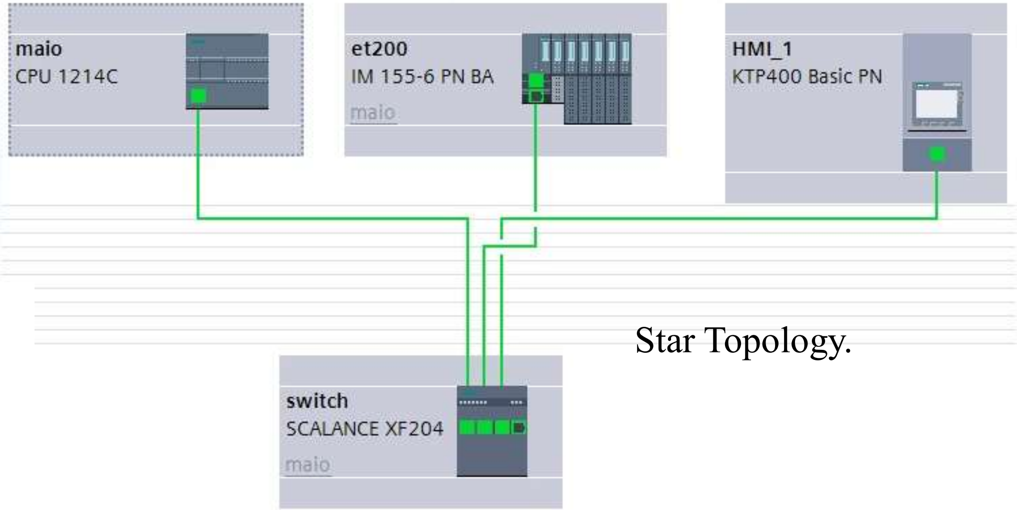
General Diagram Connections.

PRACTICAL APPLICATION AND RESULTS

Devices	IP Address	MAC Address
PLC	192.168.0.200	AC-64-17-0C-17-ED
HMI_1	192.168.0.3	E0-DC-A0-2E-5C-8D
ET200	192.168.0.45	AC-64-17-08-2B-8E
Switch	192.168.0.30	20-87-56-76-1E-31

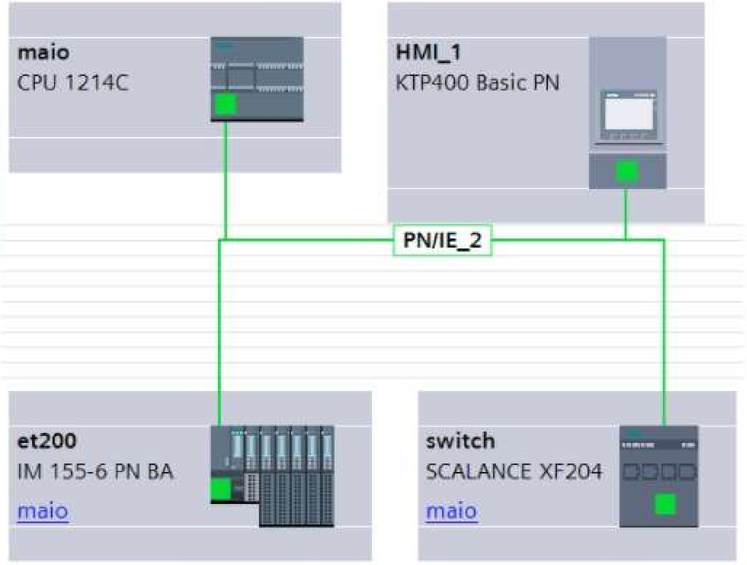
Device Address.

PRACTICAL APPLICATION AND RESULTS

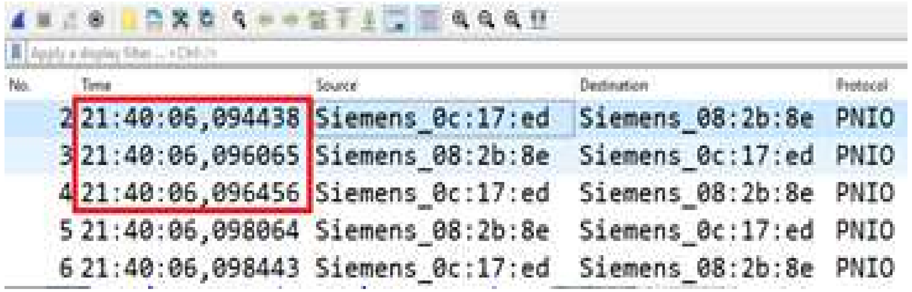


Star Topology.

Proposed Network.

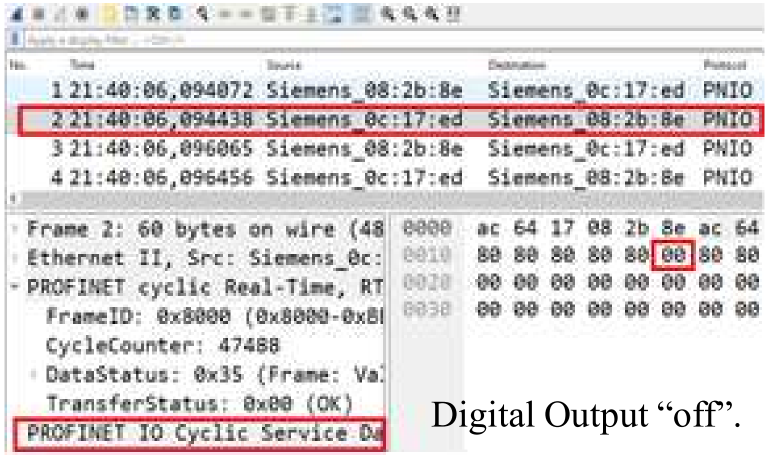


PRACTICAL APPLICATION AND RESULTS



```
No.  Time              Source              Destination         Protocol
  2 21:40:06,094438 Siemens_0c:17:ed Siemens_08:2b:8e PNIO
  3 21:40:06,096065 Siemens_08:2b:8e Siemens_0c:17:ed PNIO
  4 21:40:06,096456 Siemens_0c:17:ed Siemens_08:2b:8e PNIO
  5 21:40:06,098064 Siemens_08:2b:8e Siemens_0c:17:ed PNIO
  6 21:40:06,098443 Siemens_0c:17:ed Siemens_08:2b:8e PNIO
```

Communication time:
(Line 3 – Line 2), obtaining an approximate value of (21:40:06.096456 - 21:40:06.094438 = **2018us (2.018ms)**



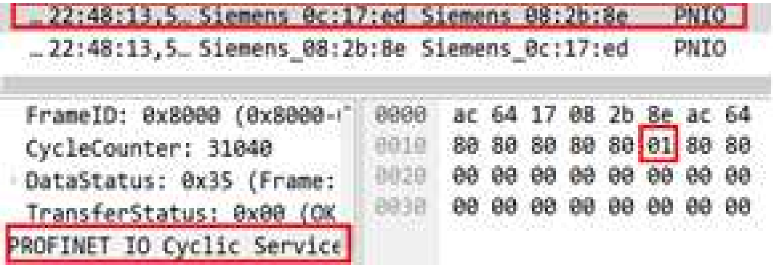
```
No.  Time              Source              Destination         Protocol
  1 21:40:06,094072 Siemens_08:2b:8e Siemens_0c:17:ed PNIO
  2 21:40:06,094438 Siemens_0c:17:ed Siemens_08:2b:8e PNIO
  3 21:40:06,096065 Siemens_08:2b:8e Siemens_0c:17:ed PNIO
  4 21:40:06,096456 Siemens_0c:17:ed Siemens_08:2b:8e PNIO

Frame 2: 60 bytes on wire (48     0000  ac 64 17 08 2b 8e ac 64
Ethernet II, Src: Siemens_0c:     0010  80 80 80 80 80 00 80 80
PROFINET cyclic Real-Time, RT     0020  00 00 00 00 00 00 00 00
  FrameID: 0x8000 (0x8000-0x8     0030  00 00 00 00 00 00 00 00
  CycleCounter: 47488
  DataStatus: 0x35 (Frame: Va
  TransferStatus: 0x00 (OK)
PROFINET IO Cyclic Service Da
```

Digital Output “off”.

WIRESHARK

Digital Output “on”.

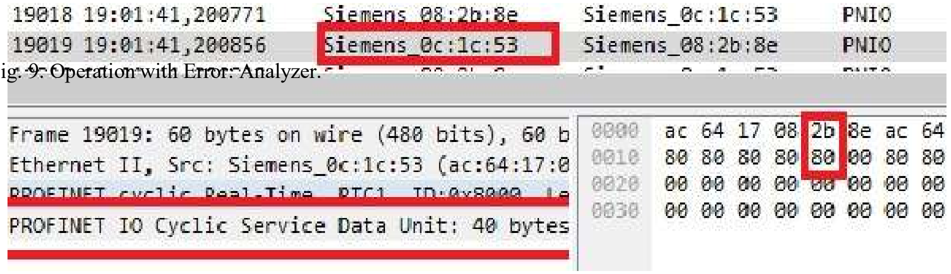


```
… 22:48:13,5… Siemens_0c:17:ed Siemens_08:2b:8e   PNIO
… 22:48:13,5… Siemens_08:2b:8e Siemens_0c:17:ed   PNIO

  FrameID: 0x8000 (0x8000-     0000  ac 64 17 08 2b 8e ac 64
  CycleCounter: 31040          0010  80 80 80 80 80 01 80 80
  DataStatus: 0x35 (Frame:     0020  00 00 00 00 00 00 00 00
  TransferStatus: 0x00 (OK     0030  00 00 00 00 00 00 00 00
PROFINET IO Cyclic Service
```

PRACTICAL APPLICATION AND RESULTS

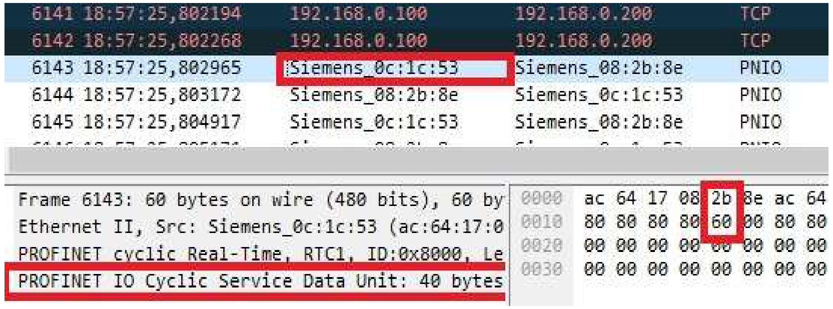
Fig. 9: Operation with Error: Analyzer.



```
19018 19:01:41,200771     Siemens_08:2b:8e     Siemens_0c:1c:53     PNIO
19019 19:01:41,200856     Siemens_0c:1c:53     Siemens_08:2b:8e     PNIO
```

```
Frame 19019: 60 bytes on wire (480 bits), 60 b    0000   ac 64 17 08 2b 8e ac 64
Ethernet II, Src: Siemens_0c:1c:53 (ac:64:17:0    0010   80 80 80 80 80 00 80 80
PROFINET cyclic Real-Time, RTC1, ID:0x8000, Le    0020   00 00 00 00 00 00 00 00
PROFINET IO Cyclic Service Data Unit: 40 bytes    0030   00 00 00 00 00 00 00 00
```

Operation No-Error: Analyzer.

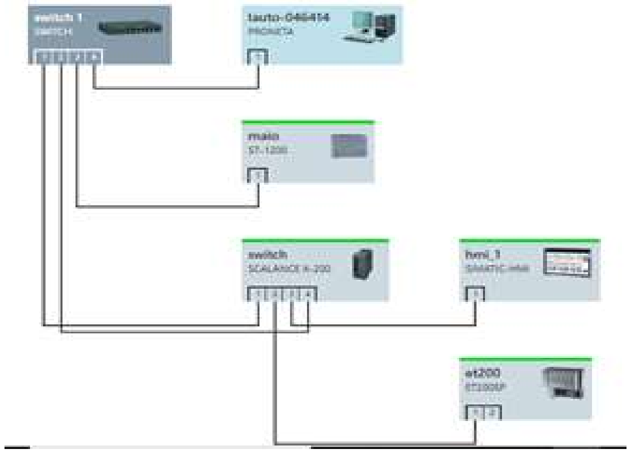


```
6141 18:57:25,802194     192.168.0.100        192.168.0.200        TCP
6142 18:57:25,802268     192.168.0.100        192.168.0.200        TCP
6143 18:57:25,802965     Siemens_0c:1c:53     Siemens_08:2b:8e     PNIO
6144 18:57:25,803172     Siemens_08:2b:8e     Siemens_0c:1c:53     PNIO
6145 18:57:25,804917     Siemens_0c:1c:53     Siemens_08:2b:8e     PNIO
```

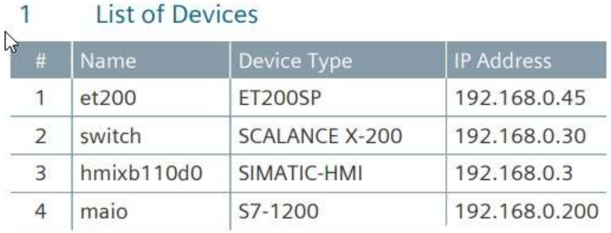
```
Frame 6143: 60 bytes on wire (480 bits), 60 by    0000   ac 64 17 08 2b 8e ac 64
Ethernet II, Src: Siemens_0c:1c:53 (ac:64:17:0    0010   80 80 80 80 60 00 80 80
PROFINET cyclic Real-Time, RTC1, ID:0x8000, Le    0020   00 00 00 00 00 00 00 00
PROFINET IO Cyclic Service Data Unit: 40 bytes    0030   00 00 00 00 00 00 00 00
```

Operation with Error: Analyzer.

PRACTICAL APPLICATION AND RESULTS



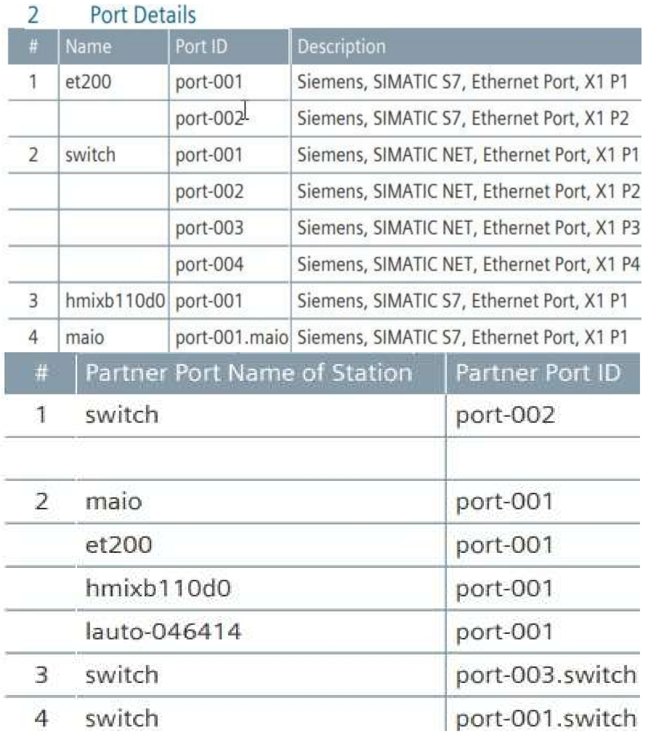
PRONETA: Network Topology.



1 List of Devices

#	Name	Device Type	IP Address
1	et200	ET200SP	192.168.0.45
2	switch	SCALANCE X-200	192.168.0.30
3	hmixb110d0	SIMATIC-HMI	192.168.0.3
4	maio	S7-1200	192.168.0.200

PRONETA: Network Devices.



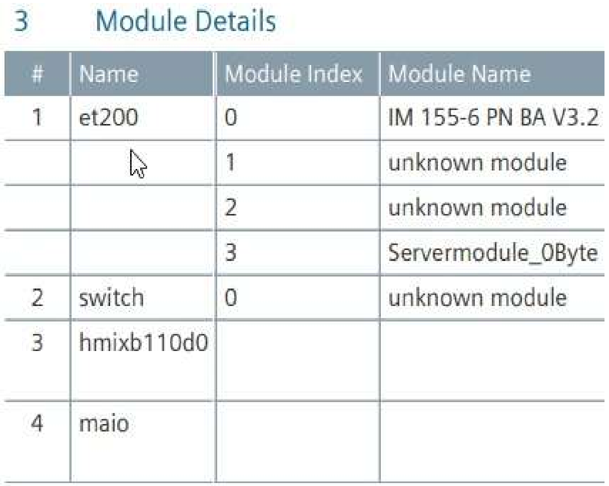
2 Port Details

#	Name	Port ID	Description
1	et200	port-001	Siemens, SIMATIC S7, Ethernet Port, X1 P1
		port-002	Siemens, SIMATIC S7, Ethernet Port, X1 P2
2	switch	port-001	Siemens, SIMATIC NET, Ethernet Port, X1 P1
		port-002	Siemens, SIMATIC NET, Ethernet Port, X1 P2
		port-003	Siemens, SIMATIC NET, Ethernet Port, X1 P3
		port-004	Siemens, SIMATIC NET, Ethernet Port, X1 P4
3	hmixb110d0	port-001	Siemens, SIMATIC S7, Ethernet Port, X1 P1
4	maio	port-001.maio	Siemens, SIMATIC S7, Ethernet Port, X1 P1

#	Partner Port Name of Station	Partner Port ID
1	switch	port-002
2	maio	port-001
	et200	port-001
	hmixb110d0	port-001
	lauto-046414	port-001
3	switch	port-003.switch
4	switch	port-001.switch

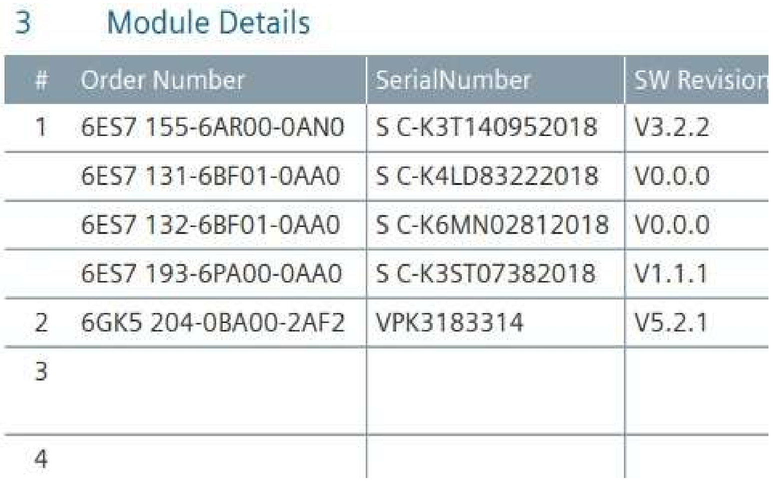
PRONETA: Communication Details.

PRACTICAL APPLICATION AND RESULTS



3 Module Details

#	Name	Module Index	Module Name
1	et200	0	IM 155-6 PN BA V3.2
		1	unknown module
		2	unknown module
		3	Servermodule_0Byte
2	switch	0	unknown module
3	hmixb110d0		
4	maio		



3 Module Details

#	Order Number	SerialNumber	SW Revision
1	6ES7 155-6AR00-0AN0	S C-K3T140952018	V3.2.2
	6ES7 131-6BF01-0AA0	S C-K4LD83222018	V0.0.0
	6ES7 132-6BF01-0AA0	S C-K6MN02812018	V0.0.0
	6ES7 193-6PA00-0AA0	S C-K3ST07382018	V1.1.1
2	6GK5 204-0BA00-2AF2	VPK3183314	V5.2.1
3			
4			

PRONETA: General Network Details.

CONCLUSION

- Network analyzers fundamental role in mitigating potential problems in communication networks.
- Several tests, simulations of problems and defects, temporal measurements, connection analyses and network addressing analyses are performed.
- Identify, mitigate and resolve problems proactively, ensuring an operation of industrial facilities.
- PRONETA network analyzer: the analysis is performed in a more graphical and intuitive way.
- WIRESHARK network analyzer: needs a higher level of knowledge, because, although it provides more comprehensive information.
- As future paper, it is suggested to do the study of other network analyzers available on the market, comparing them with those studied in this paper.

REFERENCES

1. S. Duan, Y. Zhu, J. Zhu and H. Li, "Research and Verification of Industrial Ethernet PROFINET Carried by 5G LAN-Type Service," 2024 5th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Nanjing, China, 2024, pp. 2028-2032, doi: 10.1109/AINIT61980.2024.10581731.

2. H. Mutlu, N. Akyürek and Ö. Korçak, "PROFINET Controller on Cloud," 2025 24th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2025, pp. 1-6, doi: 10.1109/INFOTEH64129.2025.10959195.

3. Liam Bee, PLC and HMI Development with Siemens TIA Portal: Develop PLC and HMI programs using standard methods and structured approaches with TIA Portal V17, Packet Publishing, 2022.

4. V. E. Ağaoğulları and Ö. Korçak, "PyPND: A Python-based PROFINET Controller for CI/CD Environments," 2025 24th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2025, pp. 1-6, doi: 10.1109/INFOTEH64129.2025.10959196.

5. Y. Kim, S. -y. Lee and S. Lim, "Implementation of PLC controller connected Gazebo-ROS to support IEC 61131-3," 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 2020, pp. 1195-1198, doi: 10.1109/ETFA46521.2020.9212096.

6. V. Harun Şahin, İ. Özçelik, M. Balta and M. İskefiyeli, "Topology discovery of PROFINET networks using Wireshark," 2013 International Conference on Electronics, Computer and Computation (ICECCO), Ankara, Turkey, 2013, pp. 88-91, doi: 10.1109/ICECCO.2013.6718235.

7. J. Göppert and A. Sikora, "Evaluation of the Secure PROFINET Application Relation Establishment Performance," 2024 IEEE 22nd International Conference on Industrial Informatics (INDIN), Beijing, China, 2024, pp. 1-6, doi: 10.1109/INDIN58382.2024.10774374.

Questions ?

Prof. PhD. Alexandre Baratella Lugli.
Control and Automation Department.
INATEL National Telecommunication Institute.
Santa Rita do Sapucai/MG – Brazil.
baratella@inatel.br
linkedin.com/in/alexandre-baratella-lugli-a0543b247
https://inatel.br/home/