XXI SNPTEE
NATIONAL SEMINAR
ON PRODUCTION AND
TRANSMISSION
OF ELECTRIC POWER

Version 1.0
23-26 October 2011
Florianópolis - SC - bRAZIL

GTM GROUP

TRANSFORMER, REACTOR, MATERIAL AND EMERGING TECHNOLOGY STUDY GROUP - GTM

WIRELESS NETWORK APPLICATION FOR ONLINE MONITORING SYSTEM AT THE SANTO ÂNGELO ELETROBRAS - ELETROSUL SUBSTATION

CLAYTON S. DURIGUETTO (*) RAFAEL P. FEHLBERG FERNANDO T. DE CARVALHO SANDRO PEIXOTO
TREETECH TREETECH TREETECH ELETROBRAS ELETROSUL

ABSTRACT

The purpose of this technical paper is to describe the wireless communication network technology integrated in the monitoring system inside the Santo Ângelo substation in order to improve performance, customize the communication network between the field and the control roomm, and make future implementations easier without using new cables and/or fiber optics.

KEYWORDS

Transformer, Converter, Monitoring, WLAN, Access Point

1.0 - INTRODUCTION

Local wireless networks, or WLAN, are an alternative to wired conventional networks, providing the same functionality in a flexible, easy configuration and good connectivity in buildings, residential areas or industries.

WLANs, therefore, address network points with the same efficiency and an even with better cost / benefit ratio than the conventional wired network in those cases.

The installation of wireless networks and new network points eliminates the need to run new cables, reducing the setup time for new positions and facilitating the construction of structures in infrastructure. A wireless network provides, therefore, all the functionality of a wired network, but without the physical constraints of cabling itself.

Currently the vast majority of wireless networks allows full connectivity and meets the standards and requirements of the international bodies. This means that once using standardized equipment, wireless networks can be interconneted with the conventional wired ones easily, and computers using wireless devices interact with wired network and vice-versa without any restriction.

In this network category, several types of networks can be defined, which are: Wireless Local Area Networks or WLAN, or Wireless Metropolitan Networks, or WMAN, WANs, or Wireless WWAN (Wireless Wide Area Network) networks, WLL (Wireless Local Loop) and the new concept of Wireless Personal Area Network or WPAN.

Therefore, the WLANs combine the mobility of the user with the connectivity at high speeds of up to 155 Mbps, in some cases.
Depending on the technology used, radio frequency and the receiver, WLAN networks can reach kilometers depending on the power of the equipment used.

(*) Praça Claudino Alves, n ° 141 - Centro - CEP 12940-800 Atibaia, SP - Brazil
Phone: (+55 11) 4413-5787 - Email: @ clayton.duriguetto treetech.com.br

2.0 - HOW THE WLANS WORK

Using radio carrier waves, WLANs establish communication between network points. Data are modulated on the radio carrier and transmitted through electromagnetic waves. Multiple radio carriers can coexist in the same medium without mutual interference. To extract the data, the receiver locks on a specific frequency and rejects the other carriers of different frequencies.

In a typical environment, see Figure 1, the transceiver device (transmitter / receiver) or access point is connected to a conventional Ethernet LAN (wired). Access points not only provide communication with the wired network but also mediate the traffic with neighboring access points in a microcell scheme with roaming similar to a cell phone system.

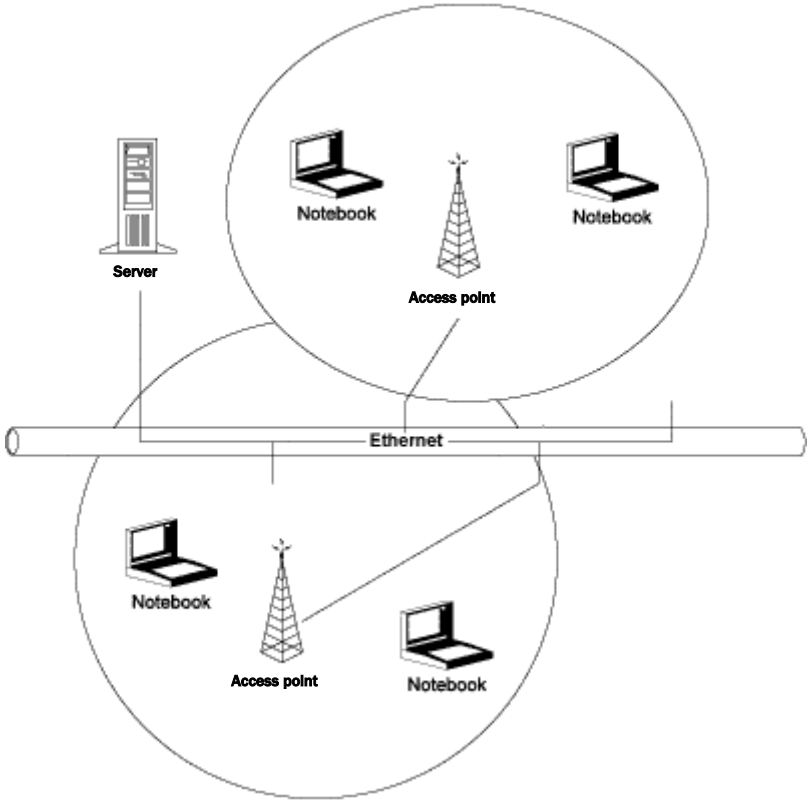

FIGURE 1 – A typical Wireless LAN Network

2.1 Topology

There are several technologies involved in wireless local area networks, each one with its own peculiarities, limitations and advantages. The Spread Spectrum systems use spread spectrum technique with broadband radio signals thus providing more safety integrity and reliability, in exchange for higher band consumption. There are two types of spread spectrum technology: the FHSS, Frequency-Hopping Spread Spectrum DSSS (Direct-Sequence Spread Spectrum), see Figure 2.

The FHSS technology uses a narrowband carrier that changes frequency into a code known to both transmitter and receiver which, when properly synchronized, has as its effect the maintenance of a single logical channel.

The DSSS generates a redundant bit-code (also called a chip or chipping code) for each transmitted bit. The larger the chip the greater the probability of original information recovery. However, a larger bandwidth is required. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission.

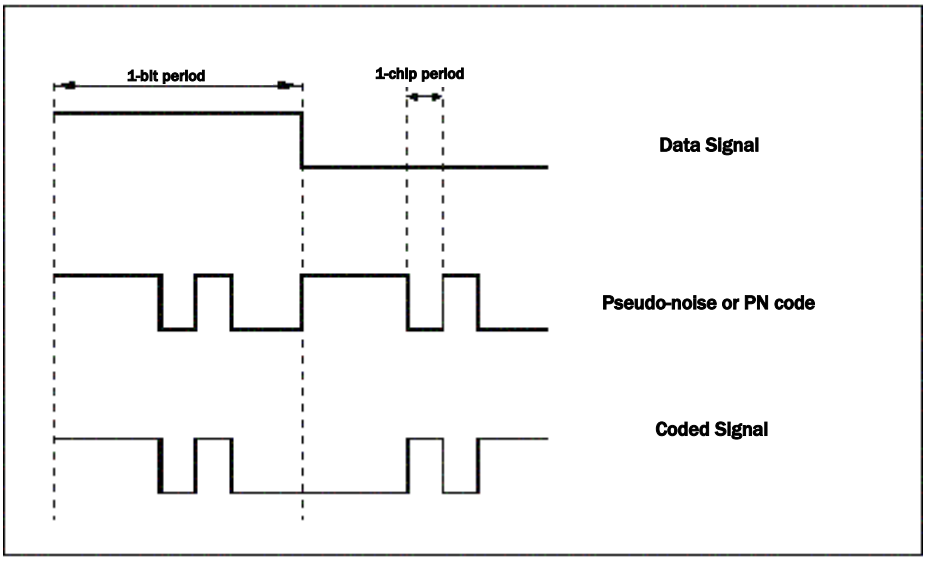

FIGURE 2 - Spread Spectrum Transmission

2.2.1 IEEE 802.11 Wireless Local Area Network

The IEEE 802.11 standard, see Figure 3, specifies three physical layers (PHY), and only one MAC sublayer (Medium Access Control) provides two physical layer specifications with option for radio, operating in the 2400 to 2483.5 MHz band (depending on the regulations in each country), and one specification with infrared option. They are:

a. Frequency Hopping Spread Spectrum Radio PHY:
This layer provides 1 Mbps operation with optional 2 Mbps. The Mbps version uses 2 levels of the GFSK modulation (Gaussian Frequency Shift Keying) and the 2 Mbps one uses 4 levels of the same modulation;

b. Direct Sequence Spread Spectrum Radio PHY:
This layer provides operation at both speeds (1 and 2 Mbps). The 1 Mbps version uses DBPSK modulation (Differential Binary Phase Shift Keying), while the 2 Mbps one uses DQPSK modulation (Differential Quadrature Phase Shift Keying);

c. Infrared PHY:
This layer provides 1 Mbps operation with optional 2 Mbps. The 1 Mbps version uses a 16-PPM modulation with 16 positions, while the 2 Mbps version uses a 4-PPM modulation.

On the side of the station, the MAC sublayer provides the following services: authentication, logout, privacy and transmission of MADU (MAC Sublayer Data Unit), and on the side of the distribution system: association, dissociation, distribution, integration and reassociation. Stations can operate in two different situations:

a. Independent Configuration:
Each station communicates directly with each other without the need of installing infrastructure. The operation of this network is easy, but the downside is that the coverage area is limited. Stations with this configuration are in the BSS service (Basic Service Set);

b. Infrastructure Configuration:
Each station communicates directly with the access point that is part of the distribution system. An access point serves the stations in a BSS, and its set is called ESS (Extended Service Set). Besides the services described above, the standard still offers the functionality of roaming in an ESS and management of electrical power (stations can turn off their transceivers to conserve power). The protocol of the MAC sublayer is the CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance).

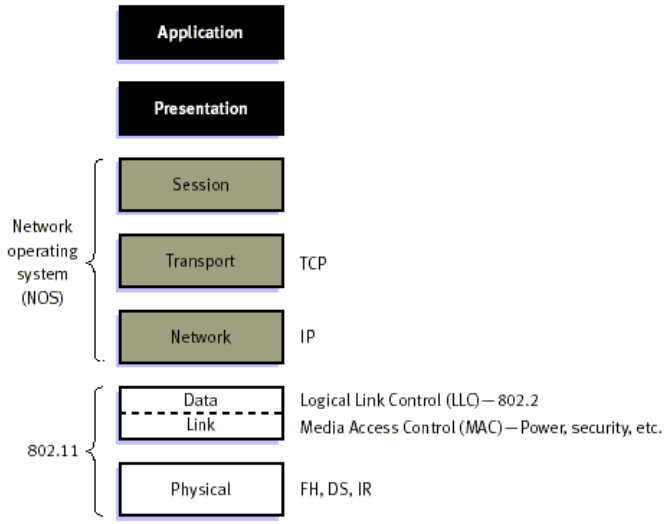

FIGURE 3 - IEEE 802.11 communication standard

3.0 - WLAN SECURITY

The market today has many concerns about the security implications associated with this type of network. On the other hand, large and medium companies are still very concerned about the fact that sensitive data is being transmitted through the air.

There are several types of security in WLAN 802.11, the model used is described in Santo Ângelo substation.

3.1 WPA Security Standard (Wi-Fi Protect Access) 802.11

Given the large number of vulnerabilities found in the WEP protocol, the group that created the standard IEEE 802.11 started to research how to develop a new security standard called IEEE 802.11i. The primary purpose was to solve all security issues found in WEP. While the standard was being developed, the Wi-Fi Alliance, responding to criticism generated by businesses concerning WEP, presented a standard called Wi-Fi Protected Access (WPA) in 2003. The WPA is based on RC4 and is a subset of specifications presented in a preliminary version of IEEE 802.11i. WPA introduces several mechanisms to solve the security problems associated with WEP:

- Rules for IV (Vector) and extended 48-bit IV - How the 24-bit used by WEP IV allowed just over 16 million different IV, making easy to have repetitions in a short time, the WPA introduces a 48-bit expanded IV. After this, more than 280 trillion different IVs are possible. Additionally, the WPA introduces rules for the selection and verification of IV's to render reinjection packet attacks ineffective.

- New message verification code - WPA uses a new 64-bit field, the MIC (Message Integrity Code), to verify whether the content of a data frame has alterations due to transmission errors or data manipulation. The MIC is obtained by an algorithm known as Michael.

- Distribution and key derivation - WPA automatically derives and distributes keys to be used for encryption and data integrity. This solves the problem of using the static WEP shared key.

3.1.1 Authentication

There are two types of authentication in the WPA protocol. One is directed to corporate networks and uses an 802.1x/EAP authentication server, therefore a complementary infrastructure; another, simpler one, is designed for small office networks and home networks (SOHO networks - Small Office / Home Office). These two types of authentication are called Corporate WPA and Personal WPA, respectively.

- Personal WPA - as an ordinary user is not able to install and maintain an authentication server, the WPA-PSK (WPA-Pre Shared Key) was created, which is a passphrase12 previously shared between the Access Point and the clients. In this case, authentication is through the Access Point. The key is manually configured on each device belonging to the network and can vary from 8 to 63 ASCII characters.

- WPA Corporate - Access Point is not responsible for any authentication. Both user authentication and the device is done through an authentication server. A complementary infrastructure is used, which consists of a server that uses the 802.1x authentication protocol together with some type of EAP (Extensible Authentication Protocol). 802.1x is a communication protocol used between the Access Point and the authentication server. This protocol was already widely used in wired networks, and also proved suitable when integrated with wireless networks. Whenever a client requests an authentication, the authentication server checks in its database if the credentials entered by the applicant are valid, and if so the client is authenticated and a key called the Master Session Key (MSK) is sent to him/her. Oftentimes, a RADIUS server is used as authentication server, but this is not required.

3.1.2 Integrity

Integrity in the WPA consists of two values. In addition to the ICV (Integrity Check Value) an integrity verification message is added to the frame, which is called MIC (Message Integrity Check).

Michael is a hash non-linear function, unlike the CRC-32. The destination address has already resulted in the priority (currently set to zero), data and an integrity key that entered into Michael to produce the MIC. The output corresponds to 8 bytes which together with the ICV form the integrity of the WPA protocol. Therefore, the integrity is represented by a total of 12 bytes, 8 generated by Michael and 4 by CRC-32, see Figure 4.

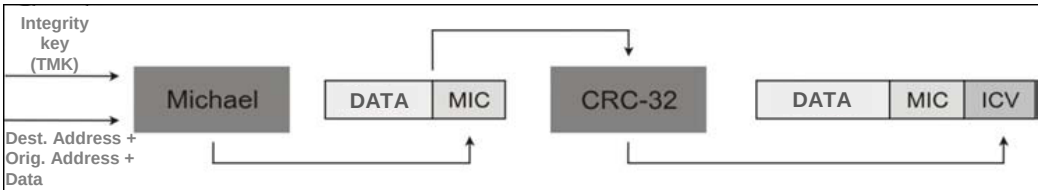

FIGURE 4 - WPA Integrity Protocol

3.1.3 Confidentiality

TKIP (Temporal Key Integrity Protocol) addresses many of the vulnerabilities in the WEP protocol. TKIP is based on the concept of temporal keys, that is, a key is used for some time and then dynamically replaced.

In the WPA in the initialization vector has 48 bits, which makes it virtually impossible to reuse vectors. In the structure of the 802.11 header field reserved for the IV there are only 24 bits, and because of this another field called IV Extended was created, which is not a part of the structure of the 802.11 header, to allocate the remainder of the IV. The IV is also used as a frame counter (TSC - TKIP Sequence Counter). Whenever a new encryption key is established, the TSC is reset. At each transmitted frame, it is incremented. Thus, frames with out of order TSC are discarded, avoiding packet re-injection.

The WPA encoding process is similar to the WEP one. The main difference is the key that will feed the RC4. This key is the result of a key combination algorithm of which the input is the inicialization vector, the MAC address of the transmitter and the data encryption key. In the end, the key generated by the key combination algorithm and the IV are passed to the RC4, see Figure 5.

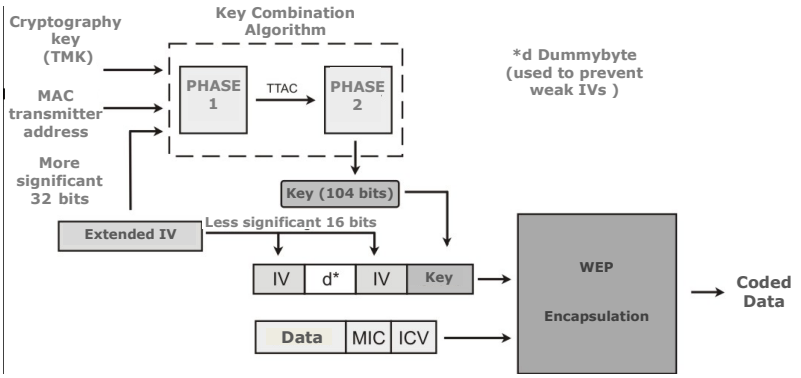

Figure 5 - WPA key combination algorithm.

4.0 - IMPLEMENTATION OF WIRELESS NETWORK AT THE SANTO ANGELO SUBSTATION

The Monitoring System for the three-phase 525/230-13, 8 kV - 224 MVA autotransformer bank of the Santo Angelo substation, TF3, aims at reducing the risk of catastrophic failures in this equipment when diagnosing its current status by detecting problems which still are incipient, as well as diagnosing future problems based on the progression of the measurements along time. For this purpose the system acquires and stores measurements done by the smart sensors on the autotransformer via RS-485/wireless network converters, and also processes data with the purpose of transforming them in useful information for maintenance.

4.1 Monitoring System Architecture

The monitoring system is based on a decentralized architecture, basically made of data acquisition equipment, data storage and processing equipment and communication medium, which connects the first two parts; equipment and data acquisition are in the body of the autotransformers itself and in the common cubicle (QCC), and consist of IEDs, microcontroller-based electronic equipment specifically designed to be installed in autotransformers, and therefore appropriate for operation in temperatures of at least -40 to +85 º C and up to 95% relative humidity. They are also immune to electromagnetic interference and radio frequency. These IEDs acquire the following type of figures: oil temperature, winding temperatures, tap changer humidity, capacitance and tangent delta on the condensive bushings, gas dissolved in oil, membrane in the conservator and dry contacts.

4.2 Data communication media

Data acquisition equipment is connected by two RS-485/wireless communication networks on the autotransformer panels and common cubicle, through a shielded twisted pair cable. The connection between the data acquisition system and the data storage and processing system located at the monitoring central, at Sertão Maruim, was accomplished through a wireless network, by adding the adequate converters and access points. Remote access is through the Eletrosul Intranet via the TCP / IP protocol, see Figures 6.7 and 8.

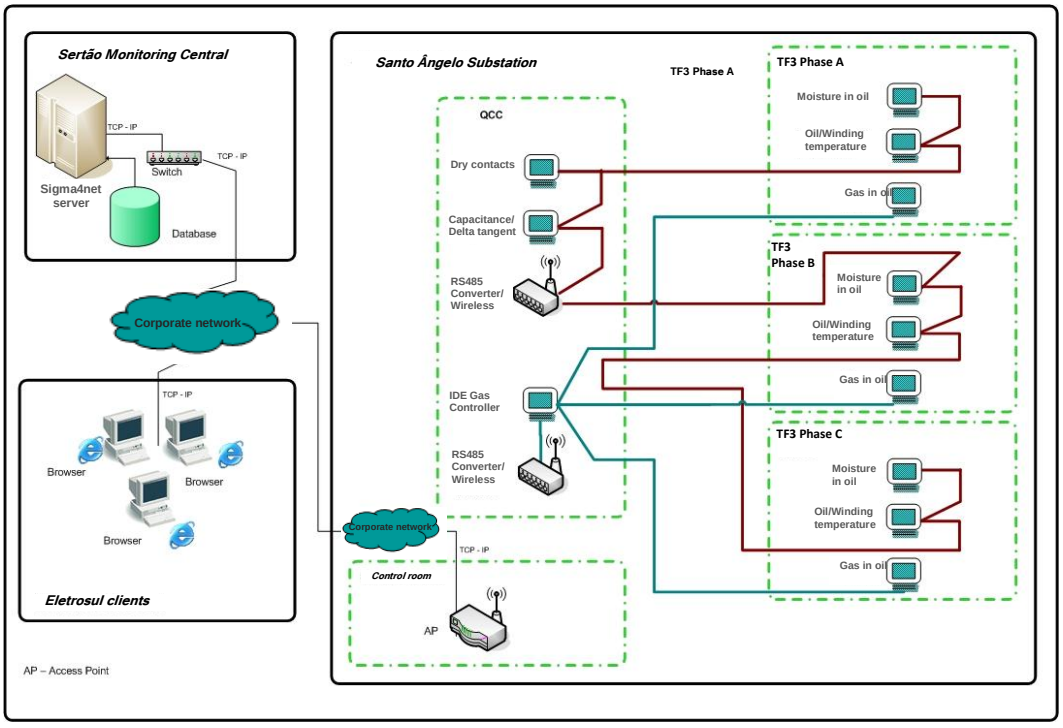

FIGURE 6 - Monitoring Architecture of the Santo Angelo substation.

FIGURE 7 - RS-485/Wireless converter panel

Translation of caption of Figure 6

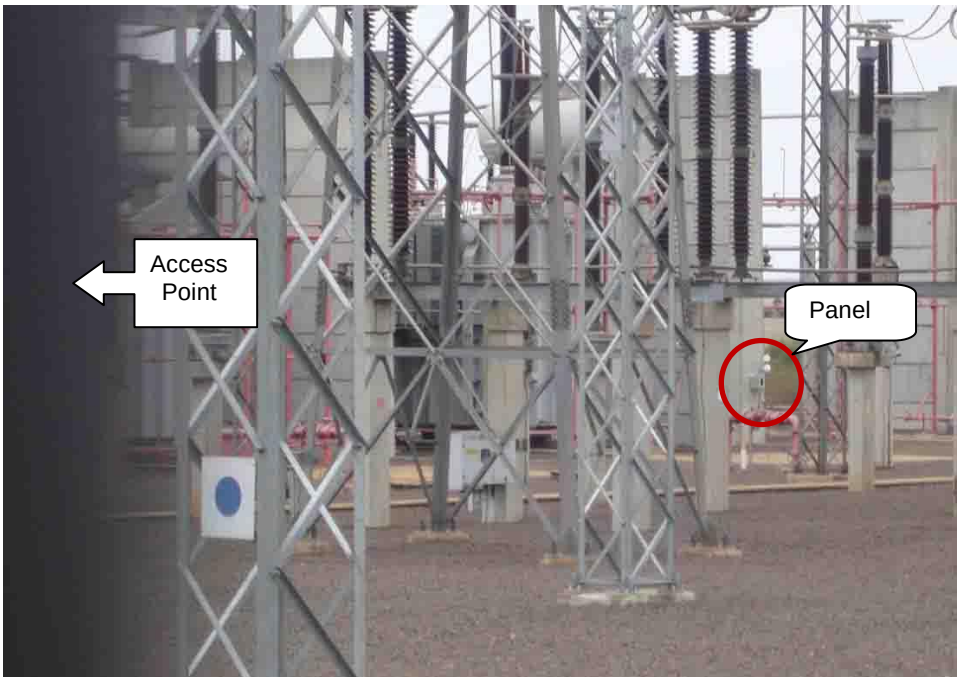

FIGURE 8 - Access point and converter point antenae

4.3 Security

The access point installed in the control room of the Santo Angelo substation has WAP-PSK authentication security and TKIP encryption method as described in Section 3.0 of this technical report; therefore, the converters installed

in the firewalls have the same configuration. For this purpose, in addition to those, their network physical addresses are listed in the access point, increasing information security even more.

5.0 - CONCLUSION

Since the monitoring system was installed at the Santo Angelo substation in November 2009, this application of wireless network is fully operational, and can be expanded to other pieces of equipment in the substation by simply adding the necessary IEDs and one wireless RS-485 converter. This reduces installation costs related to installing cables, fiber-optic converters and even additional converters.

6.0 - REFERENCES

(1) M. Ciampa, J. Olenewa - Wireless # Guide to Wireless Communications 2006

(2) S. Haykin, Moher M. - Modern Systems Wireless Communications 2007

(3) Boland, He Mousavi, H. Security issues of the IEEE 802.11b wireless LAN, 2004

7.0 - BIOGRAPHICAL DATA OF THE AUTHORS

Clayton Sperandio Duriguetto - Born in Guarulhos, SP, on August 9, 1983, Clayton has worked for Treetech Sistemas Digitais since 2001. Specializing in the development of power transformer monitoring and control systems, circuit breakers and industrial networks, Clayton works at the RD & I department. He holds a Bachelor degree in Information Systems from the Faculdade Eniac, Guarulhos – SP, obtained in 2009, and a diploma of Electrical and Electronic Technician from Instituição Senai - Hermenegildo de Almeida Campos obtained in 2000 in Guarulhos - SP.

Rafael Prux Fehlberg - Born in Porto Alegre, RS, 13 August 1981. He has worked for Treetech Sistemas Digitais since 2004 with engineering applied to equipment monitoring in substations. He obtained his degree in Control and Automation Engineering from PUC-RS in 2003.

Fernando Temotheo de Carvalho was born in São Paulo, SP on January 04, 1981, and has worked for Treetech Sistemas Digitais since 2002. A power transformer monitoring and control system, circuit breaker and industrial network specialist, Fernando works at the department of Application/Software Engineering. He received a degree in Computer Science from Universidade Uninove, São Paulo, SP, in 2004.

Sandro Peixoto - Born in Florianópolis – State of Santa Catarina, Brazil, he has worked for Eletrobras Eletrosul since 2001. He is a specialist in electrical power systems engineering and electric power substation yard equipment monitoring systems. He obtained his degree in electrical engineering in 2001 from UFSC, and is an Electronics Technician with a diploma from the Federal Technical School of Santa Catarina, which he received in 1990.