SBrT 2019 1570557404

The Prototype Implementation of an IoT-based Framework for Energy Reliability and Asset Security in Base Stations

Caique R. Miranda, Fabricio P. V. de Campos and Moisés V. Ribeiro

***Abstract*— The paper discusses an Internet of Things-based framework that is suitable for designing cost-effective Smart Base Stations that need energy delivery continuity and asset security. Also, the implementation of a prototype of a Smart Base Station that is based on the proposed IoT framework is described. In addition, a field trial of the implemented prototype is presented. Overall, we show that the discussed IoT-based framework is an important tool for reducing interruptions of telecommunication services in Base Stations and, as a consequence, avoiding expenses with fines.**

***Keywords*— Base station, Internet of Things, renewable energy, energy delivery, asset security.**

I. Introduction

During the last years, there has been exceptional growth in telecommunication market. The number of users and the demand for for cellphone and things has increased dramatically. With the introduction of smart phone devices, the use of ebook readers, the advent of the Internet of Things, Industry 4.0, and the success of social networking, the demand for cellular data traffic has also grown significantly. Hence, telecommunications companies inevitably seek to meet these new demands of wireless cellular networks, always focusing in to minimize costs. It is expected that with Internet of Things (IoT), the demand for data traffic will increase considerably [1]. In order to fulfill the these demands, mobile operators need to invest in infrastructure capable of providing the infrastructure availability 24 hours a day.

The energy consumption in Base Stations (BSs) market will increase greatly and management of available resources for energy reliability will be required with the introduction of the Fifth Generation (5G) technology. One fact that must be taken into account is the type of energy source supplying BSs, which can be renewable energy sources or green energies (e.g., solar, wind, hydro), or non-renewable energy sources (e.g., diesel). In addition, the configuration can be on-grid or off-grid. Previous researches have addressed different methods and alternatives for feeding BSs [2] [3].

Aiming to investigate this subject using the concept of IoT, this paper proposes an IoT-based framework for the management of smart BSs resources, focusing on energy saving, energy reliability and asset security. This IoT-based framework covers the majority of aspects and we can use part of it to solve specific situations faced by BSs (e.g., on-grid or off-grid). Moreover, we show that based on this framework we can guarantee energy reliability and asset security. A prototype of an IoT-based framework for a specific case validates the proposed framework.

The rest of this paper is organized as follows: Section II outlines the problem addressed in this work. In the sequel, Section III discusses the IoT-Based framework for BSs. Section IV focuses on prototype of IoT-based implementation for BSs. Posteriorly, Section V contemplates the field test results. Finally, Section VI states concluding remarks.

Caique R. Miranda, Fabricio P. V. de Campos e Moisés V. Ribeiro, Department of Electrical Engineering, Federal University of Juiz de Fora, Juiz de Fora-MG, Brazil. E-mails: caique.rocha@engenharia.ufjf.br; fabricio.campos@ufjf.edu.br; mribeiro@engenharia.ufjf.br

II. Problem Formulation

The fines caused by service interruptions are among the main problems faced by telecommunications companies. It has been recognized that power outages and thefts of equipment at the BSs facilities are the main sources of these problems that, unfortunately, are without reasonable (cost-effective) solutions [4]. Usually, these problems become worse when BSs are located in isolated places that are difficult to be accessed. As a consequence, the telecommunication companies struggle because the corrective solutions are expensive and may takes a long time period for implementation.

One feasible approach to circumventing such problem is to come up with the concept of Smart BS. In this context, the energy reliability is ensured by using a mix of renewable energy sources (e.g, solar, wind and hydro) and diesel generator. Also, the asset security may be ensured by using pervasive data networks together with sensors to monitor, manage, and guarantee the correct operation of the facility as well as to report technical and non-technical problems. Regarding energy reliability, it is important to emphasize that BSs may face unscheduled interruptions due to power outages and, as a consequence, the use of distinct energy sources can offer flexibility to deal with the intermittent energy delivery.

IoT concept is capable of offering the solution to the presented questions because the creation of an IoT-based framework is capable of improving energy reliability and asset security in BSs.

In this sense, we point out that an IoT system has to equip the BS with a network of sensors and/or actuators. The sensors are responsible for acquiring data related to physical variables (e.g., temperature, current and voltage) and relevant information (e.g., anti-theft and presence sensors). The information is shared with a BS management that, in its

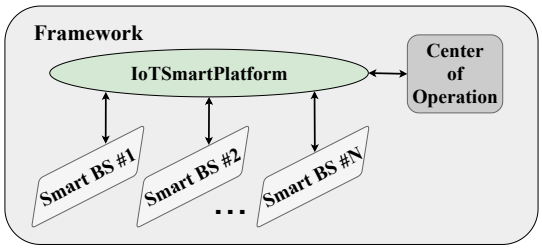

Fig. 1: IoT-based Framework for smart BSs.

turn, is capable of processing all of them to inform and/or to predict security breaches and energy outages, to report current conditions of the BS to the telecommunications headquarter, and to switch on/off loads. On the other hand, the actuators are responsible for changing the operational conditions of the Smart BS.

III. The IoT-Based Framework for smart BSs

An IoT-based framework for smart BSs needs to have a BS platform that manages and controls the energy reliability and asset security of BS equipment. It allows, the telecommunications headquarter remotely access the information operation. In this sense, we address a framework that includes monitoring of renewable and non-renewable energy sources in order to provide uninterrupted energy delivery for BSs, with the possibility of switching among these sources through remote operation. Additionally, an anti-theft system that prevents possible criminal acts is also detailed.

In this context, Fig. 1 shows the proposed IoT-based framework for smart BS. As we can see, this framework is composed of the following three main parts:

- **Smart BS #*n***: this part is responsible for collecting analogue and digital data, processing and sending them to to IoTSmartPlatform. The #*n* index is the *n*-th smart BS of the framework, where $1 \leqslant n \leqslant N$.
- **IoTSmartPlatform**: this is the platform operating in the cloud. It is responsible for connection control, data storage in databases, data security and data exchange control. The IoTSmartPlatform receive the collected data, store in the database and present him to user at the Center of Operation.
- **Center of Operation**: through an interface, the telecommunications headquarter can communicate to the BS through the IoTSmartPlatform. This part shows general information of the power supplies, retrieves data from the Smart BS, allows the operators monitor and change status.

Fig. 2 shows Smart BS #*n* and each part is detailed as follows:

- **IoTNetSensor #*n,i***: the IoTNetSensor #*n,i* is capable of extracting informations of distinct power supply (e.g., solar, wind, diesel, battery, power utility) and monitoring status of the facility. The information is shared with the so-called IoTDataConcentrator #*n*. The extraction of this data can be carried out by various sensors (e.g., Alternating Current (AC) and Direct Current (DC) voltage sensor, AC and DC current sensor, temperature sensor, pyranometer, air velocity sensor, presence sensor, anti-theft sensor). Addition to that, the IoTNetSensor #*n,i* can remotely switch electrical loads or source of energy by sending commands from the Center of Operation. The #*n,i* index refers to *i*-th IoTNetSensor of the *n*-th Smart BS of the framework.

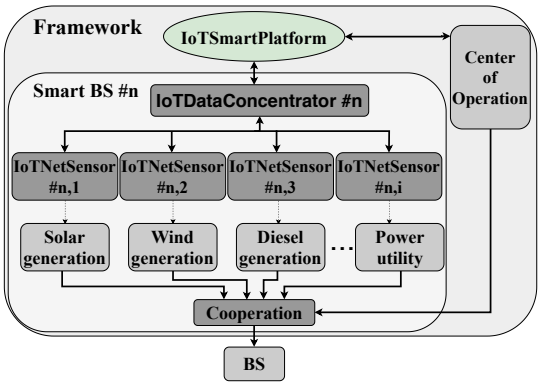

Fig. 2: Smart BS #*n* of the IoT-based Framework

- **IoTDataConcentrator #*n***: the IoTDataConcentrator #*n* receives all data from the IoTNetSensors #*n,i*, stores and send them to the IoTSmartPlatform. The IoTDataConcentrator #*n* perform an offline data treatment when the communication link with IoTSmartPlatform is lost. As soon as communication link is reestablished the IoTDataConcentrator #*n* sends all data offline to IoTSmartPlatform. The #*n* index refers to *n*-th IoTDataConcentrator of the framework.
- **Switch Source**: this part of the framework is the part that makes the switching between the sources of energy. It can be developed using remote triggering or other techniques that can be found in the literature, such as [2] [3].

For making this framework feasible, it is necessary to define the types of communications among the components. In this regard, descriptions of communication technologies suitable for being used in the proposed IoT-based framework for Smart BSs are as follows:

- **Communication between IoTNetsensor #*n,i* and IoTDataConcentrator #*n***: this communication can be carried out by wireline or wireless system. After, the protocol must be defined (e.g., profibus, modbus Remote Terminal Unit (RTU), modbus ASCII, ZigBee, private protocol) [5] [6].
- **Communication between IoTDataConcentrator #*n* and IoTSmartPlatform**: can be provided by wireline or wireless system. After, the protocol must be defined (e.g., profinet, modbus Transmission Control Protocol (TCP), EtherCAT, private protocol) [7] [8].

IV. IoT-based Implementation for Smart BS

Given the framework presented in Section III, this section describes an implementation prototype of the IoT-based framework for smart BS. This implementation focuses on energy reliability and asset security.

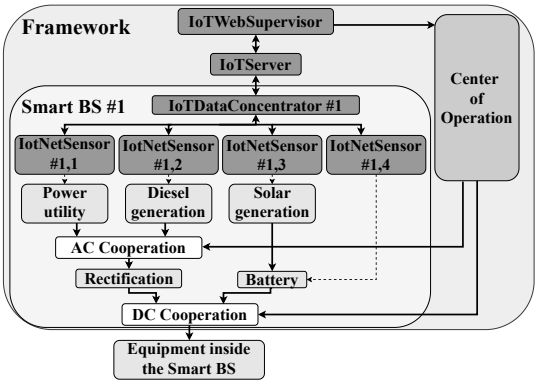

Fig. 3: The block diagram of the IoT-based implementation for a single smart BS.

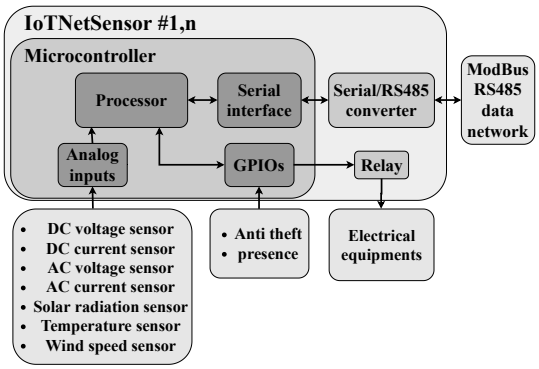

Fig. 4: The block diagram of an IoTNetSensor #1,*n*.

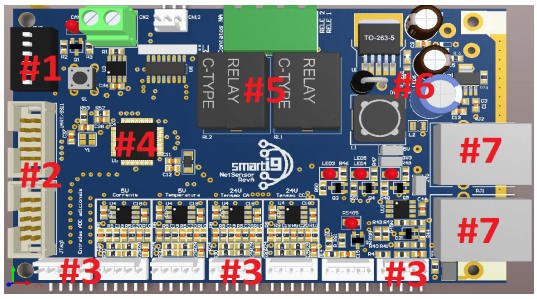

Fig. 5: The IoTNetSensor #1,*n* prototype

Fig. 3 shows the block diagram of the prototype of IoT-based framework for a single smart BS. In this implementation, we use the IoTNetSensors #1,1 to #1,4 to monitor variables of interest from power utility, diesel generation, solar generation and battery. The four IoTNetSensors are collecting data using the following sensors: Root Mean Square (RMS) AC and DC current, RMS AC and DC voltage, presence sensor and anti-thief sensor;

After the data are collected by the IoTNetSensors, they are sent to IoTDataConcentrator #1. It receives these data and send them to IoTSmartPlatform (server in the cloud) if internet connection available, otherwise the data are saved in Secure Digital (SD) Card for future retrieve. The data can be read on IoTWebSupervisor through the Center of Operation. Moreover, with the IoT-based framework for smart BS it is possible to remotely switch AC and DC sources remotely from the Center of Operation.

A. *IoTNetSensor #1,n*

Fig. 4 shows the block diagram of the IoTNetSensor #1,*n*, which is a device developed for obtaining data from several sensors installed in a Smart BS. This sensors are connected to the IoTNetsensor #1,*n* via the analog inputs and General Propose Input or Outputs (GPIOs). After processing, the data is passed to the serial interface of the microcontroller. Next, the conversion of serial into Recommended Standard (RS)-485 occurs so that the data is sent to the IoTDataConcentrator #1 by ModBus RS-485 data network.

Note that the IoTNetSensor #1,*n* is capable of triggering electrical equipment utilizing GPIO connected to relay. The command for switching electrical equipments is sent from the center of operation to the IoTWebSupervisor, and then the command passes through the IoTDataConcentrator #1 and, finally, arrives at the IoTNetSensor #1,*n*.

The prototype of the IoTNetSensor is shown in Fig. 5. Its components descriptions are as follows:

- **#1** - Dual In-line Package (DIP) switch: it is used to set the sequence of IoTNetSensor #1,*n*.
- **#2** - Joint Test Access Group (JTAG).
- **#3** - Analog inputs and GPIOs.
- **#4** - Microcontroller: The IoTNetSensors were implemented with a microcontroller TM4C123GXL and their firmwares were built in C language on the platform Code Composer Studio (CCS) of the Texas Instruments [9].
- **#5** - Relays and output to power electrical equipment.
- **#6** - Power supply.
- **#7** - Connector for the modbus RS-485 network.

B. *IoTDataConcentrator #1*

Fig. 6 shows the block diagram of the IoTDataConcentrator #1. It is the device developed with the purpose of concentrating all collected data. Its function is to receive data from all IoTNetSensors and to send these data to IoTServer through modbus TCP data network. In more detail, the data coming from Modbus RS-485 network sent to the serial RS-485 converter and, in the following, to the serial interface 2 (microcontroller peripheral). Next, the processor reads the data and processes them. After the data has been processed, they are passed to the serial interface 1 (microcontroller peripheral). The serial interface 1 send the bit stream (data) to serial/Ethernet converter. At the end, the data are sent to IoTServer through the modbus TCP network.

Another feature of the IoTDataConcentrator #1 is to take care of data if the communication link with the IoTServer is lost. Basically, it saves the data available in the IoTNetSensors in a SD card. Basically, if the communication link is lost, them the microprocessor enables a Serial Peripheral Interface (SPI) communication and data recording on the SD card. It avoids the lost of data. Note that the data is sent to IoTServer as soon as the communication links is reestablished. In addition, the IoTDataConcentrator #1 implements Human-Machine Interface (HMI) GPIOs for controlling Liquid Crystal Display (LCD) display and buttons, which are used by users

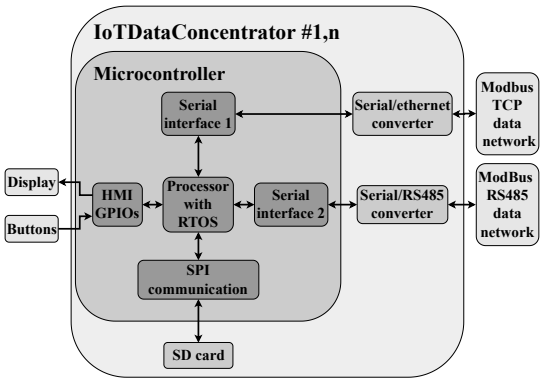

Fig. 6: The block diagram of the IoTDataConcentrator #1.

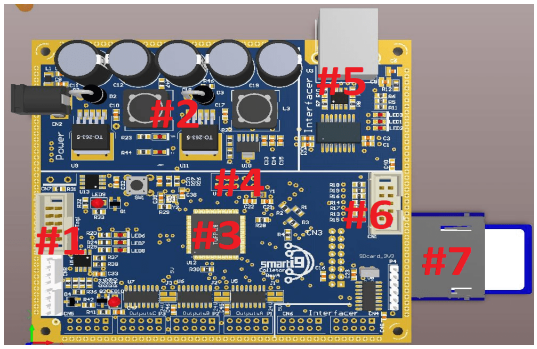

Fig. 7: The IoTDataConcentrator #1 prototype.

to access status information in the field. This is necessary if the user wants to see some information in the field. Fig. 7 shows the prototype of the IoTDataConcentrator #1. Details are as follows:

- **#1** - Connector for the modbus RS-485 network.
- **#2** - Power supply.
- **#3** - Microcontroller: it implements the microcontroller TM4C129XL. Its firmware makes use of a code that uses Real Time Operating System (RTOS) to perform all functionalities of the IoTDataConcentrator #1. This firmware was built in C language on the platform CCS of the Texas Instruments [9].
- **#4** - Connector for LCD display of the HMI.
- **#5** - Connector for the TCP network.
- **#6** - Connector for buttons of the HMI.
- **#7** - SD card.

C. IoTServer

The IoTServer is a server capable of exchanging data with IoTDataConcentrator #1, processing and storing them in a database. Also, it exchanges data with IoTWebSupervisor so that the user can access through the Center of Operation.

D. IoTWebSupervisor

The IoTWebSupervisor is basically composed of HyperText Markup Language (HTML) pages which provide remote supervision of resources. This interface is user-friendly, since it allows easy management, visualization, creation, edition and deletion of the monitored data. Through IoTWebSupervisor, it is possible to see sensor information and status, to verify which power supply is currently feeding the smart BS and send commands to switch the source of power.

E. AC and DC switch sources

The smart BS in Fig. 3 needs a 48 V DC power supply. In this regard, it is necessary to adjust the voltages to power the smart BS and choose which source of power will be used by the smart BS. Based on Fig. 3, the power utility or the diesel generator provide 220 V RMS AC. There is an AC switch source to choose which source or energy will feed the rectifier. The rectifier has the function of rectifying the AC waveform and making it 48 V DC. Also, the generated energy by the power of the solar is stored in battery. In other word, it is possible to choose whether the smart BS will be powered by power coming from the rectifier or the battery. It demands the use of DC switch source.

F. Data Flow

The data exchanges among the components of the prototype framework demands the choose of communication protocol. The choices needs to comply with the constraints of the each components and the characteristic of the environment. The chosen communication protocols are described as follows:

- **Communication between IoTNetsensor #1,*n* and IoTDataConcentrator #1**: as previously mentioned, the communication protocol chosen to interface with the IoTNetSensor #1,*n* and IoTDataConcentrator #1 was the RS-485, which has high noise immunity and the low possibility of interference or unwanted emissions, in conjunction with the modbus RTU protocol [10]. The RS-485 is a good choice and widely used in industrial process communications. The modbus RTU was chosen because it is a consolidated and free-access protocol.
- **Communication between IoTDataConcentrator #1 and IoTServer**: the communication protocol chosen to interface with the IoTDataConcentrator #1 and IoTServer is the Ethernet cable in conjunction with the modbus TCP protocol. Ethernet is the most reliable communication choice for this case, since packet loss and communication reliability is greater when compared to wireless. Similarly to the modbus RTU, the modbus TCP is a TCP/Internet Protocol (IP)-based modbus implementation . It is a cheap, easy to use, and free-access communication protocol.

V. Field Test Results

In this section, field test results of the IoT-based prototype implementation of the discussed framework are presented. The prototype, detailed in Section IV, was installed in the *Laboratório Solar Fotovoltaico* (Portuguese for Solar Photovoltaic Laboratory) (LABSOLAR), which is located at the Federal University of Juiz de Fora, Juiz de Fora, MG, Brazil.

Fig. 8 shows the temperature and DC voltage measurements of the IoTNetSensor installed at the solar plant of the LABSOLAR. We can see that the energy generation is a function of

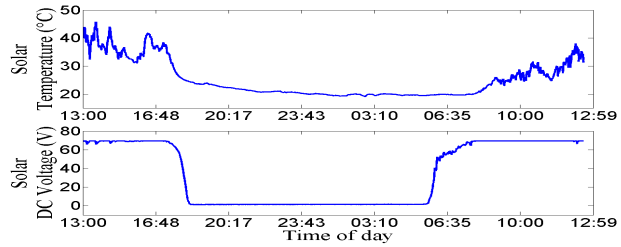

Fig. 8: Solar generation: temperature measurements and voltage measurements.

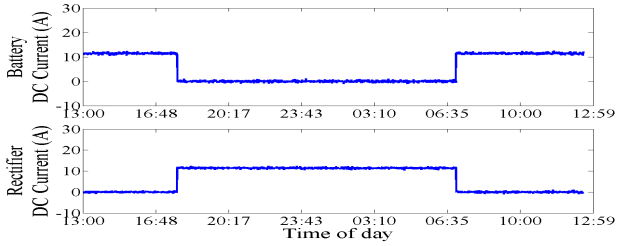

Fig. 9: Battery DC current and rectifier DC current.

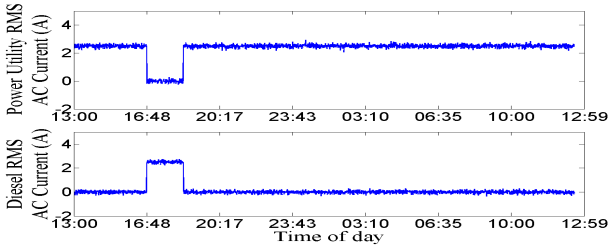

Fig. 10: Diesel RMS AC current and power utility RMS AC current.

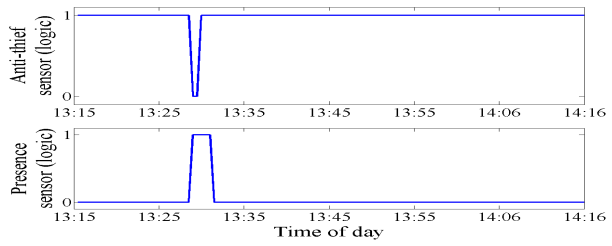

Fig. 11: Asset security: presence detection and anti-thief detection.

solar radiation, i.e., the generation is more considerable during the day than at night, when the voltage drops to values equal to 0 V. The temperature graph also follows the sunrise and sunset, presenting higher temperatures during the day.

Fig. 9 shows the rectifier and battery DC currents. As we can see, battery and rectifier are powering the smart BS. This shows that during daylight hours, the smart BS is powered by the solar generation using the charge stored in the bank of batteries. When there is no solar energy production, the rectifier is feed by the electric or diesel generated energy, which will feed the smart BS. As a result, it is possible to have savings with electric bill by using the potential of solar energy production.

Fig. 10 shows the AC currents of the diesel generator and the power utility. As can be seen, at 4:48 p.m. a power outage occurred in the power utility and, with this, the diesel generator came into action to maintain the power feeding of the smart BS. As soon as the power from the power utility is restored, the diesel generator is shut down.

Fig. 11 shows that the Asset security feature detects unauthorized access to the smart BS facility. According to this figures, the security breach occurred at 1:30 p.m. because the anti-theft sensor was set to 0 and a detection of the presence sensor was set to 1.

VI. Conclusions

In this work, we have discussed an IoT-based framework that addresses energy delivery continuity and asset security of a Base Station. Also, the implementation of a prototype of a so-called Smart BS that is based on the proposed IoT framework have been detailed. In addition, a field test of the implemented prototype have been discussed and a case study results have been reported. The attained results have shown that it is possible to monitor different type of power generation and select the best and most economical for each period of the day. Moreover, the prototype have shown the reliability effectiveness in terms of energy delivery to a BS. Finally, the results have shown that the prototype implementation of the discussed framework can be effective for dealing with non-authorized access to the BSs facility.

Acknowledgment

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001, CNPq, FAPEMIG, Smarti9 and INERGE.

References

[1] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[2] D. Niyato, X. Lu, and P. Wang, "Adaptive power management for wireless base stations in a smart grid environment," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 44–51, Dec. 2012.

[3] H. J. Hung, T. Y. Ho, S. Y. Lee, C. Y. Yang, and D. N. Yang, "Relay selection for heterogeneous cellular networks with renewable green energy sources," *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 661–674, Mar. 2018.

[4] V. O. C. Guimaraes, "Incidents in networks that impact on the provision of telecommunications services." Internet: http://slideplayer.com.br/slide/11349872/, Accessed: Apr. 18, 2019.

[5] B. R. Mehta and Y. J. Reddy, *Industrial process automation systems: design and implementation*. Butterworth-Heinemann, 2014.

[6] L. E. Frenzel, *Handbook of serial communications interfaces: a comprehensive compendium of serial digital input/output (I/O) standards*. Newnes, 2015.

[7] G. S. Sestito, A. C. Turcato, A. L. Dias, M. S. Rocha, D. Brandão, and R. da Veiga Torres, "Case of study of a profinet network using ring topology," in *Proc. IEEE Int. Symp. on Consumer Electronics*, pp. 91–96, 2016.

[8] D. Jansen and H. Buttner, "Real-time ethernet: the ethercat solution," *Computing and Control Engineering*, vol. 15, pp. 16–21, Mar. 2004.

[9] T. Instruments, "Code composer studio desktop ide for all ti microcontrollers, processors, and wireless connectivity platforms." Internet: http://www.ti.com/tool/ccstudio, Accessed: Apr. 18, 2019.

[10] T. Instruments, "Rs 485 reference guide." Internet: http://www.ti.com/lit/sg/slyt484a/slyt484a.pdf, Accessed: Apr. 18, 2019.