DOI: 10.2478/SBEEF-2020-0107

OPEN SOURCE ARCHITECTURE FOR IOT BASED SCADA SYSTEM FOR SMART HOME

S. D. GRIGORESCU, G. C. SERITAN, B. A. ENACHE, F. C. ARGATU, F. C. ADOCHIEI
Department of Measurements, Apparatus and Static Converters, Electrical Engineering Faculty, University POLITEHNICA of Bucharest, Romania
E-mail: bogdan.enache2207@upb.ro

Abstract. ***The Internet of Things is considered an emerging technology with the potential to penetrate all aspects of our lives. However, with great power comes great responsibility and the privacy and security needed for critical infrastructure or sensitive commercial operations is very different than the needs of a Smart Home. Additionally, the available security resources from the private sector are totally different than the ones available to a homeowner. In this context, we developed an open source architecture for IoT which is based on the advantages of a SCADA system and can be easily applied to a Smart Home. This architecture assures a high-security level, even for low technical skills homeowners, with minimal costs.***

Keywords: Smart Home, SCADA, IoT, open source

1. INTRODUCTION

The Smart Home was designed to provide additional comfort and security to the regular home, as well as enhanced ecological sustainability [1]. This was possible by implementing a wide variety of household sensors and actuators and means to process all the gathered data in a way that intelligent operating decisions are made, instead of manual or fixed-schedule control schemes [2].

The Smart Home can assist its inhabitants with daily tasks such as cooking, cleaning, etc. Also, it can be part of a health monitoring system that can provide timely reminders for medication or signal specialized personnel to respond in case of a medical emergency[3]–[7].

On the other hand, by constantly tracking the number of occupants and their desired choices it can adjust the indoor climate so no energy is wasted [8].

To further increase the efficiency of such a smart home a logic continuation would be to interconnect it with utilities providers. There are several steps made in this direction regarding the power grid and the internet, but other facilities like water and gas still need solid effort. The internet was the first that took into account the development of smart homes by providing means for interconnecting different types of devices: house-hold appliances, vehicles, small electronics, wearables, etc. The power grid came next, fueled by the need to integrate renewables power source with the existing ones. The solution adopted was the Smart Grid, which expands energy efficiency beyond the delivery infrastructure by allowing energy and information to be exchanged in both directions [9]. Another important feature of the smart grid is demand response which coordinates the operation of low priority home appliances (washing machines, dishwasher, water heaters), depending on the preferred energy source and the energy price [10].

All these were possible due to a large network of interconnected non-traditional devices equipped with specialized software and communication capabilities known as the Internet of Things (IoT). The IoT moves the spot-light from functionality to connectivity, meaning that, a device is more useful if it part of a network rather doing its job best, but alone [10]. On the other hand, the IoT is not simply a sum of devices and sensors interconnected – it is a dense integration of the virtual and the real world which enables the communication between people and devices to take place [9].

Like all computer networks, security and privacy are primary requirements for IoT too. However, while most of the computer networks have dedicated professional resources to attend their security, the Smart Home is a relatively remote system without dedicated specialized security systems, and with minimal technical knowledge from the house owner [11]. This situation presents several challenges to security and privacy which need to be addressed in order for the Smart Home to be feasible [1], [10].

Several researchers have analyzed this situation and developed an array of solutions from auto-configuration system, to collaborative intrusion detection (CID), to cloud security and improved Supervisory Control and Data Acquisition (SCADA) systems. In [1] an auto-configuration security system is presented, this system through its specific security updates prevents an attacker from accessing the network. Following a different approach in [12], a framework for CDI is developed. This framework gathers information from sensor nodes and edge routers to achieve efficient and cost-effective security. The Internet Engineering Task Force proposed a Constrained Application Protocol which combined to a cloud architecture becomes a powerful security protocol for authentication and communication. In [13] an IoT-SCADA system based on a deep belief network is used to analyze network traffic in order to detect malware signatures. Also, in [14] a management protocol used to secure the communication channel of all the SCADA entities is presented. This protocol makes use of a symmetric cryptography scheme, due to resource

constraints of the SCADA entities, and assures a high-security level that can be used in the Smart Home environment.

This paper presents a detailed design of a SCADA-IoT system especially design for Smart Homes. The system is using a few low-cost, and completely open source components. The system respects the basic configuration of the SCADA system (Section 2) and uses Open Process Communication Unified Architecture (OPCUA) protocol for data exchange between the SCADA components and MQ Telemetry Transport (MQTT) protocol for data communications with the IoT (Section 3). The advantages of the proposed system and its challenges are presented in the last section of the article – Section 4.

The goal of the paper is to solve the drawbacks or limitations that other similar approaches present [1], [10], [12], [15], as well as to provide an alternative framework suitable for a Smart Home environment.

2. SYSTEM DESCRIPTION

SCADA technology reached its maturity in the industrial sector, where was used to acquire data from remote devices and provide overall monitoring and control through a software platform. It performed these functions using only four basic elements i.e. Field Instrumentation (FI) devices which can be sensors and actuators, one or several Remote Terminal Units (RTUs) all linked to a Master Terminal Units (MTUs) for processing the data and the human-machine interactions. This basic configuration of a SCADA system is presented in Figure 1.

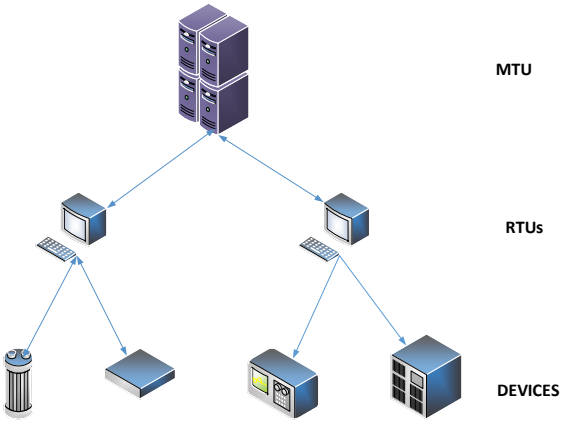

Figure 1. The basic configuration of a SCADA system

There are only two possible solutions for a SCADA system i.e. Proprietary and Open Source. A proprietary system is composed of hardware components from a single manufacturer and the communication protocols are specially developed for that hardware configuration [16]. In this case, the responsibility for system safety belongs entirely to that specific manufacturer. This configuration usually leaves the customer vulnerable, in the case of the manufacturer bankruptcy, has low flexibility in the case of an upgrade and is most of the times more expensive.
An Open Source system permits the possibility to combine components from several manufacturers. This means that no single supplier is responsible for the system security and usually a third party is involved. This solution also represents the most cost-effective one, because the customer can choose the required hardware from several producers. The biggest problem with this solution is that all the hardware must have a common communication protocol for the system to work [16].

2.1 Hardware Setup

Our proposed architecture – Figure 2, makes use of the all available Arduino Uno as the MTU and a Raspberry Pi board computer as RTU. The RTU is connected to a wireless router that has an active internet connection.

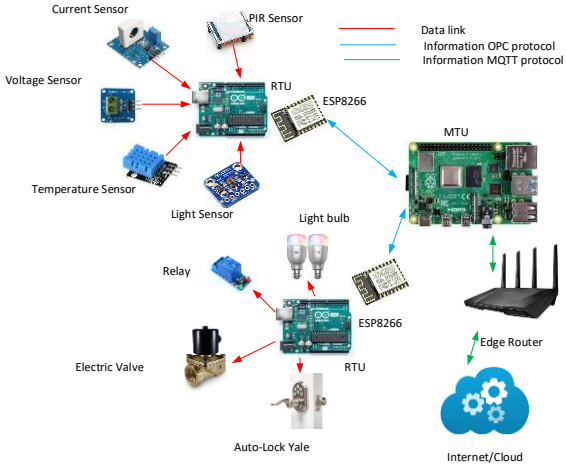

Figure 2. Proposed SCADA system

In our proposed scenario the two RTUs have distinct functions. One is used for data collection – RTU1, and the other – RTU2, performs different functions through actuators. This was chosen only for explanatory reasons, in a Smart Home the same RTU can easily perform both functions.

RTU1 gathers data from the sensors i.e. people presence (PIR sensor), current, voltage, temperature, light intensity, etc. through its all available interfaces Digital to Analog Converter (DAC), SPI, I2C. The data is sent using the ESP8266 WiFi chip to the MTU using the OPCUA protocol.

RTU2 receives commands from the MTU using another ESP8266 chip and the same communication protocol. These commands are then translated into specific functions to be performed by the actuators i.e. door lock, relays, electric valve, etc.

The MTU is a Raspberry Pi 3 B board. This is a single board computer whose design makes it suitable for the our proposed SCADA architecture. On the communication side, the MTU acts as a server for the OPCUA network and a gateway for the SCADA and the IoT Cloud.

2.2 Software Setup

The software used is all open source and represent a combination of code for Arduino and Raspberry Pi.

On the RTU side the communication is performed using the following libraries:

- OPC available on GhitHub;
- Wire for I2C communications;
- SPI for SPI communications.

The MTU has installed a Linux-based operating system and the following applications:

- NodeOPCUA for OPC communications;
- Mosquito the MQTT broker;
- InfluxDB a time-series database;
- Telegraf to bridge the MQTT broker and the database
- Grafana a platform to create Dashboards.

3. DATA COMMUNICATIONS

From the beginning, it must be noted, that the paper does not present new communication protocols, on the contrary, the proposed SCADA system uses an aggregation of already existent ones combined under a different perspective and applied to a challenging environment, a Smart Home.

The OPCUA is a communication protocol released in 2008 based on a traditional solution (i.e. OPC protocol developed for Windows stations) for permitting the communication between different types of machines. The new protocol provides a service-oriented architecture (SOA) assuring the old hardware that support only OPC with new ones in a information modelling framework [17]. Although OPCUA has received a massive improvement it still needs additional hardware as gateway or router capable of performing IoT specific protocols i.e. MQTT, CoAP to communicate with the Cloud Server.

To bridge the gap between the OPCUA and the IoT several researchers proposed a concept called heterogeneous IoT gateway. In [18], the authors developed an IoT gateway to link a Siemmens PLC with an IBM cloud service using MQTT protocol and NodeRED. In [19], the authors presented a distributed industrial IoT gateway concept which permits the communication between a PLC with Modbus to Cloud server. In [17] a micro-service (protocol) Docker has been developed in an open-source industrial IoT gateway.
The proposed configuration – Figure 3, is based on the Mosquito application to make the data exchange between the SCADA OPCUA network and the IoT.

Figure 3. Data communication applications

Mosquitto is an open source message broker that implements the MQTT protocol versions 3.1, 3.1.1 and 5.0. The MQTT protocol implements a publish/subscribe model that can be used to carry out messages between low power sensors or mobile devices.

Telegraf is an open source server agent that subscribes to Mosquitto, reads the published data by the sensors, and stores this information into the InfluxDB database.

Grafana is an open source analytics and monitoring solution that reads the data from the InfluxDB and creates a dashboard to visualize the information.

InfluxDB is a database management system chosen for recording the information in a structured manner, i.e. a time series database.

4. DISCUSSIONS

The key features of the proposed SCADA architecture are listed below:
Supervisory Control – The proposed system enables the owner the possibility to issue supervisory control commands in the case when the received information does not correspond to the predetermined values or expected range.
Monitoring – Through its Grafana Interface the system provides a dashboard for events and data monitoring that can be accessed from a mobile device or a web interface.
Reporting – All the data gathered from the sensors and the state of the actuators is stored in the InfluxDB database.
Security – The basic security measures i.e. access control, authentication, authorization, whitelists, firewalls, can be easily implemented by the homeowner due to the SCADA IoT architecture.
Ease of Use – The proposed SCADA system is easy because Grafana is very intuitively and user-friendly.
Low power – The system uses low-power components. In its core configuration, only one Arduino with an ESP8266 and a Raspberry Pi the total power consumption during operation is 2.2 W [15].
Low-Cost and Open Source – The components used are manufactured by different companies (mix and match), they are available and very cheap. Also, they are compatible with a large array of household appliances and components already available. Therefore, the consumer is not tight to a single manufacturer which is one of the key features of an open source system [15].

5. CONCLUSIONS

In this paper, an open source SCADA system based on IoT, for a Smart Home has been presented. The proposed architecture uses already available components manufactured by different companies (mix and match) and an array of open source communication protocols that had proven their merits over the years.

The solution was designed considering a house owner with reduced technical skills, but at the same time assures a high level of security.

6. REFERENCES

[1] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Inf.*, vol. 7, no. 3, 2016.

[2] F.-C. Argatu, V. Brezoianu, V. V. Argatu, B.-A. Enache, F.-C. Adochiei, and T. Icleanu, "Power Quality Analyzer for Smart Grid-Smart Home Applications," in *2019 54th International Universities Power Engineering Conference (UPEC)*, 2019, pp. 1–4.

[3] S. D. Grigorescu *et al.*, "Robotic Platform with Medical Applications in the Smart City Environment," in *2019 11th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 2019, pp. 1–6.

[4] C. Cepisca, F. C. Adochiei, S. Potlog, C. K. Banica, and G. C. Seritan, "Platform for bio-monitoring of vital parameters in critical infrastructures operation," in *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2015, p. E--7.

[5] T. Cazangiu, F.-C. Argatu, B.-A. Enache, V. Vita, and G. Stavros, "Device for monitoring people with Alzheimer's disease," in *2018 International Symposium on Fundamentals of Electrical Engineering, ISFEE 2018*, 2018.

[6] O. Drosu and M. Stanculescu, "Cardiac Stimulation Through Induced Currents," *Sci. Bull. Electr. Eng. Fac.*, vol. 17, no. 2, pp. 25–29, 2017.

[7] R.-I. Ciucu, D.-A. Dragomir, I.-R. Adochiei, G.-C. Seri\ctan, C. Cepi\csc\ua, and F.-C. Adochiei, "A non-contact heart-rate monitoring system for long-term assessments of HRV," in *2017 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 2017, pp. 5–8.

[8] O. E. Dragomir and F. Dragomir, "Development of User-friendly Tool for Energy Behavioral Change of Consumers," in *The Scientific Bulletin of Electrical Engineering Faculty*, 2016, no. 0, pp. 1–6.

[9] M. S. Hossain, M. Rahman, M. T. Sarker, M. E. Haque, and A. Jahid, "A smart IoT based system for monitoring and controlling the sub-station equipment," *Internet of Things*, vol. 7, p. 100085, 2019.

[10] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1–2, pp. 81–98, 2018.

[11] R. Ciucu *et al.*, "Innovative Devops for Artificial Intelligence," *Sci. Bull. Electr. Eng. Fac.*, vol. 19, no. 1, pp. 58–63, 2019.

[12] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy constrained IoT devices," *Mech. Syst. Signal Process.*, vol. 136, p. 106436, 2020.

[13] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks," *Appl. Soft Comput. J.*, vol. 71, pp. 66–77, 2018.

[14] H. Saputra and Z. Zhao, "Long term key management architecture for SCADA systems," *IEEE World Forum Internet Things, WF-IoT 2018 - Proc.*, vol. 2018-Janua, pp. 314–319, 2018.

[15] L. O. Aghenta and M. T. Iqbal, "Low-cost, open source IoT-based SCADA system design using thinger.IO and ESP32 thing," *Electron.*, vol. 8, no. 8, pp. 1–24, 2019.

[16] L. O. Aghenta and M. T. Iqbal, "Development of an IoT Based Open Source SCADA System for PV System Monitoring," *2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019*, pp. 1–4, 2019.

[17] P. Nguyen-Hoang and P. Vo-Tan, "Development an Open-Source Industrial IoT Gateway," *Proc. - 2019 19th Int. Symp. Commun. Inf. Technol. Isc. 2019*, pp. 201–204, 2019.

[18] A. Gavlas, J. Zwierzyna, and J. Koziorek, "Possibilities of transfer process data from PLC to Cloud platforms based on IoT," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 156–161, 2018.

[19] M. Hemmatpour, M. Ghazivakili, B. Montrucchio, and M. Rebaudengo, "DIIG: a distributed industrial IoT gateway," in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 2017, vol. 1, pp. 755–759.