Instituto Tecnológico y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación el 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

ESPECIALIDAD EN SISTEMAS EMBEBIDOS

SMART MODULAR HOME SYSTEM

Tesina para obtener el grado de:

ESPECIALISTA EN SISTEMAS EMBEBIDOS

Presentan: Carlos Roberto Mendoza Almanzar y David Díaz Marín

Director: Luis Rizo Domínguez

San Pedro Tlaquepaque, Jalisco. A 12 de julio de 2018

We would like to express our special appreciation and thanks to our advisor Professor Luis Garabito, who has been a tremendous mentor for us. We would like to thank him for encouraging our research and for allowing us to grow as engineers. His advice on both research as well as on our career have been invaluable.

We would also like to thank the CONACYT for such a great opportunity.

Abstract

A Smart Home incorporates advanced automation systems providing its home owners comfort, security, energy efficiency, and convenience at all times, regardless of whether anyone is at home. However, the use of smart technology and IoT is accompanied by high costs and lack of security. This project aims to propose a smart home system prototype named Smart Modular Home System (SMHS) that monitors IoT devices through a Wi-Fi network. The system is composed of a central device and different smart home modules synched using NFC technology. The central device and sensor controllers are based on the NXP Kinetis Cortex M0+/M4 and LPC Cortex M4 MCU families, the different modules are composed of the NXP sensors portfolio and the Wi-Fi communication is achieved using the ESP8266 controller. The smart home modules monitors door locks, lights, thermostats, and other artifacts within a limited network area with a highly customizable setup depending on the user's needs. The SMHS aims to provide security and home automation to any homeowner, being a low cost and a low power solution. Setting up the SMHS home will be intuitive, by choosing among the different modular devices available based on the necessities of the area.

Resumen

Una casa inteligente incorpora sistemas de automatización avanzados para los propietarios de una casa ofreciendo comodidad, seguridad, eficacia de energía y conveniencia en todo momento a pesar de que nadie se encuentre en casa. A pesar de eso, el uso de tecnologías inteligentes e internet de las cosas está acompañado de altos costos y ausencia de seguridad. Este proyecto tiene como propósito proponer un prototipo llamado Smart Modular Home System (SMHS), el cual monitorea dispositivos inteligentes por medio de una red Wi-Fi. El sistema está compuesto de un dispositivo central y diferentes módulos inteligentes los cuales son sincronizados por medio de la tecnología de NFC. El dispositivo central y los controladores de los sensores están basados en las familias de microcontroladores Kinetis Cortex M0+/M4 y LPC Cortex M4, los diferentes módulos están compuestos del portafolio de sensores de NXP y la comunicación Wi-Fi se logra utilizando el controlador ESP8266. Los módulos inteligentes monitorean puertas, focos, termostatos y otros dispositivos dentro de una red de área limitada con diversas opciones de configuración para cualquier usuario dentro de casa dependiendo de sus necesidades. El SMHS tiene como objetivo ofrecer seguridad y automatización para todos los usuarios dentro de sus casas a un bajo costo y bajo uso de energía. Configurar el SMHS será intuitivo, pudiendo seleccionar entre una gran variedad de módulos para las necesidades del hogar.

Content

Table of Figures

Introduction

Nowadays, there are plenty of smart home products available in the market, such as temperature sensors, motion detectors, garage door openers, lights, or cameras that monitor homes from any place with an internet connection. This “smart house” concept was first introduced in 1984 by the National Association of Home Builders (NAHB) [1]. The research and developments in this field have continued over the years giving place to the Internet of Things (IoT), a technology that allows exchanging and collecting data between different electronic devices using the internet.

In IoT, entities, objects, devices, machines, and sensors have to communicate with each other to exchange information based on communication networks; wireless sensors are one of the key devices used in IoT networks. To date, IoT plays an important role in daily activities and it is becoming a growing topic among smart applications. An example of an IoT application could be an alarm clock that is set at 6 a.m. and then notifies the coffee maker to start brewing coffee.

There are key benefits and potential applications of such technology, like managing all of your home devices from one place, maximizing home security, remote control of home functions, and increased energy efficiency, among others. However, the amount of data going through these networks contains private information that must be protected.

The proposed Smart Modular Home System (SMHS) is a prototype that monitors IoT devices through a WiFi network. The SMHS is composed of a central device, which is the brain of the system, and different smart home modules which refers to the IoT devices. It is capable of monitoring door locks, lights, thermostats, and other artifacts within a limited network area with a highly customizable setup depending on the user's needs. The different modules within the network can be monitored and controlled using a graphical user interface (GUI), showing notifications, events, or charts. The integration process of the modules to the network is simple, it is implemented using the Near Field Communication (NFC) technology, so a single tap of the central device with the IoT modules is enough to synchronize these devices and start monitoring.

The objective of the study is to create a prototype of the SMHS capable of providing security and home automation to any homeowner, as a low cost and a low power solution. Setting up the SMHS home will be intuitive, by choosing among the different modular devices available based on the necessities of the area.

1. Background

In recent years, there has been an increasing amount of research in the area of home security and protection around the world. For instance, Silviu Folea et al, propose a solution to transform a normal house into a smart house while reducing the energy consumption. This implementation uses low power sensors specialized in measuring temperature, humidity, pressure, light, noise, and dust, among others [2]; however, the use of IoT to monitor the system was no contemplated.

Another important feature of a smart system is its usability, as demonstrated by Irina-Ioana Pătru et al, with a solution for connecting devices in a single application. The use of intelligent devices for home automation improved the interaction between people and their daily home activities [3]. This is the case of the SMHS, which establishes an easy interaction between devices in an intuitive way for the users by using a graphical user interface.

The synchronization between the IoT modules with the SMHS central device is accomplished by using NFC technology. As reported by Ahmad Rabie and Uwe Handmann, with their NFC-based assisting system for controlling home activities and the adaption of home-human interface towards the needs of the user, it was demonstrated that this technology in smart systems can serve as an interface between users and home environments [4].

Previous studies have also focused in the area of home security and protection. Danish Chowdhry et al, described a smart home automation system for intrusion detection implementing a vision-based home automation systems (HAS) that integrates a web server in order to remotely access and control the status, by focusing on the vision-based system for accurate human detection [5]. However, it does not mention the use of IoT for remote monitoring. With the SMHS we propose a system that can be used to improve the security of a house by using simple and low cost IoT devices that can be more accessible than a vision-based system.

2. Theoretical Framework

2.1. Smart House

Smart house technology, also known as home automation, provides homeowners security, comfort, convenience, and energy efficiency by allowing the control of smart devices, often by a smart home app on their smartphone or another network device, this is represented in Figure 2-1. The Internet of things (IoT), smart home systems, and smart devices often operate together, sharing consumer usage data among themselves and automating actions based on the homeowners' preferences.

Fig. 2-1. Smart Home Network Representation.

Early home automation began with labor-saving machines. Self-contained electric or gas-powered home appliances became viable in the 1900s with the introduction of electric power distribution and this led to the introduction of washing machines (1904), water heaters (1889), refrigerators, sewing machines, dishwashers, and dryers.

In 1975, the first general purpose home automation network technology, X10, was developed. It is a communication protocol for electronic devices. It primarily uses electric power transmission wiring for signaling and control, where the signals involve brief radio frequency bursts of digital data, and remains the most widely available to date. By 1978, X10 products included a 16-channel command console, a lamp module, and an appliance module. Soon after came the wall switch module and the first X10 timer. By 2012, in the United States, according to ABI Research, 1.5 million home automation systems were installed. [6]

2.2. Internet of Things

The Internet of Things (IoT) drives innovation to make products and devices smarter. These smart things range from smart devices and smart appliances to industrial equipment and network infrastructure. Their target is to help people with their daily activities, making them easier, reliable, and safer. As more of these devices are created, improvements require a higher performance, advanced security, and power-efficiency.

Moreover, reliable, secure and fast connections are essential to achieve the complete capacity of IoT and it depends on the connections between each of the devices in the network, including the gateways and the cloud, this is represented in Figure 2-2. As more IoT devices are used and interconnected, integrated security solutions with the latest techniques are critical for preventing attacks and protecting private user information.

Fig. 2-2. Internet of Things Network.

2.3. Near Field Communication

The Near Field Communication technology (NFC) is a short-range wireless connectivity protocol standard. It was designed to establish an intuitive and simple communication between two electronic devices. Some of the key features of this technology [7] are mentioned below:

- Contactless proximity technology.
- Operating frequency of 13.56 MHz.
- Operating range is 10 cm.
- Can reach a maximum speed of 424 Kbps.
- Standardized in ISO/IEC (Technical Committee of the International Organization for Standardization and the International Electro Technical Commission), ECMA (Standardization, Information and Communication Technology, Consumer Electronics, Industry association.) and ETSI (European Telecommunications Standards Institute).
- Compatible with existing ISO/IEC 14443 (Identification cards, Contactless integrated circuit cards, Proximity cards international standard) and FeliCa contactless cards & reader infrastructure.
- Read/Write, Card Emulation and Peer-to-Peer modes can be implemented in one device.
- Fast, seamless pairing with Bluetooth, WiFi.
- Has the NFC Forum as a key standardization & interoperability group.

An example of the use of Near Field Communication technology is shown in Figure 2-3 in which NFC is used to pair two Bluetooth devices.

Fig. 2-3. Bluetooth Pairing with Near Field Communication.

2.4. 802.11 Communication

The Wi-Fi technology is a communication protocol based on the IEEE 802.11 standard, which is a set of media access control (MAC) and the physical layer (PHY) specifications for implementing wireless local area network (WLAN) communications. Wi-Fi works in five different frequency ranges: 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz bands that are divided into multiple channels. This wireless technology is widely used in most home and office networks to allow computers, printers, and smartphones to talk to each other and access the Internet wirelessly.

The base version of the IEEE 802.11 standard was released in 1997, and there have been additional revisions to the standard. The standard and its revisions provide the basis for wireless network products using the Wi-Fi brand so these products need to be certified in order to use the Wi-Fi brand [8].

2.5. Sensors

Sensors are devices capable of detecting movement, pressure, temperature, or even magnetic fields. Detailed information and potential applications or the sensors for the SMHS are shown below:

2.5.1 Accelerometer

An accelerometer is an electromechanical device that will measure acceleration forces. The ´g´ is referred to as the acceleration of gravity and its value is 9.8 m/s2 on Earth. By measuring the amount of static acceleration due to gravity, the angle in which the device is tilted with respect to the earth can be calculated. By sensing the amount of dynamic acceleration, the axis in which the device is moving can be analyzed.

Every acceleration range has different applications. Understanding the range of acceleration for an application enables the design of the product with the optimal accelerometer. For example, some applications start at 1.5g, as in free fall, all the way up to 40g applications for crash detection. In the case of the SMHS, the accelerometer devices can be used for door/window movement detection, free fall detection of different objects, and as an inclinometer, among others.

2.5.2 Magnetometer

A magnetometer is a device that measures the strength and direction of a magnetic field. Magnetometers are widely used for measuring the Earth's magnetic field and in geophysical surveys to detect magnetic anomalies of various types. They are also used in the military to detect submarines. One of the main applications of such devices is metal detection.

The magnetometer might be used as a vehicle detector to determine if a car is parked in the drive way or garage, or as a door/window sensor to detect if these are open or closed inside a smart house.

2.5.3 Temperature sensor

A temperature sensor is a device that detects and measures hotness and coolness and converts it into an electrical signal. These devices play an important role in many applications. For example, maintaining a specific temperature is essential for a refrigerator as the food must be in good condition. Besides, the temperature sensor can be used to control the temperature of the rooms in the smart house and a temperature detection circuit can be used as a fire detector.

2.6. Real-Time System

A real-time system depends on logical precision and looks for met the deadlines for the application it was developed. The principal duty of these systems is to produce correct results while meeting predefined requirement. Real-time systems can be defined as those applications respond to external events in a timely manner.

2.6.1 Hard real-time system

A hard real-time system is a system that must meet its deadlines with a limited degree of flexibility. The deadlines must be met, or serious affectations to the system may occur.

2.6.2 Soft real-time system

A soft real-time system is a system that must meet its deadlines but with a non-critical degree of flexibility. The deadlines can contain varying levels of tolerance and even statistical distribution of response times with different degrees of acceptability. In a soft real-time system, a missed deadline does cause system failure.

2.6.3 Response Time

It is the demanding response time requirements of hard real-time applications (often in the order of milliseconds or less) make impossible direct human intervention during normal operation or in critical situations.

2.6.4 FreeRTOS

The FreeRTOS software is a real-time operating system (RTOS), and the common standard solution for microcontrollers and small microprocessors applications.

Some of the FreeRTOS features are that it provides a single and independent solution for many different architectures and development tools, it is reliable, comes with many features and still undergoing continuous active development, and it has a minimal ROM, RAM and processing overhead. The typical RTOS kernel binary image will be in the region of 6K to 12K bytes.

2.7. NXP Freedom Development Boards

The NXP Freedom Development Boards are an ultra-low-cost development platform for Kinetis MCUs built on Arm Cortex processors. It features include easy access to MCU I/O, battery-ready, low-power operation, a standards-based form factor with expansion board options and a built-in debug interface for flash programming and run-control. [7]

2.8. Integrated Development Environment

The Integrated development environment (IDE) is a software application that allows users to develop and test software. Typically, an IDE contains a code editor, a compiler, and a debugger that the developer accesses through a single graphical user interface (GUI). An IDE may be a standalone application, or it may be included as part of one or more existing and compatible applications.

2.9. Graphic User Interface

The Graphical User Interface (GUI) allows the use of icons or other visual indicators to interact with electronic devices, rather than using only text via the command line. For example, all versions of Microsoft Windows utilize a GUI.

3. Methodology

This chapter describes the application methodology used to obtain the information from the different modules, software used, hardware involved, communication protocols, data analysis techniques and implementation of the complete system.

3.1. Software

3.1.1 MCUXpresso IDE

The IDE used for the software development is the MCUXpresso from NXP. This IDE offers advanced editing, compiling, and debugging features with the addition of MCU-specific debugging views, code trace and profiling, multicore debugging, and integrated configuration tools.

3.1.2 MCUXpresso SDK

The project is composed of a set of software development tools that allow the creation of the application for the devices used. In this case, the software development kit (SDK or devkit) used is the MCUXpresso SDK 2.4 and the LPCXpresso54628. The MCUXpresso SDK is a comprehensive software enablement package designed to simplify and accelerate the application development with NXP's LPC and Kinetis families of MCUs.

3.1.3 PN7150 Drivers

The NXP-NCI example for PN71xx NFC Controller source code in the form of MCUXpresso Projects will be used. These drivers are needed to support the host communication and the PN7150 evaluation board detection from Windows. For the thesis purpose, these example was migrated to the LPC54608 EVB.

3.1.4 emWin

The adaptability of the software makes it suitable for all kind of applications; it can be used in battery-powered single chip products with basic graphic needs to high-end embedded systems demanding high performance and sophisticated animations. Moreover, emWin is commonly used in many different target markets, such as industrial controls, Internet of Things, networking, consumer electronics, safety critical devices, automotive, medical devices, and avionics, making it a popular solution in the embedded industry. An example of a graphical user interface created using emWin is shown in Figure 3-1.

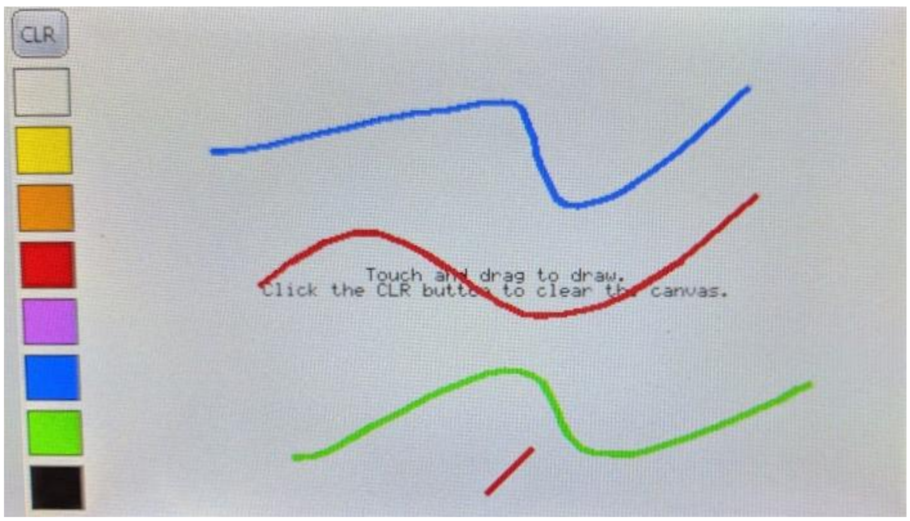

Fig. 3-1. emWin GUI Example.

3.2. Hardware

The project is composed of different evaluation boards provided by NXP. These are described below.

3.2.1 The LPCXpresso54628 Development Board

This board is comprised of a target LPC54608 device with an onboard, and J-Link compatible debug probe. The onboard probe is compatible with MCUXpresso IDE and other leading toolchains. The board is also equipped with a standard 10-pin header enabling the use of 3rd party to debug probes. In addition to standard LPCXpresso V3 features, this board includes a complete set of peripheral interfaces to enable developers to fully explore the capabilities of LPC546xx devices.

The LPCXpresso54608 (Figure 3-2) has a LCD with capacitive touch screen, which is used to display all the information related to the project.

Fig. 3-2. LPCXpresso54608 Evaluation Board.

3.2.2 PN7150 High performance NFC controller

The PN7120 (Figure 3-3) is a plug and play full NFC solution for easy integration into any Operating System environment like Linux and Android, reducing Bill of Material (BOM) size and cost. The embedded microcontroller core is loaded with the integrated firmware, simplifying the implementation as all the NFC real-time constraints, protocols, and the device discovery (polling loop), are processed internally.

These controllers are ideal for home-automation applications, such as gateways, and they work seamlessly with NFC connected tags.

Fig. 3-3. PN7120 NFC Evaluation Board

3.2.3 FRDM-KL25Z

The Freedom KL25Z is an ultra-low-cost development platform for Kinetis L Series KL1x (KL14/15) and KL2x (KL24/25) MCUs built on an Arm Cortex-M0+ processor. It features include easy access to MCU I/O, battery-ready, low-power operation, a standards-based form factor with expansion board options and a built-in debug interface for flash programming and run-control.

In this case, the FRDM-KL25Z (Figure 3-4) has in-built MMA8451Q accelerometer, which is used for the movement data detection.

Fig. 3-4. FRDM-KL25Z Evaluation Board.

3.2.4 FRDM-K64F-AGM04

This Sensor Toolbox provides a wide variety of sensor boards with compatible software tools for NXP's 9-axis solution shown in Figure 3-5 (MMA8652FC accelerometer + MAG3110 magnetometer + FXAS21002C Gyroscope). The Freedom-K64F is an ultra-low-cost development platform for Kinetis® K64, K63, and K24 MCUs.

The sensors mentioned above are used to detect the magnetic field and the acceleration data in the project, while the Freedom-K64F (Figure 3-6) computes all the information obtained.

Fig. 3-5. FRDM-K64F-AGM04 Evaluation Board.

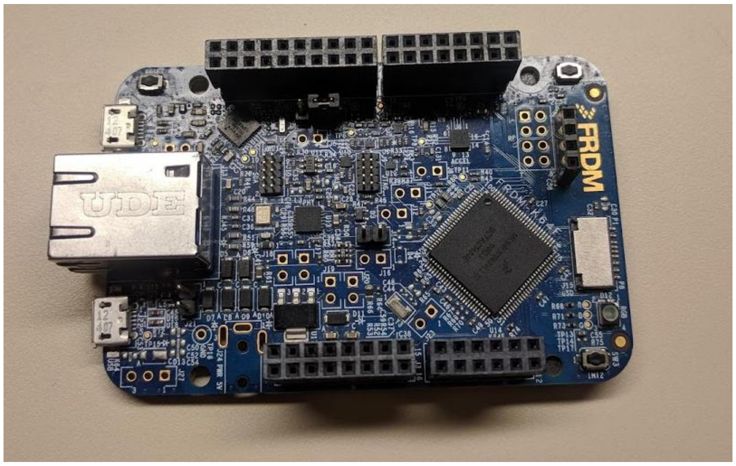

Fig. 3-6. FRDM-K64F Evaluation Board.

3.2.5 NTAG

The NTAG (Figure 3-7) is a standard NFC tag IC used in mass market applications. It is used in combination with NFC devices or NFC-compliant Proximity Coupling Devices.

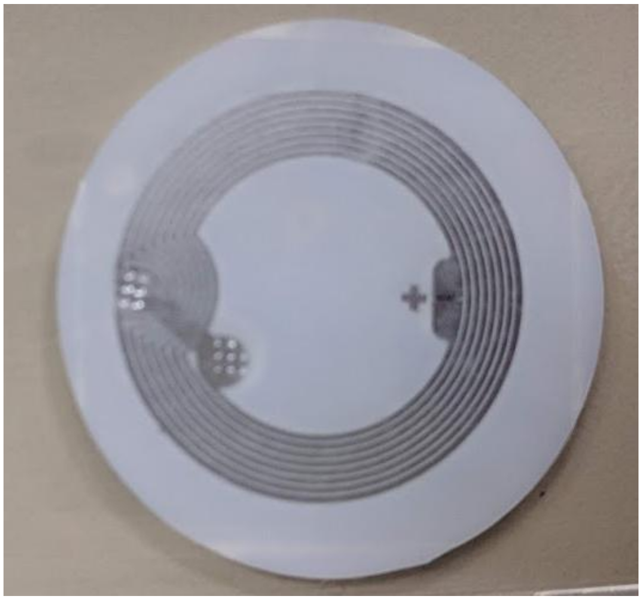

Fig. 3-7. NFC Tag.

3.2.6 ESP8266

To be able to communicate wirelessly the ESP8266 board will be used, it is a low-cost Wi-Fi controller with full TCP/IP stack and microcontroller capability produced by Espressif Systems.

4. Implementation

As mentioned in the introduction, the SMHS is a prototype that monitors IoT devices through a WiFi network. The LPCXpresso54628 Development Board is the central device of the system. It creates the WiFi network to send and receive all the information related to the house monitoring. Besides, it has the responsibility to enable the LCD display using the emWin software. The different modules within the network can be monitored and controlled using a graphical user interface (GUI), showing notifications, events, or charts.

The system is capable of monitoring door locks, lights, thermostats, and other artifacts with the help of the different sensors. The FRDM-K64F-AGM04 and the FRDM-KL25Z are used as the interface between the in-board sensors and MCU to detect the different signals, compute them and send them over the network to the central device.

The integration process of the modules to the network was implemented using the NFC technology, so a single tap of the central device with the IoT modules is enough to synchronize these devices and start monitoring.

4.1. Architecture

The architecture of the system is shown below:

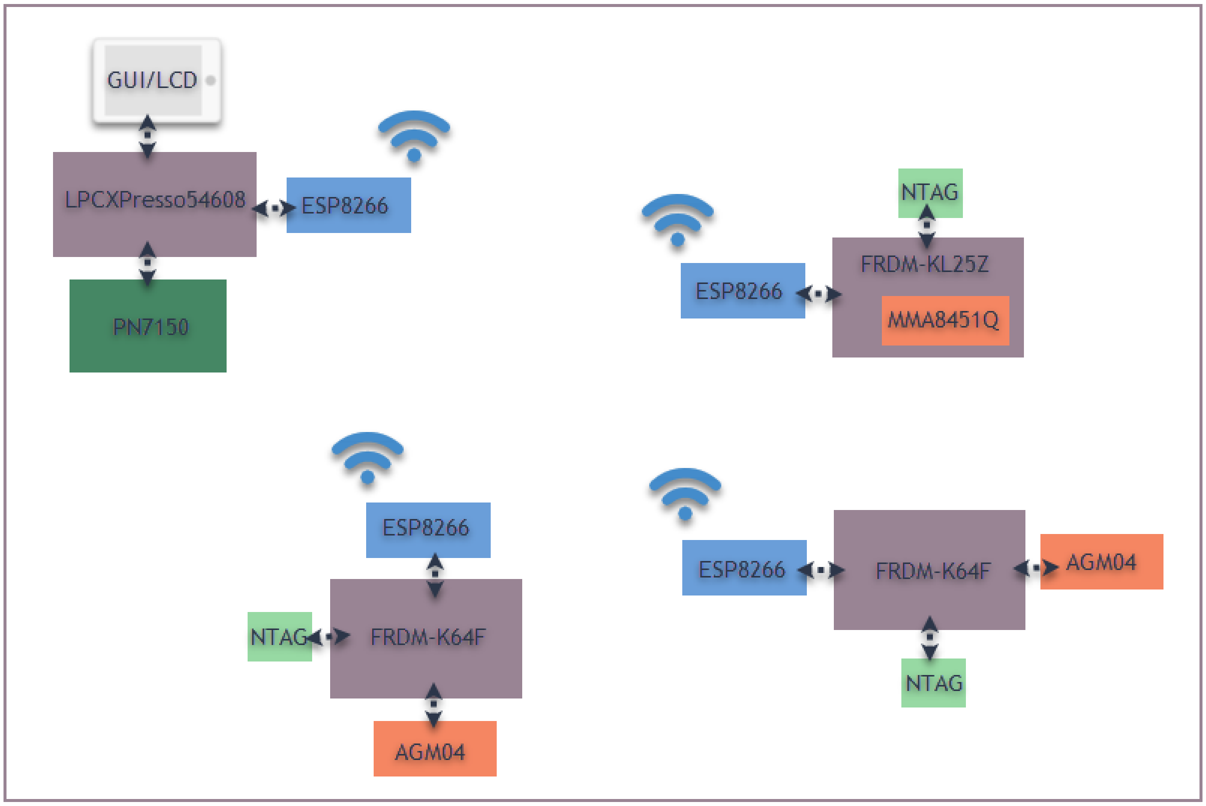

Figure 4-1. SMHS Architecture

5. Results

The results from the different modules and the central device are shown below.

5.1. Accelerometer response

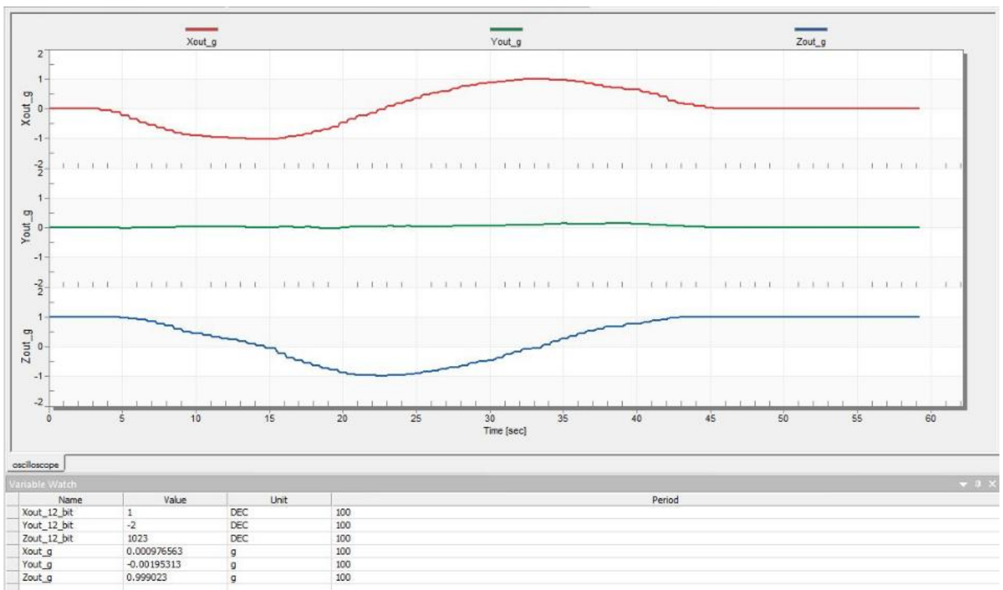

Fig. 5-1. Accelerometer response.

5.2. Magnetometer response

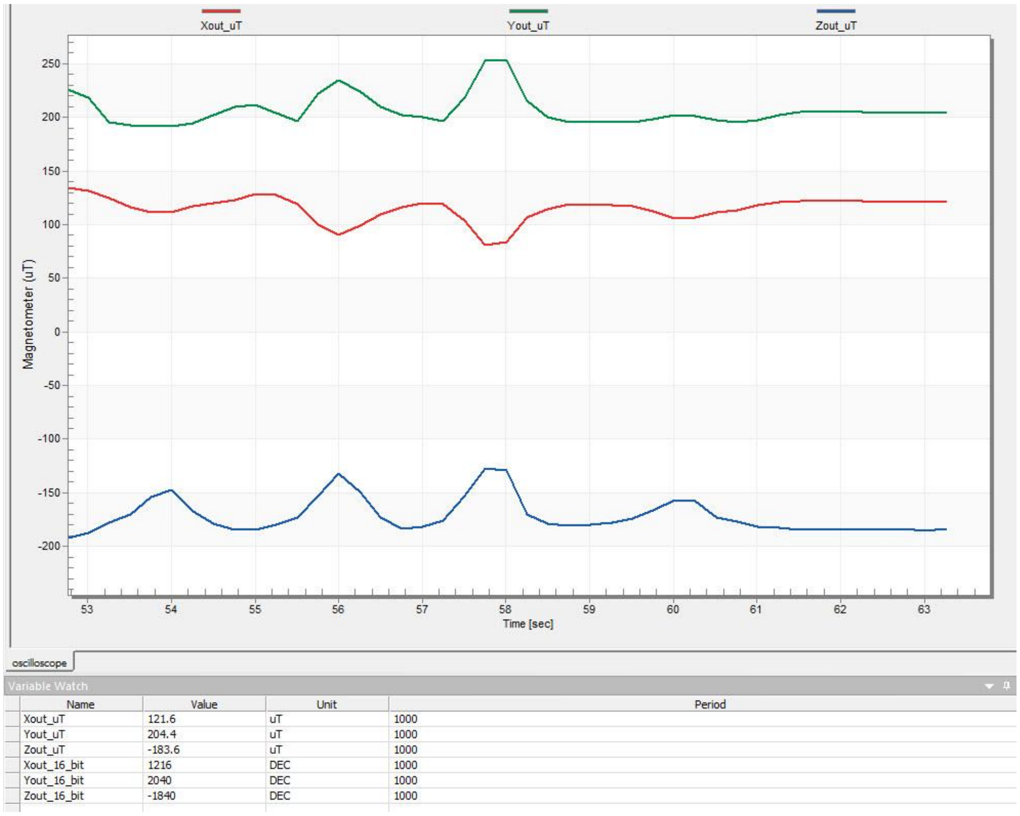

Fig. 5-2. Magnetometer response.

5.3. MCUXpresso IDE Workspace

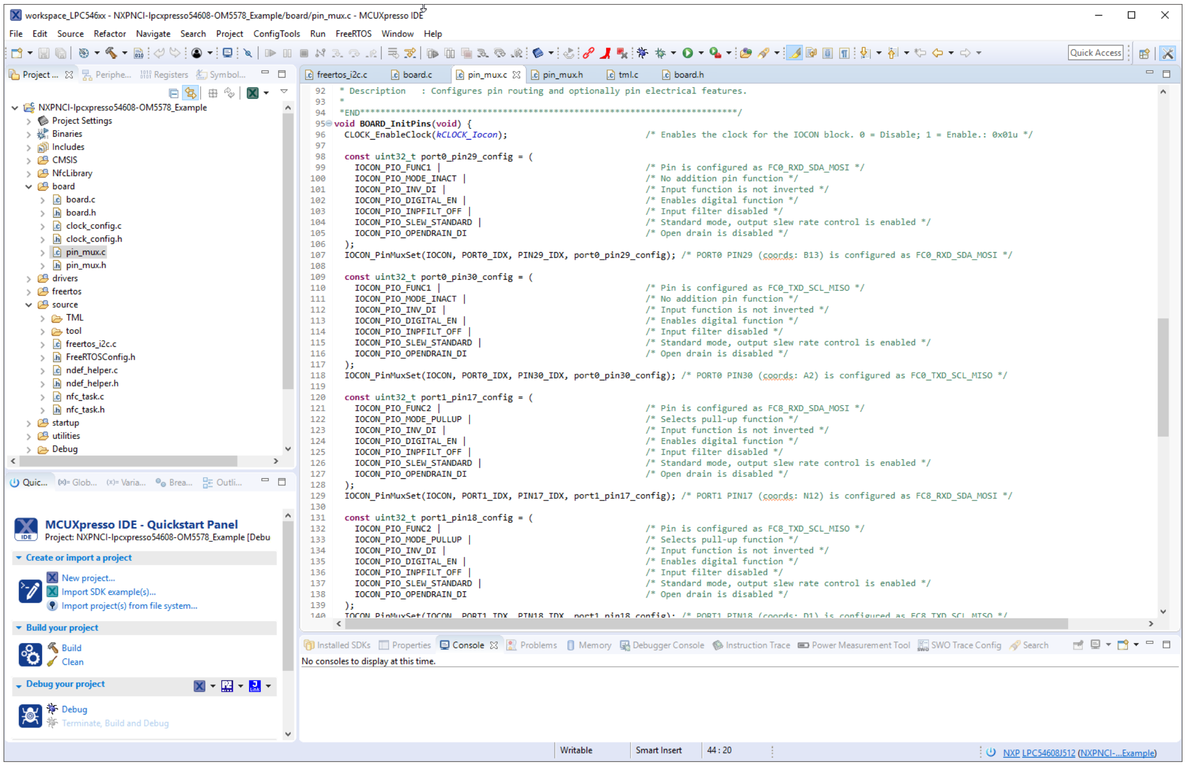

Fig. 5-3. MCUXpresso IDE Workspace.

Conclusion

The SMHS project has proposed the idea of smart homes that can support a lot of home automation systems, offering a great solution for the all the home owners interested in security and communication for a low cost and low energy consumption. The integration of the different modules with the central device succeeded. It was created a local network with a potential for using a wide variety of devices in the future. Also, the synchronization between devices with the central unit was demonstrated using different communication protocols such as NFC and Wi-Fi. Therefore, the SMHS is an intuitive system capable of creating convenience and security for all the users.

References

[1] Erec, “Home automation systems,” *Reporter*, vol. 19, Feb. 2002.
[2] S. Folea, D. Bordencea, C. Hotea, and H. Valean, “Smart home automation system using Wi-Fi low power devices,” pp. 569–574, May 2012.
[3] I.-I. Patru, M. Carabas, M. Barbulescu, and L. Gheorghe, “Smart home IoT system,” pp. 1–6, Sep. 2016.
[4] A. Rabie and U. Handmann, “NFC-based person-specific assisting system in home environment,” pp. 5404–5409, Jun. 2014.
[5] D. Chowdhry, R. Paranjape, and P. Laforge, “Smart home automation system for intrusion detection,” pp. 75–78, Jul. 2015.
[6] ABI research, “1.5 Million Home Automation Systems Installed in the US This Year,” Nov. 2012.
[7] NFC Forum, “NFC Forum Technical Specifications.” 09-Jul-2018.
[8] IEEE Computer Society, LAN/MAN Standards Committee, Institute of Electrical and Electronics Engineers, and IEEE-SA Standards Board, *IEEE standard for information technology: telecommunications and information exchange between systems : local and metropolitan area network-- specific requirements. Part 11, Amendment 4, Part 11, Amendment 4,*. 2013.