CAPSTONE PROJECT CENG355

Humber College Institute of Technology & Advanced Learning

MAIDS HOME/BUSINESS INTRUSION DETECTION SYSTEM REPORT

Submitted by: Claudio, Meis - Integration

Discipline: Computer Engineering Technology

Date Submitted: March 12, 2020

9.0 Integration

Electronics integration is the art of merging audio, video, and control systems into one seamless network of interrelated devices. MAIDS' technologies allow for dramatic possibilities with ease-of-use interfaces, bringing different platforms under the user's control, all with a single display and control interface. MAIDS provides easy-to-use integration solution allowing it to optimize the functionality and impact of the systems and providing the best outcome and value.

The MAIDS' system integrates all of the hardware (electronic components) and software (python code, Android application and web services) into a functional system that is easy for anyone to use. On the one hand, the integration of hardware components include:

a. LED sensor
b. Motion sensor
c. Sound sensors
d. USB camera
e. Custom PCB board
f. Raspberry Pi 4 platform.

On the other hand, the software components include:

a. Android phone application
b. Web services (Twilio, email and PushNote).

The system was customized to work with the required electronics (Raspberry Pi 4 embedded system and custom-made PCB board) and software, and designed from scratch. In addition, the MAIDS Home and Remote integration system gives the user the ability to control the system remotely from their smart phone or tablet.

9.1 Data Sent by Hardware: Motion/ Sound Sensors and Processor

A sensor is a device which produces an output by detecting the changes in quantities or events. Generally, sensors produce an electrical signal or optical output signal due to a physical change in some characteristic that changes in response to some excitation. **Digital Sensors** produce a discrete digital output signal or voltage that are a digital representation of the quantity being measured. Digital sensors produce a binary output signal in the form of a logic "1" or a logic "0", ("ON" or "OFF") and are typically linked to a control program that specifies acceptable levels. This means then that a digital signal only produces discrete (non-continuous) values which may be outputted as a single "bit", (serial transmission).

There are two different types of digital sensors in the MAIDS device: a sound sensor and a motion sensor. Both produce a corresponding digital signal due to changes in quantities or events. The control program decides what to do next based on the data it is fed by the sensors.

On the one hand, the sound sensor produces a HIGH (1) output through its digital output pin when a change is sound levels is detected. The digital signal is then carried by the connecting wire to the input pin of the custom-made PCB board which transfers the signal to the GPIO pin 11 of the Raspberry Pi 4 for processing.

On the other hand, the motion sensor produces a HIGH (1) output through its digital output pin when a change is radiation levels are detected. The digital signal is then carried by the connecting wire to the input pin of the custom-made PCB board which transfers the signal to the GPIO pin 13 of the Raspberry Pi 4 for processing.

For its part, the Central Processing Unit (CPU) is the part of a computer system that is commonly referred to as the "brains" of a computer. The CPU is responsible for executing a sequence of stored instructions (program). This program will take inputs from an input device (motion/sound sensors), process the input in some way and output the results to an output device (i.e. LED module, web services, etc.).

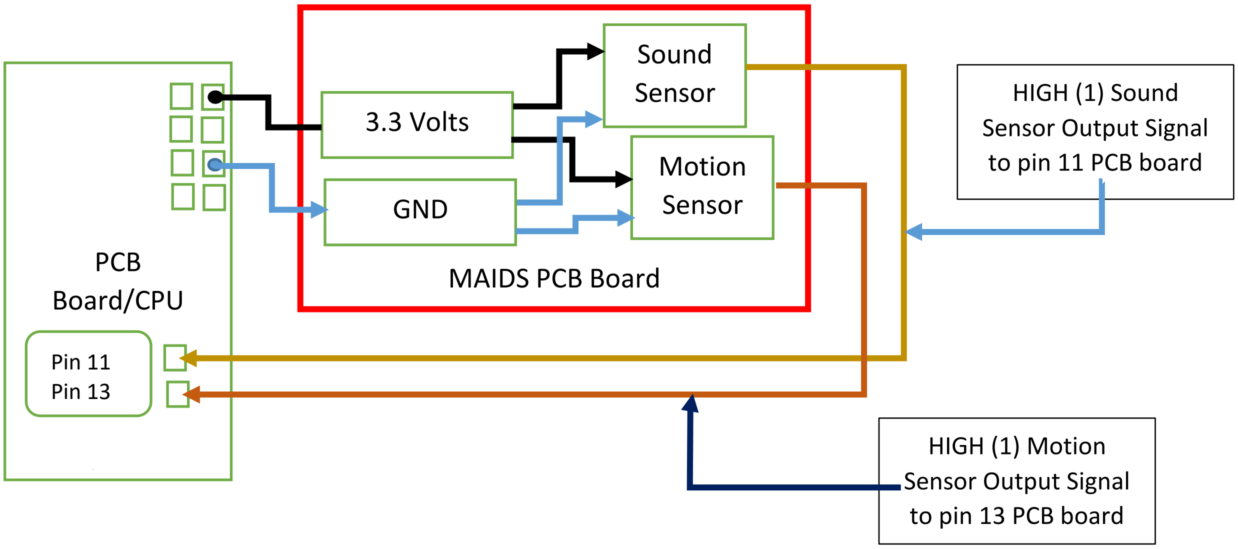

Sound Sensor
3.3 Volts
Motion Sensor
GND
MAIDS PCB Board
PCB Board/CPU
Pin 11
Pin 13
HIGH (1) Sound Sensor Output Signal to pin 11 PCB board
HIGH (1) Motion Sensor Output Signal to pin 13 PCB board

Figure 1: Data Inputs from Motion and Sound Sensors to the Raspberry Pi 4.

9.2 Data Retrieved By Mobile Application

The Android application is composed of two activities: login activity and Data/Control activity. One of the main functions of the data and control activity is to retrieve data from the remotely located MAIDS device. In particular, the Android application will retrieve intrusion data (i.e. time of intrusion, intrusion location, contact information, etc.) from the MySQL database located on the MAIDS device (database server) and a picture file (the visual record of the intrusion). By clicking on the “Retrieve Database Info” button, the Android application, through the wireless Internet, connects to the MAIDS device, locates and extracts from the database the information required, and then, transmits the information back to the Android application and displays it on the screen via a WebView element. Similarly, clicking on the “Retrieve Intrusion Photo”, the Android application connects to the MAIDS device, locates the directory where the intrusion picture is located, and then transmits the picture back to the Android phone or tablet to be displayed on the screen via an ImageView element.

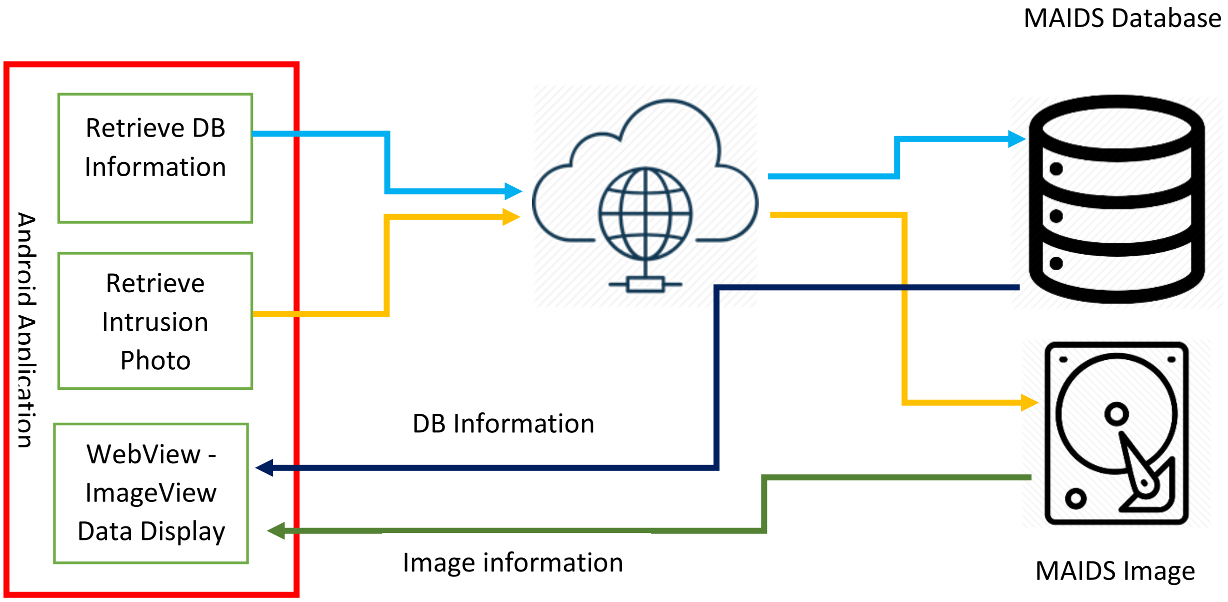


Figure 2: Data retrieved by mobile application through data activity on Android device.

9.3 Action Initiated By Mobile Application

The second Android application activity is the Control activity. The three main functions initiated by the mobile application through the control activity are as follows:

1. Activate MAIDS device (Turn it ON)
2. Deactivate MAIDS device (Turn it OFF)
3. Test LED module

By clicking the “Activate MAIDS” button, the Android application, through the wireless Internet, connects to the MAIDS device, and then executes the Python3 program named maids_final_python_code_22102019_backup1.py. The program then proceeds to execute the code that initiates the monitoring capabilities of the MAIDS device.

Similarly, by clicking the “Deactivate MAIDS” button, the Android application, through the wireless Internet, connects to the MAIDS device, and then executes the Python3 program named MAIDSOFF.py. The program then proceeds to execute the code that terminates the monitoring capabilities of the MAIDS device.

In addition, by clicking the “Test LED Module” button, the Android application, through the wireless Internet, connects to the MAIDS device, and then executes the Python3 program named TestLEDS.py. The program then proceeds to execute the code that sequentially turns the green and red LEDs thereby testing the functionality of the LED module of the MAIDS device.

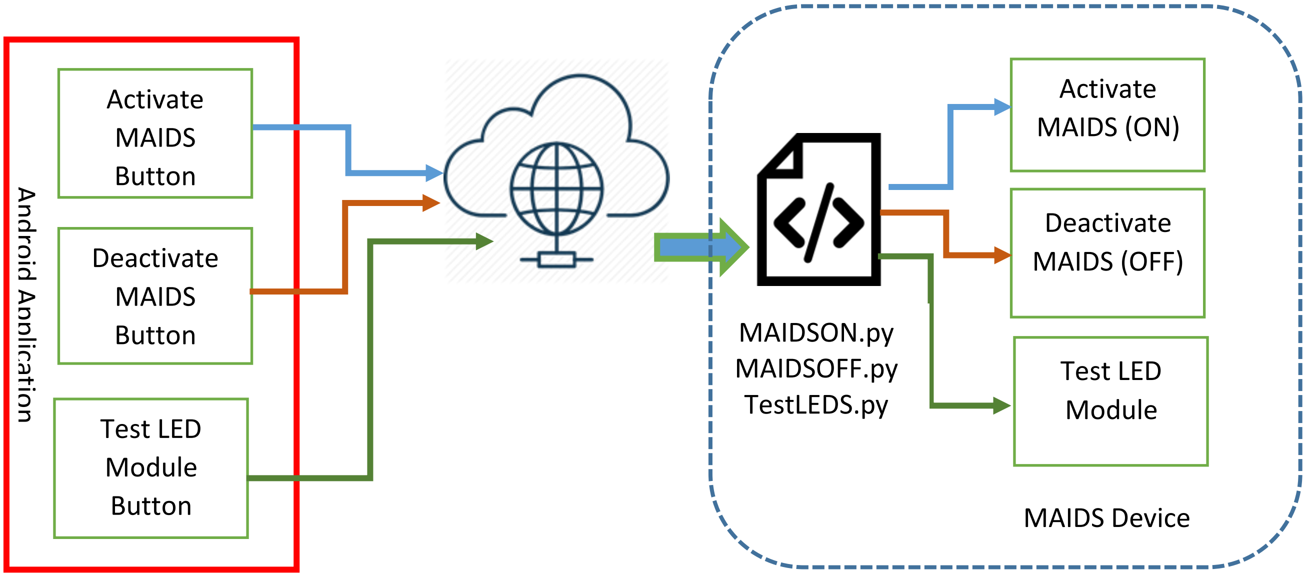


Figure 3: Actions initiated by mobile application on MAIDS device.

9.4 Action Received By Hardware

From the data and control activity there are several actions received by the MAIDS device. These are:

1. LED Module Functionality Test: The test is carried out when the MAIDS device receives via the internet the command to execute the TestLEDS.py program located in the /home/cmeis/maids1 directory.
2. LED Module Visual Display of Intrusion: If motion or sound is detected by the motion (PIR) or sound sensors on the MAIDS PCB board, they will generate an input signal. The motion/sound input signal travels through the connecting wires to the GPIO pins to the Raspberry Pi 4 Model B and the firmware processes the input signal on the particular input GPIO pin and executes the following functions (intruderwarning(), notify() and siren()) which in turn play an audible warning of the intrusion, runs the notification protocol (email with picture, push notification, phone call and SMS message), and finally plays a loud siren sound. The code for the actions mentioned is found in the function code of the maids_final_python_code_22102019_backup1.py program.
3. Activation of MAIDS device The MAIDS device executes the commands found in the maids function maids_final_python_code_22102019_backup1.py program. Its sole purpose is to run the executable code that sets up and initiates the monitoring capabilities of the MAIDS device.
4. Deactivation of MAIDS device: The MAIDS device executes the commands found in the program MAIDSOFF.py program found in the /home/cmeis/maids1 directory. Its sole purpose is to run its executable code which deactivates the MAIDS device.

5. Snap Intrusion Photo by Webcam: If motion or sound is detected by the motion (PIR) or sound sensors on the MAIDS PCB board, they will generate an input signal. The motion/sound input signal travels through the connecting wires to the GPIO pins to the Raspberry Pi 4 Model B and the firmware processes the input signal on the particular input GPIO pin and executes send_mail() function. The function executes the fswebcam application and sets the intrusion picture parameters as follows: resolution at 1280x720 pixels, a picture title ('MAIDS INTRUSION ALERT'), an intrusion subtitle ('1234 BROOK ROAD, ETOBICOKE, ON.'), a timestamp for the intrusion ('%Y-%m-%d %H:%M (%Z)'), information on the place of intrusion (‘LIVING ROOM ENTRY'), and the directory where the intrusion picture is to be saved along with its name (“/home/pi/webcam/image.jpg").
6. Add/Retrieve data to/from MAIDS Database: When the motion and sound sensors are triggered a signal is produced that executes the appendtodb() function of the maids_final_python_code_22102019_backup1.py program. The device then executes its code whose sole purpose is to add the following information to the MySQL database on the MAIDS device:
    a. Intrusion address
    b. Intrusion location (Room)
    c. Intrusion date
    d. Reporting Person
    e. Contact Phone Number
    f. Contact Email

7. Initiate REST Services: The hardware initiates the Representational State Transfer (REST) services which relies on a stateless, client-server, cacheable communications protocol when detecting an intrusion. Upon triggering of the sound or motion sensors a signal is produced that engages the following three functions in the maids_final_python_code_22102019_backup1.py program:
   a. send_androidpush(): The function calls executes the code for the pushover service using a token ID and user ID. The push notification produces includes information about the intrusion and is sent to the telephone number provided when registering to the service.
   b. sendsms(): Using the Twilio rest service with its own account ID and authorization token, the service sends an SMS message to the telephone number provided when registering to the service.
   c. callphone(): Using the Twilio rest service with its own account ID and authorization token, the service calls the telephone number provided when registering to the service and relays an intrusion message to the user.

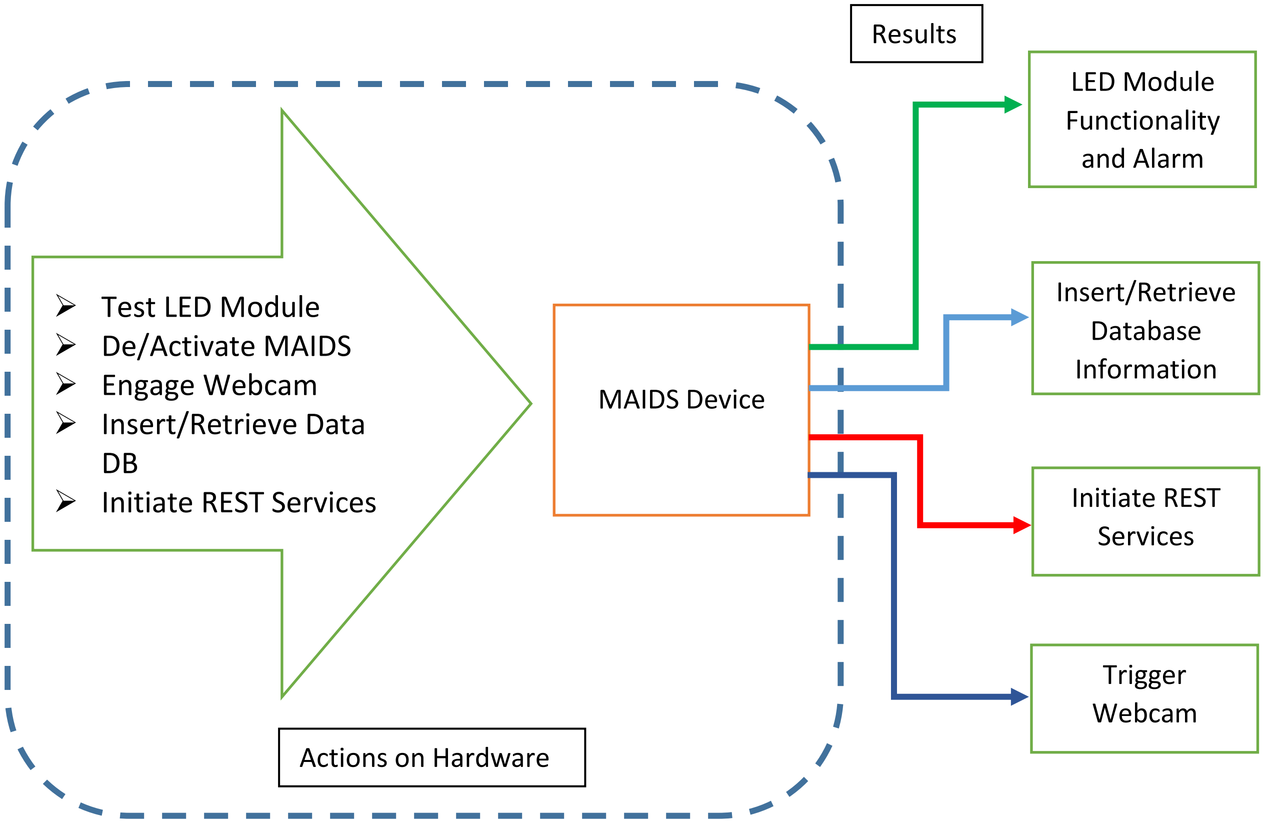


Figure 4: Actions received by MAIDS hardware

9.5 Integration Final Status Report

Prepared by Claudio F. Meis, March 2, 2020.

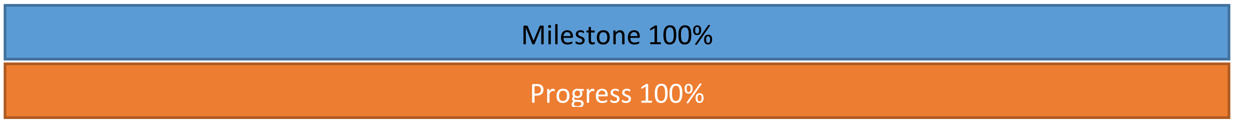
The presentation of the MAIDS project at the Capstone Project EXPO at 1:00 – 4:00 p.m. on Thursday, April 9, 2020, is still on track.

The following work has been completed on the MAIDS PCB board:

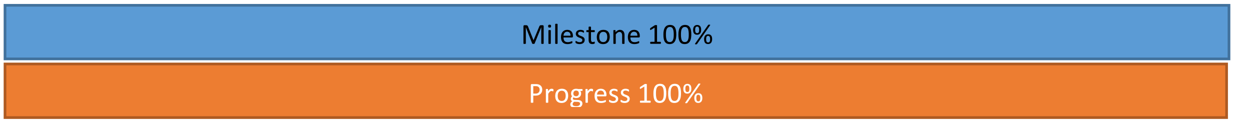
- Hardware Integration.
- Software Integration.

Progress against Milestones

Hardware Integration



Software Integration



Key Issues

No issues need to be resolved to meet Capstone Project EXPO deadline.

Action Steps

None.