Secured-E-Key
Senior Design 1
Group 11
30 April 2015

Sheldon Johnson
Enjolie Morales
Saint-Surin Paul
Shawn Gangasingh

Table of Contents

Table of Tables

Table of Figures

1.0 EXECUTIVE SUMMARY

The cutting-edge electrical engineering skills frequently change almost instantaneously from year to year as corporations in the electronics industry continue outcompeting one another on a global scale. Our project is intended to allow senior level electrical engineering students to respond to such a sporadic cycle by developing a project which allows for each of use to gain a skill or set of skills attractive to employers and that coincide with our current point in time. Secured-E-Key serves as the perfect solution to achieve our project's intent since it involves several different layers of electrical engineering including long range wireless communication, PCB development, single source multi-level power design, and development board software coding for performance optimization. Each layer distinctively varies from one another and provides one or more set of skills each of our group members can gain experience in. Secured-E-Key will enable the user to communicate with the device from any given distance and with any smartphone solely specific to the user. It will have a sufficient amount of electrical power allocated to the entire system via a set of batteries to avoid being plugged into a wall socket and to entirely separate itself from the electrical grid. A system of LEDs will display the energy status of the power source at periodic points in time to give an advanced indication as to when the batteries need replaced. The whole system will only remain active during the periods of when coded instructions execute a designated task to avoid additional needless power consumption. Video imaging data will record and stream directly to the user's smartphone as soon as a person has entered the operating vicinity of the device. Having the option to lock or unlock Secured-E-Key wirelessly via a smartphone will enable the user to decide who does and does not have a welcoming invitation to their home. Radio-frequency identification technology will put to rest the practice of requiring key ownership just to access a home.

Many capabilities associated with Secured-E-Key directly reflect multiple already present capabilities of various smart locks available to purchase in the existing marketplace. However, the technical characteristics of Secured-E-Key do not remain marketable to solely the home security industry, but to a diverse set of other electronic industries valuing the same or similar characteristics associated with the project. No matter, the proper ability and competency needed to construct Secured-E-Key will prove each senior electrical engineering student's capacity to transition from student to engineer.

2.0 PROJECT DESCRIPTION

2.1 Motivation

Contributing to the creation or augmentation of a product or service which the market place deems desirable and appealing serves as the primary motivation to creating a completely wireless smart lock security system to the front door of any house. All members of our group agreed the project needs to incorporate hardware, software, and programming which requires all group members to become accustom with either one or a combination of the three features. Therefore, by each group member concentrating their focus on one or two specific features, each member can confidently and competently gain a sufficient amount of experience to solicit to employers after graduation.

2.2 Goals and Objectives

A countless number of smart locks exist in the market place today, giving customers the absolute freedom to vote with their dollars as to which device they find most favorable. Each smart lock available to currently purchase features a wide range of capabilities which are either similar or entirely different from one another. The creation of Secured-E-Key will exploit a number of smart lock capabilities present in the market place by focusing primarily on the aspect of security without risking home or user safety.

Objective one is to guarantee the user has a keyless entry to their home through the most direct and simplistic way possible without carrying around any additional devices that require power. RFID tags serve as one potential solution to fulfilling the objective, especially due to the fact of an RFID reader attached to the door requiring an electrical power source, but not the tag itself. An alternative emerging solution which the market place could not have sustained close to five years ago is NFC technology. Nowadays, the integration of an NFC chip is present in almost every smartphone because electronic manufactures continue to increase the supply of smartphones to phase out non-smart mobile devices. Therefore, NFC technology will likely also serve as another great possibility since many people carry their smartphone with them almost everywhere on a daily basis along with an NFC reader requiring power to scan an NFC chip rather than the chip itself.

Objective two is to utilize wireless connectivity for Secured-E-Key to sustain wireless communication. The option of Wi-Fi would appear as the most apparent choice since most residential occupiers pay for the service to use to their own convenience on devices like tablets or laptops. For Secured-E-Key to take advantage of the service, a good deal of Wi-Fi microcontrollers and modules exist to fully assimilate with any kind or set of peripheral devices. Cellular networks serves as a viable alternative to support wireless connectivity, especially with countless different modules available to purchase and with many modules offering the compatibility to connect directly to a microcontroller unit to integrate more peripherals into the system or for increased computing power. Either options will provide a reliable and secure medium of wireless connectivity for the user to communicate through, but will have to be researched meticulously before a final determination as to which one will be used.

Objective three is to apply video or still framed image data streaming so the user can see who is at their front door. Video streaming would be ideal for instituting within Secured-E-Key, depending on the potential demands and unforeseen hardware levels necessary to support it. In the event of video streaming becoming a failure, streaming still framed images still provides Secured-E-Key with an appropriate medium to clearly and visually show the presence of a person who approaches the user's front door at any specific moment.

Objective four is to focus on detection and to create a self-secure operating system through the inclusion of various sensors. A passive infrared sensor will communicate to Secured-E-Key the presence of a person within close proximity of the door. A self-secure operating system supported by a gyroscope will accurately sense the position of the door and any displacement of the door as to determine when Secured-E-Key will automatically lock and unlock. It will allow for the user to remain worry free as to any possible damage the bolt may inflict to the user's door frame while closing and the manual status of their door as to being lock or unlocked.

Objective five is to create a strong layer of physical security which only the user can breach at will with Secured-E-Key. An electromagnetic strike or deadbolt operated by a servo motor will be used to lock and unlock the door. Secured-E-Key will only allow the user and no other person to control the status of the door, leaving no question as to who else will have access to the user's residence. Our group prefers doing as little mechanical alterations as possible to the lock in order to focus purely on the electrical parameters of Secured-E-Key.

2.3 Project Requirements and Specifications

Each table shows what is expected from the Secured-E-Key project. Table 1 shows the general requirements and specifications, Table 2 shows the specific hardware requirements, and Table 3 shows the software requirements.

Table 1: General Requirements and Specifications

Req. Num.	Requirement/Specification Description
1	Door must lock and unlock using some kind of radio-frequency identification technology (i.e. RFID – Radio Frequency Identification or NFC – Near Field Communication).
2	Battery power source reliant enough to supply a constant amount of current and voltage to each individual part of the system according to the varying demands and time period of each demand required of a part.
3	Sensor(s) accurately sense the presence of a person or object at the door while avoiding distractions such as wind, light, etcetera, which would otherwise cause the camera to undesirably turn on.
4	To ignore objects outside the desired range of object detection estimated to around 6 to 10 feet.
5	In the presence of an object, a camera must record video for 30 seconds or take burst of 3 photos to transmit from the front door to the user's smartphone.
6	Have the ability to lock and unlock the front door from the user's smartphone at a far distance (around >= 1 mile).

Table 2: Hardware Requirements

Req. Num.	Hardware Requirements
1	Electromagnetic strike or solenoid as an electromagnetic lock.
2	12 V DC battery source to supply the appropriate loads of current and voltage for the fluctuating demands of every part to the system so each part can adequately operate as needed.
3	The battery system must last between 3 to 6 months.
4	Radio-frequency identification technology of Secured-E-Key must identify the precise frequency which emanates from a particular RFID chip or smartphone NFC chip when scanned.
5	Microcontroller unit to integrate the electromagnetic lock, digital camera, PIR sensor, RFID/NFC technology, and smartphone communication together.
6	The PIR sensor must alert the Secured-E-Key system to wake the microcontroller from sleep-mode so the various peripherals can become active.

Table 3: Software Requirements

Req. Num.	Software Requirements
1	A smartphone must connect and communicate with the microcontroller unit through the medium type of a cloud server, created webpage, email, or via text messaging service.
2	A smartphone must receive a recorded video feed or compilation of 3 different images from a burst of 3 captured images after the PIR sensor has been activated.
3	A smartphone must lock and unlock the Secured-E-Key lock once a data transmission has sent from the smartphone over an established wireless connection.

2.4 Milestones

Focusing on research serves as the dominate characteristic to assure the overall success of creating Secured-E-Key. As a result, designating research categories and meeting at least twice a week remains paramount to keep the group on the appropriate course. At first research will comprise of finding much information not entirely useful to actually completing the project, but will serve as a necessary phase for the group to eliminate needless information and hone attention towards the more relevant kind. Fluidity must be kept within the group to make a smooth transition into writing the paper and then finally to constructing and presenting the final product. Therefore, Table 4 and Table 5 will allow the group to follow a suitable structure to accomplish the project from start to finish.

Table 4: Senior Design 1 Milestones

TASK FOR SENIOR DESIGN 1	START	FINISH
General Research and Design Expectations	16 Feb 2015	09 Mar 2015
DC to DC Power Supply		
Smartphone Related NFC Technologies		
PIR and other Sensors		
Microcontrollers		
LEDs and Video Camera		
Bluetooth/Wi-Fi/Cellular Networks		
Electromagnetic Lock		
Smartphone to Microcontroller Wireless Communication		
Finalize Design Expectations	09 Mar 2015	30 Apr 2015
DC to DC Power Supply for Whole System and Peripherals		
Smartphone to NFC Communication		
PIR and other Sensor Implementation and Integration		
Microcontroller Full System Integration		
LEDs and Video Camera System Integration		
Bluetooth/Wi-Fi/Cellular Networks Implementation		
Electromagnetic Lock Integration		
Smartphone to Microcontroller Wireless Communication		
PCB Design		
Creation of Expected Test Procedures	13 Apr 2015	30 Apr 2015
DC to DC Power Supply for Whole System and Peripherals		
Smartphone to NFC Communication		
PIR and other Sensor Implementation and Integration		
Microcontroller Full System Integration		
LEDs and Video Camera System Integration		

Table 5: Senior Design 2 Milestones

TASK FOR SENIOR DESIGN 2	START	FINISH
Hardware Tests	11 May 2015	25 May 2015
DC to DC Power Supply		
Smartphone Related NFC Technologies		
PIR and other Sensors		
Microcontroller		
LEDs and Video Camera		
Electromagnetic Lock		
Software Tests	25 May 2015	01 Jun 2015
Electromagnetic Lock		
Smartphone to Microcontroller Wireless Communication		
Hardware Construction	01 Jun 2015	19 Jun 2015
Peripherals to Microcontroller Soldering		
Software Construction	19 Jun 2015	10 Jul 2015
Microcontroller Coding		
NFC Technology Coding to Smartphone		
Various Sensor Coding		
Constructed Hardware and Software Testing	10 Jul 2015	24 Jul 2015
Testing Secured-E-Key to Check for Quality Assurance		

3.0 PROJECT RESEARCH

3.1 Similar Projects and Products

Before making any serious considerations as to the capabilities Secured-E-Key should offer and the parts which would enable our project to function, our group looked into two different projects and one current product. In each of the three areas, each offered distinct attributes as to when compared between one another, our group could clearly extrapolate the attributes we collectively favored as a group to begin consolidating everything into a possible representation Secured-E-Key would directly reflect. Our group gained a further in-depth understanding as to what qualities and features we would not want to include from comparing each of the three areas, so Secured-E-Key will appear original and avoid resembling an already existing device. According to the knowledge extracted from the three sources, our group will work more cohesively to accomplish well defined goals and project expectations, rather than arbitrarily working by trial and error without any prior understanding.

3.1.1 NOKI

The NOKI Smart Locking Interface project completed by three senior electrical engineers from the University of Central Florida created their smart lock device to focus on low power consumption and a minimal size as the driving factors to their overall project. The smart lock was powered by four AA lithium batteries, equaling to 6 V, to serve as the main power source to operate the 3.3 V and 1.9 V applications and to power the system as a whole for at least six months. The calculations of NOKI placed approximate battery life at 1.07 years at 80% efficiency which well exceeded their expectations. Secured-E-Key will follow a very similar model for the power system by relying on a single 12 V DC battery source which utilizes high performance batteries to provide a sufficient amount of power for a minimum of three months. The operation of the DC motor and Wi-Fi to control the locking mechanism, digital display, and external camera required the most average current in NOKI. Secured-E-Key will need the lowest powered wireless communication device available like a Wi-Fi module or cellular network module along with an efficient electromagnetic lock. The FlyCamOne eco V2 considered by NOKI was not used mainly as a result of higher and costlier power dissipation which destroys battery longevity. Making a final determination as to using video streaming or sending still framed images to a smartphone may end up depending exclusively on if our power system can sustain the foreseen burden. Uploading video streaming data to the internet over a stationary Wi-Fi connection will provide the appropriate medium by storing data to a location such as a cloud, but Secured-E-Key directly connecting to an available cellular network can also supply internet connectivity. NOKI chose the TI CC3000 as their Wi-Fi module of choice, but newer technologies like the CC3100 module and CC3200 microcontroller could alternatively perform better and are compatible with cloud services like Temboo and IBM Bluemix unlike the CC3000.

3.1.2 Keyless Electronic Entry System (K.E.E.S.)

The Keyless Electronic Entry System (KEES) project speaks of various kinds of embedded communication protocols important to consider for the purpose of data transfer and hardware communication. Protocols like the RS-232, RS-422 and RS-485, I2C, and SPI exposed our group to an introductory level of embedded protocols altogether. It is helpful to comprehend the fundamental characteristics of the RS-232 including 3 volts or above counting as a binary zero and -3 volts or below counting as a binary one, as well as how UART hardware microcontroller connections can establish full-duplex communications which support various peripherals at data rates up to 115.2 kbps. Long distance interfaces like the RS-422 and RS-485 can support long distances data transfers at a maximum distance of 4,000 feet, but will not apply to Secured-E-Key since such a long distance is inapplicable. The communication types of I2C working at half duplex and SPI working at full duplex will likely function as the best protocols for Secured-E-Key seeing most microcontroller units for development boards such as the Raspberry Pi, Arduino, MSP430, and countless others mount pins for one or both kinds of interfacing. Researching to pick a specific microcontroller unit to best complement the demands of Secured-E-Key will now occur with more ease than before coming across the KEES project paper by distinctively knowing how certain protocol sets briefly operate.

3.1.3 Lockitron

Lockitron is a Apigy Inc. product created by Camerson Robertson and Paul Gerhardt functioning as another conventional smart lock device, except it fits over any normally perceived deadbolt turning mechanism found on the inside portion of a door. Lockitron struck our group with an immediate appeal in direct relation to the product's ability to remain accessible on a global scale at a distance literally thousands of miles away via an Android phone or iPhone due to a device called Bridge. Bridge functions as an additional device which both creators engineered to plug into a user's electrical wall socket to allow for a constant power supply to continuously support global accessibility. Bridge is simply the Wi-Fi capability which is entirely separate but yet connects to the Lockitron device due since Wi-Fi draining too much battery life by combining Lockitron and Bridge together into one device. The particular feature of Bridge drew our attention more than anything else as a result of knowing for certain Secured-E-Key can institute a successful wireless capability via Wi-Fi or a cellular network to achieve the same global or long distance communication characteristic as Bridge itself. Lockitron also uses Bluetooth 4.0 Low Energy for the user to access their door once in the proximity of fifteen to thirty feet to the door, but Secured-E-Key will exploit either RFID or NFC as a similar kind of technology

3.2 Wireless Communication

The ability to wirelessly communicate with Secured-E-Key serves as a fundamental requirement to leave the user with the absolute assurance that their door always remains secure. The ability to receive live streaming video data to a smartphone along with wirelessly locking and unlocking the electromagnetic lock instantaneously from anywhere on Earth remains paramount. Our group considered Bluetooth as an option, but it quickly fell through due to having a maximum effective range of only 1200 meters even with the implementation of using a hyper gain 2.4 GHz high performance antenna. Therefore, Wi-Fi or cellular networks provide the best way to achieve a reliable connection and to minimize the latency periods to any data transmissions. A prolonged delay in transmitting multimedia data or wirelessly accessing the electromagnetic lock will compromise the overall security to Secured-E-Key.

3.2.1 Internet Accessibility

For simplicity, the internet serves as the best option in order to support long distance internet communication between Secured-E-Key and any smartphone. By choosing to rely upon internet connectivity, any smartphone will always face one of two extreme situations. The situations consists of a user (1) being in the presence of cellular service provided to their smartphone, in which case the whole smart lock system should work in complete harmony together as designed, or (2) being without cellular service to their smartphone, where the smart lock system will not work at all, since cellular phone service and cellular internet service rely upon the same signal. Knowing the internet serves as the optimum service for wireless connectivity, our group considered the TI CC3100 Booster Pack

3.2.2 TI CC3100MOD

The key component highly considered for a smartphone and Secured-E-Key to communicate through an internet connection is using a cloud server. The Texas Instruments CC3100 Module meets all of the specifications appropriate to provide for cloud connectivity and several layers of data security. The module features a wireless network processor which establishes a medium access controller (MAC) layer to create a clear line of communication between any smartphone and Secured-E-Key itself by using the TCP transport layer to guarantee the delivery of data packets in the corresponding order originally sent. The CC3100 harnesses two simultaneous sockets which are the transport layer security (TLS) and secure sockets layer (SSL) to provide computer network security and 256-bit AES encryption for the TLS and SSL connections. Incorporating a personal WPA2 with enterprise security to require a password to the Wi-Fi connection will protect against hackers from breaching data and the home security. Excess Wi-Fi power dissipation will stay to a minimum with a transmit gain (Tx) of 17 dBm and a receiver gain of -94.7 dBm. The CC3100 operates at currents levels of 54 mA when receiving data and 223 mA when transmitting data along with two power saving modes of 140 uA during a stand-by mode and 7 uA during hibernation with real-time clock. A supply voltage range of 2.3 to 3.6 V gives an acceptable step-down voltage level while in stand-by mode or hibernation. The surface area is not ideal, measuring in at 20.5 x 17.5 mm but the longevity of the CC3100 module component features a sufficient temperature range between -20 to 70 C (-4 to 158 F).

3.2.3 Atmel SMART SAM W25-MR210PA Wi-Fi Module

A device like the Atmel SMART SAM W25 module can establish a consistent, reliable Wi-Fi connection without compromising on security as an internet of things (IoT) application. The module itself comprises of an Atmel SAM D21G ARM-based microcontroller and Atmel ATWINC1500 network controller to deliver the smallest and lowest power 2.4 GHz IEEE 802.11 b/g/n 20 MHz connection for one on one applications measuring in at 33.9 x 14.9 mm. The SMART SAM W25 module includes crypto-authentication ATECC508 I/O operating voltages from 2.7 to 3.7 V, whereas the whole module operates between 2.7 to 4.6 V. The crypto-authentication ATECC508 provides a fully secure module solution by utilizing a secure hardware-based cryptographic storage key which relies upon security measures greater than most software-based key storage. The SAM D21G microcontroller runs up to 48 MHz and supports a full-speed USB device as a peripheral which could allow for the connection of a USB wireless network adapter to increase the amount of bandwidth available for multimedia streaming for devices such as video cameras, microphones, still-framed cameras, and much more. Recommended operating conditions of the whole module lie between 3 to 4.2 V, although ordinarily working at 3.3 V and with low power current consumption as little as 70 uA/MHz. The Atmel ATWINC1500 network controller portion of the module coordinates data movement between the PHY-MAC layers using a 54 Mbps frequency-division multiplexing scheme (OFDM) 802.11g with a transmit (Tx) and receive (Rx) rate for wireless communication which corresponds to the same data rate as most household DSL home connections. At 3.3 V, current levels reach a minimum of 60 mA for receiving data and 149 mA for transmitting data, along with allocating only 4 uA of current necessary for a deep sleep mode. To prevent the Tx and Rx signals from encountering collisions in the network, the MAC layer includes a Network Access Vector which serves as an indicator to each station as to the time period necessary to avoid from accessing the network while the network is busy. The ability of the module to hold a ten year battery lifespan on AAA batteries by pulling data at every thirty minute intervals for incorporated applications like periodic weather updates makes the Atmel SMART SAM W25 module an attractive choice to consider for Wi-Fi connectivity.

Table 6: Wi-Fi Module Power Parameters

Operation	Normal Current/Voltage Usage	
Supply Voltage	2.3 – 3.3 V	2.7- 4.6 V
Transmitting (Tx)	223 mA	149 mA
Receiving (Rx)	54 mA	60 mA
Hibernation	7 µA	4 µA

3.2.4 Cloud Connectivity

The purpose of a cloud service gives our group the ability to fulfill the obligation of connecting Secured-E-Key to a smartphone from any location on a global scale. A cloud service serves as the only option to support global connectivity to the internet since Wi-Fi normally has a maximum range for emitting an effective signal for up to 100 meters from its base location. Secured-E-Key has the option of being controlled using cloud communication from a smartphone by using either a custom made Android application or internet browser like Google Chrome. However, both options use cloud service communication in ways so inherently different from one another that each must be discussed individually.

3.2.4.1 MSP430F5529 and CC3100 Wi-Fi TI Bundle with Temboo Cloud Service

The combination of the TI MSP430F5529 with the TI CC3100 is a bundle set offering compatibility to a cloud service platform called Temboo. Temboo functions by simply programming the bundle set and connecting it to the Temboo cloud server. Temboo does support Android app development or webpage development through programming the bundle set to establish a secure internet webpage which only the user can specifically access. The user accesses the webpage by the means of a designated URL; however, the URL remains a secure source of communication between the Secured-E-Key user and their smartphone. The bundle set follows a process of creating the specific URL and only allows for it to remain in existence so long as the bundle set is executing code. The moment the bundle set finishes executing code and enters hibernation mode, the URL is no longer sustained with the bundle set and the webpage itself ceases to function; even if the user attempts accessing it otherwise.

The Temboo cloud service makes it incredibility easy to develop and maintain software and IoT applications without dealing with the multiple layers of complexity associated with virtual machines, routers, domain names, or memory configuration to create a working application. None of the members on our team have much software or application development experience to set-up such a complex structure; however, Temboo offers intricate programming processes called Choreos to develop a complete IoT application. Choreos produce code through a series of libraries where each library asks the user a series of inputs necessary for the generation and execution of the code. After filling in all the inputs, and running the library, the appropriate compiled code and header file (a file which references the main code body for instances like sending an email) will appear in a programming language chosen by the application developer. The Java language works best for Secured-E-Key and is compatible with the TI bundle; nonetheless, Temboo supports code creation for every Choreo with ten different languages to choose from. A very cool and sophisticated feature of Temboo is the option to link the initiation of each Choreo event in the library set-up phase of every Choreo to a sensor. In doing so, the sensor must first be triggered by an external event, like a PIR sensor being activated, for the chosen output hardware event of the coded script to execute, like a video camera recording for an interval of time to then send to a smartphone. The appropriate compiled code and header file each Choreo produces can be copied and pasted to any open-source electronics prototyping platform like Energia to fully test and augment both pieces of information even further or combine Choreo sets of code to create a much larger program capable of handling and executing more tasks. Temboo features over two thousand Choreos which work compatibly with internet based institutions like Yahoo weather in order to retrieve the temperature or general weather information according to a specific address(es) or coordinate set(s). Also for websites including Amazon, EBay, or PayPal to access all normal browsing capabilities unique to each individual website, except Temboo allows the developer to specifically choose which website capabilities to incorporate. Microsoft offers a particular service to translate between languages for the purposes of processing spoken audio along with written text. Secured-E-Key could use Choreos to write the appropriate code as a way to upload, operate, and execute the code over the communication medium of Wi-Fi through the Texas Instrument hardware bundle set-up of the MSP430F5529 with CC 3100 module. The Google Choreo should serve as the best option if our group chooses Temboo. The Google Choreo includes all features of the Gmail service Google extends to all Gmail account users, but allows for the application developer to choose individual features deemed significant and worthy for use, instead of having to institute all features as a whole. The Gmail Choreos most important to Secured-E-Key can be found in Table 7 below with a brief description.

Table 7: Important Choreos for Setting-Up Email

Choreo	Description
UploadAttachment	Use Zendesk which is a cloud-based customer service platform to send email attachments as a Base64 encoded file over the Zendesk server.
InboxFeed	Allows access to only read Gmail emails in a list marked as unread.
SendMessage	Sends an email using only a specified Gmail account.
TrashMessage	Move a certain message to the trash bin.

3.2.4.2 GSM/GPRS

As a possible alternative to Wi-Fi, our group can use the Global System for Mobile Communication (GSM) for wireless communication in the event we cannot properly integrate Wi-Fi to correctly function with all of Secured-E-Key's purposed capabilities. The intent of using GSM communication stems from the clear understanding that the network supports over 70% of the world's digital mobile phones in at least 168 different countries. GSM provides the service of integrating General Packet Radio Service (GPRS) which is the first level of service on GSM. GPRS also enables our group to include emailing and internet browsing into Secured-E-Key with an absolute assurance of knowing the services are supported by a large company like AT&T with a reliable and almost limitless cellular network already established. The GPRS packet operating system works off of a more outdated, but yet reliable 2.5G network with data rates between 56 to 114 Kbits/s for sending and receiving data via a packet-switching network method. Bandwidth unavailability using GPRS should not occur, especially since the system can serve multiple users from one cell tower and more than one user can share the same designated spectrum of bandwidth simultaneously. A larger supply of bandwidth offered to users makes it less costly to afford and offers more applications to customers. Therefore, Secured-E-Key can transmit and receive data to and from a smartphone over a medium like the internet in an inexpensive way.

3.2.4.3 SIM Card Network Security and Vulnerabilities to GSM

A SIM card serves as the rudimentary component for a mobile station (MS), like a smartphone, to communicate over a GSM network. A SIM card is responsible for establishing and guaranteeing GSM communication remains secure, especially for an application like Secured-E-Key. Network security consists of a registration message sent to a GSM network with an International Mobile Subscriber Identity (IMSI) unique to the specific SIM card and held by the SIM and GSM Home Location Register (HLR) to begin an authentication process. The base transceiver station (BTS) uses the IMSI from the MS to request for the HLR to provide the RAND (a generated 128-bit random number), SRES (32-bit signed response), and Kc (a generated 64-bit ciphering key from the MS). The three pieces of information allow for the HLR to locate the correct Ki (a fixed 128-bit authentication key only assigned and stored in each SIM card ever created) by the MS calculating the exact same SRES and Kc as the BTS requested for and verified by the BTS after being calculated. If the calculated SRES and Kc from the MS coincide with the SRES and Kc of the BTS, a secure network is established. One way of compromising the described SIM card network security altogether stems from a criminal contacting a person’s service provider (SP) while acting as the actual same person and asking for the transfer of the person’s cellular number to a new SIM card. By doing so, an impersonator will receive all calls and text messages as to serve only as a subsidiary to a larger scheme like phishing to acquire sensitive information such as account numbers, user names, passwords, etcetera. A situation as described will likely never happen, but since Secured-E-Key allows the user to grant entry to their home wirelessly, all scenarios must be considered and known.

3.2.4.4 SIM800H Module for Cellular Connectivity

The SIM800H module functions to provide direct communication between computers and smartphones over a cellular network. The quad-band GSM/GPSR feature allows for voice, short message service (SMS), and data transfer at low power dissipation frequencies of 850, 900, 1800, and 1900 MHz. Quad-band is an attractive feature of the SIM800H since the newest iPhone 6 and Android phones available to purchase are completely compatible with the quad-band frequencies, therefore enabling cellular communication to and from Secured-E-Key to occur. The allowable operating voltage ranges between 3.4 to 4.4 V with a recommended setting of 4 V for normal module activity and featuring a wide temperature range from -40 to 85 C (-40 to 185 F). The module has a plethora of software features including embedded TCP/UDP protocol, FTP/HTTP, MMS, email, DTMF, audio record, TTS, and embedded AT. According to Figure 1, the module can interface itself with several available peripherals such as a GSM, FM, or Bluetooth antenna, UART ports for direct connectivity to an external processor, secure digital (SD) card interface for additional nonvolatile memory storage, SIM card interface required for access to the GSM network, USB interface to debug or download software, keypad interface to enable up to 50 buttons, and audio interface to integrate a microphone for audio recordings. The module permits for the addition of a rechargeable or non-rechargeable battery for exclusively powering the RTC which provides the benefit of the RTC to continue its normal operation, even while the rest of the system is in sleep mode and to eliminate the need for excess power consumption from the main power source. A module like the SIM800H permits for global access to Secured-E-Key by employing SMS or calling the module through a cellular network like AT&T to lock or unlock the front door. On at least one YouTube video, a person demonstrates his ability to use his Android phone to call the SIM800H module and change the state of an LED wired to the module. The video provides supporting evidence that a cellular network can be used effectively to send a voltage signal high or low to the SIM800H as a way to control the electromagnetic lock.

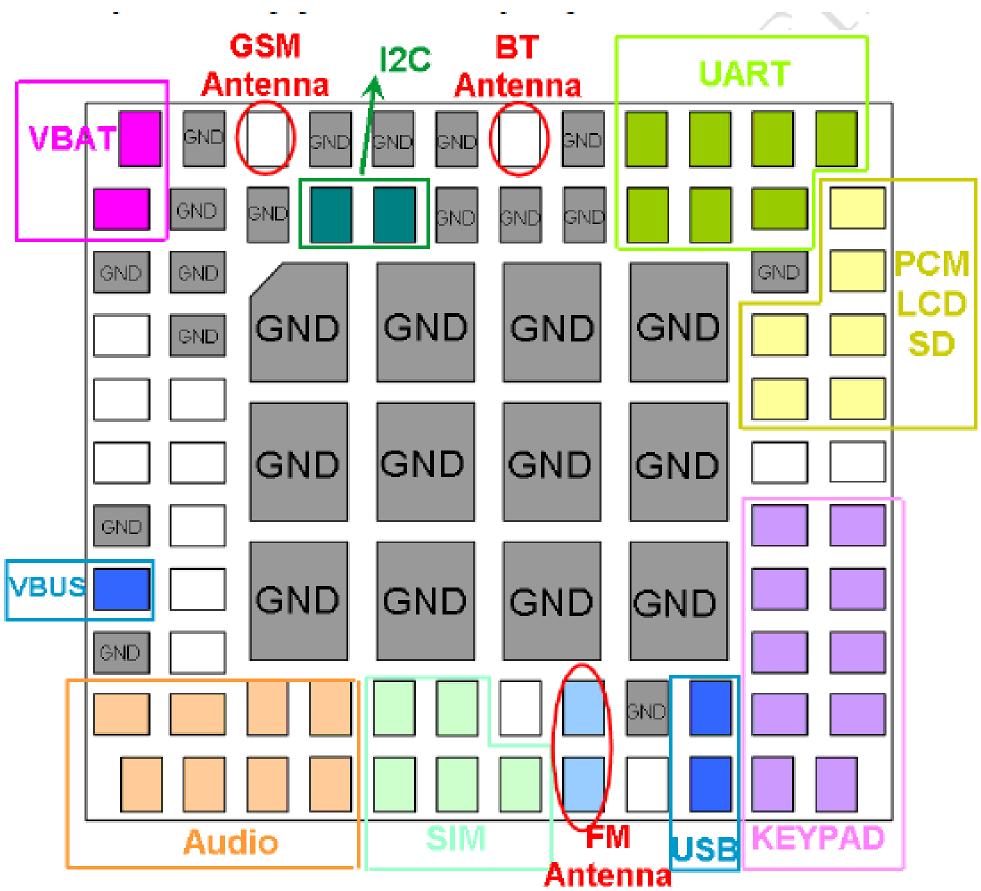


Figure 1: SIM800H Module Physical Pin Assignment
(Posted with Permission Pending)

3.2.4.5 SIM800H Module Various Bit Rates

Incorporating multimedia into Secured-E-Key creates the demand for needing to consider how the SIM800H directly deals with various bit rates. The GPSR for downlink or uplink cannot exceed 85.6 kbps on the SIM800H due to a class 12 rating which uses a total of eight available timeslots; but can only allow for a maximum of five to remain active at a time. Different data rate allocation methods like circuit switched data (CSD) allocation offers coding schemes (CS) that vary from CS-1 to CS-3 or bit rates of 9.6 to 14.4 kbps per slot, whereas CS-4 for regular GPRS data allocation uses a bit rate of 20 kbps per slot. Since GSM supports global communication, it directly affects determining which CS type will work best in relation to where a MS (like a smartphone) is to a BTS. A MS close to a BTS will use a stronger bit rate such as CS-4 while a MS farther away has a much higher probability of using CS-1. Understanding the behavior of various CS is vital to consider in order to develop Secured-E-Key since minimum CS requirements exist for supporting particular internet applications. For example, email requires CS-1, audio requires CS-3, and video requires CS-4; all serving as minimum CS level baselines required to be used in order to sustain each application. Table 8 displays the key important attributes to consider in association with CS-1 through CS-4.

Table 8: Important Attributes and Coding Schemes
(Referenced from the International Journal of Advanced Science and Technology)

	Coding Scheme			
Attributes	CS–1	CS–2	CS–3	CS–4
Reliability	High	Medium	Medium	Low
Delay	Low	Medium	Medium	High
Bandwidth	Low	Medium	Medium	High

3.2.5 SIM800H Module AT Commands

The computer language used to control GSM devices are known as AT commands. AT commands relate similarly to the C language primarily due to AT commands forming an archive of instructions with each AT command meant to follow only one particular designated task which no other AT command can execute otherwise. For example, AT+SMTPCS is the AT command for sending an email; therefore, no other AT command expect for the one mentioned has the ability to execute such a task. To find the appropriate commands to construct the proper software program for the SIM800H to run, the manufacture of the module published an AT Command User Manual fully describing each AT command in detail and its proper functionality. The benefit of AT commands stems from the straight-forward structure of the commands which afford anyone to explicitly understand and apply them without any layers of complexity; however, the only unfortunate drawback is having to spend a longer time searching for the appropriate commands to write a program simply due to the hundreds of instructions which exist. To partially solve the drawback of using AT commands, luckily AT commands can work directly with the C language in the case of needing to repeat a certain AT command continuously, like under the conditions of using a for loop, or to fulfill the demands of whatever application an application developer is working on with an improved level of ease. Secured-E-Key would purely depend on the implementation of an isolated select few sections of AT commands to make possible either video or image data streaming and text messaging between the system and a user's smartphone.

3.3 Video Streaming Capability

A video stream showing the presence of a person provides a user with more explicit situational information than a still framed camera shot. Live streaming video feed gives the consumer the ability to explicitly perceive the body language of a person as to develop a better notion to the person's intentions. If in the event a homeowner's house is unknowingly burglarized while away for an extended period of time, once discovered, the homeowner will have an archive of recordings to provide police with greater situational details of the robber's behavior as to increase the chances of the thief being accurately identified and found.

3.3.1 Multimedia Codec

Multimedia codec is a software based way to support capabilities like standard compliant video as well as a range of still-image and audio compression qualities and their bit rates. To implement multimedia codec software into a device like Secured-E-Key, it must be able to compress data at a variable rate between 40 kb/s to 4 Mb/s, have a frame rate up to 30 frames per second (fps), support standard compliances with ISO, MPEG, or JPEG standards, encode and decode digitized images or video data, and perform audio compression following the International Telecommunications Union (ITU) recommendation of G.711 (3 kHz, 64 kb/s), G.722 (7 kHz, 64 kb/s), and G.728 (3 kHz, 16 kb/s).

3.3.2 DSP3210 Processor for Multimedia Solutions

The DSP3210 serves as a module with the capabilities to process G.711, G.722, and G.728 standards along with MPEG audio for high quality applications and to filter out acoustic echoes. The 32-bit addressing space software operates off of a dedicated memory C-compiler and set of assembly language tools preprogrammed to the 256 x 32 boot read only memory (ROM). For the processor to enable video streaming under the NTSC standard consisting of 480 lines by 720 pixels per line at 30 fps, the processor uses an internal analog to digital converter to send data to an encoder. Luminance video data is sampled horizontally at 352 pixels and interpolated at 288 lines vertically, while chrominance data is sampled at a 144 lines by 176 pixels per line resolution.

The encoder chip is responsible for determining the optimum bit rate, picture quality, frame rate, and code waiting time of the compressed bit stream converted from the video data. The DSP3210 digitizes analog audio signals into a compressed data stream and buffers the audio data stream to create the appropriate delays which correspond exactly with the video-encoded bit stream. The audio and video streams are wirelessly sent to a decoder chip where the video data is decompressed into YCrCb 4:2:2 frames at the coded frame rate received. The 64 general I/O pins can be directly accessed and toggled as an input or output by programming in either a 1 or 0. The voltage range of any pin with respect to ground varies between –.5 to 6 V with the processor featuring an internal transistor rated at a breakdown voltage exceeding 2000 V to protect the processor's internal unit as a whole. Power consumption for toggling I/O pins is moderately rated at 5.25 V and -50 uA for a voltage signal to go high whereas 0 V and 50 uA for a voltage signal to go low. The processor offers a favorable low-power standby mode requiring only 300 mW in comparison to the typical 750 mW of active power dissipation. To disrupt the standby mode, an interrupt request must occur, via a sensor or designated change programmed into the processor to fully become active again.

3.3.3 TI TMS320DM368 DaVinci

Achieving high video resolution becomes a possibility with the TMS320DM368 DaVinci Digital Media Processor. Video streaming for any project normally requires the most energy and processing power, therefore, with the TMS320DM368 the voltage requirements remain moderately rated at 1.8 V per general purpose I/O pin and 1.2 – 1.35 V for the internal core to operate, but does offer multiple power saving stand-by modes. Secured-E-Key only has the necessity for one video camera, so the presence of a single dedicated set of UART pins fulfills the sole purpose of encoding and decoding video data. Video codecs such as MPEG-4 and WMV9 along with MPEG JEPEG Co-Processor (MJCP) and HD Video Imaging Co-Processor (HDVICP) video acceleration types grant our group the ability to choose from a diverse range of video cameras which remain compatible to the processor's listed specifications. Video acceleration is what encodes and decodes MPEG video data and JPEG image data under the co-processing types of MJCP and HDVICP (HDVICP deals with HD video data) to shorten processing time and save power. The processor comprises of an ARM926EJ-S core for 32-bit and 16-bit instruction sets; adequate enough to handle a maximum of 720 pixels with 30 fps for video processing. Key video processing subsystems include a hardware face detection engine, resizing engine for (1/16) to 8 times the initial video frame size, hardware on-screen display for external connectivity, image sensor and CMOS image sensor interfaces, and real-time image processing. An analog-to-digital convertor (ADC) and voice codec device, which supports the audio coding format standards of AAC-LC, G.711, MP3, and WMA, are both default and internal to the core. They can allow for the integration of an analog video camera with the additional feature of clearly processing the camera audio through the voice codec device. The flash card interface incorporates the availability of two I/O pins allocated for two secure digital (SD) card slots which can serve to store analog video data once processed by the ADC to then become stored as nonvolatile digital memory. Though information on the exact size of the TMS320DM368 processor is not explicitly mentioned on its datasheet, the device features 65 nanometer (nm) transistor technology and functions over a temperature range between -40 to 85 C (-40 to 185 F).

3.3.4 N32905U1DN Processor from the ARM926EJ-S Type

The N32905U1DN is an ARM926 based media processor designed specifically as a multi-chip package to maximize performance and minimize PCB space. For instance, the chip internally features a 1Mbit x 16 synchronous dynamic random-access memory (SDRAM) as a way to achieve a higher performance and minimize operational errors from electromagnetic interference and noise coupling. The processor supports the implementation of SD and raw NAND flash nonvolatile memory along with a USB drive subsystem as a peripheral in the case of a USB wireless network adapter for cordless data transfer. The chip enables source and destination color formats including RGB555, RBG565, and YCbCr422 as to work compatibly with CMOS image sensors, a still image capture for up to 2 mega-pixels, and video streaming for a max resolution of 640x480. Image cropping allows for image cropping sizes as high as 4096x2048. Formatting the color of each encoded and decoded image sent from the processor to the internet through JPEG codec data streaming uses interleaving YCbCr 4:4:4, 4:2:2, or 4:2:0. Choosing from one of the three YCbCr types will directly affect the sampling rate of the JPEG codec process, thus causing variations in the bandwidth and data rate of each component to an image being sent. YCbCr 4:4:4 will use the same sampling rate across each of the YCbCr components, whereas YCbCr 4:2:2 reduces the sampling rate of the two chroma components by half. Cutting the bandwidth in half causes the required bandwidth signal to drop by one-third without any noticeable change in visual quality of YCbCr 4:2:2. Lastly, YCbC 4:2:0 samples the two chroma channels every other line while the vertical resolution is halved so the data rate does not change. The N32905U1DN can send a collection of image data through a packet to help make image data streaming more efficient for Secured-E-Key through using either YCbCr 4:2:2 or 4:2:0 image formatting. Packets for Secured-E-Key would send through a Wi-Fi connection comprising of a normal transmit and receive rate along with a baud rate of 115,200 bps or over a high speed connection consisting of request to send (RTS) and clear to send (CTS) networking protocol both supported by a baud rate of up to 1M bps. When the processor is not active, the real-time clock (RTC) is designed to remain active during stand-by or power down modes which are controlled by an input pin for each particular mode. The stand-by mode keeps the 1.8 V core (capable of 200 MHz) on and turns off all IP clocks, whereas in the power down mode all power except for the RTC turns off. The processor requires 3.3 V to power the system of 80 programmable general purpose I/O pins and lies within a temperature range between -40 to 125 C (-40 to 257 F).

3.4 System Power Supply

For the power there are different methods we can do to power the smart door. You can choose between alternating current and direct current for the electricity. There is another consideration to use a mobile power supply or direct wire from the household to power the device. There are different factors to determine what the right specifications to use such looking at the power consumed by this device. Another thing we can look at is what components we would need to provide the right voltages and current to use to run all the devices. Another factor that we must consider is the efficiency of the whole system. In order to make the system mobility powered we will need to choose all the components that will optimize the power consumed.

3.4.1 Solar Energy

The first type of power source we can look into is solar energy. This can be attractive to use since it is modular and can be mounted on our device. This device would be able to recharge our device in order to provide sustainable power to system or extending the battery life of or device. Ideal situations solar energy works best in providing energy where there is direct sunlight. This might be problematic for our project since our device won't be exposed to direct sunlight because most front doors are shaded by a front porch.

3.4.2 Alternating Current

Another way to power our project is to use AC power from the houses electrical grid. An advantage of using AC as the power source is that it provides a constant source of power to our device. By using this method we eliminate the need to constantly replace the battery supply. This may seem attractive to use but it will require more work in the long run. Running wires through the walls may be difficult to install which may require paying someone. Another consideration if we were to use AC powers is finding a way to convert it to power that our electronics can use. Electronic devices cannot be directly powered by using AC. There are several processes that must be done to the electrical properties before it can be a viable power option. Electronics run by using DC power sources which produce a unidirectional voltage and current instead of a nonlinear sinusoidal wave that AC produces. The first process of changing AC into usable power is stepping down the voltage. The household output voltage is 220V RMS.

3.4.3 Battery Power

Another source of power for our project that was considered is battery power. After much research in our project it seemed that most of the electronic locks in the industry used batteries. Most of these electronics locks were able to last from several months to a year. Using batters seems like that best choice for our power source. One advantage is that it doesn't require any house hold modification to wire power to our door lock. Another advantage is that if the house hold power goes down you are still able to unlock the door since it isn't connecting to the power grid. The only disadvantage is that the batteries would have to be changed once it is low.

3.4.4 Battery Considerations

There are many properties of batteries that can be considered before choosing the right type of battery such as its capacity, discharge rate, energy density, and price. A battery capacity is a very important consideration when choosing a battery. Its capacity tells us the amount of electrical charge that is stored in the battery which is expressed in Ampere-Hours (Ah). The discharge rate tells us the relationship of the voltage level and the amount of time that has passed. This is an important consideration since we want our battery voltage to stay as high as possible when not in use. Energy density tells us the amount of energy the battery has for its given mass and volume. This can display how powerful a battery can be.

3.4.5 Battery Types

Not all batteries have the same properties and specifications. The nomenclature of the battery helps describes the dimensional, chemical, and electrical terminal characteristics of various batteries.

Batteries vary in different sizes and measurements. Batteries sizes ranges from the size of a car battery or small as a watch battery. The right battery size must be considered to fit the parameters of the project. The first parameter is the battery must fit is the placement requirement. The battery can be placed within the lock or be mounted outside the lock. Commercial batteries have standardized battery sizes. The ones that will be considered are the common consumer batteries. These batteries are all single cell round batteries with a height greater than its diameter. The batteries that were researched were AAA, AA, C, and D. The D battery is the largest common consumer battery produced. It has a diameter of 34.2mm and a height of 61.5mm. The C battery is the second largest and has a diameter of 26.2 and height of 50mm. The AA the third smallest and has a diameter of 14.5 and a height of 50mm. The AAA is the smallest and has a diameter of 10.5mm and height of 44.5mm. Comparing the dimensions of the electric strike lock AA or AA will be viable options to use for internally.

There are many types of battery composition in the market. The main types are primary batteries which are zinc-carbon and alkaline batteries and secondary batteries which include nickel-cadmium, nickel metal hydride (NiMH) and lithium-ion (Li-ion) cells.

Out of all of the types of batteries out there alkaline batteries are the most common type of batteries, which was why it was the first battery considered. Zinc-Manganese Dioxide Alkaline battery has a high rated capacity but only if a small amount of power is slowly drawn. This could be advantage since this project is aiming for low power consumption. Typical battery sizes ranges AAA, AA, C, and D. Considering battery size and capacity the AA size would be optimal. The average discharge rate for this type of battery is 5 percent a year. Alkaline batteries have a moderate energy density ranging from .4-.59 for batteries. The average battery capacity for AA is about 2400mA.

Another type of primary battery is lithium battery. Out of all the battery compared Lithium batteries have the highest shelf life of 15 years. This feature is optimal for this project since it will be powering the system for months at a time. The common capacity for these batters is about 3000 mAh which is higher than the alkaline batteries.

Another battery consideration is Lithium Ion type. This is a type of secondary batteries which must be charged before being used but can also be recharged. The battery can be charged more than 500 times before it cannot be used which is about the same compared to other rechargeable batteries. The battery has no memory effect which allows the batteries to keep its capacity over its lifetime compared to Ni-MH batteries. It is one of the fastest growing battery technologies in the industry. It also has a very high energy density since it has a higher voltage per cell. Typical voltages for Lithium ion cells are almost always 3.7V which is makes it much higher than the standard voltage cell for most batteries. The self-discharge rate is anywhere between 5 and 10 percent per month. This could be problematic to use if it is expected to replace the battery after a couple months. Li-Ion batteries have one of the highest energy densities compared to other batteries which can range from .36 to .96 MJ/L. The price of this battery can be more expensive than most other commercial batteries. Lithium batteries can deviate in size and shape from the standard battery types AA, AAA, C or D. The battery can be small and cylindrical and have no terminals, or large and cylindrical with the terminals. The battery can even found to be prismatic in shape. The shape variation can all for better implementation for an outside battery module or even side the lock casing its self. The size can be much bigger than a standard commercial battery size. This is very optimal to use if the battery power supply would be implemented outside the door lock module. Since Lithium ion has one of the highest energy density considered, the external battery can provide multiple more times of more energy for its physical dimensions compared to other battery types.

Nickel-Metal hydride is another option considered for this project. It is one of the cheapest from of rechargeable battery type. Ni-MH can carry a capacity of 2700mAh. Its specific energy is about .36MJ/kg. Depending on which type of Ni-MH battery you get the discharge rate can be very low. Newer models can hold

70 to 85 percent of their full charge after a year. This will affect life of the lock system if it is expect to several months of battery life. The nominal cell voltage for Ni-MH is 1.2v. This is the lowest voltage out of all the battery types being considered. Ni-MH batteries are cheaper in pricing compared to Li-ion but more expensive than Primary single use batteries which can reduce the total cost of the project. The cost per Kw is 18.50$ compared to 24$ to produce one KW of power.

Table 9: Consolidated Battery Type Specifications

Battery Type:	Capacity (mAh)	Voltage (V)	Price($)	Discharge Rate (%per month)	Energy Density (MJ/kg)
Alkaline	2400	1.5	.75	2-3	.4-.59
Ni-MH	2700	1.2	3.25	10-15	.36
Li-Ion		3.7	5	1-2	.36 to .96
Lithium	3000	1.5	2	.1	.87

3.4.6 Battery Selection

The 3 different types of batteries are considered based off of its functionality. The first battery is Sounddon new energy lithium ion 16850 battery. The second consideration is Duracell DC1500 Ni-MH battery. The final battery that was considered was lithium ion batteries. The lithium ion's batteries nominal voltage is 3.7V and its battery size is 18650. Looking at the battery's size it is possible to place the batteries inside the lock. The capacity of the battery when fully charged is 2200mAh and is approximately. As seen from Figure 2, the discharge rate is fairly linear between 0 and approximately 90% the discharge capacity which is between 3.5 to 4 volts and then exponentially decreases from 3.5 to 2.7V. The recommended discharge voltage should not be below 2.75. This could affect the consideration of the batteries or project design if a component would require anything below this voltage. The rate of discharge stays proportional to the rate of voltage drop. The total discharge capacitance only varies by 10 percent based off of discharge rate. This can work well for the power source if a component draws a high amount of current for a short period of time such as the electronic door lock. The maximum amount of current that should be drawn is twice the capacitance of the battery which is 4.2A at full charge. The 3.7 nominal battery voltages can be beneficial since it will require 3 times as less batteries to increase the voltage of the power source if another battery was added in series.

This leaves room for the more batteries to increase the capacitive energy of the power source by putting them in parallel to each other. This will effectively double the capacitance if they if two of them are parallel. The battery is approximately 3 dollars. If the system were to only draw .2C which is approximately 400mA the battery life is approximately 300 minutes.

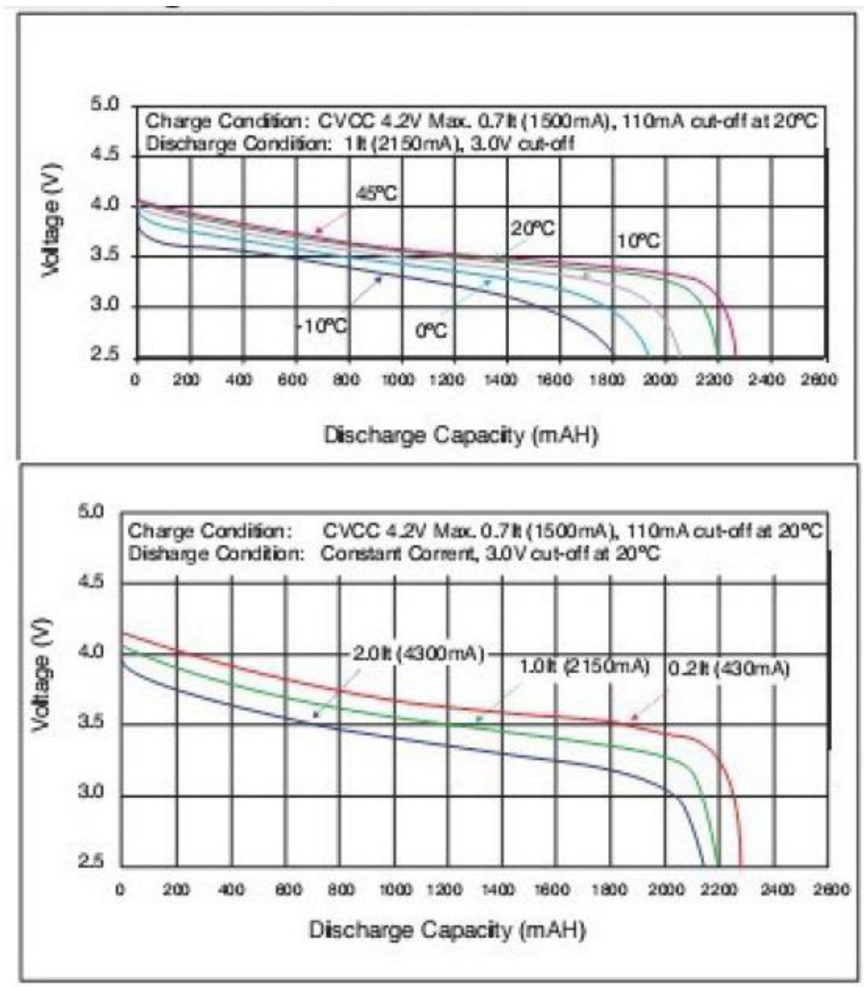


Figure 2: Discharge Characteristics of Lithium Ion Batteries
(Permission Granted From Datasheet)

The Duracell DC1500 Ni-MH battery is a consideration to be used as a power source. The DC1500 is an AA battery, which makes it convenient to be used since most electronics uses AA and is small enough so that it could be used within the electronic lock. The nominal voltage for this battery is 1.2V this could affect the number of batteries implemented in the device to reach the right power specification. The rated capacity is 2450mAh at full charge. The discharge rate is less linearized compared to Sounddon lithium ion battery. The discharge rate is less steep between 90% and 100% of the charged voltage. Once the voltage drops below this threshold the voltage drops rapidly to the allowable discharged voltage. When the rate at which the drops to the discharged voltage is higher than a discharge rate that is lower. This can be observed in Figure 3. If a component that uses high current draw is used, using this type of battery would be unbeneficial. Overall the amount of time it takes to deplete the voltage is the same as the Sounddon lithium ion.

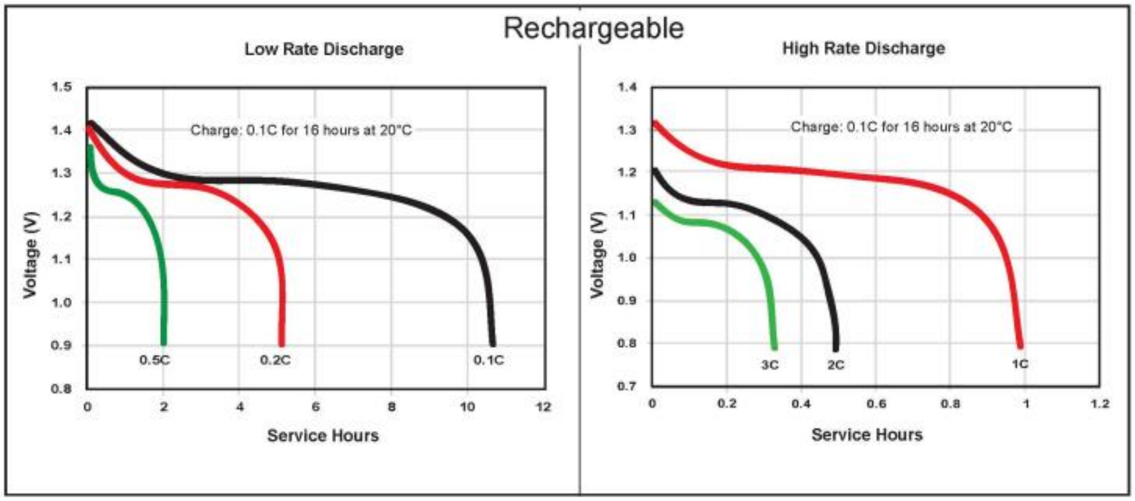


Figure 3: Duracell DC1500 Ni-MH Battery Discharge Rate Performance (Permission Granted From Datasheet)

3.4.7 Power Regulation

Secured-E-Key power supply will have to power all of the electronic components. Each component has its own specific voltage and current requirement in order for it to work. If the input voltage that is being produced is less than the component's operating voltage the component will not operate or unexpected behavior can occur. This is effect is known as a brown out. Brown outs can cause the control signal to fall below the threshold at which the digital circuits can detect. The will make the machine not function as it is supposed to. If the voltage is supplied the component is higher than its operating voltage not only will the device will not operate correctly but the device can overheat and can be destroyed. To prevent this problem it will be necessary to step down the voltage of the power source in order fit these specific voltage requirements. The linear regulator device will be able to solve this problem. There are two different forms of linear regulators, a buck converter which is used as a DC to DC step down or a boost converter which is used as a boost converter. If the project were to use a DC-DC step by using boost converter then the power supplies voltage would have to be less than the converted output voltage. The boost converter will step up the voltage by stepping down the current proportionally so satisfy the conservation of energy rule. The method is problematic and impractical to use for the system. The DC-DC step down method is more effective to use since better current will be able to be drawn.

3.4.8 Regulators

There are many considerations when choosing DC-DC step-down regulators. The first requirement is that it must satisfy the voltages above. Once it satisfies the voltage It must also be able the handle the voltage of the power source. Many regulators have a given input voltage handler that it can operate at. If the input voltage doesn't fit the minimum requirement or drops below it, then the regulator will stop outputting the correct voltage. Normally the minimum input voltage is somewhat higher than the output voltage. The regulator must also be able to handle the load requirement of the system. If it is too high the device may burnout. The efficiency of the device is also another consideration. The less efficient the device is the more the power is not used for anything. This is important in helping to extend the life of locking system if batteries were to be implemented.

There are two types of DC-DC step down regulator converters to choose from. The type is a linear regulator. The resistance in this regulator changes according to the load which creates a constant voltage output. This regulator works by creating a voltage divider with a variable resistance and continually dissipates the voltage of the input and output as a form of heat. The second way is using a switching regulator. A switching regulator works by taking a packet of energy from the voltage input source and move it to the output. This can be done by implementing an electrical switch and a controller which regulates the amount of energy that is passed. One advantage of a switching regulator is that the energy loss is very small which makes it very efficient. Typical efficiencies are about 85 percent for switching regulator while linear regulator efficiency are about 40 percent and can go as low as 15 percent. It is very practical to use switching regulators since one of the goals is to minimize power consumption and maximize efficiency. Another consideration of the linear regulator that might be problematic is heat. There is a possibility that some components might over heat if too much current is drawn. As a result of these problems linear regulator has a much lower load current than a switching regulator. The disadvantages of a switching regulator is that the cost is higher and the circuit complexity is more advanced than linear regulators in which it may require inductors or transformers depending on the circuit design.

3.4.8.1 TPS62173

The TPS62173 made by Texas instruments is a Step-Down Converter that could be used for the regulators. The devices output isn't fixed but instead it can be adjusted from .9V to 6V. This can be especially useful for powering devices that require a low voltage or a nonstandard voltage of 3.3 or 5 volts that most devices use. The device can handle an output load current of 500mA. The TPS62173 is very energy efficient at stepping down voltages. The device is capable of reaching an efficiency of 90 percent if the voltage input is 5 volts and stepping it down to 3.3V. The device is capable of increasing its efficiency by entering in to a power save mode. This state occurs fluently when the load current decreases to a quiescent current of 17uA. This is very useful for when the system is in power down mode when there isn't a presence to detect. The only time the system won't enter power save mode is if the voltage input is 15% less than the regulated output. Another useful feature is that the device is capable of entering shutdown mode in which the current is less than 2uA. This can be very useful when the devices connected are not needed and shutdown to save power. The device has a high voltage input that ranges from 3 to 17 V.

3.4.8.2 TPS62140

The TPS62140 made by Texas instruments is a Step-Down Converter that could be used for one of the regulators. Like the TPS62173 the output voltage is adjustable from .9V to 6V. Unlike the TPS62173 the TPS62140 can handle a higher output current of 2A. This should be more than enough to handle the load that the locking system will require. The efficiency is slightly higher than the TPS62173 and can reach around 95% at with an input voltage of 5V. It also has similar power features such as power savings and power down mode.

3.4.8.3 TLV73325PDQNR

The TLV73325PDQNR made by Texas Instruments is a linear regulator that is part of the TLV733P series. It is a low drop out linear regulator (LDO) which means that the regulator can regulate the output voltage even when the supplied voltage is close to the output voltage. This can be beneficial for extending the life of the devices that are being supplied power. The input voltage range is very limited to 1.4 to 5.5 volts. TLV73325PDQNR has a fixed output voltage of 2.5V. The circuit design will be fairly simplistic since it won't require capacitors for the input or output. The TLV73325PDQNR can handle a maximum current load of 300mA. As a result only a few devices will be able to be regulated. The device has three different functional modes, Normal operation, dropout operation and disabled mode. When in the normal mode the device will function as it is supposed to by regulating the voltage output. Dropout operation will occur when the input voltage is lower than the voltage output plus the specified voltage and the device is operating correctly. When it is lower than the dropout voltage the output voltage will start to deviate. When the device is in disabled mode the device will not function.

3.4.8.4 TPS62122

The TPS62122 made by Texas instruments is a switching regulator. It as a wide input range of 2V to 15V which is only 2V less compared to switching regulators. The TPS62122 can produce a variable output voltage that ranges from 1.2V to 5.5V. This is acceptable range at which most electronic devices operate at. TPS62122 is capable of having an efficiency of 96 percent if the voltage is 5.5V. This is the highest efficiency compared to all the other regulators. The efficiency of the device is traded off for a low current load of 75mA. The regulator would only be used to provide a voltage that 1 or 2 devices can use. The TPS62122 has a power saving mode and a power down mode just like the other switching regulator but has a lower quiescent current of 11uA.

3.4.8.5 Regulator Summary

The following Table 10 summarizes the properties of the DC-DC step down regulators.

Table 10: Consolidated Properties of Voltage Regulators

Model	TLV73325	TPS62140	TPS62173	TPS62120
Regulator Type	Linear	Switching	Switching	Switching
Min Input Voltage	1.4V	3V	3V	2V
Max Input Voltage	5.5V	17V	17V	15V
Fixed or Variable output Voltage	Fixed	Variable	Variable	Variable
Min output Voltage	1V	.9V	.9V	1.2V
Max output voltage	3.3V	6V	6V	5.5V
Max current Load	300mA	2A	500mA	75mA
Shutdown Current	.1uA	1.5uA	1.5uA	.3uA

3.5 Sensors

The purpose of Secured-E-Key is the mobility of home security through the capability of a smart phone. Therefore, sensors will play an important part in how Secured-E-Key will accomplish this home security capability. The type of sensors that implements security the best is motion detection sensors, therefore Secured-E-Key will utilize motion detection sensors. How the Secured-E-Key motion detection sensor will be implemented is by having the motion detection sensor placed inside the lock itself. The sensor will then trigger a human presence in its field of view and send a signal to the camera to take a picture and send it through a nearby internet provider to the user’s smart phone.

3.5.1 Capacitive Sensors

Capacitive sensors were considered as a choice for Secured-E-Key's motion detection capability. Capacitive sensors are mainly used to detect metals, nonmetals, solids and liquids, and work by generating an electrostatic field when a target enters its line of sight. However, capacitive sensors were quickly turned down due to many factors that did not fit the requirements and specifications of Secured-E-Key. The main factor was that the capacitive sensor's electrostatic field is highly sensitive to outside environmental factors such as mist, dirt, or dust which affects the sensing output. This serves as a big issue for Secured-E-Key because Secured-E-Key is supposed to function in an outside environment. The other factor capacitive sensors were not chosen is due to only being able to sense within a very short range such as one inch which is unacceptable for Secured-E-Key because the requirements and specifications were to detect at least 6 feet in front of the door lock to maximize home security. Capacitive sensors would have been appropriate to use if the project required a small range sensing such as liquid levels, or checking certain material levels; however, the project Secured-E-Key is based on a smart lock system with mobile security.

3.5.2 PIR Sensors

The most common sensors used for motion detection are PIR (Passive Infrared Sensors) which detect motion by sensing infrared levels by objects within its detection radius. PIR sensors have the ability to filter out various movements which seemed the best fit to implement for Secured-E-Key due to its capabilities of sensing motion very effectively and covering a wide angle of sensing as well. PIR sensors would be implemented by sticking out of the smart-lock to cover the door's given perimeter and when the signal is tripped by a human presence, the PIR sensor sends a signal to the ARMS processor to notify the camera to take a picture and send it to the home user's mobile phone. The PIR sensor is very important because it is the first component that starts the process for Secured-E-Key.

3.5.2.1 Parallax PIR Sensors

The Parallax PIR Sensor is a motion detection sensor that checks for detection by sudden changes in the Infrared perimeter. The Parallax PIR sensor uses a 3-pin SIP. The operating voltage is 3-6 volts and operating current is 12-23 mA. The output communication uses logic, meaning when motion is detected a high signal is set out to the output pin. The logic signal can be read by a microcontroller or can be used to drive an external load which would then require a transistor or MOSFET. The Parallax PIR sensor can detect motion up to 30 feet away and detect an angle range of 90 degrees. It also has an easy interface for any microcontroller which is a good feature to have because the sensor will be able to work on any microcontroller of the choosing used for Secured-E-Key. The Parallax PIR sensor also has a jumper setting which makes it able change from a normal mode to reduce sensitivity mode which means it can reduce at up to half the original range, which in this case would be up to a maximum range of 15 feet. For Secured-E-Key the reduced sensitivity range would be used because the range set for Secured-E-Key would be roughly 6 feet.

3.5.2.2 Parallax Wide Angle PIR Sensor

The Parallax Wide Angle PIR sensor operates and functions very similar to the previous Parallax PIR sensor. The operating voltage is 3-6 volts and operating current is 12-23 mA. The detection range is 30 feet and the output communication uses logic as well. The main difference between the Parallax Wide angle PIR sensor and the basic Parallax PIR sensor is that the Parallax Wide Angle PIR sensor has a wider detection range of 180 degrees. This wide angle feature gives it the advantage to detect movements in more wide open areas. For Secured-E-Key this wider angle range would give the lock better security because the angle is increasing the detection range by covering more area for detecting motion. The Parallax Wide Angle PIR sensor also includes a “night-time mode” feature to detect motion in decreased lighting conditions and an adjustable sensitivity feature to tune sensitivity levels for different operating conditions. The Parallax Wide Angle PIR sensor also uses a 4 pin SIP instead of a 3 pin SIP used in the basic Parallax PIR sensor. The fourth pin is EN which is utilized as an optional pin to connect the PIR sensor to a standard servo extension cable if needed.

3.5.2.3 ZMotion Detection Module II

The ZMotion Detection module II is a motion detection sensor with a maximum detection range of roughly 23 feet and a detection angle of 95 degrees. The operating voltage is 2.7-3.6 volts and the operating current is 8.9 mA. The ZMotion module combines a Zilog motion detection microcontroller with a PIR sensor and clip-on lens. The ZMotion Detection module II operates in two modes. It can operate in Hardware mode which just activates an output signal when motion is detected, allows to adjust the sensitivity and delay, offers optional ambient light input, and includes a sleep mode to allow for low power consumption. The other mode it operates in is Serial mode which is a software mode that allows the sensor to communicate with another processor within the system over a UART. The serial interface operates at 9600 bps, no parity, 8 data bits, and 1 stop bit. The serial interface also accesses wider selection of activation times, sensitivity, and ranges, has a unique Hyper Sense feature that can automatically increase sensitivity after motion is detected. These features are helpful and useful if this sensor is chosen for Secured-E-Key. The ZMotion Detection Module uses an 8 pin interface connector, Table 11 shows the function of each pin.

3.5.2.4 PIR Sensor Conclusion

After researching various PIR sensors, it was evident of what PIR sensor was desired for the implementation of Secured-E-Key's motion sensing capability. The PIR sensor chosen was based on the compatibility with any microcontroller, ease of use for both hardware and software components, and detection ranges that included distance and angles. Each of the three PIR sensors researched had their own unique functions and capabilities that fit the criteria for Secured-E-Key's requirements and specifications. Overall, PIR sensor chosen for Secured-E-Key will be considered the most optimal and efficient for the lock. Table 11 shows a comparison of the three PIR sensors researched as well as the characteristics desired for Secured-E-Key.

Table 11: Comparison of PIR Sensors

Model	Parallax PIR Sensor	Parallax Wide Angle PIR Sensor	ZMotion Detection Module II
Size (mm)	32.2 x 24.3 x 25.4	36 x 36 x 20.2	25.5 x 16.7 x 11
Operating Power (VDC)	3 – 6	3 – 6	2.7 – 3.6
Operating Current (mA)	12 – 23	12 – 23	8.9
Trigger Type	internal	internal	external
Output Type	logic	logic	digital
Detection Angle (°)	90	180	95
Detection Range (ft)	30	30	23
Operating Temperature (°C)	0 – 50	0 – 50	0 – 70
Price	10.99	11.99	10.80

3.5.3 Inductive Proximity Sensors

Another type of sensor that was considered for Secured-E-Key's motion detection capability was inductive proximity sensors. Inductive sensors are mainly used for detecting metal by emitting an electro-magnetic sensing field. When a metal target enters the field, it triggers a change in state at the output from induced currents. Inductive sensors were considered for Secured-E-Key because it can withstand water, oil, dirt and other outside environmental factors which were a major advantage compared to the capacitive sensors; however, it was turned down as well because it's ideally used for detecting metal objects. For Secured-E-Key there is no guarantee that when a person enters the sensing field that they have metal on them and this is a major issue because home security is at risk and Secured-E-Key's requirements and specifications were to maximize security. Also, the inductive sensors detection range is 2 inches which is too small for Secured-E-Key since the minimum range is 6 feet. Inductive sensors would have been appropriate if the project required metal detection from machinery or metal products; however, inductive sensors are inefficient for the project requirements and specifications of Secured-E-Key.

3.5.4 Gyroscope Sensors

Gyroscope sensors are sensors that measure and sense rotational motion in 3 directions. Gyroscopes were the chosen component to be utilized for Secured-E-Key because they will be used for door positioning to track the door when it's opening or closing. The gyroscope would measure the positioning of the door when it's opened or closed. It would work by sending a signal to the ARM's processor to make the decision when the door is open the smart lock is unlocked and when the door is at the position of closed the smart lock is locked.

3.5.4.1 ITG-3200

The gyroscope ITG-3200 is a triple axis sensor of InvenSense MEMS products and was considered for Secured-E-Key. Its features a 16 bit analog-to-digital converter in order to digitize the triple axis outputs, and it supports I^2C interface. It also features a robust 10,000 g shock tolerance which could be ideal for Secured-E-Key if the door encounters hard slams or vibrations. It also features power supply flexibility by offering a separate VLOGIC reference pin in addition to its analog supply pin that can set the logic levels in the I^2C interface mode. The ITG-3200 also has a low operating current and wide VDD supply voltage. Overall, the ITG-3200 offers low frequency noise that simplifies the application development; however, it only supports one communication protocol which can be an issue if Secured-E-Key chooses to use a different communication protocol such as SPI or UART.

3.5.4.2 ITG-3400

The gyroscope ITG-3400 is a triple axis sensor of Invensense MEMS products as well and was considered for Secured-E-Key. The ITG-3400 features the 16 bit analog-to-digital converter just like the ITG-3200 to digitize the triple axis outputs, but it also features a user-programmable full scale ranges of +/- 250, 500, 1000, and 2000 dps, which can be useful for Secured-E-Key for more precision in tracking both fast and slow motions of the door. The ITG-3400 also features an on-chip FIFO that can lower system timing and reduce power consumption by allowing a system's microcontroller to burst read sensor data and then go into a sleep mode while the ITG-3400 collects more data. The ITG-3400 also supports SPI or I^2C interface, has low operating current, has a wide VDD supply voltage that offers a separate digital IO supply, and features the 10,000 g shock tolerance just like the ITG-3200. Overall, the ITG-3400 supports all the features as the ITG-3200 but has added programmable features not offered in the ITG-3200 that can make Secured-E-Key's motion control process better.

3.5.4.3 MAX21000

The gyroscope MAX21000 is a triple axis sensor of the Maxim Integrated products and was considered for Secured-E-Key. The MAX21000 features the 16 bit analog-to-digital converter to digitize the triple axis outputs, and can digitally program full scale ranges of +/- 250, 500, 1000, 2000 dps in User Interface mode and +/- 31.25, 62.5, 125, 250 dps in Optical Image Stabilization mode. The MAX21000 supports SPI and I^2C interfaces and features a flexible FIFO with 4 different FIFO modes available. The MAX21000 features low power capabilities and offers 4 power modes. The MAX21000 also features the 10,000 g shock tolerance as well. Overall, the MAX21000 offers more flexibility and variety compared to the ITG-3200 and ITG-3400. Therefore, the MAX21000 gyroscope can offer the best development and motion control process for Secured-E-Key.

3.5.4.4 L3G4200D

The gyroscope L3G4200D is a triple axis sensor of the STMicroelectronics products and was also considered for Secured-E-Key. The L3G4200D features the 16 bit analog-to-digital converter to digitize the triple axis outputs, and has the full scale range of +/- 250, 500, and 2000 dps and is capable of measuring rates with a user-selectable bandwidth. The L3G4200D supports I^2C and SPI digital output interfaces and also features the FIFO capability. The L3G4200D also provides unprecedented stability over temperature and time and features low power capabilities, and offers a power-down and sleep mode. The L3G4200D also features the high shock tolerance of 10,000 g just like the previous gyroscopes researched. Overall, the L3G4200D supports the same features as the previous gyroscopes; however it has limitations in areas of programmability and flexibility compared to the others. Therefore the L3G4200D would not be a potential choice for Secured-E-Key.

3.5.4.5 MPU-6000

The gyroscope MPU-6000 is a 6-axis sensor of Invensense MEMS products and was considered for Secured-E-Key as well. The MPU-6000 has a 3-axis gyroscope, a 3-axis accelerometer, and a digital motion processor (DMP) hardware accelerator engine with an auxiliary I^2C port that can interface with a digital sensor such as magnetometers or pressure sensors. This can be beneficial for Secured-E-Key because it can eliminate the process of having to use separate gyroscope and accelerometer components. The MPU-6000 features a three 16 bit analog-to-digital converter for digitizing the gyroscope outputs and a three 16 bit analog-to-digital converter for digitizing the accelerometer outputs. The MPU-6000 features a user-programmable gyroscope full scale range of +/- 250, 500, 1000, and 2000 dps and a user-programmable accelerometer full scale range of +/- 2, 4, 8, and 16 g. The MPU-6000 supports both I^2C and SPI communication protocols and has the FIFO buffer to help lower the system power consumption and offers low power DMP as well. The MPU-6000 also features the high shock tolerance of 10,000 g and minimal cross-axis sensitivity between the gyroscope and accelerometer axes. Overall, the MPU-6000 offers better features compared to the previous gyroscopes and can eliminate t

3.5.4.6 Gyroscope Conclusion

After researching the gyroscopes, it was decided that gyroscopes were not going to be used for Secured-E-Key because the gyroscope offered more capabilities than what was intended for Secured-E-Key's purposes. Overall, Table 12 shows a comparison of the gyroscopes researched. Table 13 references the operating current and standby current for the gyroscope and accelerometer in the MPU-6000.

Table 12: Comparison of Gyroscope Sensors Researched

Model	ITG-3200	ITG-3400	MAX21000	L3G4200D	MPU-6000
Size	4 x 4 x 0.9 (mm)	3 x 3 x 0.9 (mm)	3 x 3 x 0.9 (mm)	4 x 4 x 1 (mm)	4 x 4 x 0.9 (mm)
Operating Power	1.71 – 3.6 (V)	1.71 – 3.45 (V)	1.71 – 3.6 (V)	2.4 – 3.6 (V)	2.375 – 3.46 (V)
Operating Current	6.5 (mA)	3.2 (mA)	5.4 (mA)	6.1 (mA)	3.8 (mA)
Standby Current	5 μA	1.6 mA	2.7 mA	1.5 mA	refer Table 13
Axis Detected	3	3	3	3	6
Communication Protocol	I^2C	I^2C/SPI	I^2C/SPI	I^2C/SPI	I^2C/SPI
Angular Velocity	+/- 250 – 2000	+/- 250 – 2000	+/- 31.25 – 2000	+/- 250 – 2000	+/- 250 – 2000
Operating Temperature	-40 – +85 °C	-40 – +85 °C	-40 – +85 °C	-40 – +85 °C	-40 – +85 °C
Price	$9.95	$8.01	$5.84	$6.76	$10.83

Table 13: Operating Current and Standby Current for MPU-6000

	Accelerometer	Gyroscope
Operating Current	500 (μA)	3.6 (mA)
Standby Current	10 μA at 1.25 Hz 20 μA at 5 Hz 60 μA at 20 Hz 110 μA at 40 Hz	5 μA

3.5.5 Accelerometer Sensors

Accelerometer sensors are sensors that measure acceleration forces, as well as vibrations and motion. Accelerometers were considered for Secured-E-Key because they were going to be implemented within the door to track the door's movement of opening motion and closing motion. How the accelerometers were going to function for Secured-E-Key was by having the accelerometers be placed inside the door and measure the forces and motions of the door opening and closing and the accelerometer would then send a signal to the ARMS processor to make the decision when the smart lock should be locked or unlocked; However, it was decided that Secured-E-Key would not be using accelerometers because accelerometers did not meet the objective of Secured-E-Key needs of door positioning.

3.5.6 Magnetic Sensors

Magnetic sensors are sensors that are used for detection of speed as well as position. Different types of magnetic sensors fall within this category such as Hall Effect sensors, MEMS magnetic field sensors, and Magnetic Reed switches. For Secured-E-Key the magnetic sensor would be used to track the positioning of the door when it's open or closed. The advantages of using magnetic sensors in Secured-E-Key is it offers detection without wear and tear, the magnetic sensor can detect magnets through the walls of non-ferrous metal, stainless steel, aluminum, plastic, or wood, and has long sensing ranges. Overall, magnetic sensors were the chosen component to be implemented for Secured-E-Key.

3.5.7 Photoelectric Sensors

The last type of sensor considered for Secured-E-Key's motion detection capability was the Photoelectric Sensor. Photoelectric sensors emit an infrared, red, or laser light beam as well as the ability to reflect the beam back to the sensor to detect an object. Photoelectric sensors are produced in 3 different types through beam, retro-reflective, and diffuse. The Photoelectric sensor was considered mainly because it's a better alternative to capacitive sensors and unlike inductive sensors, Photoelectric sensors can detect non-metal objects. For Secured-E-Key each of the different types were considered, starting with diffuse, the emitter and receiver are both in one component. The diffuse emits a light beam which then touches a surface opposite the beam and scatters the light in different directions, and one source of light gets reflected back to the receiver. When a person or object breaks one of the scattered beams the output gets activated. This type of Photoelectric sensor was not chosen because it seemed inefficient for Secured-E-Key purposes because it is reflective dependent and the detection range was only between two inches and six feet, which is just hitting Secured-E-Key's minimum range of six feet. The next type of Photoelectric sensor considered was the retro-reflective which uses 2 components an emitter and reflector. The emitter emits a beam onto a surface and the beam is then reflected back from the reflector. The retro-reflective detects by having a person or object breaks the line of sight of the emitter and reflector causing the output to activate. For Secured-E-Key this type is a little more efficient compared to the diffuse and the maximum detection range is 65 feet; however, it is uncertain if this particular type can be used outside with environmental factors. The last type is the through beam which consists of two components, an emitter and receiver. The emitter and receiver are displayed directly opposite of each other where the emitter emits a light beam directly into the receiver. The Through beam detects by having a person or object "trip the wire" or in other words breaks the beam causing the output to activate. For Secured-E-Key this type of Photoelectric sensor was considered the best choice out of the other two types because it can be used in outside environments such as dirt, dust, or mist and it has a detection maximum range of 328 feet. Table 14 shows a comparison of each type of the Photoelectric sensors.

Table 14: Advantages and Disadvantages of Each Photoelectric Sensor Type

Type	Advantage	Disadvantage
Diffuse	cheapest out of all three requires only 1 component	less accurate out of all three smallest detection range
Retro-Reflective	detection range better than diffuse more reliable than diffuse	requires 2 components smaller detection range than through beam
Through Beam	can be used in harsh environments best detection range out of all three	most expensive out of all three requires 2 components

3.5.7.1 Photoelectric Sensor Conclusion

After researching the three different types of Photoelectric sensors and comparing them to the previous sensors, the end result was that even though it is better than the capacitive and inductive sensors, Secured-E-Key would not use the Photoelectric sensor as the first option because of the main factor that it requires a break in the beam of light to be activated. This requirement of the Photoelectric sensor makes home security risky because it can be any object moving in the line of sight that can break the beam, not just a person. Also, the Photoelectric sensor doesn't cover a wide angle detection range such as the PIR sensor so security is compromised again from not covering every angle possible for maximum security. Even though the Photoelectric sensors are able to work effectively with Secured-E-Key, it doesn't deliver enough maximum security that's required in Secured-E-Key's requirements and specifications.

3.6 Communication Mediums

Communication is a fundamental component of wireless technology. In order for the Secured-E-Key to open the door wirelessly and securely there has to be an established wireless connection between the door and a user's device that have the capabilities to conduct such communications. There can be many possibilities to accomplish this functionality; however, for Secured-E-Key the main specification and requirement was security with mobility. In this case, the user device that was chosen for Secured-E-Key was the user's smart phone because it has the capability to operate various security features as well as be mobile at the same time. The various communication mediums that were considered met this specification and requirement as well as offered other capabilities to establish a safe secured short range communication connection between the lock and user's smart phone device.

3.6.1 RFID

RFID (Radio Frequency Identification) was considered as an option for the communication medium because it has applications in security. The RFID technology uses radio waves to automatically track or identify objects or people. The RFID consisted of three components a reader (transceiver), antenna, and a passive/active tag (transponder). It operates on three different frequencies low-frequency (125 KHz – 134 KHz), high-frequency (13.56 MHz), and ultra-high-frequency (850 MHz-950MHz). Secured-E-Key would only need to operate on the low-frequency of 125 KHz – 134 KHz because the project's specification and requirement was to have short range communication capability between the user's smart phone and the lock by having the user walk to the door and unlock the door using the smart phone as a key. The RFID technology also uses tags which only come in two types, either active or passive. The difference between the two are active tags generates its power through the use of batteries and passive tags generate power from the reader through the use of electromagnetic waves. For Secured-E-Key passive tags would be chosen to use because passive tags are mainly used for shorter distances, use less memory and are much lower in cost than active tags. The next step would be to choose what type of chip embedded in the passive tag to use. The types of chips to choose from are Read-Only, Read-Write, or Write Once Read Many (WORM). For Secured-E-Key WORM would be the best choice because the chip only needs to be programmed once with the objective to open the door, and once the chip has been programmed the tag can be read from the smart phone as many times as needed. The tags also depend on other characteristics such as format, size, metal/non-metal compatibility, and antennas. The RFID system is highly useful for wireless communications; however, for the purposes of Secured-E-Key the RFID technology requires the implementation of more components than necessary for communication between a smart phone and lock.

3.6.2 NFC

NFC (Near Field Communication) was considered as an option for Secured-E-Key as well. NFC is one of the newer technologies being employed today and is a subset form of existing RFID technology. The NFC was mainly considered because its standard function is wireless communication at 13.56 MHz within a range of four inches which is ideal for short range communication that reduces the likelihood of unwanted interception. The NFC consists of a microchip embedded inside a smart phone which is known as the emitter and a smart tag that has the capability of being read and/or written and can transmit data when the smart phone (emitter) is waved within four inches in front of the tag. Most smart phones today are manufactured with NFC chips implemented in them for the convenience of making payments, transferring data or tracking information. For Secured-E-Key, a smart phone with the NFC capability was a requirement and specification; however, the specification can be modified by acquiring a sticker tag which could enable the user to use NFC if the user had a phone that did not have the NFC capabilities. The tag type could be either the microchip active or passive tag. Table 15 shows the characteristics if the passive sticker tag was chosen as the communication for Secured-E-Key. In order to communicate with the NFC within the phone or the NFC tags an NFC development board will be used to implement the NFC communication between the smart phone and the door lock. Various NFC boards were considered for Secured-E-Key; however, the requirement and specification was to find an NFC board compatible with the ARMS processor and have easy implementation.

Table 15: Characteristics of Passive NFC Tag for Secured-E-Key

Format	NFC Chip	Tag Size	Antenna Size	Scan Strength	Price
White Sticker	NTAG213	22mm (round)	22 mm (round)	7 out of 10	$0.71
On-Metal Sticker	NTAG203	19mm x 19 mm	15mm x 15 mm	3 out of 10	$3.90

3.6.2.1 NXP PN532

The NXP PN532 was considered for Secured-E-Key's NFC communication. The NXP PN532 is an NFC chip that is considered the most popular NFC chip because it's embedded in most smart phones today and other NFC devices as well. The NXP PN532 is embedded in various NFC/RFID breakout modules to tailor to various microcontrollers and projects, which can be beneficial for Secured-E-Key by having a variety of modules to choose from. The PN532 supports four different operating modes which include Reader/Writer mode supporting ISO 14443A/MIFARE and FeliCa, Reader/Writer mode supporting ISO 14443B, Card Interface Mode supporting ISO 14443A/MIFARE and FeliCa, and Peer to Peer mode. The Reader/Writer mode ISO 14443A can operate distances up to 50 mm depending on the antenna size, tuning, and power supply. The Card Interface mode can operate distances of about 100 mm depending on the antenna size, tuning, and external field strength. The Peer to Peer mode can operate distances up to 50 mm depending on the antenna size, tuning, and power supply. The PN532 also supports I2C, SPI, and Serial UART protocols. Overall, the PN532 is an effective choice for Secured-E-Key because of the various modules the PN532 chip is embedded in which choosing a module that has easy implementation and, the various modes it supports which gives options in how the smart phone can communicate with the smart lock.

3.6.2.2 Dynamic NFC Transponder RF430CL330H

The Dynamic NFC Transponder RF430CL330H is part of the Texas Instrument (TI) NFC communication devices and was considered as a choice for Secured-E-Key's NFC communication medium. The RF430CL330H is a dynamic transponder interface that uses a Tag Type 4 device that can combine wireless NFC interfaces such as Wi-Fi or Bluetooth and a wired SPI or I^2C interface to connect the RF430CL330H to the ARMS processor. The SPI and I^2C interface allows reading and writing of the NFC data exchange format (NDEF) messages in the SRAM and can also be accessed and updated wirelessly through an ISO 14443B-compliant RF interface that supports data rates of up to 848 kbps. The RF430CL330H also provides the flexibility to be used with various antennas. Overall, the RF430CL330H Dynamic NFC interface transponder can be utilized for Secured-E-Key by enabling the smart lock to communicate with a NFC-enabled smart phone. The dynamic NFC transponder is an effective choice for Secured-E-Key since it offers support for high performance, easy to use hardware and software, and has the capability to optimize power.

3.6.2.3 TRF7970A

The TRF7970A is an RFID/NFC transceiver and is part of the TI family as well. It was also considered for Secured-E-Key for the communication medium. The TRF7970A uses parallel data communication or serial 4-pin SPI interface for its communication protocols. The TRF790A supports 3 different communication modes that include NFC peer to peer, card emulation, and proximity reader/writer ISO 14443A/B or FeliCa and vicinity reader/writer ISO 15693. The TRF7970A supports NFC Tag Types 1,2,3, and 4 and has integrated encoders, decoders, and data framing for data rates up to 848 kbps. The TRF7970A also features a large FIFO buffer for RF communication, an RF field detector for programmable wake-up levels for the NFC passive transponder emulation operation and for NFC physical collision avoidance, and 8 selectable power modes. The TRF7970A offers an add-on of the MSP430 Bootstrap Loader that allows users to communicate with the embedded memory within the MSP430 which could be useful for implementation for Secured-E-Key if needed. Overall, the TRF790A offers flexibility with built-in programming options and built-in user configurable programming options, which makes hardware and software implementation easy for Secured-E-Key.

3.6.2.4 NFC Conclusion

After researching various NFC devices, it was evident of what features were desired to be implemented as the communication medium for Secured-E-Key's alternative way of opening the door. These features included having the hardware compatible with the ARMS processor, NFC Tag Type that offers read/write capabilities, low power capabilities, and easy software implementation. These features and having the programmable and flexible features were highly considered as well. Overall, Table 16 shows a comparison of the NFC devices researched and the desired characteristics for Secured-E-Key.

Table 15: Comparison of NFC Researched

Model	NXP PN532	RF430CL3304	TRF7970A
Operating Frequency	13.56 MHz	13.56 MHz	13.56 MHz
Supported Protocols	ISO/IEC 14443A/MIFARE ISO/IEC 14443B/Reader;Writer mode only	NFC Tag Type 4/ISO 14443B	ISO/IEC 18092 ISO/IEC 21481 reader/writer Peer 2 Peer card emulation
Operating Voltage	2.7 – 5.5 V	3 – 3.6 V (no RF Field present) 2 – 3.6 V (RF Field present)	2.7 – 5.5 VDC
Communication Interface	SPI, I^2C, HSU	wired: SPI or I^2C wireless: 13.56 MHz/ISO 14443B	Parallel 8 bit or 4 wire SPI
Operating Temperature	-40 - +125°C	-40 - +85°C	-40 - +110°C
Price	$27.49	$19.00	$50.00

3.7 Microcontroller

For the Microcontroller and processor there are many aspects and features to a microcontroller. There is the speed of the processor, the memory size, power consumption and software for handling it or cost. There are many pros and cons when finally choosing a processor. When choosing a processor you sacrifice performance for cost or power to performance.

3.7.1 Microcontroller Board Types

For this project many microcontrollers where considered but ultimately one has to be chosen. In this project the Raspberry Pi, the Atmega328 and the Launchpad Ativa C and LPC2148 microcontrollers were looked at to show the wide variety of capabilities and features that could be used for our project. The ideal microcontroller for secured-e-key project is enough processing power to stream pictures from a camera and send it to a cell phone. The microcontroller must not draw too current to sustain battery life for a reasonable amount of time. Table 17 shows the specifications of each microcontroller board researched.

3.7.1.1 Raspberry Pi

The Raspberry Pi 2 is a computer about the size of credit card that is developed by the Raspberry Pi foundation. This is popular for electronic hobbyists since 5 million of these have been sold. The raspberry pi has many features. The raspberry pi 2 features an ARM Cortex-A7 CPU along with a VideoCore IV dual-core GPU. This can help support video playback if you needed to replay any previous videos. It has 1GB of RAM and an onboard storage. There are also 4 USB ports which is perfect for cheap and easy WIFI adapters to be added to the Raspberry Pi to wirelessly connect to the internet. You can also connect to the internet via Ethernet since it comes with an Ethernet Port. You can also install many sensors or hardware to the Raspberry Pi 2 since it has 40 GPIO Pins. There is also a camera interface (CSI) which will make it very easy to implement a camera if we needed to. The selling price is 35 dollars which seems very good for all the features that it has. Many Peripherals and features can be seen from looking at the picture including Multiple USB, HDMI, audio and a Ethernet ports.

3.7.1.2 Arduino

The Arduino Uno has an Atmega328 processor with a clock speed of 16MHz. The Arduino Uno is an AVR microcontroller. It is very easy to use its hardware and software which is why it is used by many hobbyists and electronic enthusiasts. The hardware is very easy to connect to the Arduino Uno because there are many circuit board shields that are specifically designed to connect directly to the Arduino. The board has a 5 volt linear regulator and a 14 out pins (6 PWM) which makes it good for adding sensors to our project. The Arduino has a IDE and a Cross platform that is written in Java. The IDE makes it easy comes with a software library with makes operations much easier. The simplicity of design of the Arduino board is very simplistic. The microcontroller processor only has 32 pins which make it easier to soldier and create a PCB design. Since many people use Arduino there are many PCB design to use as a reference for CAD programs.

3.7.1.3 Launch Pad Tiva C

The Launch Pad TIVA C is another microcontroller considered for this project. The Tiva C series is part of the launch pad kit developed by Texas Instruments. This launch pad is a platform that makes it easier to prototype projects. Texas Instruments has also developed booster packs to modularize hardware and sensors to the Board. TI offers multiple points of entry for Software program for the Launchpad. Energia is an open-source software that makes it as easy to programs as an Arduino. For the hardware The TIVA C series features an ARM Cortex-M4F processor which can be clocked up to 80MHz. It can feature 2 QEIs. It also features 32 KB of SRAM and 4 I^2C circuit. The Tiva C features 2 12 bit analog to digital converter modules each with a sample rate of 1 million samples per second. Also the TIVA C features 2 analog and 16 digital comparators. The Tiva C features two 2 PWM (pulse width modulator) modules and 4 PWM generator block and a control block which is used to make 16 total PWM outputs.

3.7.1.4 LPC2148

The LPC248 was the final microcontroller considered and chosen for this project. It is a very used that is a part of the ARM-7 family. It is manufactured by Phillips and has peripherals that are already prebuilt which makes it a good option for beginners or application developers. It has 512kbytes of flash program memory. 32kbytes of Sram, 45 I/0 pins that operate at 5V and an external oscillator of 25 MHz. This device is capable of running up to 60MHz for its clock speed. Its 32bit ARM7TDMI-S CPU is capable of real time emulation and embedded trace support. This allows you to carry out real-time debugging by using trace equipment. Serial communication interface ranges from UART, SPI, SSP to I2C bus and USB 2.0. This is very convenient for communication gateway or protocol converters.

Table 16: Processor Specifications

Microcontroller Type	LaunchPad TIVA C	Arduino Uno	Raspberry Pi 2	LPC2148
Processor	ARM Cortex	AT Mega 328	ARM Cortex	ARM 7
Cost	20$	10$	35$	
Speed	80MHz	16MHz	900MHz	60MHZ
Memory	256 KB	32KB	1GB	512KB
Voltage	3.3V	5V		3.3
Software	Energia, Code Composer	Arduino IDE		
I/O Pins	16	14	40	45
Active Power Consumption	48mA	20mA	300mA	70mA
Standby Power Consumption	1.8uA	.8uA		
Serial Interfaces	4 I2C,	4SPI, I2C	CSI,DSI,I2C	

3.7.2 Power Consumption

The power consumption is an important aspect when considering a microcontroller. When making a mobile battery powered device it necessary to minimize power consumption. In order to reduce power consumption for a microcontroller many manufactures implement CPU states. This is one feature to take into consideration along with the power dissipation

3.7.2.1 Tiva C Power Consumption

When looking at the Power states The TIVA C had multiple programmable power state configurations Run, Sleep, Deep Sleep, and Hibernate which can be seen in Table 18. It also had Wake-Up Interrupt Controller (WIC) with clock gating to allow the change in states. These multiple states make it a very attractive option to optimize and reduce power consumption. At the maximum clock rate of 80mHz it draws a current of 50mA. This is the most efficient performance to power ratio compared to the Atmega328 and LPC2148 microcontroller.

Table 17: Characteristics of Tiva C Power Saving Modes

Mode	Run	Sleep	Deep Sleep	Hibernate
MCU Current Consumption	47.81mA	9.67mA	1.35mA	1.38uA
TPS62177 Mode	Power Saving	Power Save	Power Save	Power Save
Efficiency	88	87	84	6.4
Battery Current	23.9mA	4.89mA	.71mA	9.5uA
System Clock	80-MHz	16 MHz	30 kHz	0

3.7.2.2 LPC2148 Power Consumption

LPC has two reduced power modes: Idle and Power down mode. When the LPC2148 is in idle mode the execution of instructions are suspended but all the peripherals to the microcontroller may continue to function. To resume the active state the peripherals may send interrupts or the microcontroller can be reset. The other state of the microcontroller is power down. In this state the oscillator stops running but the state of the processor, registers, memory, are preserved.

3.7.2.3 Raspberry Pi Power Consumption

The raspberry Pi 2 consumes about 230 mA of current when in idle. When under load it consumes about 300 mA. The raspberry Pi 2 is powered through a USB chord. The raspberry Pi 2 runs off of 5V. These factors make it impractical to mobilly power the device with batteries. 4 rechargeable batteries would provide 4.8V just enough threshold voltage to power the device. After it drops below 4.8 volts the system will quickly become unstable. If 4 Alkaline batteries were used, the voltage supplied will be 6V. This is higher than the acceptable tolerance for this device. This voltage is potentially dangerous and can potentially destroy the device. Another reason why batteries are impractical to run the devices is the fact that batteries cannot sustain the Raspberry Pi 2 for a long period of time before dying out.

3.7.3 Hardware Performance

Another aspect to analyze of a Microcontroller is its hardware performance. When comparing CPU speed the Raspberry Pi 2 ARM Cortex-A7 had the highest clock rate of any of any other CPU that was looked. Running at 900MHz the CPU is about 56 times faster than the ATMEGA328 of the Arduino Uno’s 16MHz and 11 times faster than the Tiva C’s ARM cortex M-4 80MHz processor. Not only is it multiple times faster than the other CPUs it is a quad core processor. The Raspberry Pi 2 also has Broadcom VideoCore IV GPU clocked at 250 MHz. An onboard GPU and high clock rate quad core CPU makes it perfect for high video computation which could be useful if we would do facial or voice recognition. For the memory the Raspberry Pi 2 has 1GB of memory that is shared with the GPU. The Tiva C ARM Cortex M-4 has 256 KB and the Arduino Uno ATMEGA328 has 32KB of memory. After looking at these specifications, the Raspberry Pi’s CPU performance clearly outmatches all of the other CPUs. This may seem attractive if we are doing high computations, however for doing any other operations such as unlocking a door or reading other sensors, it is unnecessary performance for what we are doing and the ATMEGA328 might not be able to do any advanced features if we are doing video streaming to the internet.

3.7.4 Microcontroller Peripherals

The Peripherals of the microcontroller is important to use because it dictates what and how many devices can be connected. For the Secured-E-Key project the microcontroller must be able to communicate with the GSM communication module, NFC reader, a camera, Infrared sensor and the door lock. The PIR sensor has a single bit high/low output communication. The NFC TRF970A has 3 I/O pins that must be wired. The TLL JPEG camera uses 2 I/O ports which uses TTL communication. The GSM SIM800H uses 7 pins to communicate to the MCU. Many microcontrollers come with many internal peripherals such as Analog to digital converters (ADC), Pulse Width Modulation (PWM), Real Time Clock (RTC), and General Pin Input and Output (GPIO). The microcontroller may require external peripherals such as USB, or an oscillator.

3.7.4.1 Internal Peripherals

The GPIO or General-Purpose input/Out is a generalized pin that has no specialized functionality. GPIO are mainly used on systems on a chip, embedded devices or programmable logic devices. GPIO can be configured to be an input or an output, or be enabled or disabled. Input values are readable typically being high being a 1 and low being a 0. This can allow the microcontroller’s sensor to read information but setting it as in input. The input GPIO can also be used as in interrupt which can be used to wake a microcontroller. The microcontroller can also control devices such as the lock by setting the GPIO as an output. The output values are writable or readable. In order to choose the microcontroller it must have enough GPIO to handle all of the peripheral requirements stated. The

Tiva C has 16, the Raspberry pi has 40, The Arduino has 14 and the LPC2148 has 45. The LPC2148 seems ideal for multiple sensors but all 45 pins won't be used. One attractive feature is that it can disable GPIO functions for optimizing power.

The PWM or pulse with modulation is a technique used to encode a message into a pulse signal. It is a form of modulation to encode information for transmitting a signal. It works by using a rectangular pulse waveform and varying the average value of the wave form. This is particularly useful for amplifying speakers if it were to be used for sound. Another useful aspect of this is that it could possibly drive servo motors to control its position possibly for a lock. Most of the microcontrollers come with this features including all of the microcontrollers researched.

ADC or analog to digital converter is a peripheral that converts a physical continuous signal voltage to a digital number that represents the signals amplitude. The conversion involves the input being quantized but introduces an error. To compensate for this multiple samples of the input are periodically converted. ADCs are useful for multiple applications, such as audio recording devices, digital signal processing such as TV tuners cards or measuring instruments. ADC is essential for Secured-eKey project for sensors detecting the presence at the door. The microcontroller must create a binary number to decide if a presence is at the door. The LPC2148 comes with two ADC with a maximum of 10 bit of data. This means that the possible values are between 0 and 1023. The voltage ranges from 0 to 3.3 volts being read with 0V representing 0 value and 3.3 representing 1023. Anything higher than 3.3V would still output 1023. The ATMEGA328 microcontroller has 1 ADC converter but has 6 analog input pins. An analogic multiplexer is implemented to allow 6 devices to be connected but it can only read one device at a time. The Atmega328 also has a 10 bit data that is converted. The voltage resolution ranges from 0V to 5 volts. The ATMEGA can have a 8bit mode which can be advantage for noisy environments. The Raspberry Pi 2 doesn't have an ADC which could cause more work to add implement an ADC to the project.

RTC or Real time clock is an integrated circuit peripheral that accurately keeps track of the current time. It is often in personal computers, servers or embedded systems. Keeping track of time may be used in Secured-eKey project to be used as a data log. When the door is unlocked or a sensor detects a presence, the microcontroller will be able keep and store a data log of the time these incidents occurred.

3.7.4.2 External Peripherals

The USB drive is an essential external peripheral device for a microcontroller. The USB is a strong consideration since all personal computer uses it to communicate to electronic devices. The USB maximum voltage is between 4.75V and 5.25V. The maximum capable current is .5 to .9A for general purpose USB. This should be more than enough for a computer to power the microcontroller. USB 2.0 is capable of having a data rate of 480 which is more than enough to program the microcontroller. USB physical features are useful for physical design since it the plug dimension sizes varies. This will allow better flexibility for PCB design.

An external peripheral that some microcontroller may need is an external oscillator component. These microcontroller may use it to generate a clock signal which some parts of the microcontroller system may require. For the LPC2148 the oscillator is used to generate the system clock and allows for data to be transferred for USB. Another implemented oscillator will allow the 2148 to have a real time clock. The ATMEGA328 and the ARM Cortex-M4F doesn't require a need for an external oscillator since it has an internal one.

3.7.4.3 Peripheral communication

Another aspect that must be considered for the microcontroller is the peripheral communication. Peripheral communication is a necessity for a microcontroller to interact and connect to its peripherals. There are two methods of communication serial and parallel communication. Serial communication conveys multiple bits simultaneously while serial communication conveys information on bit at a time. Most embedded systems use serial communication since it only requires one I/O pin. There are many serial communication interfaces to choose from for embedded systems. The main types of serial communications that were researched were RS-232, I2C and SPI. Table 19 shows the characteristics of the communication protocols researched.

3.7.4.3.1 RS-232

The RS-232 is a type of serial communication developed by the Electronic Industries Association. It is a complete standard not only in electrical characteristics but also physical characteristics that include the pin-outs and hardware connection that can be seen. The RS232 average transmission rate is about 20Kbps, more than enough for making simple communication to most peripherals. Data is sent by the transmitter varying the voltage above and below 3V. Typical RS-232 communication has a start bit, data bits, parity bits and stop bits. Another feature that the RS-232 is capable is full duplex operation. This means that it can simultaneously transmit and receive data.

3.7.4.3.2 I2C

The Inter-Integrated Circuit bus (I^2C) is a serial communication developed by Philips Semiconductors. It is half duplex which means that da, synchronous, bus which means that there are two clearly defined communication paths. The two wires are data serial data line (SDA) and clock line(SCL). These lines are controlled by pull up resistors and an open drain drivers. As a result I2C can consume more power than SPI. There is two way communications between the microcontroller and the peripheral but they can't communicate simultaneously. I2C is also a multi-master bus. This means that is a master/slave bus that can have multiple masters. This can be advantageous to use if a peripheral need to be controlled by multiple devices. Many peripheral devices support I2C because of the low general I/O pins required which makes it easier to program and easier to implement. I2C is especially used for DAC and ADC, which makes good for the PIR motion sensor.

3.7.4.3.3 SPI

The Serial Peripheral Interface (SPI) is a synchronous serial bus that was developed by Motorola. The SPI bus uses four signals for communicating; the master slave in (MOSI), master slave out (MISO), serial clock (SCK) and active-low slave select(/SS). The setup as a master and slave between the peripheral and the controller uses unidirectional communication for the MISO and MOSI lines to achieve high communication rates of 1Mbps. The disadvantages of the SPI is that the that wiring is more complex and more wires are need especially If there are multiple slaves which can be seen in the figure. Typical devices that can be good for this communication are USB, ethernet, or SD cards. Below is a table that compares all of the serial communication.

Table 18: Characteristics of Communication Peripheral Protocols

Name:	RS-232	I2C	SPI
Synchronous or asynchronous	asynchronous	synchronous	synchronous
Type	peer	Multi-master	Multi-master
Duplex	Full	half	full
Max Devices	2	varies	>1000
Max Speed	20	3400	3+1(8)
Pin count	2(4)	2	

3.7.5 Software Environment

The microcontrollers researched also include a software environment. Each of the microcontrollers software environments have their own implementation and functionality for the devices they run on. Each software has its own characteristics that can be beneficial to Secured-E-Key.

3.7.5.1 Tiva C

One of the software that is supported for the Tiva C is TivaWare. This software is maxed for TM4C12x which is a suite designed to simplify and speed up the development of the TM4C12x microcontroller applications. It has a free license and allows users to build full-function and easy to use code. The Tiva C is fully written in the C programming language. The library for TivaWare has a graphics library which contains a set of graphic primitive and widget that allows the user to create a graphical user interface. The Tiva C library also has a set of function that is used to control the peripherals. Another aspect of the TivaWare is that it has a PinMux Utility which helps users create custom schematics for applications. Another support TivaWare is CMSIS which is an ARM Cortex Microcontroller Software Interface Standard. The CMSIS DSP library has saved common algorithms which can help save time instead of creating it from scratch.

3.7.5.2 Arduino Uno

Arduino software is an IDE which is an integrated development environment. This is a software application that provides a full range of facilities to computer programmers. Arduinos IDE is also a cross-platform application that is written in Java. Other features include a code editor with features such as brace matching, syntax highlighting and automatic indentation. The program that is written in for the Arduino IDE and is called a sketch. This can be written in C or C++. Another easy feature of Arduino IDE is that it comes with a software library called Wiring. This is an open source electronic prototyping platform. This makes it easier for the user to make the common input and output operations.

3.7.5.3 Raspberry Pi 2

The software environment for the Raspberry Pi is Linux-kernel is it uses operating systems. Linux based operating systems generally require knowledge of its command line which may be complicated if the user have not used this platform. To make things easier a graphical user interface that resembles windows operating system. In order to use the operating systems a person has to use NOOBS installer. One operating system that can be installed into Raspberry Pi is Raspbian which is developed by an independent organization. The operating system is based off of Debian which is an ARM float hard float and was made to be optimized for the Raspberry Pi. Raspbian also comes with 35000 Raspbian packages. In order to use The SD card must be flashed. A minimum of 4GB of storage is needed to install it. Raspbian comes with Rasperry Pi software. This makes it very convenient to use and enable camera usage. By using the raspi-config the user can enable the camera module. Another useful feature of Raspbian Pi is that it comes with the gcc compiler that allows the user to create programs using c programs. It can also allow the user to manipulate the GPIO by direct register manipulation.

3.7.5.4 LPC2148

The software that supports the LPC2148 is is KEIL tool which is made by ARM. The program that it uses is called uVision. This software supports 8-bit, 16-bit

and 32 bit ARM microcontrollers. uVision offer software packages and configurations to support the ARM 9 and ARM 7 which is what the LPC2148 runs off of. This software package provides RAM functions that enable high speed interrupt code and in system flash programming. This could be helpful to help stream pictures from the camera by utilizing ARM 7 linear 4GB memory space. uVision also comes with a debugger that comes in two operating modes, Simulation and Target mode. Simulator mode helps simulate target systems such as peripherals that are connected to the microcontroller. Simulation mode can allow for software testing without the hardware environment. This can be helpful for simulating scenarios that would otherwise destroy the hardware peripherals.
The debugger feature also comes with target mode. This allows uVision to connect to the physical hardware. Driver packages make it possible to interface to these components. The emulator part of the target mode makes it possible to connect the microcontroller pins of the target hardware.

3.8 Camera Modules

One of the central elements of the project is a video camera that will record the presence of anyone that will approach at a distance of two (2) feet of the front door. This distance is reasonable because we want to record the door activities, because any longer distance would be very annoying in then sense that someone could be just passing by without being really interested in coming to the house; we do not want this information. The camera, once activated, will send the video to one of the house occupant's android device who will, at his/her desire, allow access to the visitor. The micro-video camera will be incorporated in a relatively small assembly that will be mounted in the lock system of the door. For that purpose, we had to consider different parameters like size, picture quality, voltage ect. in finding the right video camera. Therefore, in order to come up with the best camera that can fit our project adequately, we explored different video cameras from different brands and vendors, and among those studied we are going to talk about the TTL Serial JPEG Camera with NTSC Video, the HackHD - 1080p Camera Module, LW-MINI110 Camera Module and the FlyCamOne eco V2Camera Module.

3.8.1 TTL Serial JPEG Camera with NTSC Video

The TTL Serial JPEG Camera with NTSC Video is sold $ 39.95 by adafruit.com and a priori it shows some great features that could make it fit a project like Smart Key. Although it could accomplish some different tasks, according to the seller, it was built specifically for security systems and in that regard it can do two (2) main things which are: outputting NTSC monochrome video (with the capability of taking snapshots of that video in color), and transmitting those data over the TTL serial link. The advantage that video camera would offer because of the NTSC varies from higher frame rate – about thirty (30) frames per second – that would reduce visible flicker, to Atomic Color Edit, which is the ability to edit at any four (4) field boundary point without disturbing the color signal, and to less inherent picture noise – almost all pieces of video equipment achieve better signal to noise characteristics in their NTSC form. Besides that, this camera can snap pre-compressed JPEG pictures at 640x480, 320x240 or 160x120 which literally means it can make them nice, small and easy to store on a SD card, not to mention its particularity of having manually adjustable focus, auto — white — balance, auto – brightness and auto – contrast , and also motion detection. The camera has an operating voltage of 5 V and draws 75mA. Table 20 shows the specifications of the TTL Serial JPEG Camera.

Table 19: Specifications of TTL Serial JPEG Camera with NTSC Video

CMOS Pixels	30M
Pixel size	5.6µm x 5.6µm
Exposure	Automatic
SNR	45DB
Dynamic Range	60DB
Frame speed	640 x 480
Scan mode	Progressive scan
Viewing angle	60 degrees
Monitoring distances	10 meters, maximum 15 meters (adjustable)
Baud rate	Default 38400, Maximum 115200
Current Draw	75 mA
Operating Voltage	DC +5V

3.8.2 HackHD - 1080p Camera Module

The HackHD - 1080p Camera Module was one of the cameras that we looked at while we were working on this project. As a matter of fact, this camera present some very nice features that we could take advantage of in building Smart Lock. It is a relatively small camera that has the ability to capture video at a rate of thirty frames-per-second. As its name says it, it has a 1080p HD resolution with an aspect ratio of 16:9 which makes it very desirable, and it does not use more than 3.7V in operating mode. The camera size is 65x40x25mm and its video can be either stored on SD card to be viewed at a desired time, or fed to a device and streamed using open CV software. It can be activated just by pushing one single button, and that makes it easy to be controlled by a microcontroller or a simple sensor. For convenience purposes, the camera was designed so a LED can be attached to it to indicate its status. This camera module comes with a microphone that could be used to communicate with the person that is coming to the house in case we were interested in adding that feature to the Smart Lock, but that was not the case, considering the amount of work that we had to do. However, despite all those great features that the HackHD - 1080p Camera

Module comprises, it was not our choice because it is way too expensive when we consider all the other parts that we will need, because it is 159.95 dollars everywhere it’s listed like Sparkfun.com and Karlssonrobotics.com. Table 21 shows the specifications of the HackHD - 1080p Camera Module.

Table 20: Specifications of HackHD - 1080p Camera Module

Resolution	1080P HD
Frame Rate:	30 FPS
Coding	H.264
Aspect Ratio	16.9
File Format	AVI
Storage	SD card (2GB – 32 GB)
Lens	2.5mm (EFL), F2.8 160 degree (diagonal)
Control input	Single contact momentary switch
Video Output	Composite video
Power Supply	External 3.7V, 1100mAH minimum
Power Output	3.7V DC, 500mAH
Working Temperature	-10 degree C to +45 degree C
Storage Temperature	-20 deg C to +70 deg C

3.8.3 LW-MINI110 Camera Module

As we were doing our research for this project we fell on this website that is called ecvv.com that is selling the LW-MINI110 Camera Module for a ridiculously cheap price which is less than one USD. This camera module captured our attention when it comes to our project for many reasons. First of all, it is a very small unit that can be mounted without much difficulty in an electronic lock case that does not offer too much leverage. In fact, it’s the smallest that we have considered so far : 10mmX10mmX15mm of size. It has a very low illumination requirement which is 0.008Lux that makes it suitable for our project in the extent that it can capture pictures or video of very good quality in an almost dark environment, adding to the fact that its aperture coefficient of lens is 1.2. This camera also has a high speed image processing core, and its video will not be delayed even if the door where it is mounted moves with an abrupt motion. Its resolution is 520 TVLines, which is good enough to allow us to identify without any problem anyone that would walk towards the door. One of the unique features of this camera module is the fact that it does not require too much power. As a matter of fact its operating voltage is 3.3 V to 6 V, and its current 0.75 mA. The LW-MINI110 Camera Module is a video camera that is equipped with a microphone to allow us, if we were to choose it, to communicate with the visitor without having to add any microphone to the project. Table 22 shows the specifications of the LW-MINI110 Camera Module.

Table 21: Specifications of LW-MINI110 Camera Module

Size	10mmX10mmX15mm
Resolution	520 TVLines
Pixels	NTSC: 656(H)X492(V); PAL: 786(H)X576(V)
Illumination	.008 Lux/1.2
Sensor	1/3 CMOS
Lens and View Angle	0.5mmF2.0/55°
S/N Ratio	48dB
Function	Automatic Gain Control
Video output	1.0V p-p/75.0 ohm
Audio Output	1.0Vp-p/1Kohm
Operating Voltage	3.3V – 6V
Current	75mA
Operating temperature	-20°C to +50°C

3.8.4 FlyCamOne eco V2Camera Module

The FlyCamOne eco V2 Camera module cost 39.95 dollar on electronics123.com and it is capable of snapping pictures and it can record nice video as well. This camera is equipped with a speaker that is synchronized with the camera's function of recording videos; that is, it captures both images and sound while recording. This will be a plus to the extent it will allow any visitor to leave a voice message to the house occupant, without having to do anything else than talking, in the case access is not granted to him to the house. The pictures and video captured by the FlyCamOne eco V2 have a resolution of 720X480 at a rate of 30 frames per second. According to the information available on the supplier website, this camera has one green LED and one red LED that respectively indicate when it is on standby and when it is recording. This camera module is equipped with a ribbon through which the data is transferred from the camera itself to the board, and once this data is available on the board it can either be send to SD card or be fed to a device and streamed using open CV. Contrarily to the previous camera modules that we considered in this project, this camera module is built in a pivoting head that cannot be mounted inside the case an electronic lock as we would like it to be; however, it can be easily mounted at desired position on the door itself. The module is also built with a mini-USB that is used to transfer the data that was transferred primarily to the mother board. To aliment the camera we will use a 3.7 Volt and 1000mAh Lithium-Polymer battery.

Definitely, because of all these features that fit very well our Smart Lock project, we have decided to use the FlyCamOne eco V2 in our project instead of any of the other ones that we talked about. Table 23 shows the specifications of the FlyCamOne eco V2.

Table 22: Specifications of FlyCamOne eco V2Camera Module

Size	30mm X 57mm X 7mm
Camera Lens	22mm X 24mm X 28mm
Resolution	720 X 480 pixel
Operating Voltage	3.7V
Weight	15 g
Rate	30 FRS
Storage	SD card 8GB

3.9 Door Lock Systems

Our project is about home security; that is, most of the elements that are going to be implemented in the system will contribute to enable us to remotely control the lock. Therefore, we need an electronic lock that can suit our project. For that purpose, as we did for the previous parts, we have researched a relatively wide variety of locks in order to find the one that fits the best our Smart lock project. Among those researched, we are going to talk about The Lockey E-910 R, The Morning Industry Single Cylinder Brass Touch Pad and Remote Electronic Deadbolt-QF-01P, Diax MVM Motorized Electric Rim Lock and The Gatehouse Electronic Motorized Deadbolt.

3.9.1 Lockey E-910 R

The Lockey E-910 R costs 89.93 dollars on handlesets.com. This lock system has an LED illuminated keypad that is very convenient at night time. The many features of that lock include a six available user codes, a one-time user code. It also has the auto-stop function and audible and visual confirmations. One of the things that are so special about The Lockey E-910 R is the fact that it comes with a quick user code changing that allows the user to reset his or her code, and it’s programmed to be connected to a remote control for faster access. It’s also equipped with an auto latch bolt locking detection that prevents incomplete door locking, so if by inadvertence someone leaves without locking the door, it will be locked automatically after a few seconds. It’s easy to install and it does not require much complication for the connection because it just takes 4 AA batteries, therefore no wire is needed. After carefully examining the Lockey E-910 R, we have decided not to utilize it in the Smart Lock project because its housing is not big enough to house all the different parts that are going to be utilized. Table 24 shows the specifications of the Lockey E-910 R.

Table 23: Specifications of Lockey E-910 R

Outer Size	5 1/2”H x 3 1/8” W x 1 3/16”D
Inner Size	7 1/4”H x 2 3/4”W x 1-3/4”D
Backset Size	2-3/4’’, 2-3/8’’
Fits Door Thickness	1 3/8’’ – 2’’
Operating Temperature	-4°F - 185°F
Bolt Type	Motorized
Number of User Codes	6
Height	5.5, 7.25
Door thickness	1-1/2’’, 2’’
Cross Bore	2-1/8’’

3.9.2 Morning Industry Remote Electronic Deadbolt-QF-01P

Our research led us to the Morning Industry Single Cylinder Brass Touch Pad and Remote Electronic Deadbolt-QF-01P that can be bought for the amount of $169.99. This lock system has an unlit keypad that allows the combination of up to 10 user codes that can be entered from thirty feet away from the door through a remote control that comes with the lock. One of the things that are unique with this lock is the fact that you can program as many remotes as the number of user codes. The lock was built for residential usage and has a very nice polish Brass finish that would elevate the éclat of a brand new door or heighten the shine of an outmoded one. It comes with a set of two keys that can be utilized if for any reason the electronic features would fail; added to that, the deadbolt uses a common 5-pin SC keyway for security and can be re-keyed to match other 5-pin SC keys. This lock system is reliable because it is graded III by the American National Standard Institute. The Morning Industry Single Cylinder Brass Touch Pad and Remote Electronic Deadbolt-QF-01P Deadbolt presents a lot of features that could make it fit our Smart Lock project, but if we choose it we would have to replace most of its electronic components and to add more parts that would not fit in its body case, and that would require a lot of transformation that is unnecessary. For that reason the Morning Industry Single Cylinder Brass Touch Pad and Remote Electronic Deadbolt-QF-01P will not be utilized in this project. Table 25 shows the specifications of the Morning Industry Remote Electronic Deadbolt-QF-01P.

Table 24: Morning Industry Remote Electronic Deadbolt-QF-01P Specs.

Outer Size	5.75’’Hx3.25’’Wx0.25’’D
Inner Size	5.75’’Hx3.25’’Wx1.75’’D
Operating voltage	4 AA batteries
Bolt Type	Sgl Cyl Deadbolt
Number of User Codes	10
Height	5.75
Door thickness	1-3/8’’ to 1-3/4
Cross Bore	1.25’’

3.9.3 Diax MVM Motorized Electric Rim Lock

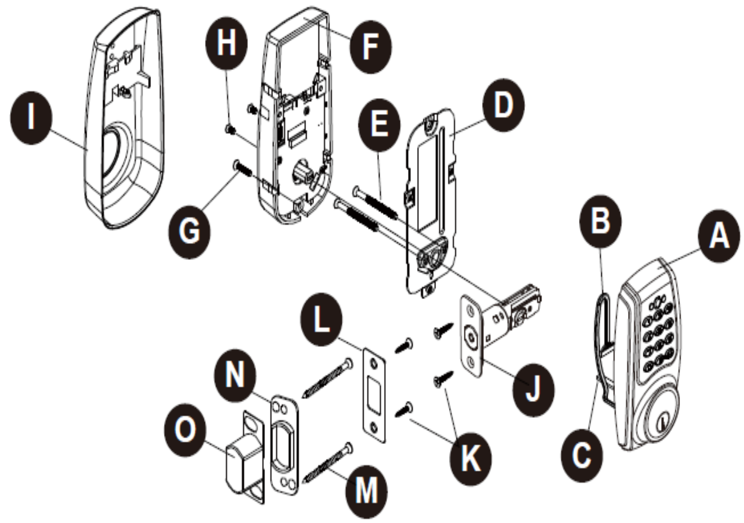
The Diax MVM Motorized Electric Rim Lock is a lock that can be found at locksonline.co.uk for the cost of £ 61.43, an equivalent of $65.88 US at the time that we are working on this project. At the opposite of all the previous lock system that we already considered, the Diax MVM Motorized Electric Rim Lock is a very simple electric lock system that mainly features a motorized deadbolt that is powered by a 12V DC voltage. The lock is equipped with an adjustable cylinder follower, a secure fasten cylinder, and it comes with adjustable length screws. This lock is known for his high level of security for pedestrian gates, internal and external doors. The way it functions is simple button that the user pushes on in order to trigger the release of the deadbolt or to pull it back. When the door is pushed back, if it goes all the way, it will close automatically—a feature that can be overridden when we will implement all the different features of the Secured-E-Key. As several different electronic lock, the Diax MVM comes with a set of three keys to override its electronic ability in the event that there is malfunction in the electronic system. One of the things that make this lock different from the other ones besides its simplicity is the audible feedback that allows the user to feel when the deadbolt is engaged or returned. It is also good to mention that it suits all type of doors—metallic or wooden. The mounting is a very simple process because it does not require any special skill. The product comes fully assembled, and to mount it we just need screw driver, a ruler to get the right measurement in order to position the lock properly, and a pencil. The door is 120 mm wide, 100mm high and 40mm deep. After carefully looking at all those lock systems in the light of what we really need for our project in term of lock, we have decided that the Diax MVM Motorized Electric Rim Lock is the lock that is not going to be utilized on the Secured-E-Key. In fact, the main reason we were interested in that lock is its simplicity. Its implementation will not require much work; just a simple connection to the microcontroller will be necessary. However, it requires too much power. Its operating voltage is above the capacity of our power system.

3.9.4 The Gatehouse Electronic Motorized Deadbolt

The Gatehouse Electronic Motorized Deadbolt can be found at Lowes for the amount of 74 dollars and it was built for residential usage. This lock system is equipped with a 10-digit keypad that allows the user to setup up to 10 different codes, and an alarm that goes off if someone tries to mess up with system or after four unsuccessful attempts. The lock system is self-powered with 4-AA batteries that not only sustain the functionality of the lock system but also provide power for the LED indicator of the batteries status and the enlightened keypad. The lock system is user friendly to the extent that it allows the user to reset the system to factory setting if the code is forgotten, and also to delete the codes one by one or altogether as wanted. The lock can function manually by pushing a button or as regular lock if there is an electronic problem by using the key, and it has an auto locking mode that will lock the door after ten seconds. Once the automatic mode is activated, there will be a beep sound coming from the lock and an LED will flash to indicate that the latch has been engaged and the door is locked. When we consider carefully the features and specifications of the Gatehouse Electronic Motorized Deadbolt through the light of the requirements of the Smart Lock, we have decided that The Gatehouse Electronic Motorized Deadbolt is the lock system that is going to be utilized in the Smart-Lock project because of its size. In fact, among all three of them that we researched on for the purpose of that project, it is the only one that shows the dimension that can match the need of the Smart Lock. Table 26 shows the specifications of the Gatehouse Electronic Motorized Deadbolt and Figure 4 shows the different parts that make up the Gatehouse Electronic Motorized Deadbolt.

Table 25: Specifications of the Gatehouse Electronic Deadbolt

Outer Size	6.75’’ H x 3.5’’ W x 1.15’’D
Inner Size	8.25’’ H x 4.0’’ W x 1.4’’D
Number of Cylinder	1
Security Grade	2
Backset Size	Adjustable
Fits Door Thickness	1-3/8-in to 1-3/4-in
Projection	1.4-in
Bolt Type	Motorized
Number of User Codes	10
Power source	4 AA batteries
Alarm	Audible



PART	DESCRIPTION	QUANTITY
A	Exterior Assembly	1
B	Power Strip	1
C	Tailpiece	1
D	Mounting Plate	1
E	2-1/8 in. (54 mm) Mounting Bolt	2
F	Interior Assembly	1
G	13/16 in. (20.5 mm) Screw	1
H	5/16 in. (8 mm) Screw	2

PART	DESCRIPTION	QUANTITY
I	Interior Cover	1
J	Latch	1
K	3/4 in. (19 mm) Wood Screw	4
L	Strike Plate	1
M	3 in. (76 mm) Wood Screw	2
N	Reinforced Strike Plate	1
O	Dust Box	1

Figure 4: Image to the Different Parts of the Gatehouse Electronic Deadbolt (Printed with Pending permission)

3.10 Audio

One of the interesting features of the Secured-E-Key is its capability to allow the visitor hear a prerecorded message that welcome him or her to the house. The way that is supposed to work is once the door is open, the sensor will send the message to the microcontroller and will release the message. The audio components that were researched included various speakers and microphones.

3.10.1 Speakers

For the purpose of Secured-E-key, we needed a speaker with the characteristics of size, power consumption and sound quality. As we did for all the other parts that we are using in that project, we analyzed a variety of speakers in order to find the one that fits our smart lock. Among those that we analyzed, we will talk in this paper about the Piezo Speaker COM-07950, and the Mini Metal Speaker from Adafruit.

3.10.1.1 Piezo Speaker COM-07950

This is a small round speaker that cost $1.95 US on sparkfun.com. It has the capability to operate around an audible range of 2.048 Khz. According to the seller, it is the kind of speaker that fits a small project like the Secured-E-Key when it comes to create simple music or user interface. This speaker has an operating voltage of 3.5 V, and its maximum current consumption does not go over 35 mA. Its coil resistance is about 42 ± 6Ω and outputs a sound of 85 dBA. It is good for outdoor projects because it can resist temperatures in the range of -20°C to + 60°C. It is a small speaker at 12 mm in diameter. However, its height of 8.5 mm is too big to make it fit inside of the outer case of the Gatehouse lock system that we are using for this project. Because of that reason, the Piezo Speaker COM-07050 will not be utilized for Secured-E-Key. Figure 5 shows the graph of its frequency response in a range of 20 Hz 20,000Hz.

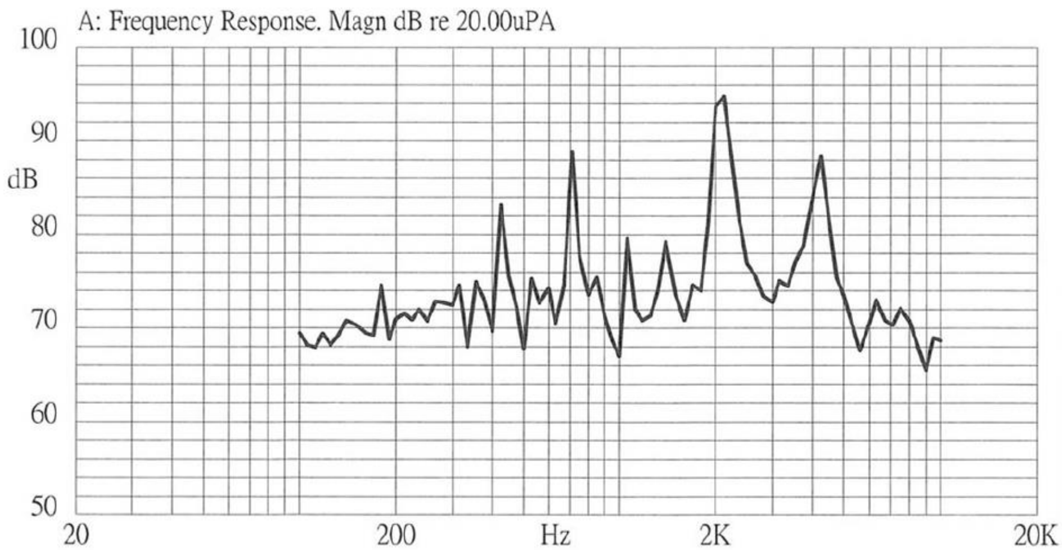


Figure 5: Graph of the Frequency Response of the COM-07050
(Printed with Permission)

3.10.1.2 Mini Metal Speaker

The other speaker that we researched was the Mini Metal Speaker that can be found at adafruit.com for the price of $1.50 US. It is a very small speaker that has less internal resistance than the previous one. Actually, it was designed for small project that does not require more than 8Ω and it consumes less than 0.5 W in operating mode. It has a flat cone shape and its metal body is extremely light according to the description that is available on the user's website. They say it works great with D amplifier board that is the analog signal to be amplified will be converted to a series of pulses by pulse width modulation and pulse density before being applied to the amplifier. One of the advantages of that speaker is the fact that is more efficient than analog amplifier, with less power dissipated as heat when it is in active mode. The speaker has a diameter of 28 mm and a height of about 3.5 mm. Its frequency goes from 600 Hz to 10 Khz with and operating temperature that varies from -20°C to + 55°C. The Mini Metal Speaker is the speaker that we will use in that project because of its height. It fact, it is so flat that it will fit very well inside of the case of the gatehouse lock where it is going to be incorporated. Figure 6 displays the graph of its frequency response from 20 Hz to 20,000 Hz.

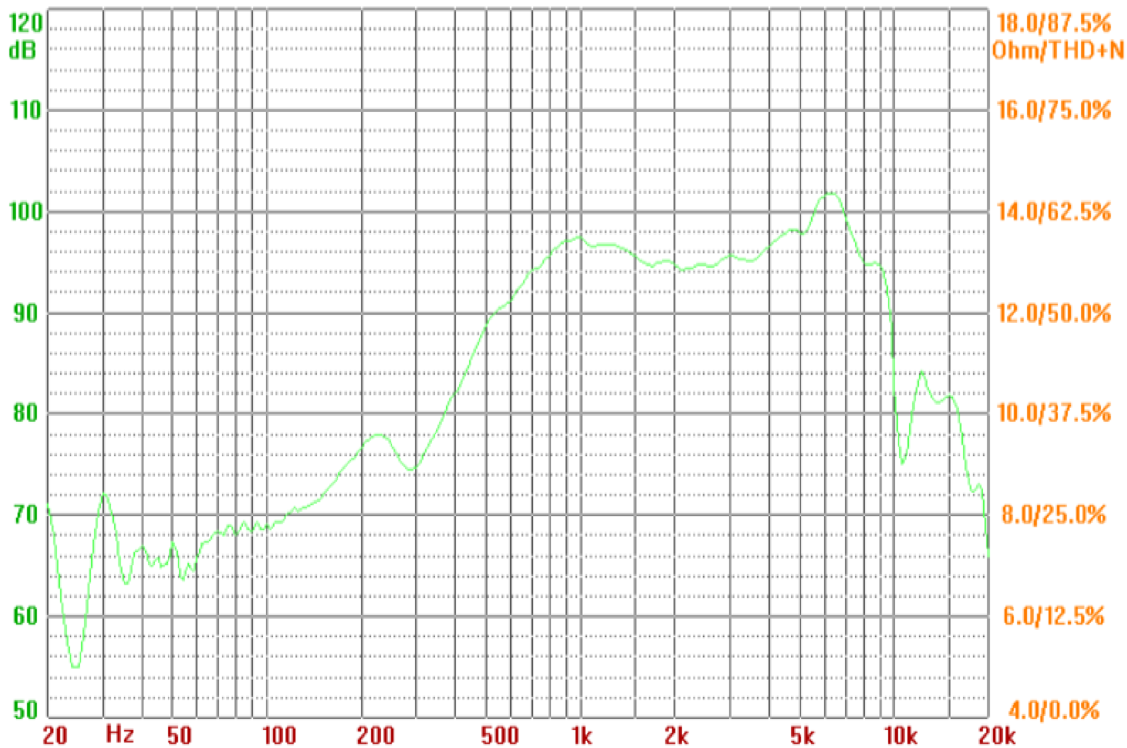


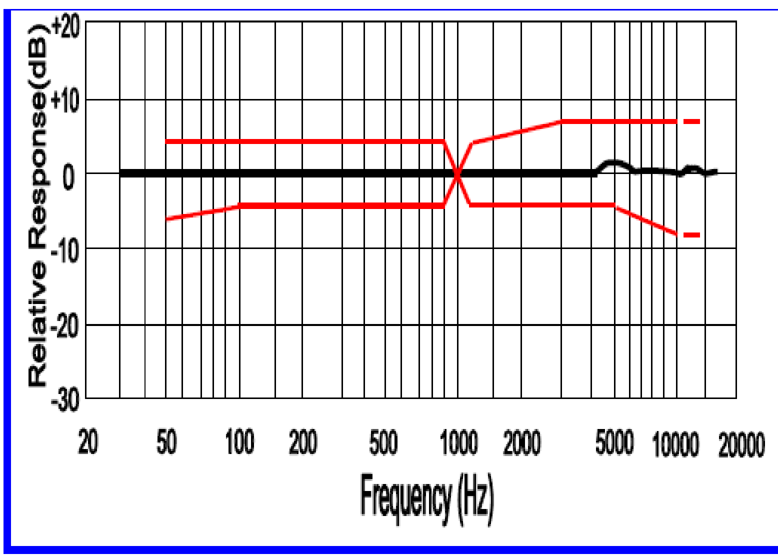
Figure 6: Graph of the frequency response of the Metal Speaker
(Printed with Permission)

3.10.2 Microphones

One of the unique features that we primarily intended to incorporate in the Secured-E-Key is the ability to communicate with the visitor. For that purpose, we wanted to integrate a microphone in the system, so anytime someone walks to the door, his or her presence would activate the recording system and send the message to the user who would respond at his or her wish. For that reason we researched different microphones in order to choose the one that would fit better the Secured-E-Key project, in terms of size, sound quality, power consumption and some other factors that can affect the design of our project. Among those that we researched, we are going to talk about the BOB-09964 Electret Microphone, the CMA-4544PF-W Electret Microphone, and the Electret Microphone Amplifier - MAX4466 with Adjustable Gain.

3.10.2.1 BOB-09964 Electret Microphone

The BOB-09964 was considered with respect to this project because of its specifications that somehow match the requirements of the Secured-E-Key. This microphone can be found at Sparkfun.com for $7.95. It is a very small device that can be coupled with 100 x op-amps to amplify the sounds of voice, steps and door-knocks. Actually, its diameter and height are respectively 9.7mm and 4.5mm. The sound produced by the microphone is big enough to be picked up by a microcontroller's Analog to Digital converter. This unit would not require much effort from us because it comes fully assembled. It has and operating voltage that varies from 2.7 V to 5.5 V. The BOB-09964 is an Omni directional microphone that can give a very good performance because of its sonic qualities, low handling wind and pop-noise effect. Its frequency is in the range of 100 to 10,000 Hz with a maximum current usage of 0.5mA, and its sensitivity is -46 ± 2.0 at 1 KHz with maximum sensitivity to noise ratio of 58 dB. It is also easy to install with its three pins of 4.5 mm long, 0.6mm diameter and 2.54mm spacing designated to the voltage source, the ground, and the audio. One of the most interesting factors of the BOB-09964 is its operating temperature that varies from -20 degrees Celsius to 60 degrees Celsius. This is very important for the project because the Secured-E-Key requires a microphone that can be very resistant to the severity of the weather because the microphone, according to the design, was going to be mounted on the outside of the door, and would have to face the different level of temperature. Figure 7 shows the graph of the frequency response of the BOB-09964 and Figure 8 shows the schematic of the gain stage microphone that we are printed with permission of the website.



Frequency (Hz)	Lower Limit (dB)	Upper Limit (dB)
50	-6	+3
100	-3	+3
800	-3	+3
1000	0	0
1200	-3	+3
3000	-3	+8
5000	-3	+8
10000	-8	+8

Figure 7: Frequency Response BOB-09964 Electret Microphone
(Printed with Permission)

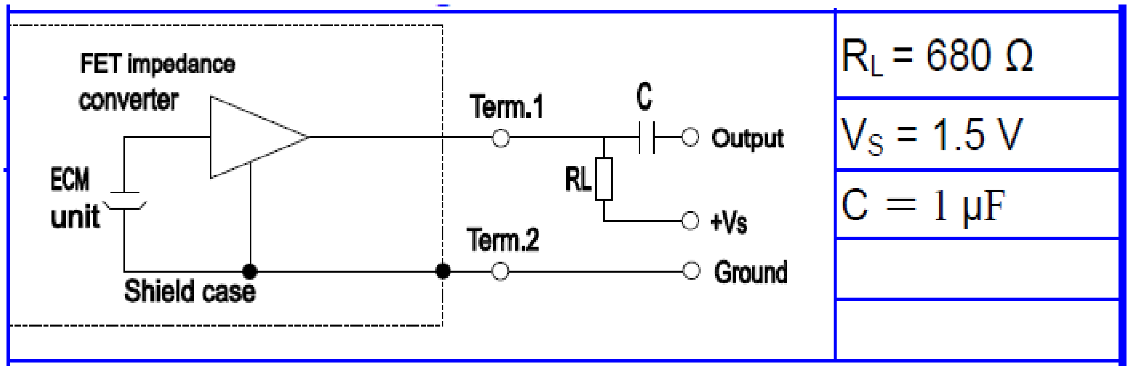


Figure 8: Schematic of the Gain Stage of the BOB-09964
(Printed with Permission)

3.10.2.2 CMA-4544PF-W from Adafruit

The Electret microphone CMA-4544PF-W is very microphone that costs $0.95 at Adadfruit.com. It is a very small microphone designated for embedded project like the Secured-E-Key, and its dimensions are 9.7mm of diameter and 4.5 mm of height. However, contrarily to the previous one, it does come fully assembled. It contains a vibrating element that will out put a few millivolt peak-to-peaks. We would need and an op-amp to amplify the signal so it could match our expectation; some chips are designated with the amplifier built in in which case we can wire up directly. As the previous one, this microphone is an Omni directional microphone that can give a very good performance because of its sonic qualities, low handling wind and pop-noise effect, and the drawback of the use of an Omni-directional is not to fear in that case because we are using only one microphone, so there would be no proximity disturbance. The Electret microphone CMA-4544PF-W has a sensitivity of -44 ± 2 dB at 1 KHz with signal sensitivity to noise ratio of 60 dB. Its frequency varies from 20 to 20,000 KHz with respectively a standard operating voltage and current consumption of 3V and 0.5mA. This microphone is mainly made of Aluminum, therefore it is very light. Its terminals are pin type, they are hand soldering only, and the entire device weights about 0.80 g. We would like to mention also its operating temperature of -20 degrees to +70 degrees that makes it very resistant to either very cold or very high temperature. The output of the microphone will be connected to a capacitor of 1μF and external load resistance of 2.2KΩ. Figure 9 shows the graph of the Frequency Response of the Electret microphone CMA-4544 PF-W and Figure 10 shows the schematic of the gain stage of the Electret microphone CMA-4544 PF-W.

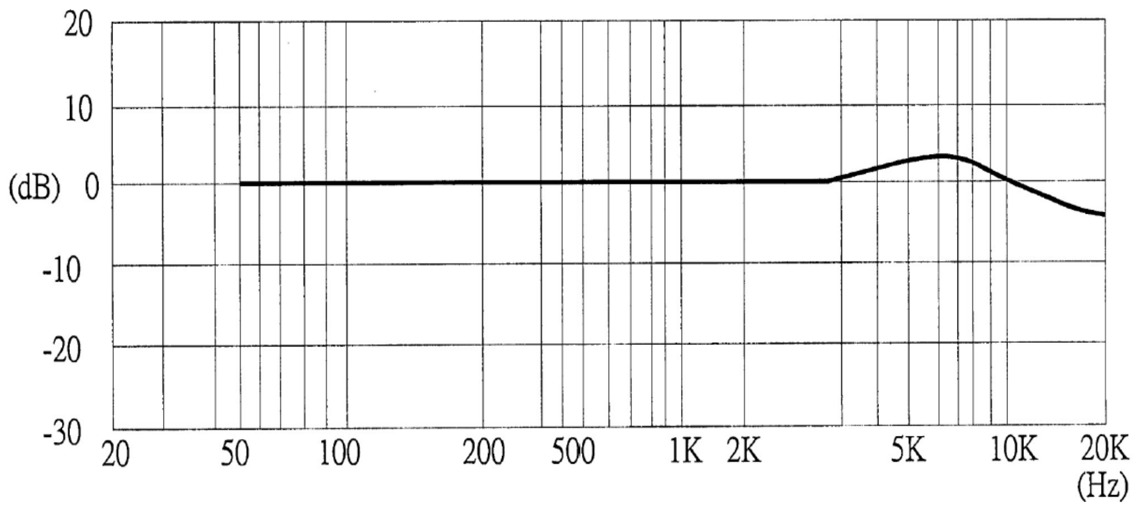


Figure 9: Frequency Response of the Electret microphone CMA-4544PF-W
Printed with Permission

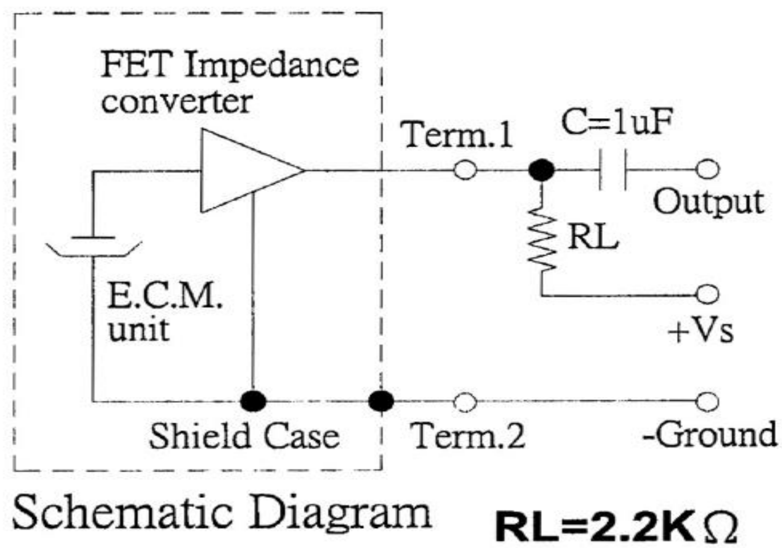


Figure 10: Gain Stage Schematic of The Electret microphone CMA-4544PF-W
(Printed with Permission)

3.10.2.3 Microphone Conclusion

When we really looked at both microphones that we just described, we saw that obviously both of them could fit to some extent the Secured-E-Key. In fact, either one of them could provide the sound quality that we need quality, have the size and the overall performance required. However, we have chosen to utilize the BOB-09964, because it coms fully assembled and requires less operating voltage. Table 27 shows a comparison of the characteristics of each microphone researched.

Table 26: Comparison of the Microphone
(Parameters Referenced from Datasheet)

Model	BOB-09964	CMA-4544PF-W
Operating Voltage	1.0 V to 10 V	3 V to 10 V
Operating Current	0.5 mA	0.5mA max.
Operating Frequency	100-10,000 Hz	20-20,000 Hz
Output Impedance	680 KΩ	2.2 KΩ
Size	9.7mmX4.5mm	9.7mmX4.5mm
Sensitivity	-46 ± 2 dB	-44 ± 2 dB
Signal to Noise Ratio	58 dB	60 dB
Operating temperature	-20°C to +60°C	-20°C to+70°C
Directivity	Omni-directional	Omni-directional
Weight	0.7g	0.8g
Easiness	Easy	Less easy

3.11 Light-Emitting Diodes

Despite the fact that the lock that we are intended to use in the Smart-Lock project has LEDs that are used for different purposes, since we are not going to utilized most of the features of the lock system, we are planning on installing our own LEDs, in that case two of them, to show the status of the battery. A green LED to indicate that the battery is in good condition and a red LED to alert that the battery needs attention. We choose to use LEDs as indicators because in today's technology, LEDs play a big role for many reasons including its flexibility and power consumption. In fact LEDs come in all kind of shape and size and they are the most energy efficient light producers. For this project, we are using surface-mount diode (SMD) instead of through-hole because the surface-mount LEDs have a lot more advantages than the through-hole. The SMD is bonded onto the PCB surface, allowing better heat dissipation and higher component density. As a result, they have higher energy efficiency, higher lumen output, higher color rendering index (CRI), lower lumen depreciation and better thermal resistance. We are using a red LED that has a wavelength that varies from 610 nm to 760 nm and produces a light of 3500 milli-candelas (mcd) that is very good when we consider the color, and a green LED with a wavelength that goes from 500 nm to 570 nm that has a luminosity of 11000 mcd. These LEDs have respectively a power consumption of 110 mW under a temperature that can go from -25°C to 85°C, and 120 mW with an operating temperature of -40°C to 100°C.

The red LED that we are planning on using is the kingbright's AA2214SES/J3-AMT. This LED is made of AlGaInP and its size is 2.2X1.4mm. It has a reverse voltage of 5 V and DC forward current of 50 mA with an electrostatic discharge threshold (HBM) 3000 V which is high enough to protect the LED from burning. And the green LED is the AA2214CGsK from kingbright also. It is made of the same material and has the same dimension as the red LED, but its power consumption of 75 mW is less than for the re LED which is 150 mW. That being, the LEDs' power usage is not going to be our main problem in designing the power system for the Secured-E-Key.

3.11.1 Timers

Even though LEDs are energy efficient, we think that having them on all the time would be to waste the power that is needed to operate the system. To palliate to that situation, one of the option that we could opt for is to install a flasher that will have the ability of lowering the power consumption by flashing the light instead of leaving them steady all time, and at the same time it will switch LEDs when either the battery is in good condition or goes down. Figure 11 shows the schematic of the Flasher circuit.

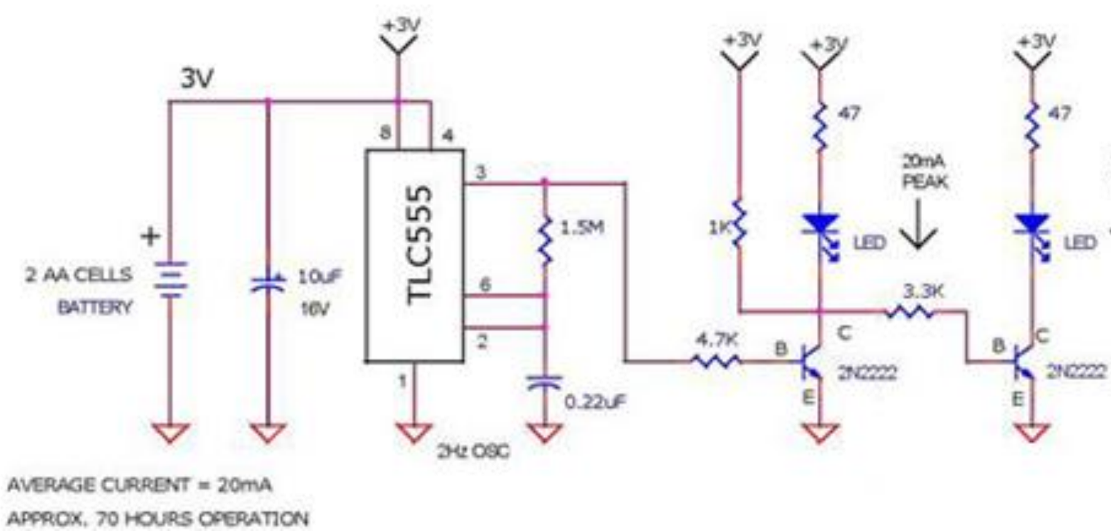


Figure 11: The schematic of the Flasher circuit
Printed with pending permission

3.11.1.1 TLC 555I Timer

As for this flasher, we can use a timer to provide time delay between the flashes for the purpose of saving energy. The timer TLC 555C from TI, which is the most common timer that is being used for decades or the TLC 555I that can give us about the same performance; however, it would require a little bit more power. The TLC 555I has a threshold voltage that varies from 0.95 V to 1.65 V. That means when the voltage at Pin-6 denoted (THR) is in that range which is supposed to be 2/3 of the value of Input voltage (Vcc), the output of the timer is at logic-0; that is, it is on low. Its minimum and Maximum trigger voltage are respectively is 0.4 V and 0.95 V; that is, whenever the voltage at the trigger Pin (# 2) is in that range which is less than 1/3 of Vcc, in our case 3V, the timer triggers and the output Pin is on high. The amplitude and minimum pulse width required for triggering depend on the voltage of the timer and its operating temperature. However, the operating temperature of the TLC 555I varies from -40 degree Celsius to 85 degrees Celsius, which makes it apparently suitable for the Secured-E-Key. The TLC 555I outputs a voltage of 2.5 V to 2.85 V which in our case would be enough to turn on the LED; so, in that regard, this timer could fit perfectly our project. However, when we consider its trigger voltage, it would be too low for our system that will provide a minimum voltage of 1.8 V to trigger Pin. If we would have to choose it, it would be damaged from the start. For that reason, the TLC 555I will not be utilized in the Secured-E-Key.

3.11.1.2 CSS 555 Timer

The CSS 555 micro-power is a timer can be found at customsiliconsolutions.com. It operates the same way as the TLC 555I; however, it has some very important characteristics that differ it from the previous one. It outputs a voltage in the range of 1.35V to 4.73V depending on operation mode. But most important of all, its trigger voltage varies from 30 to 36 percent of the Vcc which can be, in our case, 1.8 V if Vcc is set up to 5V – a very probable case. That makes it suitable for our project in that regard. Moreover, the CSS 555 micro-power timer consumes very little power and it is equipped with EEPROM that gives it the ability to conserve its setting even in the case of power loss. Therefore, after careful considerations, we decided to utilize the CSS 555 micro-power as the timer needed to flash the LEDs in the Secured-E-Key project. Table 28 shows a comparison of the characteristics of each Timer researched and Figure 12 shows the schematic of the CSS555 Micro-Power.

Table 27: Comparison of the Timers with Referenced Datasheet Information

Model	TLC 5551	CSS 555 Micro-Power
Trigger Voltage	0.4 V to 0.95 V	From 30% to 36% of VCC
Output Voltage	2.25 V to 2.85 V	1.35 V to 4.73 V
Operating Temperature	-40°C to 85°C	Not specified
Threshold Voltage	0.95 V to 1.65 V	Not specified

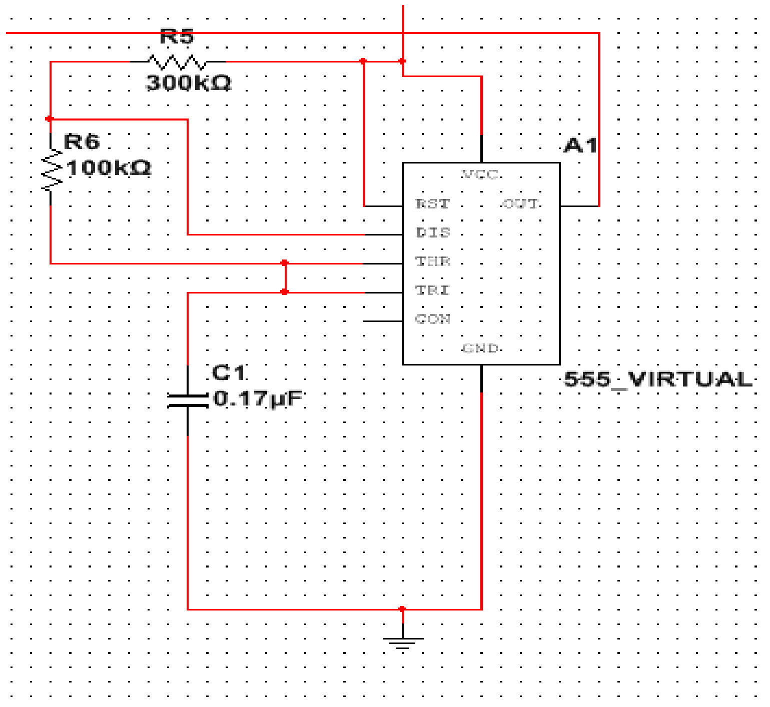


Figure 12: Schematic of the CSS555 Micro-Power

3.11.2 Voltage Comparator

The LEDs that are designated to indicate the status of the battery is a very important part of the Secured-E-Key project to the extent that without anything to show if the battery is in good shape or not, we could be running out of power and not knowing anything about that. This problem could result in the dysfunctionality of the Secured-E-key, and that would contradict the very meaning and purpose of that project which is SECURITY. For that purpose, as stated in a previous section in the Hardware part, one red and one green LEDs will be used to respectively indicate the status of the battery. To achieve that goal, we have opted to use a voltage comparator with an Op-Amp that is less problematic than the first 2 options that we talked about. However, we will include the CSS 555 timer in the design in order to produce the flashing of the LEDs. We will talk more about this voltage comparator when we will work in the design section, but for now let us just say that basically depending on the voltage of the battery, one LED will flash at a time. Figure 13 shows the mathematical expression that can explain how the voltage comparator will work. Figure 14 shows the schematic of the representation of the voltage comparator's circuit.

$$V = \begin{cases} V_{s+},; if\ V_1 > V_2 \\ V_{s-}; if\ V_2 < V_2 \\ 0 \quad ; if\ V_1 = V_2 \end{cases}$$

Figure 13: Equations of the Voltage Comparator

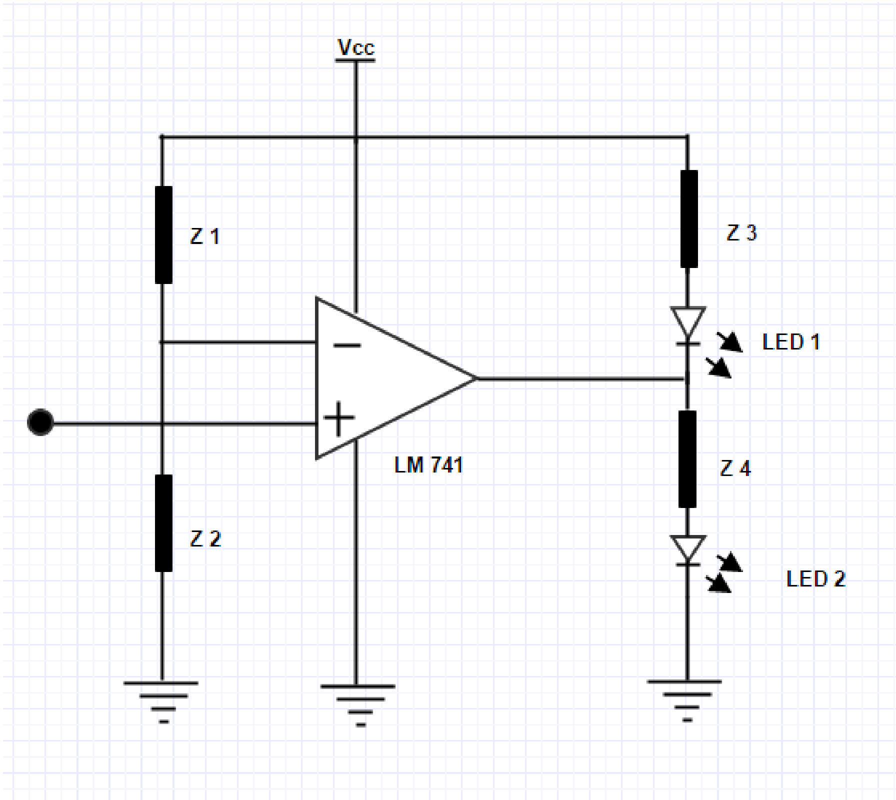


Figure 14: Voltage comparator for the LEDs

4.0 DESIGN EXPECTATIONS

4.1 Hardware Development

For Secured-E-Key the hardware components decided upon were specifically chosen because each of these components best fit the necessary requirements and specifications for the hardware design. Each of the components are explained in detail of its given parameters and how it will be implemented into the Secured-E-Key lock.

4.1.1 Power Supply

Each electronic device that will be used will have its own voltage and current requirement. Many of these voltages can vary significantly which can range from 3.3 to 5v. All of the voltage and maximum current drawn can be seen on Table 29. This will be helpful when choosing the right regulators to use to regulate the voltage that is being sent to each device.

Table 28: Secured-E-Key Maximum Voltage and Current of Peripherals

Component	Min Voltage Input (V)	Max Voltage Output (V)	Max Current Load (mA)	Power Dissipated (W)
NFC TRF7970A	2.7	5.5	130	.715
PIR Sensor (#555-28027)	3	6	3	.018
NXP LPC2141	3	3.6	90	.324
Oscillator	3.3	5	50	
SIM800H	3.4	4.4	200	.880
Gyroscope MAX21000	1.71	3.6	100	.36
FlyCamOne Cam v2	3.7	6		
MAX232	-.3	6	8	.048

4.1.2 Regulator Circuit Parameters and Functionality

The regulators chosen are implemented into a circuit design that will be utilized in Secured-E-Key. Each circuit design has a given purpose for various hardware components within Secured-E-Key which will help function the lock as one unit.

4.1.2.1 TPS62173 Circuit

The TPS62173 switching regular device's voltage output will be set to 5V and will be used to power the Fly Cam One v2, the electronic lock, the MAX232 and the PIR sensor. The TPS62173 has 8 pins that are used for the devices operation. PGND located at PIN 1 is the ground state. VIN at PIN 2 is the battery power source that will be used as the input voltage. EN at PIN 3 is an input pin that can enable or disable the use of the device. AGND at PIN 4 is the analog ground. FB at pin 5 is the voltage feedback that can change the output voltage value by using a voltage divider. VOS at PIN 6 is an input pin that senses the output voltage for control loop circuitry. SW at PIN 7 is a switch node, connected to the internal MOSFET helps make the device operate and function. PG at pin 8 is an output pin that shows if the output voltage is above or below the normal regulation voltage. The TPS62173 regulator is designed using RLC elements to build the circuit. A 2.2uH is connected to the output SW. An LC filter is made by combining L1 and Cout in parallel. A 2.2uH inductor and a 22uF capacitor were chosen based on the recommended specifications. This will effectively help stabilize the switching device creating a double pole for the corner frequency and converter. To help stabilize the input voltage for transient events and to decouple the converter from the supply, an input capacitor Cin of 10uF was used in parallel to the input voltage. Finally a pull up resistor of 100k ohms was placed at PG to pull the logic levels to make a High=VOUT and a low showing VOUT is less than the regulated voltage. Figure 15 shows the TPS62173 circuit design.

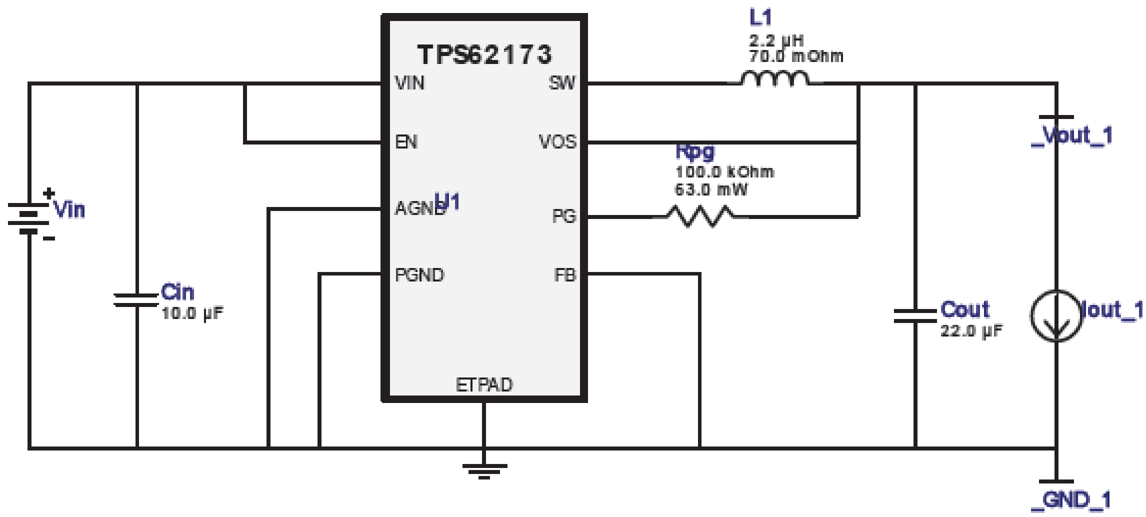


Figure 15: TPS62173 Circuit Design

4.1.2.2 TLV73325PDQN Circuit

The TLV73325PDQN linear regular device voltage output is fixed at 2.5V. The device will regulate the voltages for the gyroscope and the LED status indicator. The regulator has a total of 5 pins. The EN located at pin 1 is an output enable pin. The function of this pin will turn on the device if the pins input voltage is greater than .9V or turn off the device if the voltage is less than .35V. GND at PIN 2 is the ground pin. IN at PIN 3 is the power source input. PAD at PIN 4 doesn't have any internal connection, therefore serves no purpose. The OUT at PIN 5 is the output voltage pin for the device. Since the TLV73325PDQN is a linear regulator, few passive components are needed to build the circuit. Only 2 capacitors used for the circuit design. The Cout and Cin capacitors are set at 1.0uF and are used to optimize the output's transient response. Figure 16 shows the TLV73325PDQN Circuit Design.

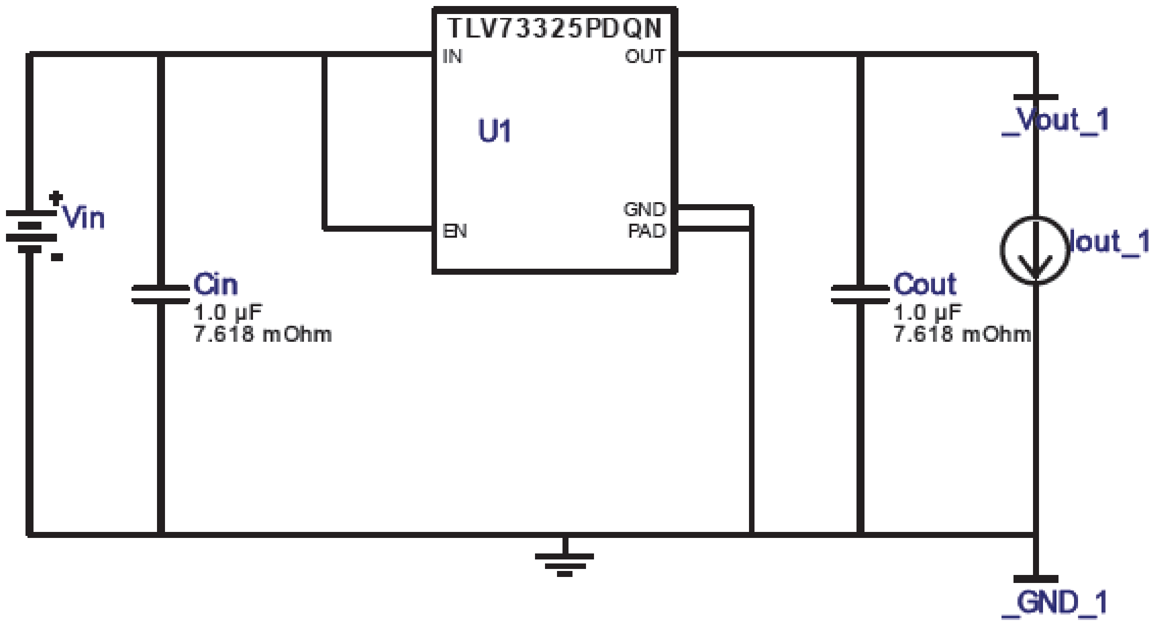


Figure 16: TLV73325PDQN Circuit Design

4.1.2.3 TPS62140A Circuit

The TPS62140A switching regulator output is set to 3.3V. The device will power the USB Drive to the LPC2148, the SD Card Holder, The LPC2148 and the NFC interface transponder. The device has a total of 10 pin that will be used to operate the device which be seen in Figure 17. SW at a switch node, connected to the internal MOSFET helps make the device operate and function. PGND is the ground state. VIN is the battery power source that will be used as the input voltage. EN is an input pin that can enable or disable the use of the device. AGND is the analog ground. FB at is the voltage feedback that can change the output voltage value by using a voltage divider. VOS at is an input pin that senses the output voltage for control loop circuitry. The FSW is the frequency select pin in which frequency can range from 1.25MHz at logic low or 2.5MHz at logic high. The SS/TR is a soft-start tracking pin that sets the internal voltage rise time. This can be used for tracking or sequencing. The DEF pin is an input pin that allows for output voltage scaling. Since project won’t require voltage scaling the pin will be connected to ground. The TPS62140 will need RLC elements to build its circuit design. The Cin capacitor is set to 20uF and is used to optimize the transient voltage response. The Cout is set to 22.0uF and will be used perform the same function. Since the voltage output is 3.3V Rfb2 is set to 562k Ohms and Rfb1 is set to 180k. L1 value is set to 2.2uH will allow use a lower switching frequency to get a low ripple. A 100k Ohm pull resistor will be used to go to high impedance when the device turns off.

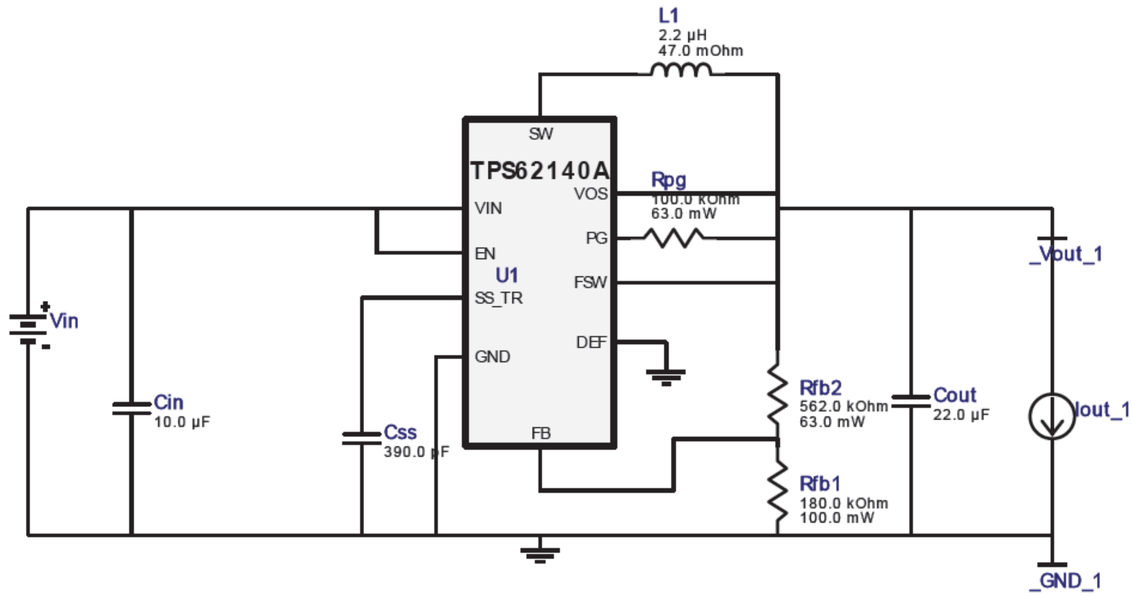


Figure 17: TPS62140A Circuit Design

4.1.2.4 TPS62122 Circuit

The TPS6128 is a switching regular with an output voltage that is adjusted to 4V. This device will only power the SIM800H device. The device uses a total of 7 pins to operate the device which can be seen in Figure 18. SW at PIN 1 is a switch node, connected to the internal MOSFET helps make the device operate and function. VOUT at PIN 2 is the voltage output pin that will connect to the SIM 800H. FB at PIN 3 is the feed black pin for the regulator. EN at PIN 4 is an input pin that can enable or disable the use of the device. VIN at PIN 5 is the input pin for the supplied power. GND is at pin 6 and is used for the ground. Just like the other switching regulators RLC elements will be used to create the circuit. Cin and Cout capacitors are used to optimize the transient voltage response. Rfbt and Rfbb used for the feedback divider. Since the output voltage is set to 4V the resistor for Rfbt is set to 330k Ohm and 82k Ohm for Rfbb. Cff is also set the 18pF to achieve optimal regulation performance.

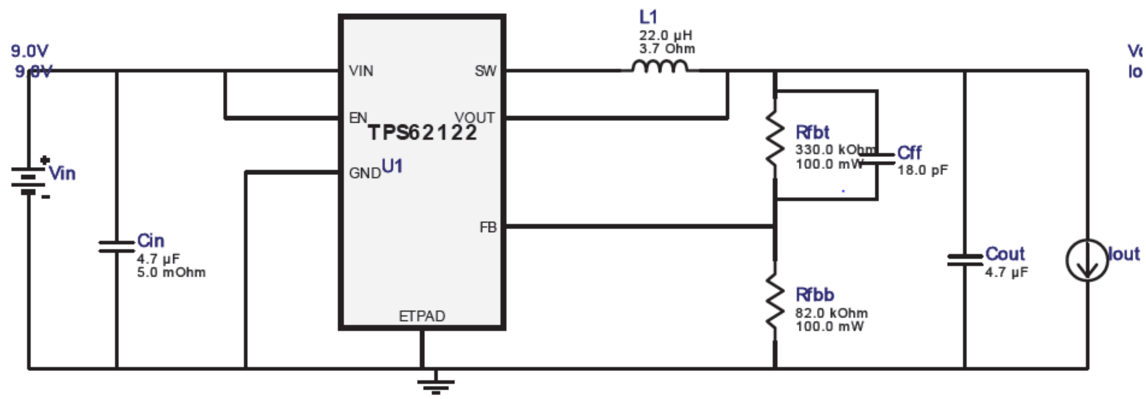


Figure 18: TPS62122 Circuit Design

4.1.3 NFC Hardware Architecture

The communication medium chosen for the NFC capability for Secured-E-Key was the TI Dynamic NFC Transponder RF430CL330H because its capabilities best fit the criteria needed for Secured-E-Key. The RF430CL330H was mainly chosen because it supports the communication interface of I^2C, it supports the reader/writer capabilities that will be used to connect the RF430CL330H with the smart phone, and that it's implemented on a target board that features an on board-antenna; however, the RF430CL330H does offer the option to use an external antenna if needed. The communication interface of ISO 14443B also allows NFC connection handover for alternative carriers such as Bluetooth, Bluetooth Low Energy (BLE), and Wi-Fi to be easily implemented as communications as well. Overall, the RF430CL330H offers the flexibility of being a fully programmable device and easy implementation that Secured-E-Key needs for its requirements and specifications.

4.1.3.1 Antenna

The RF430CL3304 includes an on-board antenna where the dimensions and parameters are based on the application requirements. The antenna connects with the RF communication interface module which is based on the protocol of ISO 14443B to the outside world. The two pins connected to the antenna are ANT 1and ANT 2. The antenna is based on a resonance circuit using the external antenna and the on chip capacitor that usually has a typical capacitance of 35 pico-farads with a tolerance of +/- 10 percent. An additional capacitor can be added to allow an inductance variation for lower inductance variance coils. Figure 19 shows the formula used to calculate the resonance frequency. Where C is the total resonance capacitor C_{RES} = C_internal + C_external, and L is the antenna inductance.

$$fres = \frac{1}{2 \times \pi \times \sqrt{L \times C}}$$

Figure 19: Equation of Resonance Frequency

For the resonance frequency, the chosen values for each component included the antenna inductance L= 2.66 micro-henrys, the total resonance capacitor C = 51.8 pico-farads for $C_{internal}$ = 35 pico-farads and C_{tune} = 16.8 pico-farads, and the resonance frequency f_{res} = 13.56 MHz. Table 30 shows the values that are the recommended operating conditions for the resonance circuit. If an additional external antenna were desired to change the resonance frequency, there would be two additional capacitors connected in parallel to the pins ANT 1 and ANT 2 in order to adjust the new resonance frequency. The antenna quality factor can be calculated with formula shown in Figure 20 where Q is the quality factor, f_{res} is the resonance frequency, and BW is the bandwidth.

$$Q = \frac{fres}{BW}$$

Figure 20: Equation for Antenna Quality Factor

For the quality factor the recommended quality factor is 30 so with the resonance frequency of 13.56 MHz, the recommended bandwidth can be calculated. Thus, the calculated bandwidth is 452 kHz. A passive quality factor should be less than 50; however, in the case of using an external antenna, a higher Q factor may exist so an external resistor should be added in parallel to the external capacitors to lower the Q to a reasonable range of 30 to 40. Figure 21 shows the schematic of how the external antenna would be connected to the RF430CL330H for the purposes of changing the resonance frequency and adjusting the Q factor.

Table 29: Recommended Operating Conditions for Resonance Circuit

Description	Symbol	Minimum	Nominal	Maximum
Resonance Frequency	f_{res}		13.56 MHz	
Antenna Input Voltage	V_{ANT_peak}			3.6 V
Impedance of LC circuit	Z	6.5 kOhms		15.5 kOhms
Coil Inductance	L_{RES}		2.66 µH	
Total resonance capacitance	C_{RES}		51.8 pF	
External resonance capacitance	C_{Tune}		16.8 pF	
Tank Quality Factor	QT		30	

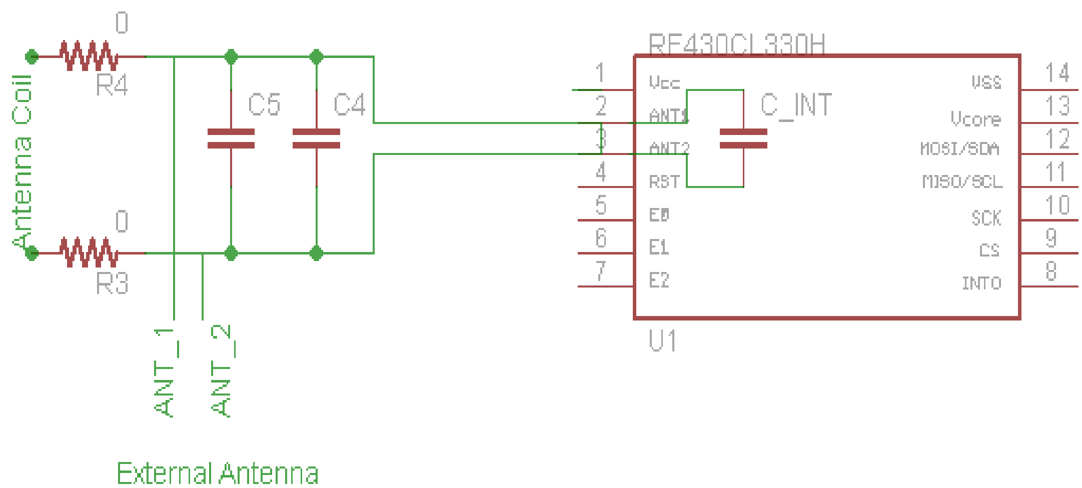


Figure 21: Schematic of External Antenna

4.1.3.2 Pin Configuration

For the NFC, Figure 22 shows the schematic of the RF430CL3304 pin connection configuration for Secured-E-Key. Pin 1 is the power supply voltage, the RF430CL330H intakes a voltage of 3 – 3.6 volts when no RF Field is present and 2 – 3.6 volts when an RF Field is present. The operating power chosen for the RF430CL3304 will be 3.3 volts. Pin 2 and 3 are the antenna inputs in which they both connect to an 10 micro-henry inductor in parallel with a 300 pico-farad capacitor. Pin 4 is the reset input that connects in series to a 100 milli-farad capacitor to ground. Pin 5 is an input for the I^2C address select 0 or the SPI mode select 0. Pin 6 is an input for the I^2C address select 1 or SPI mode select, and Pin 7 is an input for just the I^2C address select 2. Pin 8 is an interrupt output and Pin 9 is an output for the Serial Communication Mode select which is utilized during the device initialization. Pin 9 is also an input for chip select in SPI mode and Pin 10 is an SPI clock input. Pins 8, 9, and 10 will not be used because the communication protocol that will be used for Secured-E-Key is I^2C, so these pins will be grounded. Pin 11 can be an input or output pin depending on which communication protocol is utilized and it's the SPI Slave out in SPI mode or the I^2C clock in I^2C mode. Pin 11 connects a node from 4.7 kOhms resistor to the node at Pin1. Pin 12 can be an input or output pin as well, it's used as the SPI Slave in in SPI mode or I^2C data in I^2C mode. Pin 12 connects a node from 4.7 kOhms resistor to node at Pin 1. Pin 13 is the regulated core supply voltage and connects a 470 milli-farad capacitor to the ground and Pin 14 is used as ground. Table 31 shows the pin description of the schematic.

Table 30: Pin Description of RF430CL330H Schematic

Pin	Name	Description
1	VCC	power supply
2	ANT1	antenna input 1
3	ANT2	antenna input 2
4	RST	reset input (active low)
5	E0	I^2C address select 0
6	E1	I^2C address select 1
7	E2	I^2C address select 2
8	INTO	ground
9	CS	ground
10	SCK	ground
11	SO/SCL	I^2C clock
12	SI/SDA	I^2C data
13	VCORE	regulated core supply voltage
14	VSS	ground

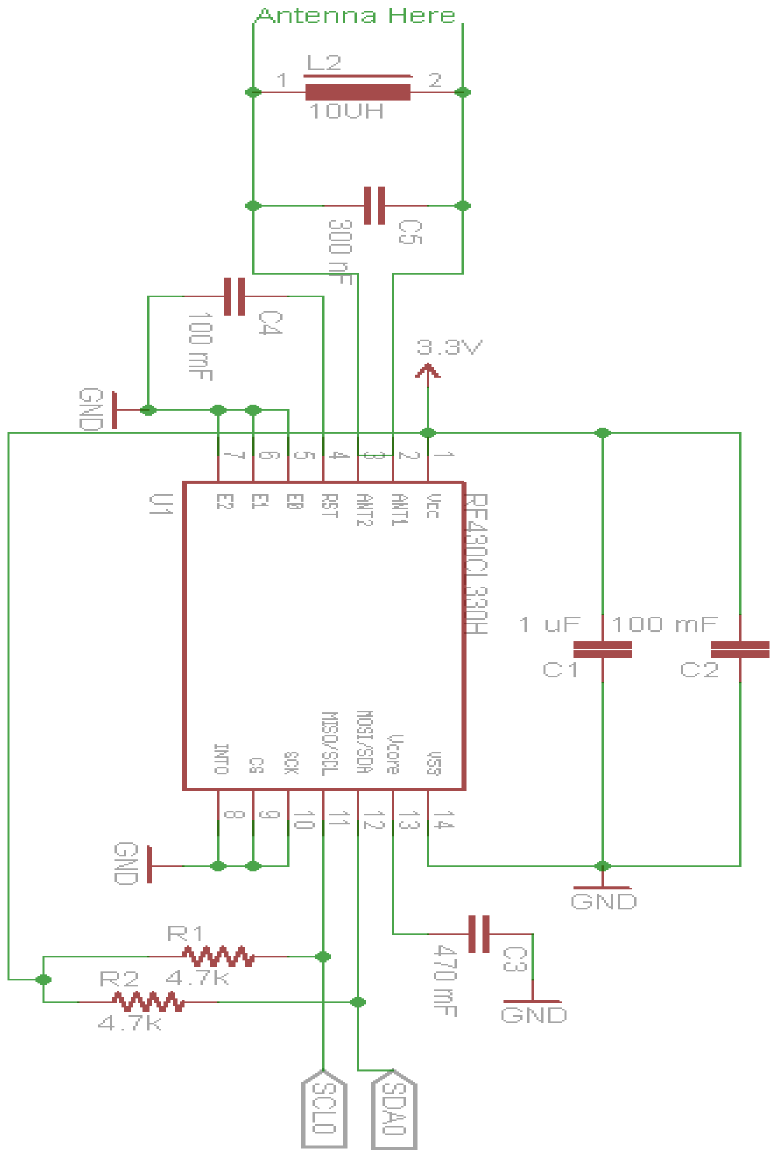


Figure 22: Pin Configuration of RF430CL330H Schematic

4.1.4 PIR Sensor Design

The PIR sensor chosen for Secured-E-Key will be the Parallax Wide Angle PIR sensor because its capabilities best fit the requirements and specifications of Secured-E-Key. The Parallax Wide Angle PIR sensor was mainly chosen because it was the only PIR sensor with a detection angle of 180 degrees which is considered a beneficial asset in ensuring security in Secured-E-Key's given area parameters. It was also chosen because of its simplistic design of having 4 pins with 1 as ground, 2 as power, 3 as output voltage, and 4 as an optional pin to connect to a standard servo extension cable. This pin set-up would be easy implementation for the ARMS processor used in Secured-E-Key. Table 32 shows the pin functions and Figure 20 shows the layout of the PIR sensor. The resistor shown in Figure 23 can be between 0 and 4.7 k-Ohms The Parallax Wide Angle PIR sensor has simple settings that can be easily implemented which include a "night-time mode" shown in Table 33 and sensitivity adjustment levels shown in Table 34. The Parallax Wide Angle PIR sensor also doesn't require any software implementation which makes it again an easy choice for Secured-E-Key as well. Overall, the Parallax Wide Angle PIR sensor provides the best capabilities of easy implementation of hardware and software for Secured-E-Key compared to the other PIR sensors researched. Table 35 shows the specifications of how the Parallax Wide Angle PIR sensor will be best utilized for Secured-E-Key.

Table 31: Pin Function (reference)

Pin	Symbol	Type	Function
1	GND	ground	ground
2	VCC	power	power supply
3	OUT	output	HIGH = movement / LOW = no movement
4	EN (optional)	input	PIR enable; HIGH = Enable / LOW = Disable

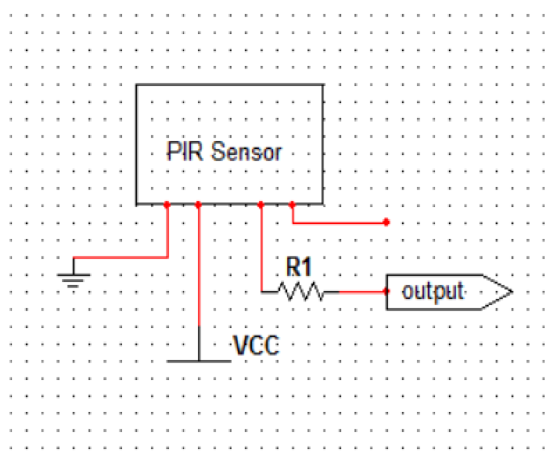


Figure 23: Parallax Wide Angle PIR Sensor Layout

Table 32: Mode Setting (reference)

Symbol	Mode	Description
1	night-time	only activated at night (depends on light conditions of environment)
2	all time	activated all the time

Table 33: Sensitivity Adjustment (reference)

Direction	Description
Clockwise	decrease trigger sensitivity
counterclockwise	increase trigger sensitivity

Table 34: Parallax Wide Angle PIR Sensor Specifications

Symbol	Description	Minimum	Typical	Maximum	Secured-E-Key
VCC (V)	Supply Voltage	3.3	5.0	6	3.3
ICC (mA)	Supply Current (no load)	2.8	3	3.2	2.8
GND (V)	Ground reference connection	-	0	-	0
VIH (V)	Signal High (input)	2.4	3.3	5.0	3.3
VIL (V)	Signal Low (input)	-0.3	GND	0.3	GND
VOH (V)	Signal High (output)	2.4	VCC	-	3.3
VOL (V)	Signal Low (output)	-0.3	GND	0.3	GND

4.1.5 Gyroscope Design

The Gyroscope sensor chosen for Secured-E-Key will be the MAX21000 because its capabilities best fit the criteria needed for Secured-E-Key. The MAX21000 was mainly chosen because it offers many options that can be configured accordingly for Secured-E-Key. These options include having both I^2C and SPI communication protocols that can be configured either way for the chosen ARMS processor, and offers flexible embedded FIFO that allows consistent power saving for the system and has the ability to wake up when needed to burst data out. The FIFO offers 4 different modes of off, on, interrupt and snapshot. The MAX21000 also is the only gyroscope that offers 4 different power modes of normal, eco, standby, and power down which gives Secured-E-Key the option to select the appropriate mode between power consumption, accuracy, and turn-on time. The MAX21000 is also the only gyroscope that offers a programmable full scale angular velocity ranging from +/- 31.25 to 2000. The MAX21000 also offers an evaluation board adapter option that can make the MAX21000 easily connect to an ARMS processor as opposed to soldering the MAX21000 chip itself onto a PCB board. Overall, the MAX21000 is the most suitable option for Secured-E-Key because it offers many options for its features compared to the other gyroscopes researched and has an evaluation board adapter option that can be easily implemented into Secured-E-Key's ARMS processor if that was desired. Table 36 shows the MAX21000 specifications for Secured-E-Key.

Table 35: MAX21000 Specifications

Symbol	Description	Minimum	Typical	Maximum	Secured-E-Key
VDD (V)	supply voltage	1.71	2.5	3.6	2.5
I_{VDDN} (mA)	current – normal mode		5.4		5.4
I_{VDDS} (mA)	current– standby mode		2.7		2.7
I_{VDDT} (mA)	current – eco mode		3.3 3.0		
I_{VDDP} (μA)	current – power down mode		8.5		

4.1.5.1 Pin Gyroscope Configuration

For the gyroscope, Figure 24 shows a schematic of the MAX21000 pin connection configuration for Secured-E-Key. Pin 1 is the supply voltage, the MAX21000 intakes a voltage between 1.71-3.6 volts. The operating power chosen for the MAX21000 will be 2.5 volts. Pins 2 and 3 are labeled N.C for not internally connected, so those pins will be grounded. Pin 4 is an SPI and I^2C clock. For Secured-E-Key the communication protocol that will be utilized is I^2C, so for Pin 4 in I^2C mode the IO has selectable anti-spike filter and delay to ensure correct hold time. Pin 5 is ground and Pin 6 is an SPI In/Out pin or an I^2C serial data. Pin 7 is the SPI Serial Data Out or the I^2C slave address LSB and Pin 8 is the SPI chip select/Serial Interface Selection Pin. Pin 10 is reserved which must be connected to the ground. Pin 12 is the data synchronization pin that's used to wake up the MAX21000 from power down/standby mode and this pin is used to synchronize data with the camera. Pin 12 is directly connected to the processor used for Secured-E-Key. Pin 14 is the analog power supply which is bypassed to ground with a 0.1 microfarad capacitor and 1 microfarad capacitor.

Pin 15 is VDD as well and has to be tied to the VDD of Pin 14. Table 37 shows the pin description of the schematic.

Table 36: Pin Description of MAX21000 Schematic

Pin	Name	Description
1	VDD	Supply Voltage
2, 3	N.C.	not internally connected
4	SCL_CLK	I^{2}C clock
5	GND	ground
6	SDA_SDI_O	I^{2}C Serial Data
7	SA0_SDO	I^{2}C slave address LSB
8	CS(G)	SPI chip select/Serial Interface Selection
9	INT2	not utilized
10	RESERVED	ground
11	INT1	not utilized
12	DSYNC	Data Synchronization
13	RESERVED	leave unconnected
14	VDDA	Analog Power Supply
15	VDDT	Must be tied to VDDA

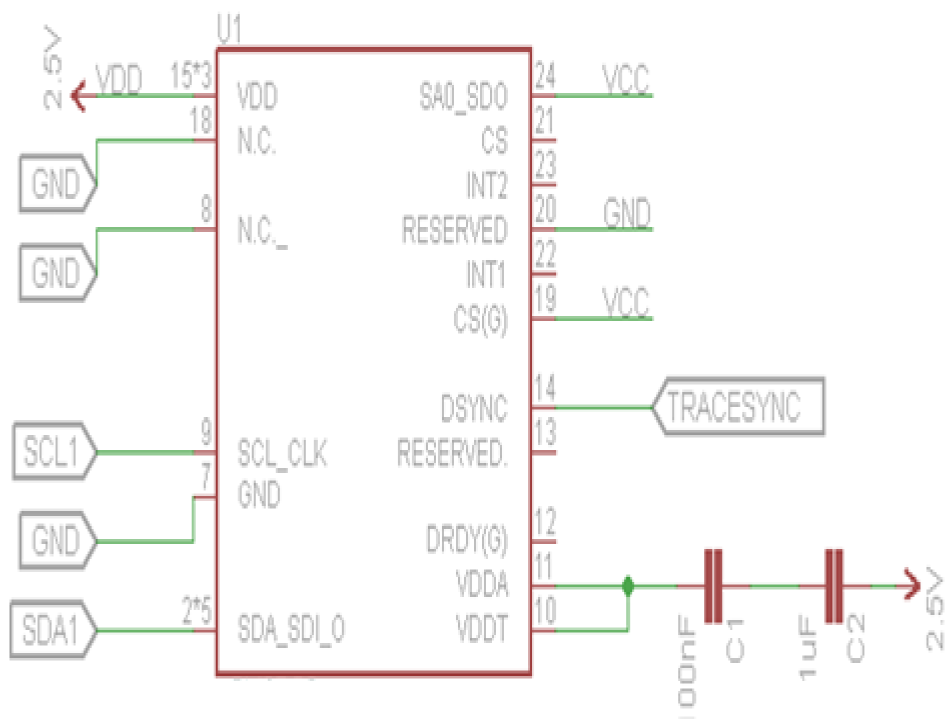


Figure 24: Pin Configuration Schematic of MAX21000

4.1.6 Microcontroller Design

The microcontroller is the platform for which most of the peripherals are connected to. The SIM800H GSM module, RF430CL330H NFC reader, PIR sensor, USB port and LED indicator and HC-49 oscillator, and the MPU6050 gyroscope sensor, and the electric strike lock and the battery indicator will be connected to the LPC2148. The pins of all of these peripherals have to matched to the appropriate pins to the LPC2148. Some of these devices will require RLC elements for it to be properly configured. Table 38 and Table 39 show all of the LPC2148 pins and what devices will be connected to it.

Table 37: Occupied LPC2148 Microcontroller Pins

Microcontroller PIN Number	Function	Peripherals Connected to
1	P0.21/PWM5/AD1.6/CAP1.3	-
2	P0.22/AD1.7/CAP0.0/MAT0.0	-
3	RTCX1	HC-49
4	P1.19/TRACEPKT3	
5	RTCX2	HC-49
6	VSS	-
7	VDDA	-
8	P1.18/TRACEPKT2	-
9	P0.25/AD0.4/AOUT	-
10	D+	USB PORT
11	D−	USB PORT
12	P1.17/TRACEPKT1	-
13	P0.28/AD0.1/CAP0.2/MAT0.2	-
14	P0.29/AD0.2/CAP0.3/MAT0.3	-
15	P0.30/AD0.3/EINT3/CAP0.0	-
16	P1.16/TRACEPKT0	-
17	P0.31/UP_LED/CONNECT	USB LED
18	VSS	-
19	P0.0/TXD0/PWM1	MAX232
20	P1.31/TRST	-
21	P0.1/RXD0/PWM3/EINT0	SIM800H, MAX232
22	P0.2/SCL0/CAP0.0	-
23	VDD	MAX21000
24	P1.26/RTCK	-
25	VSS	-
26	P0.3/SDA0/MAT0.0/EINT1	MAX21000
27	P0.4/SCK0/CAP0.1/AD0.6	USB
28	P1.25/EXTIN0	-
29	P0.5/MISO0/MAT0.1/AD0.7	-
30	P0.6/MOSI0/CAP0.2/AD1.0	-
31	P0.7/SSEL0/PWM2/EINT2	-
32	P1.24/TRACECLK	-
33	P0.8/TXD1/PWM4/AD1.1	MAX232
34	P0.9/RXD1/PWM6/EINT3	MAX232
35	P0.10/RTS1/CAP1.0/AD1.2	SIM800H
36	P1.23/PIPESTAT2	-
37	P0.11/CTS1/CAP1.1/SCL1	RF430CL330
38	P0.12/DSR1/MAT1.0/AD1.3	SIM800H
39	P0.13/DTR1/MAT1.1/AD1.4	SIM800H
40	P1.22/PIPESTAT1	SIM800H
41	P0.14/DCD1/EINT1/SDA1	RF430CL330
42	VSS	RF430CL330
43	VDD	MAX21000
44	P1.21/PIPESTAT0	-

Table 39: Occupied LPC2148 Microcontroller Pins

45	P0.15/RI1/EINT2/AD1.5	MAX21000
46	P0.16/EINT0/MAT0.2/CAP0.2	-
47	P0.17/CAP1.2/SCK1/MAT1.2	RF430CL330
48	P1.20/TRACESYNC	-
49	VBAT	-
50	VSS	-
51	VDD	-
52	P1.30/TMS	RF430CL330
53	P0.18/CAP1.3/MISO1/MAT1.3	-
54	P0.19/MAT1.2/MOSI1/CAP1.2	-
55	P0.20/MAT1.3/SSEL1/EINT3	-
56	P1.29/TCK	RF430CL330
57	RESET	-
58	P0.23/VBUS	USB PORT
59	VSSA	-
60	P1.28/TDI	RF430CL330
61	XTAL2	HC-49
62	XTAL1	HC-49
63	VREF	-
64	P1.27/TDO	RF430CL330

4.1.6.1 Microcontroller Peripherals

To be able to run the microcontroller a oscillator must be implemented. The oscillator that was chosen for the LPC2148 is the HC-49/U. The HC-49C is manufactured by Multicom is made for industrial applications and microcontrollers. The HC-49/U can produce a wide frequency which can ranges from 1.8 to 32MHz. This frequency range is applicable to the LPC2148 frequency requirement of 12MHz. This is important in determining how stable the oscillator is.

As seen on the Figure 22, the oscillator has two pins. The LPC2148 will be using two HC-49/U oscillators for the design. The first oscillator will be used as a Real time clock for the microcontroller. The Pins of the oscillator connects to RTXC1 and RTXC2 of the microcontroller. RTXC1 of the microcontroller receives the input voltage of the pin. RTXC2 acts as an output voltage to the oscillator pin. RTCX1 is located on pin 3 and RTCX2 is located on pin 6. The minimum voltage that voltage Pin can use is -.5 volts and the max voltage is 1.8 volts. The typical voltage uses is 1.8 volts. The second oscillator will use XTAL1 and XTAL2 pins of the microcontroller. The function this oscillator is to act as the internal clock for the microcontroller to operate and for clock generator circuits. XTAL1 is the input for the oscillator and XTAL2 is for the output from the oscillator amplifier. XTAL1 is located on pin 62 and XTAL2 is located on pin 61 of the microcontroller.

For the XTAL oscillator to operate at the frequency of 12MHz the proper capacitors had to be chosen. The recommended setup circuit is two capacitors in parallel as can be seen in the diagram to create the load capacitance. Feedback resistance is already integrated into LP2148. For the operation frequency of the oscillator to be 10 MHz to 15MHz the recommended Load Capacitance must be 20pF. This means that the two capacitors C11 and C12 in parallel has to be 39pF which can be seen in Figure 25. The Oscillator for the RTC has the same circuit set up except the capacitance load is 13pF and the two capacitances for C14 and C13 is 27pF.

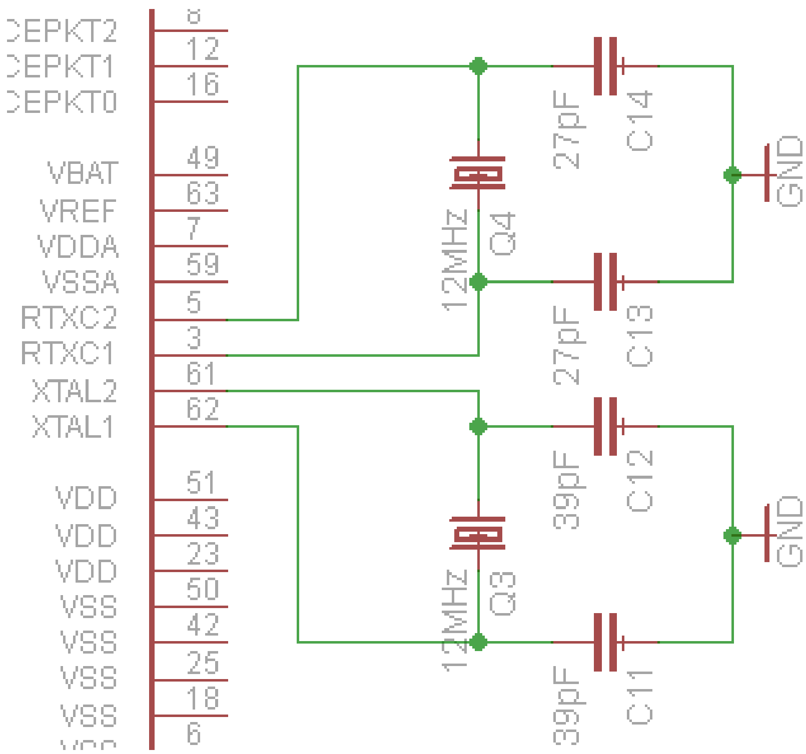


Figure 25: Oscillator Schematic Set-Up

4.1.6.2 USB Port

In order to communicate and program the LPC2148 a connection must be made to the computer and the microcontroller. USB communication was chosen since the LPC2148 and personal computers come with this functionality.

LPC2148's USB device controller has 5 ports for the USB device. There are two pins that are used for differential data signals. The first pin for data signal is D+ which is located on pin 10 and the second one is D- which is located on pin 11. There are two output pins to power the USB device. The Vbus pin is used as the input line voltage for the USB connector .The pin is used to indicate the presence of USB bus power and to allow a USB reset to occur if the signal is high. It is located on pin 58 of the microcontroller.

In order to use the USB it must be able to be powered. As seen from Figure 26, several circuit elements and design considerations were made to power the USB device. The USB will be fed 3.3V which fits under the max voltage of 4.75V to

5V. 33 ohm resistors were added to D+ and D-, pins to limit the amount of current and prevent a short. A 1.5k ohm pull up resistor was used to connect it to D+ pin and VDD supply voltage. This will essentially help identify the USB as a full speed device by pulling up the voltage to 3.3V. The capacitor that is connected to D-, D+ to ground was used as a decoupling capacitor. This is used to help filter unwanted high frequency noise. A 100k ohm pull-resistor to pull down the voltage to zero to ensure a logic low level. This will help ensure that the USB device is properly disconnected.

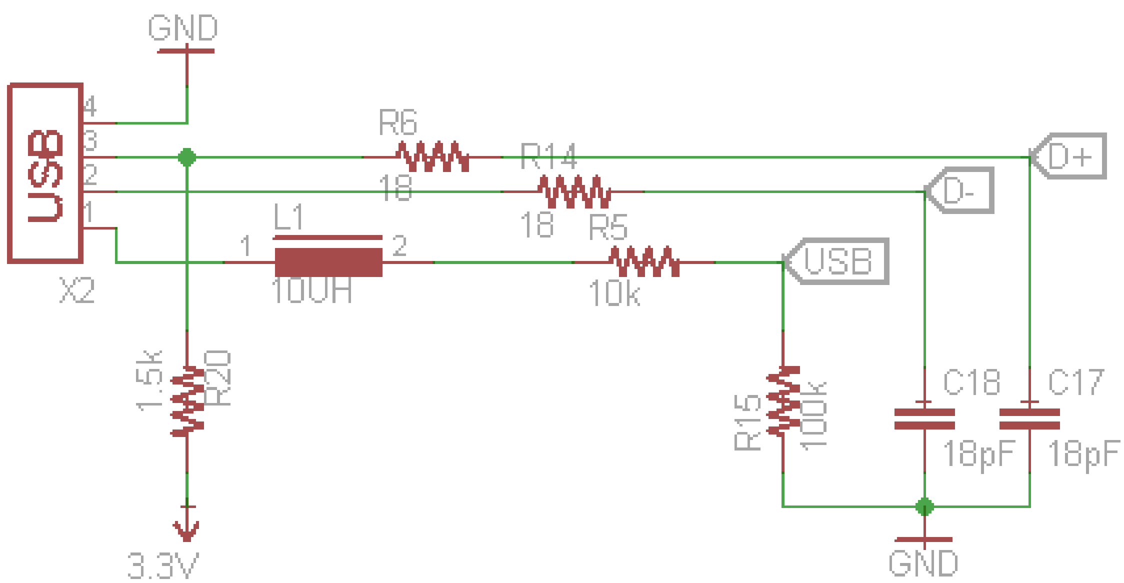


Figure 26: USB LPC2178 Schematic Set-Up

The LPC2148 also has a UP_LED connect located at port 17. UP_ LED port will be able to tell the user when the device is configured and not configured. Once the USB is connected a signal is used to switch an external 1.5 kΩ resistor under the software control. Figure 27 shows the LED USB schematic set-up.

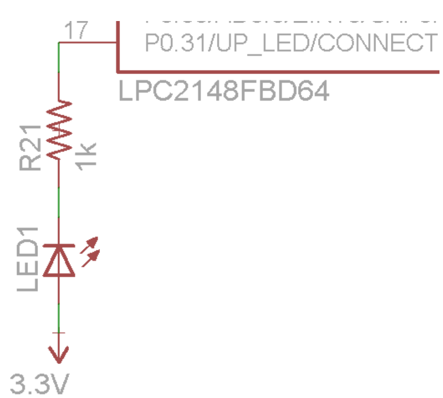


Figure 27: LED USB Schematic Set-Up

4.1.6.3 SIM800H

The SIM800H was Chosen as the GSM wireless communication method. The microcontroller has to communicate to the SIM800H in order control it, to relay and receive information. The LPC2148 microcontroller and the SIM800H will communicate using the RS232 serial protocol. The LPC 2148 uses 5 pins to communicate to the microcontroller RTS, CTS, UART/DRT, UART/DCO and UART/RI which can be seen in Figure 28. The RTS pin is located on Pin 35 and is the Request To Send output for UART1 to verify if the other device is ready for data reception. The Clear to send is located on pin 37 and is input for UART1 means that the SIM800H ready to accept data from the microcontroller. The DSR1 located at pin 38 is a Data Set Ready input for UART1 shows that The SIM800H will be ready for commands. The DTR1 located at pin 39 is a Data Terminal Ready output for UART1 shows that the wireless device is ready to receive, initiate, or continue a call. The RXD0 located at pin 21 is Receiver input for UART0.

When connecting the 5 wires from the SIM800H to the LPC2148 1k ohm resistors are used in between connections since UART will be operating at 3.3V. A 5.6k pull down resistors will be attached to RXD, RTS and DTR connections. This will allow the SIM800H to perform specific functions such as waking up the module.

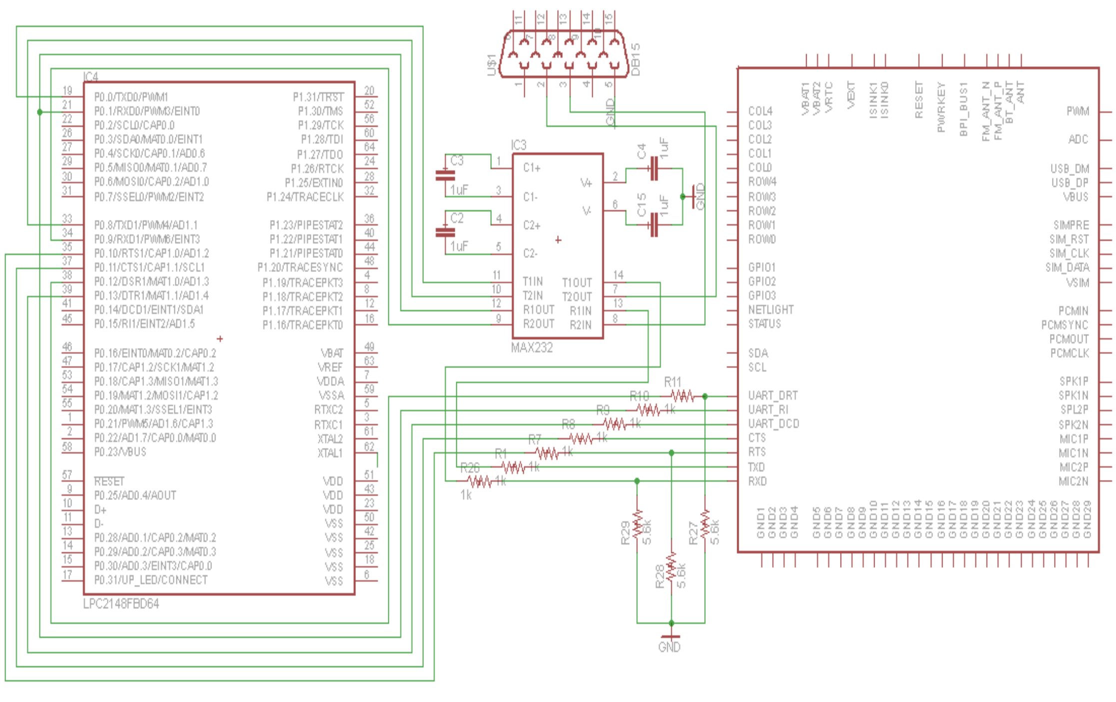


Figure 28: SIM800H to LPC2148 Schematic of Appropriate Connection Pins

4.1.7 Camera Design

The FlyCamOne eco V2 Camera Module come with UART connection possibility, but the Eagle library does not have this type of connector. Therefore, we will use a VGA connector which the closest that we were able to find that fits our design. The way the connection is going to work is that the pins 2 and 3 of the VGA connector will be connected respectively to the pins 7 and 8 of the MAX232, which is a dual driver/receiver that typically converts the RX, TX signals. When this process will be completed, the pins 10 and 9 of the MAX232 will be respectively attached to pins 1 and 7 of the microcontroller. Once the data is available at the microcontroller's level, it can be processed according to the task that we want to complete, which is to send it to the user through a text message. Figure 29 shows a schematic of the circuit the way it appears on the PCB.

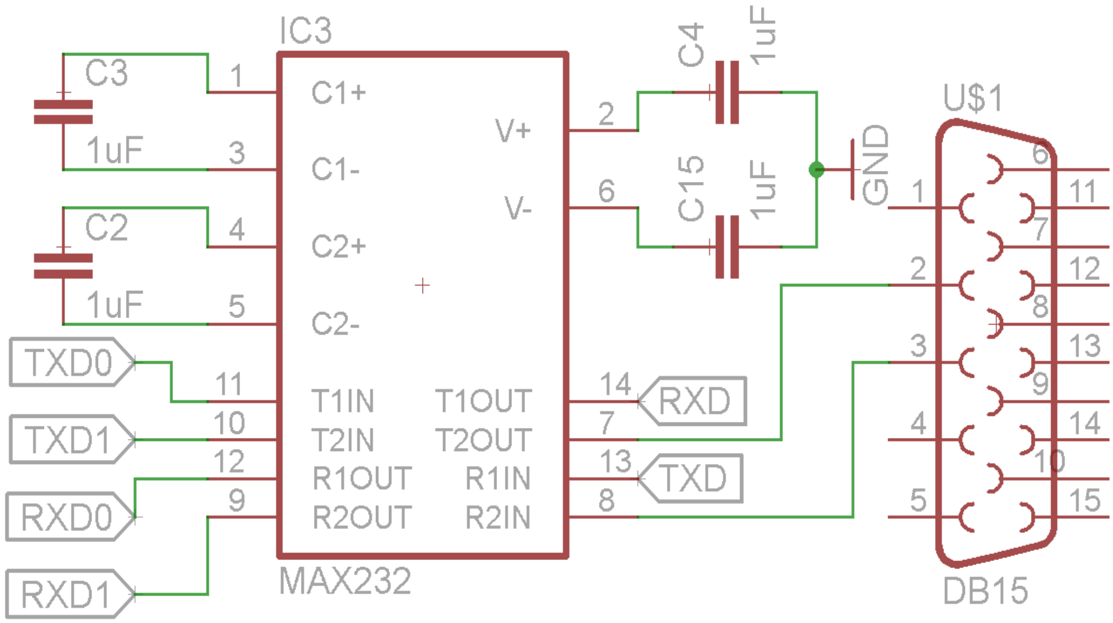


Figure 29: Circuit Diagram of the Connection to the Camera of the actual PCB

4.1.8 LED Voltage Comparator Implementation

The Vcc port of the voltage comparator will be connected to a 9 V- line on the PCB. The 9 V is the voltage necessary to power the LM 741AH/883 op-amp. V1 is going to be connected to the line that shows the minimum voltage of the system, which 2.0 V. The way that this is going to work is whenever the voltage of the system goes below 2.5 V the red LED will start flashing to show that there is an emergency regarding the battery because very soon the system is going to reach its minimum voltage. This is an alert to us so that we can address that problem and fix it as soon as possible; otherwise the whole system will crash. Regarding the other scenario, as long as the system does not reach the 2.5 V threshold that we set up, the green LED will keep flashing. Figure 30 shows the schematic of the Voltage Comparator with the green LED flashing when the system doesn't reach minimum voltage and Figure 31 shows the schematic of the Voltage Comparator with red LED flashing when the system reaches its minimum voltage.

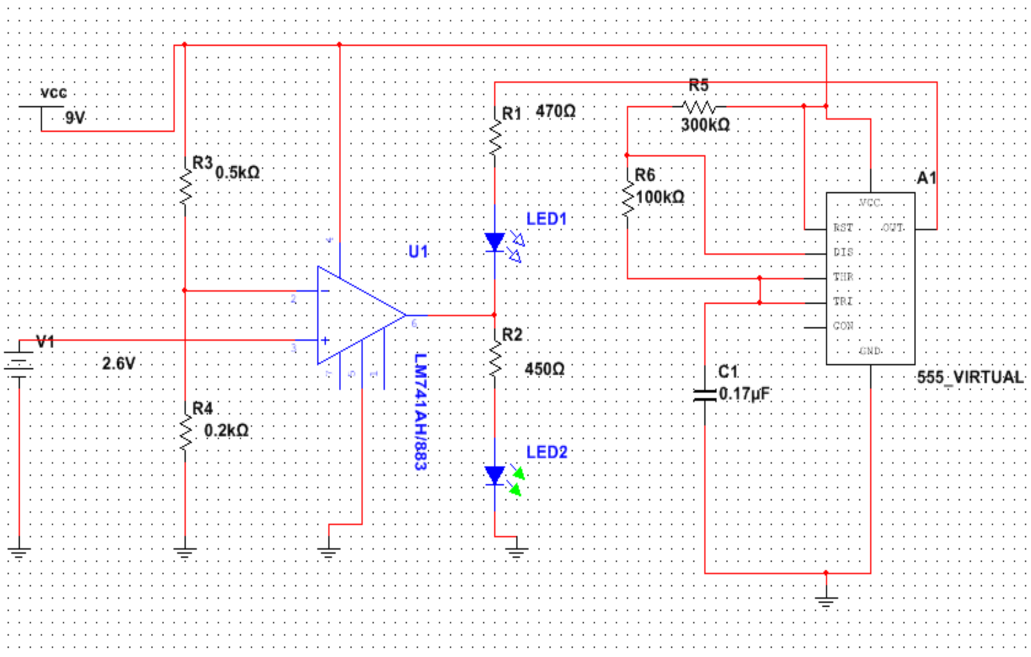


Figure 30: Schematic of the Voltage Comparator with green LED flashing when the system does not reach its minimum voltage

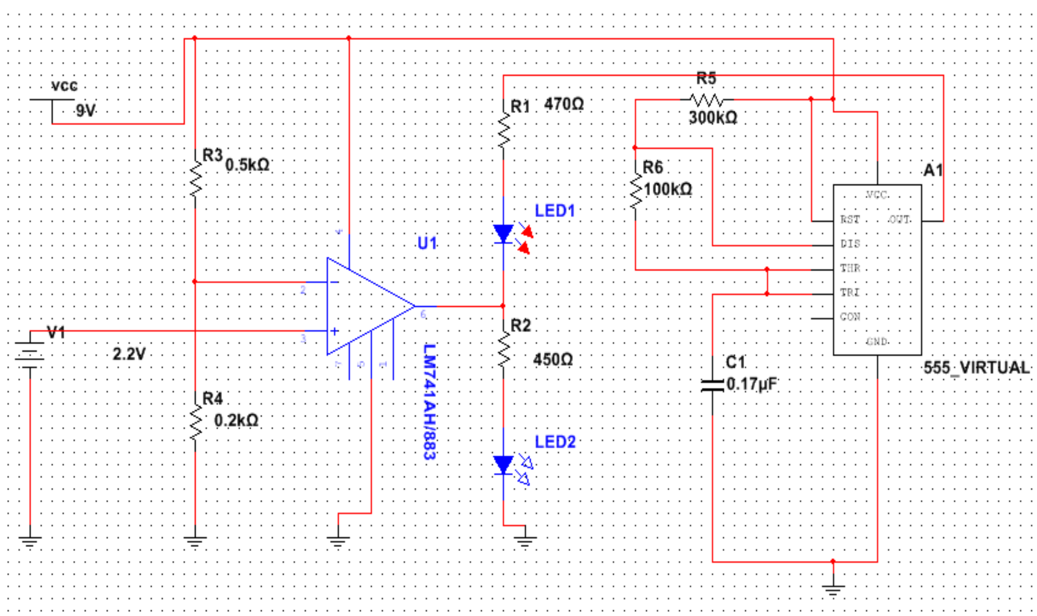


Figure 31: Schematic of the Voltage Comparator with red LED flashing when the system reaches its minimum voltage

4.1.9 SIM Card Holder and Voltage Suppressor Array

Knowing GSM requires the implementation of a SIM card as the basis for Secured-E-Key to connect to the network, the Molex91228 ChipSIM connector is designed for data transfer in conjunction with a removable SIM card for applications like GSM, GPRS, SMS, and MMS. The device can handle up to 50 V DC as a whole unit and a maximum current of .5 A per contact; delivering a spectacular rating beyond the power demands Secured-E-Key requires. As displayed, Figure 32, for the SMF05CT1G is a transient voltage suppressor array used to protect the serial and parallel ports of the ChipSIM connector. The five cathode lines to the suppressor each can handle a peak power dissipation of 100 W per line where the maximum transient rises in 8 us and falls to half the maximum in 20 us. Since each line places a single Zener diode to act as the transient suppressor, the leakage current per line varies from .07 to 5 uA along with a breakdown voltage between 6.2 to 7.2 V to adequately defend the SIM card from voltage spikes. The VSIM pin of the SIM800H module powers a 1.8 V or 3 V SIM card as the only options and provides the only voltage necessary to the SIM holder as a way to save energy by eliminating the need of any external power

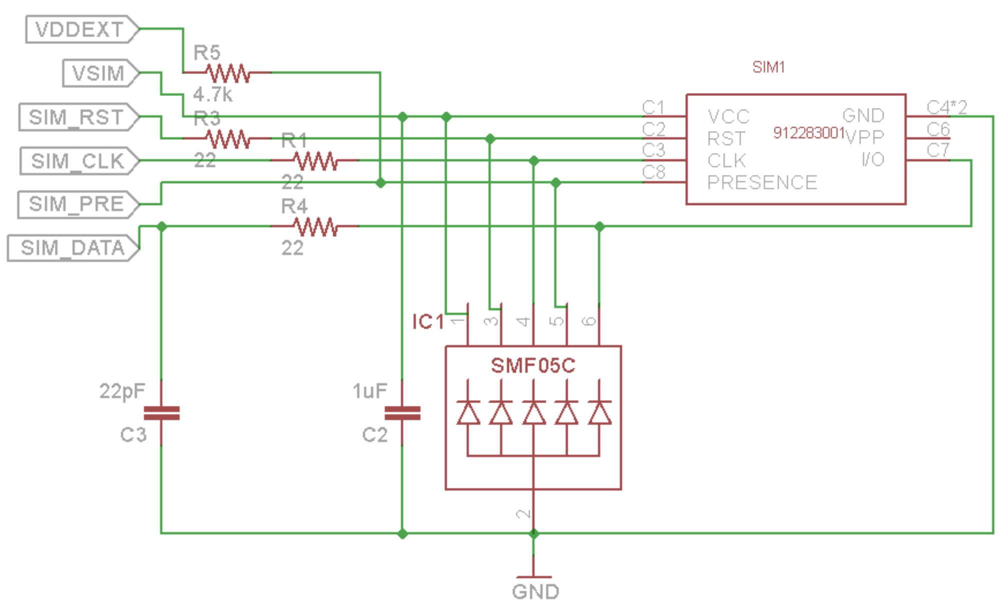


Figure 32: SIM Card Holder with Voltage Suppressor

4.2 Final Design Hardware Schematic

Final hardware design of Secured-E-Key with all previously mentioned hardware components integrated into one circuit is shown in Figure 33. Passive elements equal to footprint sizes comprising of 1210, 0805, 0603, and 0402 will work well for constructing such a board, especially to help minimize board space.

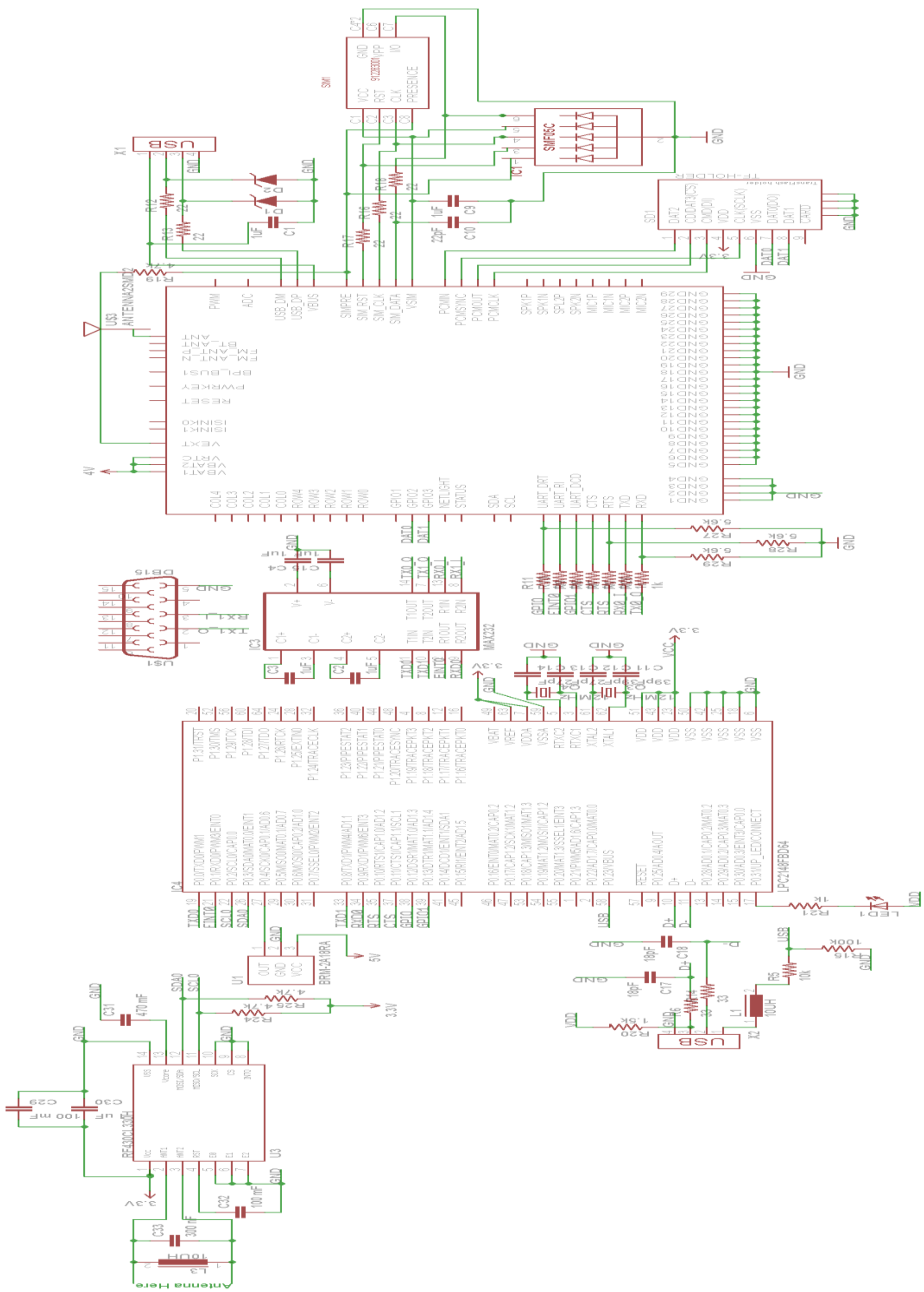


Figure 33: Schematic of all Integrated Hardware Components

4.3 Power Supply Peripheral Performance

Secured-E-Key power supply will have to power all of the electronic components. Each component has its own specific voltage and current requirement in order for it to work. If the input voltage that is being produced is less than the component's operating voltage the component will not operate or unexpected behavior can occur. This is effect is known as a brown out. Brown outs can cause the control signal to fall below the threshold at which the digital circuits can detect. The will make the machine not function as it is supposed to. If the voltage is supplied the component is higher than its operating voltage not only will the device will not operate correctly but the device can overheat and can be destroyed. To prevent this problem it will be necessary to step down the voltage of the power source in order fit these specific voltage requirements. The linear regulator device will be able to solve this problem. There are two different forms of linear regulators, a buck converter which is used as a DC to DC step down or a boost converter which is used as a boost converter. If the project were to use a DC-DC step by using boost converter then the power supplies voltage would have to be less than the converted output voltage. The boost converter will step up the voltage by stepping down the current proportionally so satisfy the conservation of energy rule. The method is problematic and impractical to use for the system. The DC-DC step down method is more effective to use since better current will be able to be drawn.

4.3.1. Active and Standby Current Consumptions

Developing and integrating a power supply into Secured-E-Key based upon the accurate power specifications of every peripheral, module, and microcontroller must be thoroughly analyzed in depth to form power consumption estimates. Each piece of hardware will only draw as much current necessary to work at any given moment in time which directly corresponds to the specific operation and the demand of current coinciding with that specific operation. Therefore, conserving current is the primary objective to follow to make sure each part of hardware uses the least amount of current possible. The power estimates will serve as a concrete foundation for the group to know how to optimize the longevity of the battery powered source to the whole PCB and to make final determinations as to whether a different part or set of parts need substituted to minimize power consumption even further during the actual construction of Secured-E-Key. The power source comprises of four distinct individual power supplies each with a particular voltage unique to each supply as a way to service a designated set of loads as seen in Figure 34.

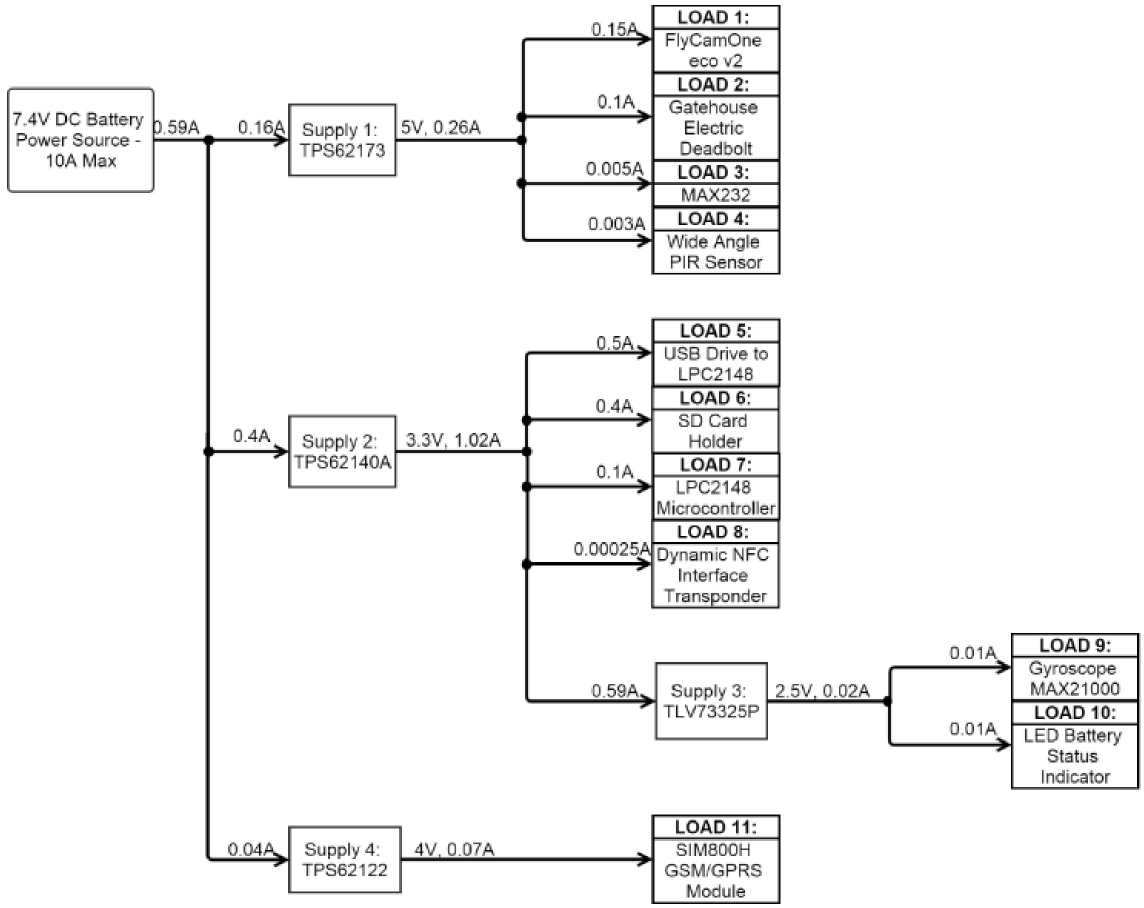


Figure 34: Visual Model of Power Distribution to All of Secured-E-Key (Referenced from TI Webench)

Voltage Supply 1 from Figure 34 powers four different loads, each requiring a recommended bias of 5 V when active, according to each datasheet to achieve the most ideal performance. The FlyCamOne eco v2 will become active for a maximum of three seconds each time a picture is snapped with current dissipation reaching a maximum of 100 mA before returning to standby mode at 100 uA. The Gatehouse Electric Deadbolt takes up to 100 mA to unlock and lock the deadbolt while demanding virtually 0 mA when not in operation. The MAX232 only serves to transfer data between the FlyCamOne eco v2 and LPC2148 microcontroller, so the MAX232 does not stay active longer than the three seconds of the camera staying active at a current dissipation of 5 mA until returning to standby at a consumption of 0 mA. Contrary to the rest, the Wide Angle PIR Sensor fluctuates between active and standby for about one second intervals each, so long as the sensor continues picks up a moving infrared signature within the sensor's proximity. The current consumes rises to a maximum of 3 mA, but consumes only .15 mA in standby mode. Due to the PIR sensor being controlled by the LPC2148 microcontroller, the I/O pin connected to the sensor can be programmed to keep the sensor in standby for a chosen length of time such as a sixty seconds. Remaining in standby mode stops the user from receiving redundant MMS messages to alert them to the presence of the same person as a way to save energy. Of course if the person stays at the front door after the sixty second duration, the user will receive further notifications to stay aware of person's constant presence.

Voltage Supply 2 from Figure 34 powers four different loads which optimally run at 3.3 V without any of the loads risking potential damage or failure. The SD card attached to the SIM800H module and USB drive attached to the LPC2148 microcontroller both have a normal operating amperage between 50 to 100 mA. The maximum current load can reach up to 500 mA after a device, like Secured-E-Key, has configured either component to permit the allocation of a much higher amperage for high-powered applications. When not in use, Secured-E-Key will only have to allocate 10uA of quiescent current to each component in order for either of them to remain in standby. The LPC microcontroller uses the V_{BAT}, V_{DDA}, and V_{DD} pins to power the microcontroller unit, but will only require pins V_{DD} and V_{BAT}. Pin V_{DD} powers the core and all I/O ports, whereas pin V_{BAT} powers the RTC; but regardless, both require only 3.3V for active mode. All standard GPIO pins can each handle current as high as 100 mA and have a 5 V tolerance, though Secured-E-Key will only need a maximum of 3.3 V for any GPIO pins used to power attached external components which should not exceed 5 mA each during the active execution of a task. The power down mode of the microcontroller turns off the registers, peripheral registers, and internal SRAM but preserves their exact same values as before being powered down as a means to resume the preserved conditions of the original operations once awoken to the active mode again. Power down mode only requires a typical current dissipation of 40 uA for I_{DD} and 20 uA for I_{BAT}. The Dynamic NFC Interphase Transponder functions at 3.3 V for writing into the NFC Data Exchange Format (NDEF) memory under the I^2C standard as a way to operate when activated by an NFC chip, causing a current spike of 250 uA for no longer than a one second duration until returning to the standby mode with a current consumption as low as 10 uA.

Voltage Supply 3 is powered by Supply 2 as a way to step down the voltage from 3.3 V even further to 2.5 V for both the Gyroscope MAX21000 and LED battery status indicator. Four separate power modes exist for the Gyroscope MAX21000 including normal, eco, standby, and power down modes. Normal mode serves as the most ideal mode so Secured-E-Key may exploit using the entire spectrum of frequencies from 0 to 400 kHz, while only consuming 5.4 mA during active periods of sensing a displacement in the position of the front door amid opening and closing estimated at 3 second intervals. The most energy efficient mode is powering down, needing only a modicum current draw of 8.5 uA and can automatically wake up through a programmable interfacing of the Data Synchronization Pin (DSYNC) found on device to the LPC2148. The LED battery status indicator consumes a maximum of 10 mA when actively illuminating the green or red LED, but alternatively requires a negligible standby current amount too small to consider.

Voltage Supply 4 oddly enough has the essential task of simply powering the SIM800H module at a recommended current of 70 mA and voltage of 4 V as the backbone to provide cellular service over the GSM network between Secured-E-Key and the user's smartphone. GSM cellular connectivity cannot exist without employing a SIM card requiring 3 V with an operating current of 10 mA and standby current insignificant enough to disregard it from any calculations. The GSM network will enable mobile capabilities like MMS for sending pictures and SMS messages for accessing the door lock through GPRS at an amperage of 149 mA as the best operating current available for the SIM800H module. The standard time necessary for MMS to send to a smartphone is between five to ten seconds, whereas SMS messages only take two to three seconds. Current consumption over GPRS uses a total of 5 timeslots at a time with a distribution of 4 downlink slots and 1 uplink slot to provide a sufficient download rate of 80 kbits/s to meet the standard times of MMS and SMS messaging to send to a smartphone. When not in use, the SIM800H stays in a power down mode taking 50 uA.

In the graphs of Figure 36, the active and standby current value to each individual voltage supply can be determined. By summing the active and standby currents of each hardware component attached to their particular voltage supply, our group could find the output current to each voltage supply. Figure 35 shows the formula to the output current follows as:

$$I_{output} = \sum [(I_{load-1} + I_{load-2} + \ldots + I_{load-n})] \text{ (mA)}$$

Figure 35: Equation of Output Current

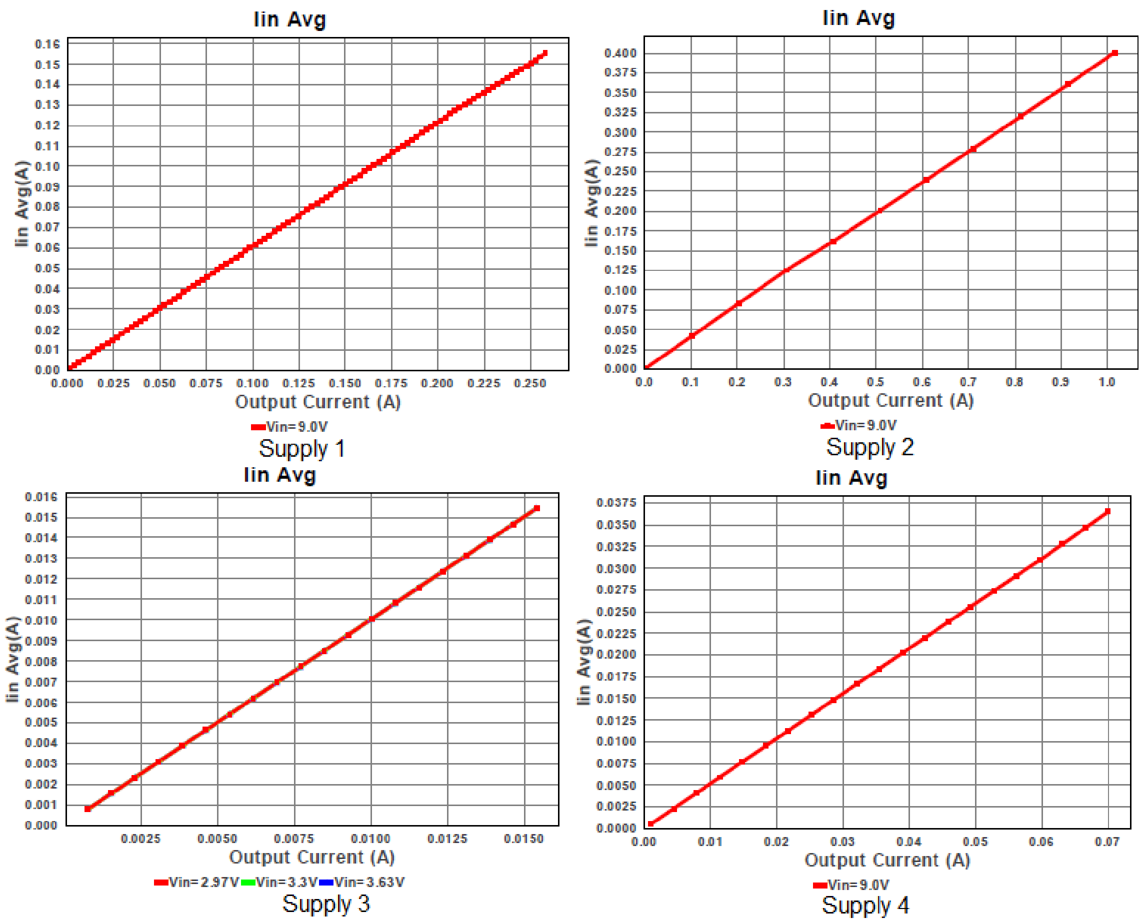


Figure 36: Input to Output Current Reading to Each Voltage Supply (Referenced from TI Webench)

By finding the output current in both the active and standby mode separately, the active or standby input currents required of each voltage supply could be determined. Hence, our group was able to find current values to both the active and standby modes of each voltage supply, instead of only considering the hardware component amperages. Gathering both pieces of information provide more accurate calculations to the total average current that Secured-E-Key's power supply will have to support. Table 40 shows the optimum current distribution to all of Secured-E-Key's components.

Table 40: Optimum Current Distribution to all of Secured-E-Key Components

Component	Active Current (mA)	Standby Current (mA)
Supply 1	155.24	.1866
FlyCamOne eco v2	100	.100
Gatehouse Deadbolt	100	0
MAX 232	5	0
PIR Sensor	3	.150
Supply 2	201.02	.0903
LPC2148 USB Drive	50	.010
SD Card Holder	50	.010
LPC2148 Microcontroller	200	.060
NFC Transponder	.250	.010
Supply 3	15.434	.0085
Gyroscope MAX21000	5.4	.0085
LED Battery Indicator	10	0
Supply 4	135.95	.018
SIM800H GSM Module	70	.050
SIM Card	10	0
SMS	149	0
MMS	149	0

4.4 SOFTWARE DEVELOPMENT

4.4.1 GYROSCOPE SENSOR Software

The MAX21000 gyroscope sensor software is available for download when the gyroscope is purchased through the Maxim Integrated website. The software can control the different power modes, configure other registers, and the different ranges of angular velocity. The MAX21000 gyroscope can also be controlled by an external device such as a microprocessor, another sensor, or a different kind of device through the data synchronization pin DSYNC which can enable a number of synchronization options. There is also a sensor software for when the MAX21000 is implemented onto the Maxim inertial demo (MInD) evaluation kit to evaluate the MAX21000 performance. The MInD software can be downloaded on the Maxim Integrated website as well. The MInD software can control various registers that include the streaming mode, data streaming, and the clock frequency.

4.4.2 NFC Software

The software the RF430CL330H uses is the ISO 14443B that operates with the NFC Tag Type 4 specifications and supports the NFC data exchange format (NDEF) requirements. Through the RF interface the user can read and update the contents in NDEF memory and the NDEF memory will be stored as long as the power is maintained; however, the NDEF memory will be lost if the power is removed. The ISO 14443B is mainly used for the applications where the primary reader/writer module is an NFC enabled phone. How this will work for Secured-E-Key is by having the RF430CL330H transfer data which in this case would be the data to unlock the door, to and from the smart phone by RF. The ISO 14443B uses commands for the reader/writer module to manage communication. The NFC Tag Type 4 also uses its own commands for its communication.

4.4.3 SIM800H Embedded Software

The appropriate software designated to control the SIM800H module and create a harmonious environment where all hardware, peripherals, and virtual capabilities of Secured-E-Key work together cohesively is with AT commands. AT commands provide the fundamental basis to programming GSM/GPRS modems and module devices by simply putting the characters of “AT” before inserting the name of a command. Figure 37 shows the flow chart of a generalization to the full context of the software program that Secured-E-Key will execute.

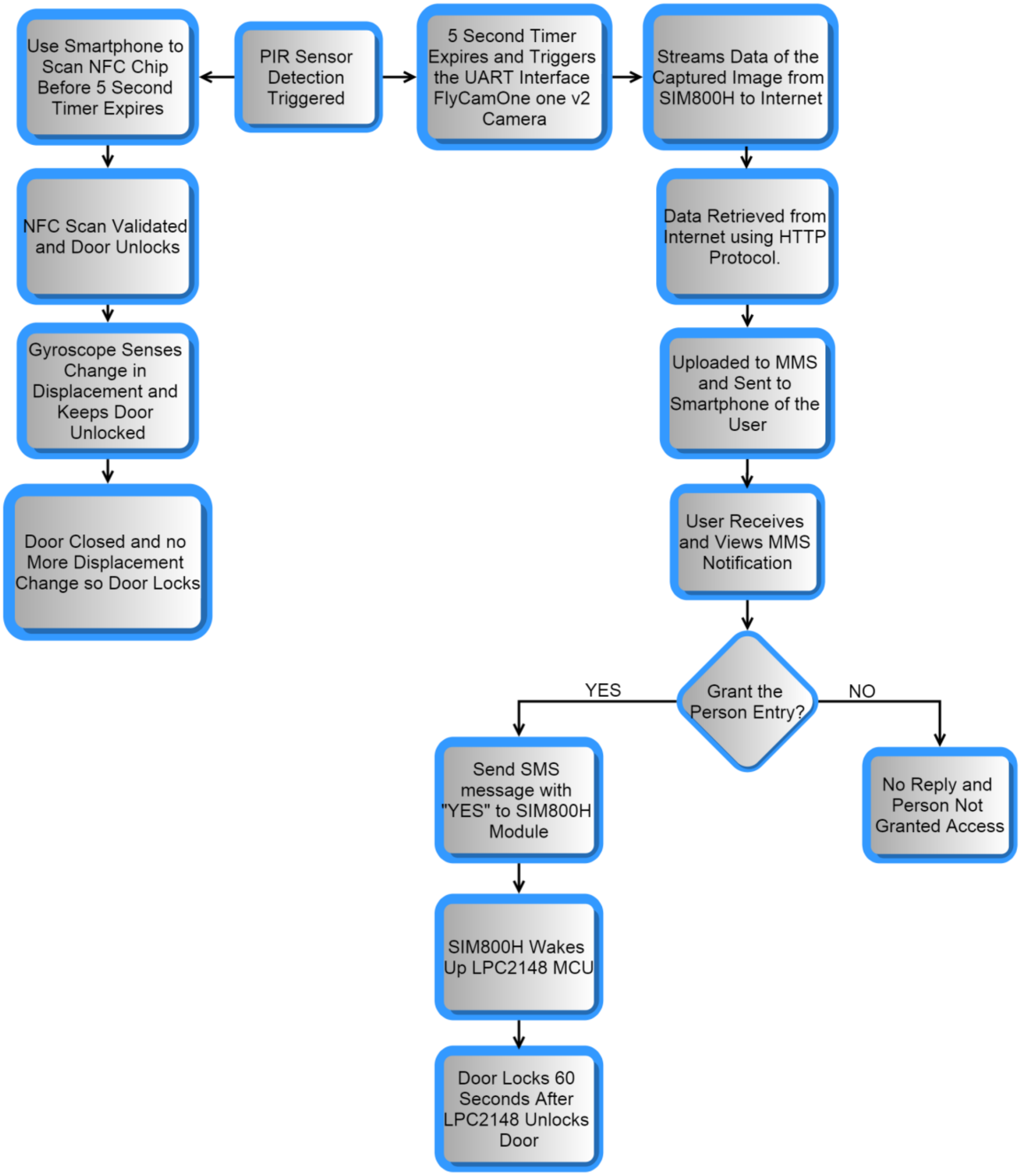


Figure 37: Secured-E-Key SIM800H Flow Chart

4.4.3.1 Multimedia Messaging Service (MMS) and AT Commands

The MMS protocol serves as the most straight-forward and sustainable way of Secured-E-Key to transfer data from the smart lock device to any smartphone. MMS only functions through HTTP and uses characters supported by the ASCII code standard for English letters, symbols, and numbers. The data size of any MMS cannot exceed 300 kbytes, which remains limited to either an image file

300 kbytes large or combination of an image and text file, although the maximum text file corresponds to a maximum size of 15.360 kbytes. Whatever image is sent through the MMS protocol, MMS must always be initialized first and can only cycle through multiple images continuously (one right after the other) in the corresponding order MMS originally initialized each image. After the initialization of MMS, specifying the URL to the location of the photo being sent through MMS is necessary. Now the image data of a size less than 300 kbytes can be sent through the UART pins connected to the MAX232 integrated circuit (IC) so the data is received and processed by a Data Carrier Detect (DCD) to be sent from a GSM antenna over a cellular network. The desired recipients of the MMS are defined by adding an email address or cell phone number, but an additional option to include secret recipients by using the same kind of contact information is available too. Once the recipient receives the MMS via their smartphone, it will display the image file, the data size of the image, the image file name, the ASCII characters of the text file, and contact information of the MMS sender. The Secured-E-Key software characteristics of the whole methodical process necessary to successfully send and receive MMS from the SIM800H to a smartphone happens by coding with most of the AT commands presented in Table 41.

Table 41: Necessary AT Commands for MMS Software Implementation

AT Command	Command Description
AT+CMMSCURL	Set the URL of the MMS center
AT+CMMSPROTO	Set the protocol parameter and mms proxy
AT+CMMSCID	Set the network parameters for MMS
AT+CMMSSENDCFG	Set the parameters for sending MMS
AT+CMMSEDIT	Enter or exit edit mode
AT+CMMSDOWN	Download the file data or title from UART
AT+CMMSDELFILE	Delete the file of the edited MMS by the file index
AT+CMMSEND	Start MMS sending
AT+CMMSRECP	Add recipients
AT+CMMSCC	Add copy recipients
AT+CMMSBCC	Add secret recipients
AT+CMMSDELRECP	Delete recipients
AT+CMMSDELCC	Delete copy recipients
AT+CMMSDEBCC	Delete secret recipients
AT+CMMSRECV	Receive MMS
AT+CMMSVIEW	Get the mms into buffer and show the information
AT+CMMSREAD	Read the given file of the MMS in the buffer
AT+CMMSRDPUSH	Read the information of the MMS PUSH message
AT+CMMSUA	Set user agent
AT+CMMSSTATUS	Get MMS status
AT+CMMSINIT	Initialize MMS function
AT+CMMSTERM	Exit MMS function
AT+CMMSSCONT	Save MMS context

4.5.3.2 Short Message Service (SMS) Protocol and AT commands

Accessing Secured-E-Key wirelessly to unlock and lock the front door can be done with SMS which is simply a text messaging service for cellular devices and sends a message up to 160 characters per message. As Figure 33 mentions, sending a text message with the characters of nothing more than “YES” from the user will grant the person standing outside their front door entry into the premise of their home. SMS messaging contains an aspect called the validity period which allows a person to designate the precise period of time the SMS message is held at the SMS center before being permanently deleted from the network. The SMS center only stores SMS messages while the receiving mobile device (smartphone) is off, until a user finally turns on the device and receives the SMS messages. If the validity period expires before the user turns on the mobile device, the SMS message(s) are deleted, and the mobile device receives nothing. Extending the validity period for several hours remains important, especially during the occurrence of a Secured-E-Key user’s smartphone running out of power. At the point of power being restored and powered on, the stored MMS messages previously sent from the SIM800H need to arrive to the user’s phone so the user can remain aware of who approached their front door. SMS messaging primarily uses validity periods, but MMS shares the same capability and serves as the dominant messaging service for Secured-E-Key purely from a messaging implementation stand-point.

4.4.3.2.1 Important SMS Software Characteristics

Certain software characteristics of SMS are particularly important to the AT command created Secured-E-Key SIM800H Flow Chart program to optimize the program’s performance and security. For instance, GSM/GPRS modules feature a message status report option of being activated to show whether an SMS message successfully arrived to a recipient’s mobile device. The message status report will execute consecutively each time the SIM800H module sends an SMS message, the option must only be activated first for the continuous execution to occur. Beyond the message status report lies the characteristic of the SIM800H module’s option to supply message submission reports as to see if any errors or failures transpired, like wrong SMS message format or busy SMS center, when the SMS message arrives at the SMS center. Receiving a message submission report will normally consist of what error or failure happened and the cause of either one. If all else fails and the module does not receive receipt of a message submission report a subsequent amount of time later, a great likelihood exists of the submission report being lost. Sending another SMS message to the SMS center normally serves as the best remedy to assuring the receipt of a message submission report occurs. Putting it all together now, if an SMS message arrives at the mobile device successfully, the SMS center should receive a message delivery report from the mobile device that communicates the SMS message transmission was successful, or specifies any potential problems such as “not enough storage space” or “unsupported

SMS message format" in the event of any errors or failures occurring. By the mobile device sending a message delivery report to the SMS center, the SIM800H module can request for a message status report to inquire about the overall completion of a successful SMS message having sent from one device to another device. To verify whether the software characteristics to SMS between the SIM800H module and a mobile device occur as mentioned above, a computer interface like HyperTerminal is necessary to test everything. The software characteristics have to be implemented to Secured-E-Key by coding with AT commands. The AT commands in Table 42, serve as the appropriate SMS messaging commands to choose from.

Table 42: Necessary AT Commands for SMS Message Software Integration

AT Command	Command Description
AT+CMGD	Delete SMS message
AT+CMGF	Select SMS message format
AT+CMGL	List SMS messages from preferred store
AT+CMGR	Read SMS message
AT+CMGS	Send SMS message
AT+CMGW	Write SMS message to memory
AT+CMSS	Send SMS message from storage
AT+CNMI	New SMS message indications
AT+CPMS	Preferred SMS message storage
AT+CRES	Restore SMS settings
AT+CSAS	Save SMS settings
AT+CSCA	SMS service center address
AT+CSCB	Select cell broadcast SMS messages
AT+CSDH	Show SMS text mode parameters
AT+CSMP	Set SMS text mode parameters
AT+CSMS	Select message service

4.4.4 Simple Mail Transfer Protocol (SMTP)

The standard emailing service for the internet is SMTP and permits the sending of attachments too. A user must establish the minimum parameters of email in their code before sending anything. The SMTP server address and port information serve as the fundamental criteria of email set-up. Assigning the SMTP server address directly depends on what chosen email provider is being used, whereas the SMTP port consists of a port number that designates connecting a computer to a network. As an example, using Gmail as a provider would yield a SMTP address of Smtp.gmail.com and the SMTP port 25 is most commonly used port for sending email, but may be blocked by some IP address due to port 25's acceptance of malware and spam traffic to flow through the network. Two other standard ports to serve as an alternative are port 587 or port 465, which both provide the choice of applying an encrypted (like TLS) or unencrypted network connection. After positioning the SMTP address and port into place, the rest of the email parameters can be situated. The choice of including a username and password remains optional, but the essential SMTP attributes comprise of the recipient email address, subject line, email body, email attachment, and the AT command created to send the email. The maximum data available for sending an attachment in an email remains limited to 1,360 bytes for the SIM800H module; therefore, MMS will be used instead of email. Although Secured-E-Key will not use email, knowing the in-depth structure as to how applying email would have worked, assures our group has at least consider all available options worth exploring.

4.4.5 Microcontroller Software Design

In order to get the microcontroller to perform the specified functions software design will have to be considered. The basic purpose of this project is to get from a locked to an unlocked door. For the door to be unlocked there must be NFC confirmation or GSM confirmation from the owner. Before the coding process starts the behavior of the microcontroller must be designed first. A finite state machine and a flowchart were created to model this. Once these model are built the firmware and code are then chosen the program the microcontroller.

4.4.5.1 Finite State Machine

For to get NFC confirmations and GSM confirmations to get the door from a locked state to an unlocked state or vice versa there are more complex processes that take place. These are essential for building the overall structure for the microcontroller program. There first design consideration is the states and events that take place in the Microcontroller from when the door closed to being opened. A finite state machine was developed to show all the state and events of the microcontroller which can be seen in Figure 38.

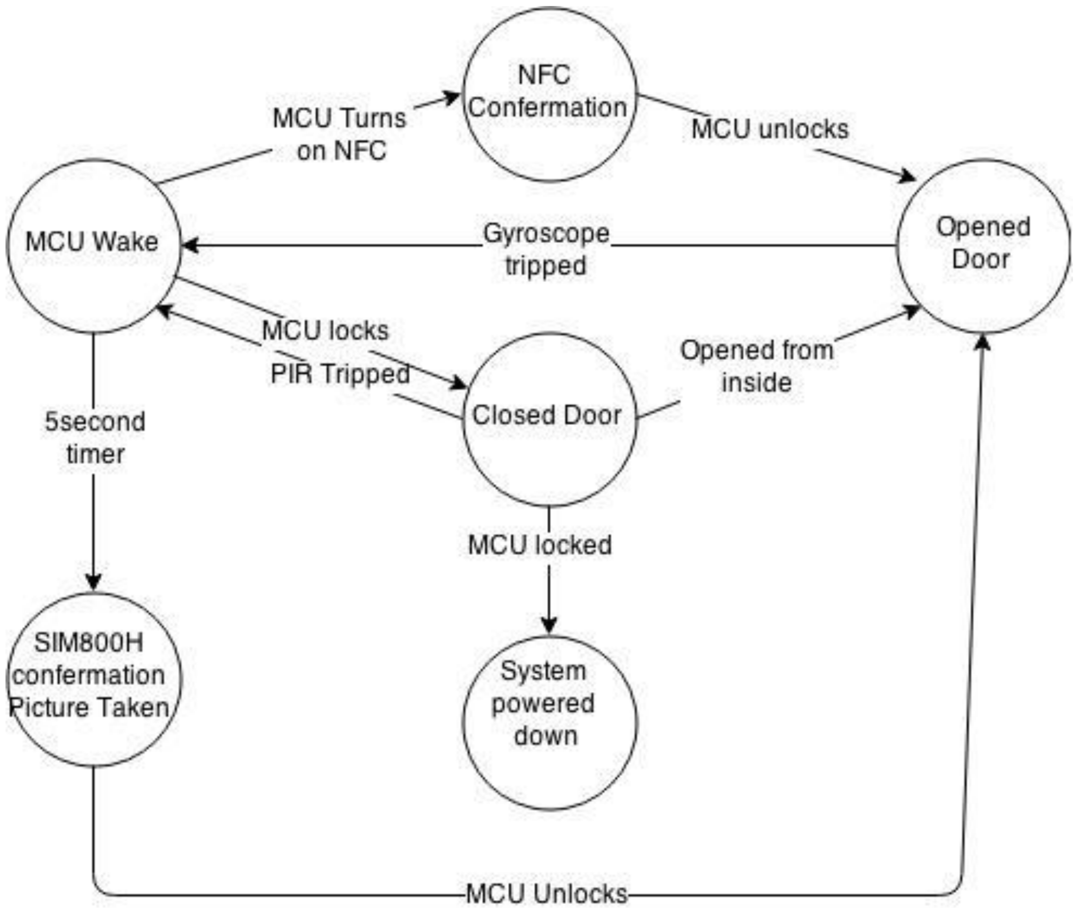


Figure 38: Microcontroller Finite State Machine

The closed door state will lead the system power down state. This event leads to the state of the NFC and MCU module to turn on. The event of the PIR sensor being tripped from the closed door state can lead to the event state of the microcontroller to wake up and the NFC to turn on. Programing considerations must be made to create this new state. The NFC state leads to the event of opening the door. For this to happen, commands must be made to tell electric strike to unlock. In order for the state of a picture taken and the SIM800H being on, the timer must pass 5 seconds from the MCU being on. The state of the door being open comes from the state of the MC unlocking door from NFC or SIM being on state. This state leads the state of the SIM800H the NFC being off and the door being closed. For this to occur, the microcontroller must be programmed to create the state of the electric strike locking.

For the MCU to go into from the door being closed, the microcontroller must be programed for the MCU to go to sleep from the state of the door being closed. The states and events Table 43 was created to deduce and summarize the information.

The states of a component can directly affect the state of another component. The State machine figure can help deduce this in to fundamental logic. When the PIR sensor is not detecting motion or gyroscope is detecting position. The MCU will always be powered down, and the SIM800H, NFC and timer will be off. It is always certain that the door is locked. When both the gyroscope and the PIR sensor are tripped, the MCU is on and the SIM800H, NFC and timer is off. A logic table, Table 43 is created to show the relationship of the PIR and gyroscope sensor input to the state of the door being opened or closed and the MCU, SIM800H, NFC and timer. 0 represents the sensor reading a logic low or not being tripped and 1 being logic high and being tripped

Table 43: Logic Table of Hardware Devices Executed Through Software

PIR	GYRO	Locked/ Unlocked	MCU	SIM800H	NFC	TIMER
0	0	Locked	Power down	unused	unused	off
0	1	Unlocked	On	unused	unused	off
1	0	Locked or Unlocked	On	On	usable	On
1	1	Unlocked	On	unused	unused	Off

Not only does the table help with organizing the state structure of the program but it also helps with power consumption. The finite state helps optimize power consumptions by powering the devices for as long as the event that takes place or as long as the state requires those devices. The state machine also minimizes power consumption by only powering specific devices and turning them off or putting it in a power saving state. When no one is at the door and it is locked it is unnecessary to have any of the components on except the sensor or to have the SIM800H, NFC on when the door is open.

A flowchart will help understand the general logic and workflow for the microcontroller. The flow chart will help create the conditional statements for the algorithms to be coded. This will allow the microcontroller to make decision and execute commands in a step by step process based of the input variables. There will be necessary functions that must be called into perform specialized microcontroller tasks. Conditional statements will have to be made for the PIR, NFC, gyroscope, and GSM devices. To help start the algorithm the PIR sensor must be tripped by detecting a presence at the door. If it does The MCU must be waken up to use all the peripherals. Once that is done, the NFC confirmations condition must be met. This is implemented the camera doesn't take a picture and the GSM won't ask for confirmation since the user has an NFC device. If the condition is not made it checks to see if the timer has reached 60 seconds first in order to power down the MCU and its peripherals and minimize power consumption. If 60 seconds have passed and 5 seconds has then then the camera will proceed to take a picture and ask for GSM confirmation. If the NFC or GSM confirmation has been met then the door will be unlocked. Finally a gyroscope condition will have to be implemented in order to see if the user has entered inside. If the user never entered the door will lock after 60 seconds and the MCU will power down. Figure 39 shows the flow chart of the microcontroller.

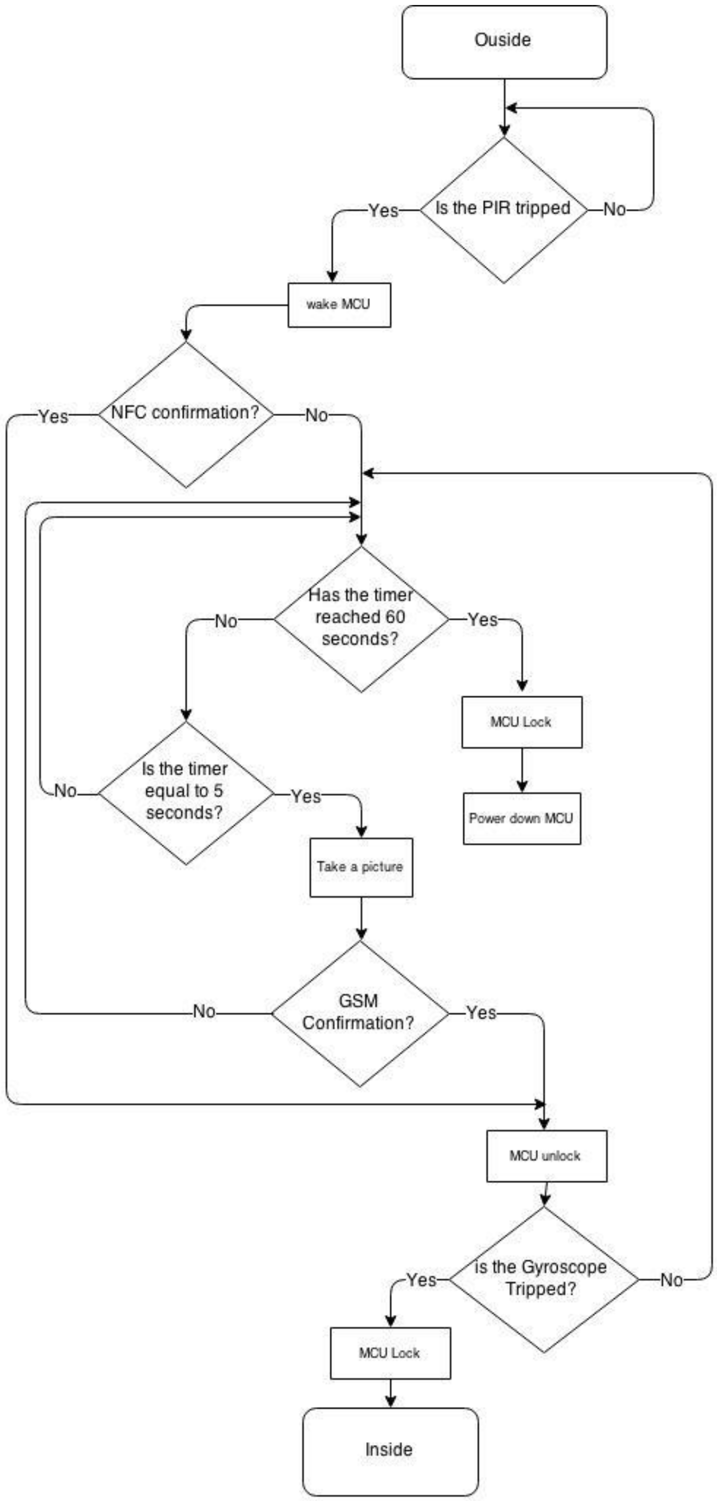


Figure 39: LPC2148 Microcontroller Controlled Flowchart

4.4.5.2 Microcontroller programming

KEIL tools features an MDK-ARM microcontroller development kit will be used to help program and code the LPC2148. The behavior of the microcontroller was designed to optimize and minimize power consumption by turning off the MCU and its peripherals when necessary. The LPC2148 has 3 different power modes, execution, idle and power down. When the system is in idle mode peripheral functions continue to operate and are able to generate interrupt to cause the processor to enter execution mode.

The hardest part of creating a microcontroller system is getting the startup code written and configuring all of the devices and core peripherals. To interface the microcontroller to its peripherals the CMIS-Driver will be needed to be used. CMIS is a software API that creates the peripheral driver interface for middleware stacks. The API groups that are included are I2C, MCI, NAND, Flash SPI, USB and USART, all of which will be used to connect to the devices.

4.4.5.3 Microcontroller USB

Software programming will have to be implemented to perform to all the Capabilities of the USB communication. One of the functions that USB has is being able to detect the attachment of the USB device and makes the host aware of the same. This initial communication is called “Bus enumerations”. To implement this communication the “HID USB Library” and “User Application” must be downloaded to be used as the firmware. For the host side no drivers will need to be downloaded but the host application Delphi must be downloaded.

4.4.5.4 Pin LPC2148 Configuration

Before the microcontroller can use the peripherals the code must be written to configure the GPIO for the LPC2148. The microcontroller has two 32 bit wide I/O ports that give 64 pins. In KEIL the port are defined as P0 and P1. The general format for defining pins and port is PX.Y where X is the port number and Y is the Pin number on the port. By default the peripherals that are contained on the CPU is always enabled. This is unwanted since it will consume more power than necessary. The LPC2148 comes with Power control for peripheral (PCONP) feature that allows the user to enable or disable pins. The USB pin is disabled by default so it won’t need to be changed. This feature can be accessed in the Power control dialog box in KEIL tools. Once the unnecessary pins are disabled the pins’ function has to be defined. The LPC2148 GPIO pins have 4 registers IOPIN, IODIR, IOCLR, and IOSET. The IOPIN register is the value register which tells the current state of the pin. The IODIR is the port pin control register which will help define the direction of the pin. IOCLR is the Output Clear Register controls the current state of the pins. This can help clear the value of the pins by writing a 1 value. The IOSET port output register controls the state of the output register with the IOCLR. This will tell the MCU to tell the pin to output a value.

KEIL C programming uses its own registers to modify the microcontroller pin and registers. Table 44 displays all of the commands to modify the microcontroller’s pins.

Table 44: Commands for Operating Pin of the LPC2148

Command	function
IOSEL0	Selects the function of pins P0.0 to P0.15 of
IOSEL1	Selects the functions of pins P0.16 to P0.31
IOSEL2	Selects the functions of pins P1.16 to P1.31
IO0DIR	Configures the pins of port 0-P0 as input or output pins
IO1DIR	Configures the pins of port 1-P1 as an input or an output
IO0SET	Sets the pins of Port0-P0 to logic 1
IO0CLR	Sets the pins of Port0-P0 to logic 0
IO1SET	Used to set the pins of Port1-P1 to logic 1
IO1CLR	Sets the pins of Port1-P1 to logic 0

5.0 PROTOTYPE AND TESTING PLAN

5.1 Financial Budget

The total cost of the project was split among the 4 group members. The supplies were purchased using online retailers such as Sparkfun, Ebay, Adafruit, and Texas Instruments. In case a part that was shipped is defective excess parts were purchased to prevent the waiting to time for the part to arrive. This method allowed for more efficient project assembly. Table 45 shows the total cost of each component purchased for Secured-E-Key.

Table 45: Total Cost of Secured-E-Key

Part	Cost Per Unit($)	Quantity	Total Cost($)
Gatehouse Lock	$64.95	1	$64.95
Driver SN754410	$2.99	1	$2.99
Adafruit Fingerprint Scanner	$49.95	1	$49.95
LED	$2.99	1	$2.99
Magnetic Reed Switch	$10.59	1	$10.59
NFC Module	$24.00	1	$24.00
PIR Mini Sensor	$9.99	1	$9.99
Micro SD Card	$4.00	1	$4.00
TTL Serial JPEG Camera	$39.95	1	$39.95
LM3488	$3.30	1	$3.30
Lithium Ion Battery	$2.25	4	$9.00
LM3481	$2.40	1	$2.40
Atmega 2560	$5.65	1	$5.65
ESP8266	$7.00	1	$7.00
Wooden Door and Frame	Free	1	Free
PCB Board Fabrications	$84.45	3	$84.45
		Total Price:	$317.57

5.2 Testing Procedures

5.2.1 NFC Testing

Objective 1: The NFC device will have to be tested in order to use it for confirmation. The NFC will be tested to see if it is able to scan NFC phones. To do this a LED can be implemented for verification.

Procedure:
Step 1: Connect the NFC to the PCB along with the LED and power the devices.
Step 2: Hold the NFC device to the reader
Step 3: Wait for the LED to light up to verify that the device is working

Expected Results: A confirmation will happen and the LED should light up.

Objective 2: Another aspect of the device that should be tested is the range. This is important so that the minimum operation distance is known. This test should occur once the NFC is able to read and confirm devices.

Procedure:
Step 1: Make sure that all of the components are connected and that NFC transponder is functional.
Step 2: Move the NFC device slowly to the transponder until it is within range.
Step 3: Wait for confirmation to occur by the LED lighting up and record the distance with a ruler.
Step 4: Repeat the confirmed distances multiple times
Step 5: Get the average distance to see if it falls within the specified operation distance that is on the products datasheet

Results: Once there is a verified confirmation, maximum know operational distance is known. This can safely tell that the device can perform within the operation distance.

5.2.2 Electric Lock Test

Objective: To test to see if the electric lock can properly operate under the proper voltage conditions.

Supplies:
Gatehouse electric door lock
Adjustable Voltage Source greater than 6V
Breadboard
Transistor
Button
Resistor
Arduino Uno

Preparation: Built a circuit that connects the electric strike to the emitter and the power source to the collector with the pull down resistor connected to ground and the Arduino Uno connected to the base.

Procedure:
Step 1: Verify that circuit is properly built and the transistor is in the right position.
Step 2: Set the Arduino to send an output voltage.
Step 3: Wait for the strike to unlock
Step 4: Tell the Arduino to stop sending an output voltage
Step 5: Wait for the electric lock to lock again

Expected Results: The lock should open when the Arduino sends a small current to the transistor so the electric strike can unlock and lock after there is no current.

Objective: To test the operational voltage conditions of the lock

Preparation: Use the previous circuit to test the lock except use an adjustable voltage source that can reach 6V.

Procedure:
Step 1: Verify that circuit is properly built and the transistor is in the right position.
Step 2: Set the Arduino to send an output voltage.
Step 3: Wait for the strike to unlock
Step 4: Tell the Arduino to stop sending an output voltage
Step 5: Wait for the electric lock to lock again
Step 6: Reduce the Voltage source
Step 7: Repeat until the lock is not operational

Expected Results: The outcome of this testing should show the range of operation for the door lock. This can help show the minimum value that the battery voltage can be until the device is not operational.

5.2.3 Battery Monitoring

Objective: To see if the battery monitor is operational and that it is operating at the proper conditions.

Supplies:
Battery Monitor
Adjustable voltage supply up to 7.4V

Preparation: make sure that the battery monitoring circuit is properly built and the setup is correctly made.

Procedure:
Step 1: Verify that the Voltage source is properly connected
Step 2: Set the Voltage source to 7.4V
Step 3: Wait for the Green LED to turn on
Step 4: Lower the Voltage until the yellow light turns on.
Step 5: Record the input voltage

Expected Results: The Green LED should turn on when the voltage is 7.4V and reach yellow when it is 5.5V. This will properly tell the right conditions that the lights will operate at.

5.2.4 Microcontroller Testing

Objective: The LPC2148 will have to be tested to see if all the peripheral devices are properly configured and that the microcontroller can be successfully programmed to function the way it should.

Supplies:
LPC2148
LED
Resistor
KEIL ARM tools
USB

Procedure:
Step 1: Connect the LPC2148 to the computer
Step 2: Create a program that will tell the LED to turn on.
Step 3: Upload the program and wait for the LED to turn on

Expected Results: The LED should turn on when the instruction code is uploaded to the microcontroller. This is one of the first things most programmers do to test to see if the microcontroller is configured, fully operational and connected.

5.2.5 SIM800H Testing

Objective: The SIM800 must be tested to see if It is able to receive a signal and then to see if it is able to transmit a message.

Supplies:
SIM800
Arduino Uno
LED
Resistor
Cellular Device

Preparation:
Connect the SIM800 to the Arduino Uno along with the LED to an analog output pin. Program the Arduino to turn on the LED when it receives a signal and then transmit a message when the LED is turned on.

Procedure:
Step 1: Verify that The SIM800H and the LED is properly connected
Step 2: Send a signal to the SIM800H
Step 3: Wait for the LED to turn on
Step 4: Look for the message to be send to the cellular device

Expected Results: The LED should be able to turn on When a message is sent and the Cellular device should be able to receive a message. This basic testing illustrates that there is two way communication between the SIM800H module. This results is a simplified test for opening a door with GSM communication.

5.3 Expected Model of the Final Product

At that stage of our project, one of the point that we to specify is how we are going to assemble everything once we are done with the electronic part of the project, that is, we need to explain the position of all the peripherals and their connection to the PCB when we will mount everything. Just before talking about that, we want to mention as we were working on the design section that will be showed later in this paper, we encountered some constraints that made us decide to have a separate box for the PCB, the batteries and the LEDs. In fact, we realized that the case of the lock would not be big enough to house all those parts, and adding the box will not affect negatively our design. We needed to make some analysis in order to find out what could be the best way to assemble all the element of the Secured-E-key, because the efficiency and the durability of the Secured-E-key depend not only on the design of the system, but also on how everything is mounted on the door.

The first way that we considered when we had to decide about where to place all the external parts of the Secured-E-key was to put the camera and the PIR sensor on the outside of the door with the camera on top of the sensor, and the connection would have to be made inside with the lock system and the PCB, with the PCB mounted on the wall. With that design option, not only we would need to use long wires to connect the PCB on the wall to the camera and the sensor, which could engender more power dissipation in the wire and the junctions themselves, but in the long run, the constant back-and-forth motion of the door would break the cooper filaments, and that would result in a malfunction of the security system that we intended to re-enforce in the first place when we started working on that project.

The second way that we considered was to keep the same position of the camera, the sensor and the lock, but this time we would have the PCB mounted on the door. At the opposite of the first option, that way of assembling the system would not need long pieces of wire to connect the parts to the PCB; that means, the system would have less power loss. Moreover, there would be no back-and-forth motion to break the wire, and the overall system would look more beautiful. When we considered carefully these analyses, we decided to opt for the second assembly. Figure 40 displays the outside and inside of how Secured-E-Key will look when mounted on the door and Figure 41 shows the LED display of the battery monitor.

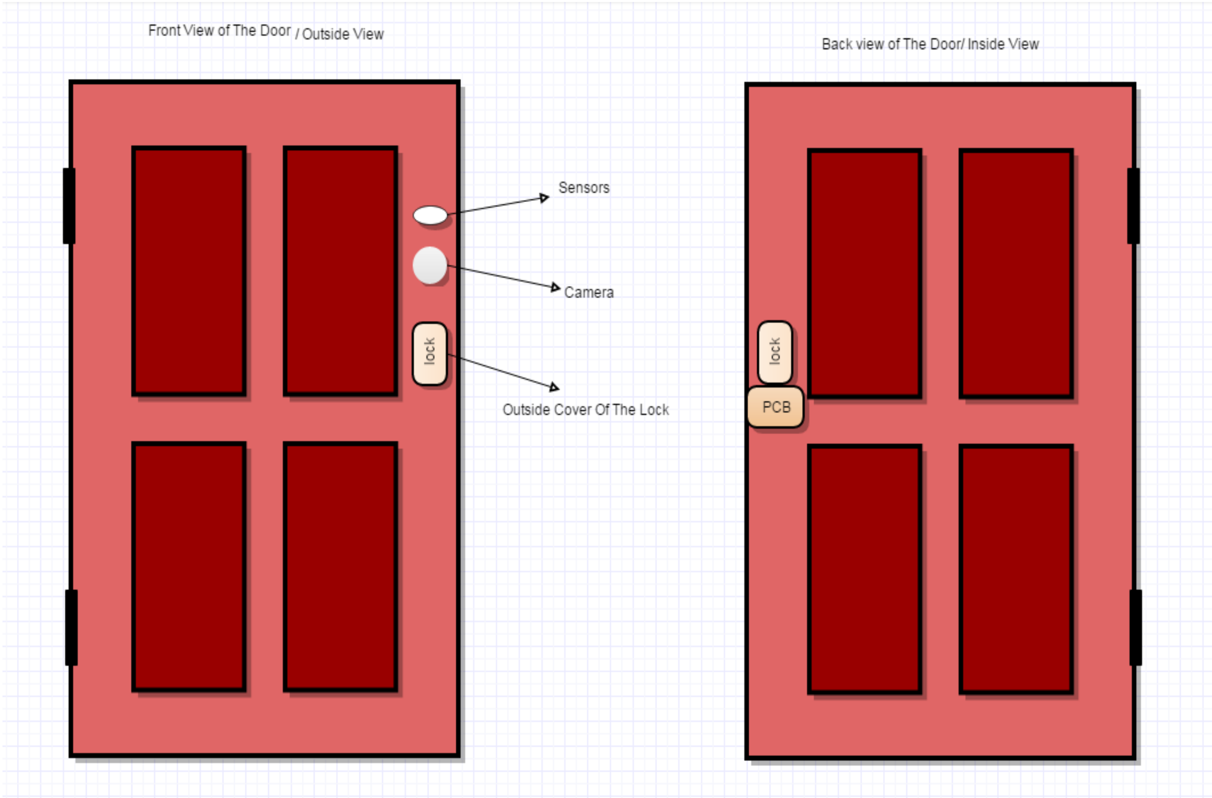


Figure 40: Outside and Inside View of The Secured-E-Key mounted to Door

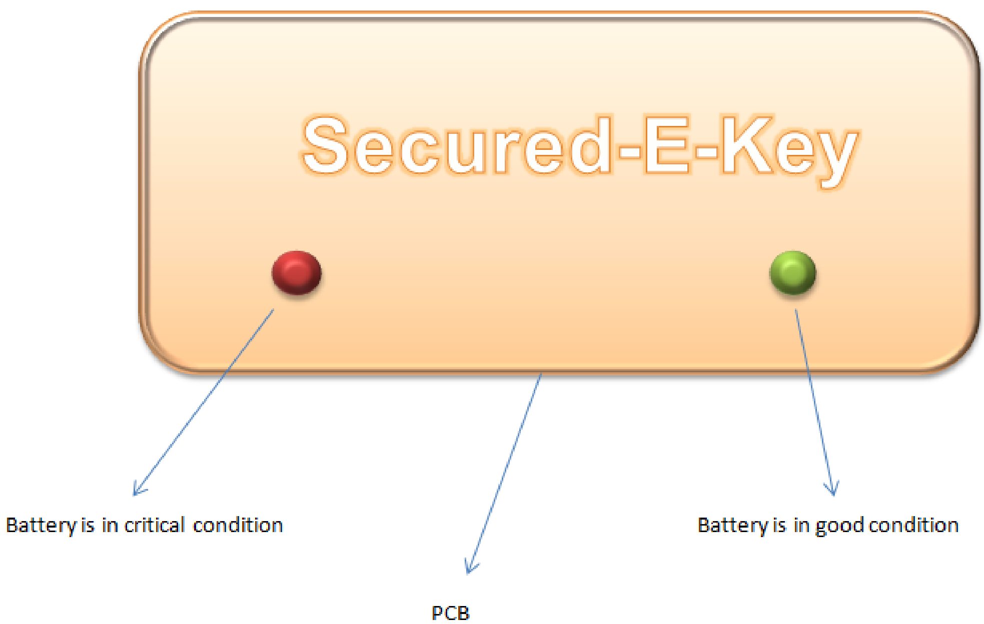


Figure 41: Picture of the PCB with the LEDs

5.4 PCB Construction and Integration

A final and important project to must be done is producing a printed circuit board (PCB) for the final design. Creating the PCB will allow for better integration of all of the electronic devices and components that will be used. It will also allow for better organization giving a professional look to it. There are ways for creating a PCB for the project. The first ways is Sending a CAD design of the board to a company and allowing them to create and ship the board. The other method is obtaining all of the parts that will be used and then assembling the PCP by hand. One advantage of allowing a company to manufacture the board is that it will allow less room for mistakes. If the PCB were chosen to be assembled by hand then it is more likely that a component will get damaged and the liability will be on the group. The disadvantage of having a PCB manufactured by a company is that it will cost significantly more to produce.

5.4.1 PCB Retailers

There are many companies that are able to manufacture PCBs. 4pcb is website for the company called Advanced Circuits. They offer to standard options for PCB creation. The first option is creating a Full Spec 2-Layer PCB for $33 each. There is a minimum of a 4 board requirement. The second option is a Full Spec 4-Layer PCB design for $66. Advanced Circuits also have a sponsorship program that can help pay for the PCB design if necessary. OSH Park is another company that produces PCBs. They have 2 options for PCB design. The first option is a 2 layer board that will cost $5 per square inch with 3 boards that are included in the price. They can also produce a 4 layer board at a cost of $10 per square inch that also includes 3 boards in the price.

5.4.2 Design Considerations

Before a PCB can be sent to the company a schematic must be made to entail the design. There is much software that is capable of doing this. Eagle CAD is a very popular option for PCB design since it is free to download and to use. There a many library and files which contain electronic parts which will make it easier to use. Considerations much be made when creating a schematic for the PCB. The design must have a template for the Card dimensions so that all of the circuitry can be put on the board. The positions of the components and the heat sink must also be determined. The stack layer must also be determined based on the complexity of the project. There are also different standard technology that will be can be used. The Through-hole technology creates the board so that electronics can be mounted by leads and inserting them through holes on one side of the board. Then it is soldered on the other side. This can add to the boards cost since holes have to be drilled. Another technology that is used is the surface mount. Many electronic components are designed to have metal tabs so that it can be soldered directly onto the board.

6.0 APPENDIX

6.1 Permissions

Permission Request to Use SIM800H PCB Layout Figure

Sheldon Johnson <sheldonjohnson159@gmail.com> Apr 21 (9 days ago)

to simcom

Hello,

I am an undergraduates electrical engineering student at the University of Central Florida working on a senior design project which will use the SIM800H GSM/GPRS module your company produces. I would like to request for permission to use the figure attached to this email in my senior design paper.

It comes from the datasheet I have also attached. You can find the image on page 55 of the document.

The university requires me to request for permission in order to use images I find.

I would greatly appreciate using the diagram and it would help me explain the design I have created within my report very much.

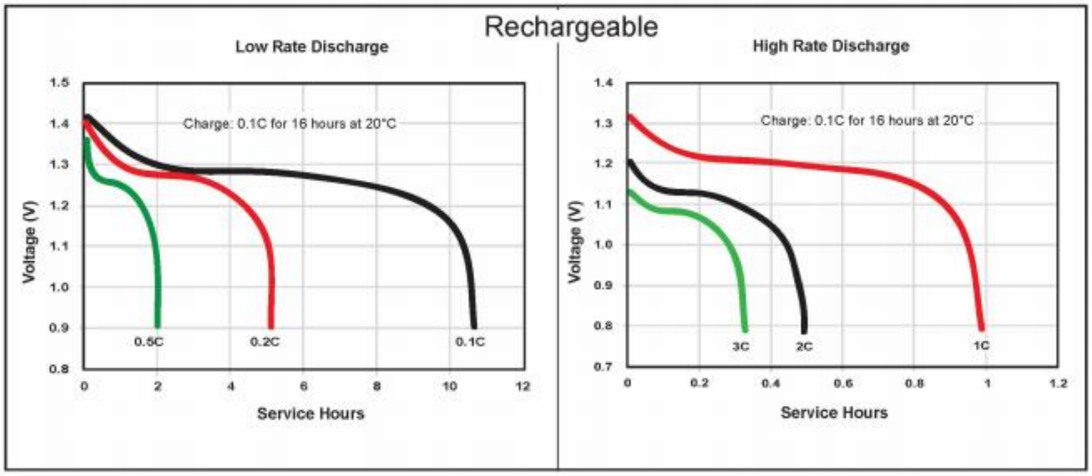
Thank you,

2 Attachments

SIM800H_Hardware_Design_V1.01

SIM800H Datash...

Authorized consent of the battery diagrams from the data sheet image below.



Information and contents in this data sheet are for reference purposes only. They do not constitute any warranty and representation is subject to change without notice. For most current information and further details, please contact Duracell.

Page 1 of 2

Document #: RE-A

DURACELL Rechargeable

DC1500

Size: AA 2450 mAh (HR6)

Rechargeable NiMH Battery

NiMH

1- Authorization from Custom Silicon Solutions

avr 23 à 3h29 PM

Paul,

The data sheets are copyrighted so you are free to use them as long as they are properly referenced and attributed.

Regards,

-Mike

Michael McDaid

Director of Sales

Custom Silicon Solutions, Inc.

Cell: 949-275-3193

Tel: 949-872-2426

www.customsiliconsolutions.com

From: Saint-Surin Paul [mailto:surin67@yahoo.fr]
Sent: Thursday, April 23, 2015 11:30 AM
To: form@customsiliconsolutions.com
Subject: Custom Silicon Solutions Contact Request

First Name :	Saint-Surin
Last Name :	Paul
E-mail Address :	surin67@yahoo.fr
Phone Number:	4072335320
Company :	student
Industry :	Other
Time frame to get started :	A.S.A.P
What are your interests?	Updates on Products & Services

Please enter any questions or comments in the following form:	Hi, my name is Saint-Surin Paul and my team I are working on a senior design project at UCF (University of central Florida). I did some research on the CSS555 micro-power timer listed on your website. Actually, I was very glad to see that you have all the datasheet available for the part that you are selling. The purpose of my email is to ask for your permission so I can use the data sheet for the item that I mentioned in my paper. I don't want to pressure you, but I would like to mention that without your permission our research on this item will not be complete because I can not include it on my paper without that. A special anticipated thank you!
IP Address :	132.170.212.51
Referral URL:	http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CCoQFjAC&url=http%3A%2F%2Fwww.customsiliconsolutions.com%2Fproducts-for-ASIC-solutions%2Fstandard-IC-products_no.aspx&ei=JTU5VYSrEorFsAXRrIHYBQ&usg=AFQjCNHPO0WL0RQ_BXxMOYSbOr9mNXZ9YA&sig2=FrAwsOrf8gYzEVKFp2sudg&bvm=bv.91427555,d.b2w

2- Authorization from sparkfun

Saint-Surin Paul <sainsu67@gmail.com> Apr 23 (4 days ago)

to website

Hi,
my name is Saint-Surin Paul and my team I are working on a senior design project at UCF (University of central Florida). I did some research on two microphone. listed on your website which are the BOB-09964 and the COM-08635. Actually, I was very glad to see that you have all the datasheet available for the part that you are selling.
The purpose of my email is to ask for your permission so I can use the frequency response graphs and the stage gain graphs for both items that I mentioned. I don't want to pressure you, but I would like to mention that without your permission our research on those items will not be complete because I can not include them on my paper.

A special anticipated thank you!

SparkFun Customer Service <cservice@sparkfun.com> Apr 24 (3 days ago)

to me

Hello!

Sure! Go for it. Anything available in the data sheets is going to be public knowledge. So you are fine!

Best Regards,
Shay Woods

Customer Service Representative
SparkFun Electronics
www.sparkfun.com
303.945.2984

6.2 Bibliography

1- [Online]. Available: http://www.yashplus.com/2013/11/how-ic-555-works-fundamentals-of-ic-555-its-basic-applications/ [accessed 3 25 2015]

2- [Online]. Available: http://en.wikipedia.org/wiki/555_timer_IC [accessed 3 25 2015]

3- [Online]. Available: http://www.customsiliconsolutions.com/downloads/Revised%20Standard%20products/CSS555C_Spec.pdf [accessed 4 10 2015]

4- [Online]. Available: http://www.customsiliconsolutions.com/products-for-ASIC-solutions/standard-IC-products_no.aspx [accessed 4 10 2015]

5- [Online]. Available: http://www.lowes.com/pd_399128-51800-G2X2D01_0__?productId=3799025 [accessed 4 13 2015]

6- [Online]. Available: https://www.sparkfun.com/products/retired/10061 [accessed 4 14 2015]

7- [Online]. Available: http://www.lingwei-cn.com/html_products/Super-MINI-DIY-VideoAudio-Camera-122.html [accessed 4 14 2015]

8- [Online]. Available: http://www.handlesets.com/?gclid=Cj0KEQjwgoKqBRDt_IfLr8y1iMUBEiQA8Ua7Xcu [accessed 4 15 2015]

9- [Online]. Available: https://www.locksonline.com/ [accessed 4 15 2015]

10-[Online]. Available: http://www.adafruit.com/products/1890 [accessed 4 15 2015]

11-[Online]. Available: http://www.kingbrightusa.com/product.asp?catalog_name=LED&product_id=AA2214SES/J3-AMT [accessed 4 16 2015]

12-[Online]. Available: http://www.afiata.com/ [accessed 4 16 2015]

13- [Online] available: http://simplytronics.com/products/ST-00081 [accessed 4 16 2015].

14- [Online] available: http://datasheets.maximintegrated.com/en/ds/MAX21000.pdf [accessed 4 18 2015]

15- [Online] available: http://www.ti.com/lit/ds/symlink/rf430cl330h.pdf [accessed 4 17 2015]

16-[Online]. Available:http://www.ti.com/product/MSP430F5529/description[accessed 4 17 2015]

17-[Online]. Available: http://www.4pcb.com/ [accessed 4 5 2015]

18-[Online]. Available: https://oshpark.com/ [accessed 4 5 2015]

19-[Online]. Available: http://blog.optimumdesign.com/through-hole-vs-surface-mount [accessed 4 17 2015]

20-[Online]. Available:http://www.oscilent.com/spec_pages/PNDescrpt/Tolerance.htm[accessed 4 8 2015]

21-[Online]. Available: http://www.engineersgarage.com/arm-projects/how-to-start-programming-arm7-based-lpc2148-microcontroller[accessed 4 8 2015]

22- [Online]. Available: http://data.energizer.com/PDFs/nh15-2300.pdf [accessed 4 10 2015]

23- [Online]. Available: http://ww2.duracell.com/media/enUS/pdf/gtcl/Product_Data_Sheet/NA_DATASHEETS/DC1500%20NiMh-%202450mAH-AA.pdf[accessed 4 13 2015]

24- [Online]. Available: http://www.ti.com/lit/an/spma066/spma066.pdf[accessed 4 13 2015]

25- [Online]. Available: http://www.ti.com.cn/cn/lit/ds/spms376e/spms376e.pdf[accessed 4 13 2015]

26- [Online]. Available: http://arduino.cc/en/main/arduinoBoardUno[accessed 4 13 2015]

27- [Online]. Available: https://www.sparkfun.com/datasheets/Components/SMD/ATMega328.pdf[accessed 4 13 2015]

28- [Online]. Available: http://www.raspberrypi.org/products/raspberry-pi-2-model-b/[accessed 4 17 2015]

29- [Online]. Available: http://www.mobileappsystems.com/blog/raspberry-pi-operating-systemsLPC2148[accessed 4 17 2015]

30- [Online]. Available: http://www.keil.com/product/brochures/uv4.pdfPeripherals[accessed 4 17 2015]

31- [Online]. Available: http://www.embedded.com/design/connectivity/4023975/Serial-Protocols-Compared[accessed 4 17 2015]

32- [Online]. Available: http://www.adafruit.com/products/751?gclid=Cj0KEQjw27etBRDA3-ux4p3c58EBEiQAkJzTAMDbXq7j6pP1T7vpozMB7-5i8paaFDXsIIzErpHZY0AaAnoW8P8HAQ [accessed 24 7 2015]

33-[Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDoQFjADahUKEwih8f-x7OrGAhVCKx4KHehhCo0&url=http%3A%2F%2Fwww.adafruit.com%2Fdatasheets%2FESP8266_Specifications_English.pdf&ei=FoKtVaGOL8LWeOjDqegI&usg=AFQjCNG9qkY0vU9suD7gm74UvB7rqnNnjg&sig2=KHTNFnlfmm6xPQ3Ia1gUUQ&bvm=bv.98197061,d.dmo&cad=rja [accessed 24 7 2015]

34-[Online]. Available: http://www.ti.com/product/lm3481 [accessed 24 7 2015]

35-[Online]. Available: http://www.ti.com/product/lm3488 [accessed 24 7 2015]

36-[Online]. Available: http://simplytronics.com/products/ST-00082 [accessed 24 7 2015]

37-[Online]. Available: http://www.nxp.com/documents/short_data_sheet/120112.pdf [accessed 24 7 2015]

38-[Online]. Available: http://www.adafruit.com/product/397 [accessed 24 7 2015]

"Programming Arduino Getting Started with Sketches". McGraw-Hill Nov 8,

Retrieved 2013-03-28. (Arduino Software)