ECEN 5053-003 (S'19)

Assignment – 3

Paper on Product Tear-down

Review Paper

Project Details	*Description*
Created By:	**Rushi James Macwan**
Date:	**14th April 2019**
Project Title:	**Paper on Product Tear-down**
Class Name	**Developing Industrial IoT** **ECEN 5053-003 (Spring-2019)**
Tear-down Product:	**WSDCAM anti-theft wireless remote controlled security system for doors/windows**
Time spent after this assignment	**10-12 hours**

Introduction

There has been a growing need for safety, security and privacy as technologies have advanced and resources are being exploited more than ever before. These needs have continuously shaped the way we architect our lives keeping in mind the security threats. Physical attacks that involve thefts and burglaries is one of the most common issues that the society faces. Over the ages, different locking/security mechanisms and systems have been developed to protect public or private resources. However, often the technologies that have been devised to secure our residences or public resources lack simplicity and fall short of providing strong and reliable safety. This paper incorporates a thorough breakdown of a typical Industrial IoT product that is used to provide efficient and reliable security alarm system for something as simple as doors and windows of a house. The proposed alarm system provides a very simple and ultra-low cost solution for an alarm system that provides an effective to discourage thefts and burglaries.

The following sections will include the following aspects pertaining to the Industrial IoT product which is at the focus of this paper:

1. Introduction to the Industrial IoT Product
2. Device market and application area
3. Architecture and design of the product
4. Block diagram of the product
5. Technical details and descriptions
6. Power requirements and product life-span
7. Bill of Materials
8. Security concerns
9. Concluding remarks
10. Appendix

Please note: On several occasions the terms “product” and “system” have been used interchangeably. It has been assumed that most Industrial IoT projects are both collectively a product and a system as it incorporates the use of multiple connected elements.

The WSDCAM anti-theft wireless remote controlled security system for doors and windows

Introduction to the Industrial IoT Product

Autonomous security systems that require insignificant human intervention is blooming by leaps and bounds. Evolving security systems involve robust and reliable wireless remote controlled operation. This facilitates the user with an easy operation while caring only so little about the physical constraints. Moreover, the security systems today incorporate an alarm system that is stimulated by an unauthorized breach/access inside the network of sensors and actuators that is under the surveillance of the system.

WSDCAM provides one such anti-theft alarm system that discourages thefts and burglaries. WSDCAM provides a solution which features a wireless remote controlled operation of the alarm system. The focus of the product is upon securing the doors and windows of a building. The alarm system generates an alarm

siren whenever a door/window (wherever the system is embedded) is opened or closed or if the unit experiences vibrations. This idea ensures that unauthorized accesses to a building stimulate the alarm system to produce effective alarm signals to prevent security breaches.

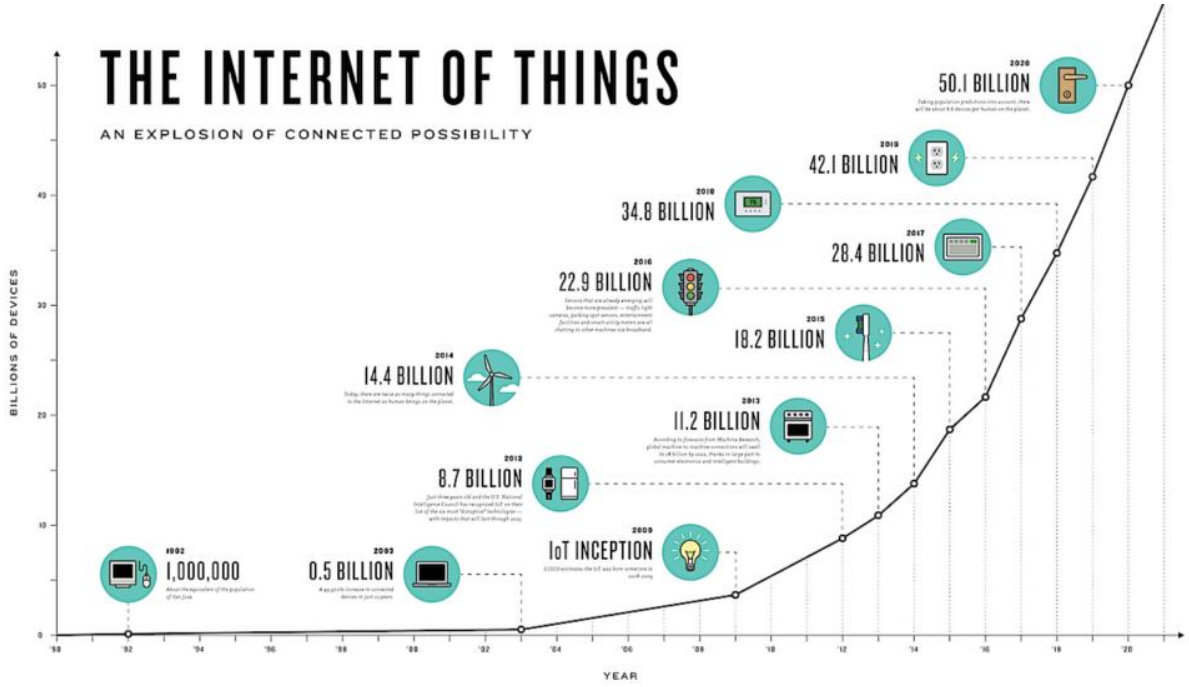
Device Market and Application Area

Security systems have a growing device market today. The applications are far and wide. Various companies and organizations today are embarking on a journey to design smart, robust and reliable solutions that can ensure a safe and secure society. However, in spite of all the efforts, it is impractical to achieve a cent percent secure environment but it has become increasingly more difficult to break into the developing security systems.

One of the companies working on the security and alarm systems is Telit. The company is building the world's first 4G/LTE mobile monitoring camera. "Nubo connects to 4G/LTE mobile networks and Wi-Fi, so customers can stay connected no matter where they go. Small and rugged, Nubo is weatherproof so it can be used almost anywhere. The revolutionary 4G/LTE camera has opened up the market for mobile video monitoring. It is a versatile LTE camera that connects over a cellular or wireless network and helps consumers and businesses see their valuables anytime, anywhere."[1]

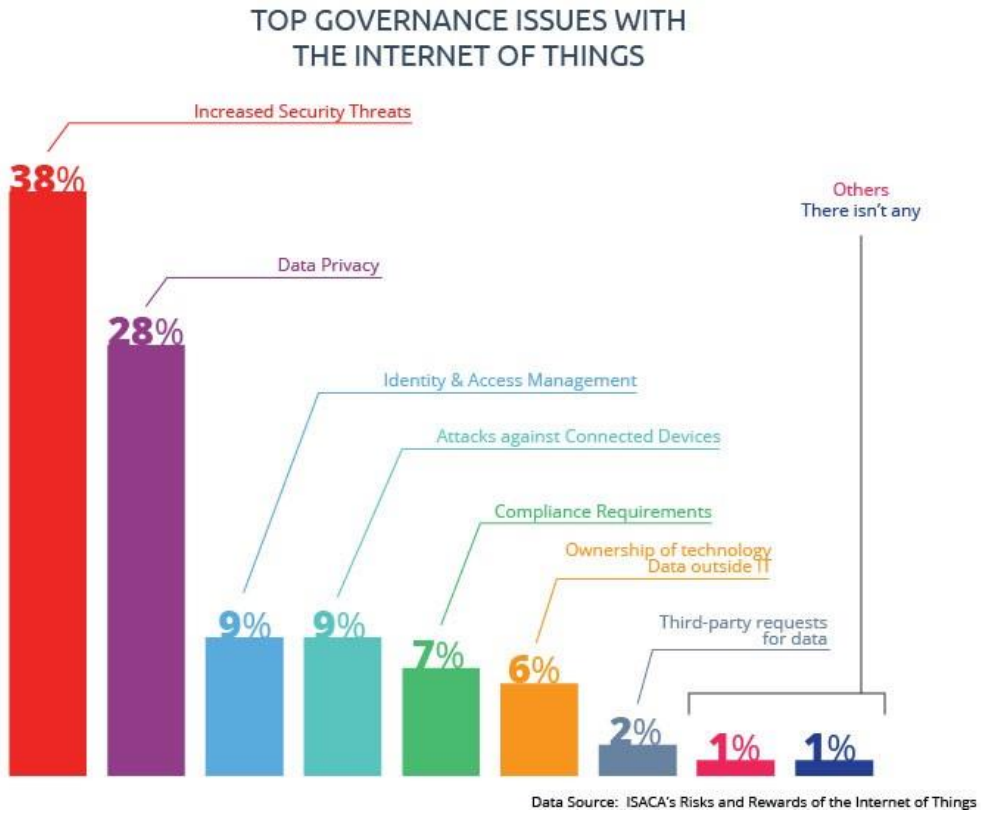
At the same time, various IoT companies are working on the software side of the safety issues which involve topics like network security, authentication, encryption, public key infrastructure (PKI), API security and specially security analytics.[2] On the other hand, CISCO has been working hard to develop smart home security solutions. One of its solutions involved the use of Linksys video surveillance camera system which sends its users a video recording of the place when a motion is detected where the system is located in absence of the users.[3]

The growth of these security system applications have impacted the security device/system market by several folds. The security system industry has inflated by several folds as the Internet of Things has empowered companies and organizations to connect on a scale that has never been seen before.



Source – Medium (link)

On the other hand, the growth of the IoT technologies have resulted into several governance issues. According to a study, increased security threats and data privacy issues are the top most concerns that have come up with the extensive use of the connected devices or in other words the Internet-of-things world.[4]



Source – Medium (link)

Based on the above studies, the paper will deeply focus on the other facets of the security alarm system that is at the focus of the paper.

Architecture and design of the product

WSDCAM provides a reasonable security alarm solution in the form of an industrial IoT product. This product is designed such that it incorporates the use of the following three physical elements:

1. A Host Locking Platform (HLP)
2. A wireless Remote Control Device (RCD)
3. A magnetic stick

The HLP is essentially a door/window alarm device that produces a siren whenever an unauthorized access is performed. The RCD is used to configure the HLP in one of the following modes:

1. Armed mode
2. Disarmed mode
3. Doorbell mode
4. Emergency/panic mode

The user has the freedom to set the HLP to the armed mode so that it produces an alarm whenever the door/window is opened or closed. The disarmed mode is exactly opposite of the armed mode where the HLP does not react to the door/window movements. The doorbell mode as its name suggests, produces a "dingdong" sound whenever the door/window experiences a movement or vibration. Lastly, the panic mode ensures that the user can produce an emergency alarm during crucial circumstances wherein the HLP does not have to consider the door/window movements/vibrations.

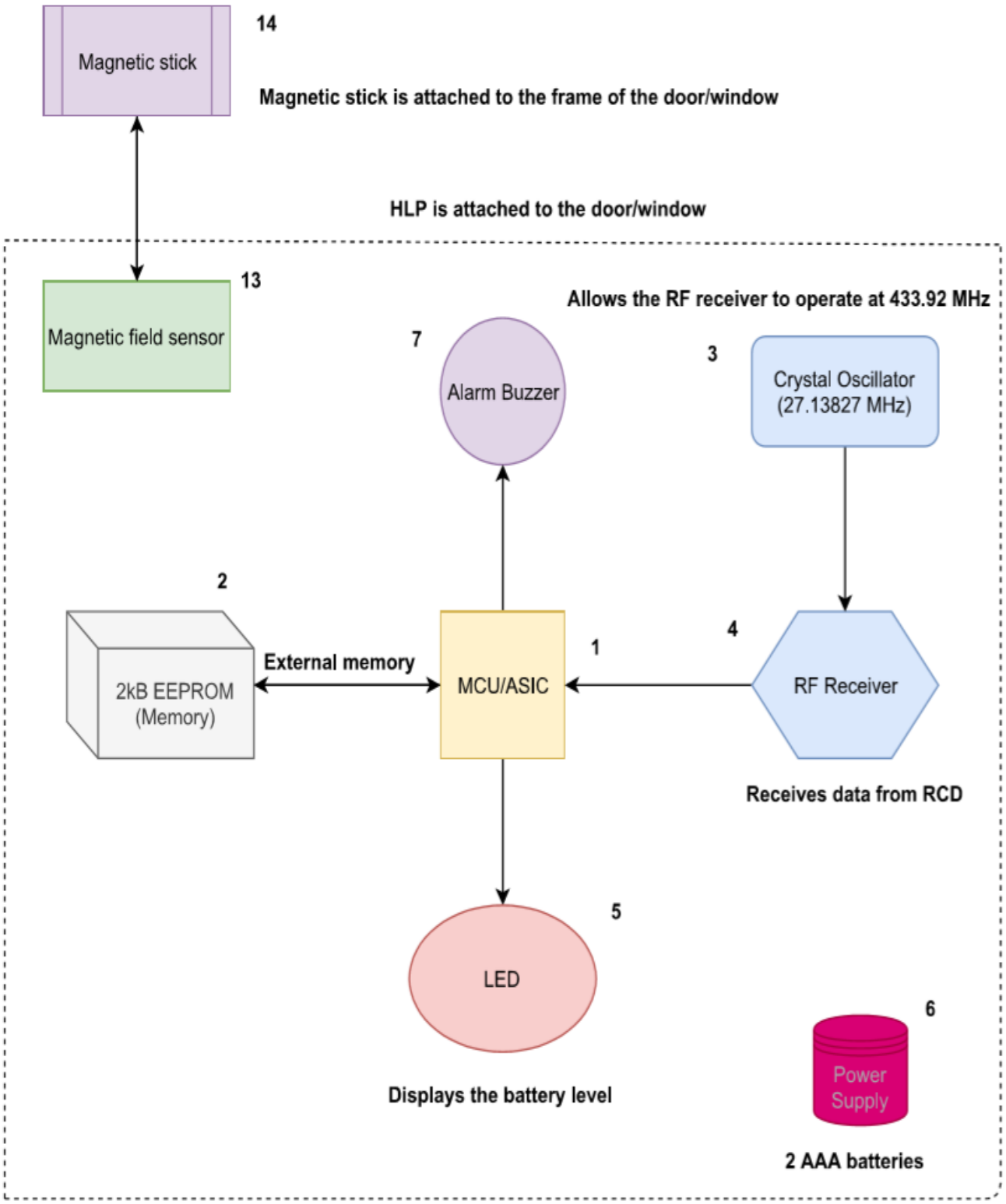
The HLP is attached to the door/window which has to be kept under surveillance. Adjacent and parallel to the HLP, the magnetic stick is attached on the frame of the window or door. The magnetic stick is essentially a magnetic that generates a permanent magnetic field in its vicinity. The HLP is kept within a distance of 10mm from the magnetic stick so that it can reliably interact with the magnetic stick through its capability to interact with the external magnetic fields. Whenever the door/window is opened, the HLP loses contact with the magnetic stick and this stimulates the HLP to produce an alarm signal as per the mode that user has set for the HLP using the RCD.

It is important to point here that one HLP can connect with up to eight RCDs and one RCDs can connect with multiple HLPs. This is inherently characteristic of the Bluetooth protocols concerning the configuration of a Piconet which allows a network of up to eight connected devices.

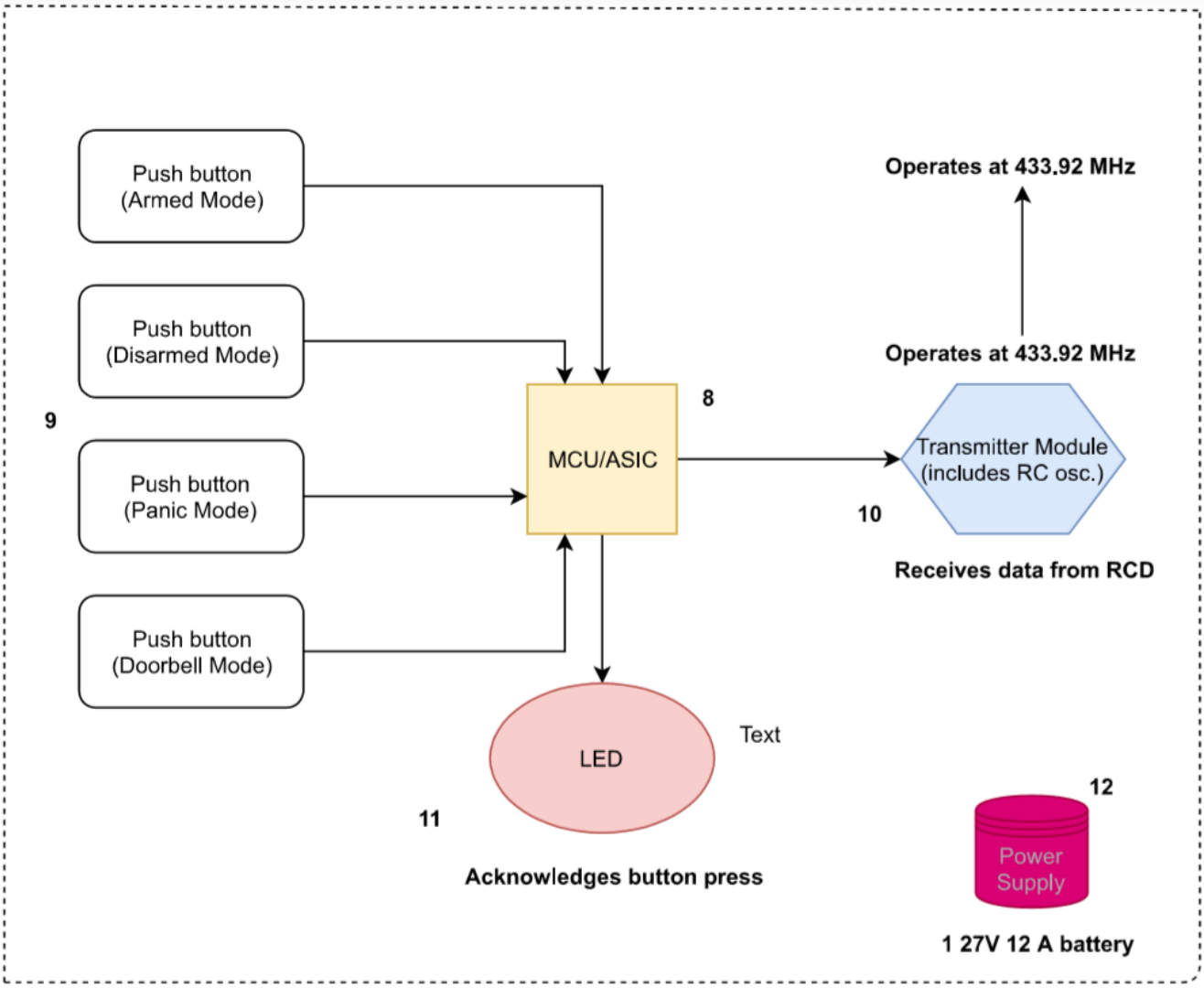
In addition to the above physical elements, the product requires appropriate power sources in both the locking platform and the wireless remote devices. The product has a battery life-span of up to 2 years assuming that the product is installed in a location that is indoor and that the number of remote operations is limited to a maximum of 5 times a day. Since the product is an Industrial IoT product, it will have its own power requirements and security issues which will be later discussed in the paper.

Block diagram of the product

The block diagram shown below includes all the three physical elements that go into realizing the product. The individual fragments of the block diagram have been numbered from 1-14 which will appear at length on the bill of materials associated with this paper.



HLP Block Diagram



RCD Block Diagram

Technical details and descriptions

The WSDCAM Alarm System involves the following 14 elements that will go into the building of the product:

Elements on the HLP unit:

1. MCU/ASIC
2. 2kB EEPROM External memory
3. 27.13827 MHz Crystal Oscillator
4. RF receiver
5. Battery status LED
6. 2 AAA Batteries
7. Alarm Buzzer

Elements on the RCD unit:

8. MCU/ASIC
9. Push-buttons
10. Transmitter Module (includes the Crystal Oscillator)
11. Push-button status LED
12. 1 27V 12A battery

Apart from the above elements, the following two elements will stimulate the alarm system:

13. Magnetic field sensor on the HLP unit
14. Magnetic stick fixed on the door/window frame

Please note: The part numbers provided on the HLP and RCD does not match with any of the appropriate parts available on the internet. Therefore, it has been assumed that both the HLP and RCD units operate using one of the two elements: either an MCU or an ASIC.

Hardware Execution Sequence:

The product involves the following sequences of events which stimulates the alarm system to warn the user of a particular theft or burglary:

- Initially, the user presses the one of the push buttons on the RCD to register the RCD with the HLP or to set the HLP into a particular mode (e.g. armed mode). The MCU/ASIC on the RCD will respond to the user request by turning on the blue LED on the RCD for about one second.
- While the above process takes place, the MCU/ASIC on the RCD will send orders to the RF transmitter on the RCD to send appropriate mode configuration or user registration RF signals to the RF receiver on the HLP.
- The RF receiver will on the HLP will respond to the received signals by passing appropriate signals to the MCU/ASIC on the HLP. The MCU/ASIC on the HLP will stimulate the buzzer in order to provide the user with an acknowledgement that the said mode has been established. If the mode establishment fails, the MCU/ASIC will not be stimulating the buzzer which would imply that the user will retry the process.
- The MCU/ASIC on the HLP will also blink the red LED on the HLP for every few seconds once it has been triggered into one of the modes. The LED will also notify the user if the battery level falls below a particular threshold.
- The MCU/ASIC on the HLP will also store the user RCD authentication code to the EEPROM external memory along with the mode that has been set. This ensures that every time a user is added or the mode is changed, the MCU/ASIC on the HLP will update the EEPROM external memory.
- While a mode other than the disarmed mode has been set for the HLP, the magnetic field sensor on the HLP will interact with the magnetic stick adjacent to it within a 10mm distance located on the door/window frame.
- If the door/window is opened, closed or vibrates then the field sensor will experience variations in the signal reception from the magnetic stick and will send appropriate signals to the MCU/ASIC on the HLP.
- The MCU/ASIC on the HLP after receiving triggering signals from the field sensor on the HLP will send the signals to the buzzer and the alarm will turn on as per the sequence of events and the mode the HLP has been set to.

Software Processes:

- While the software elements associated with this product cannot be clearly analysed, it is very clear that both the HLP and RCD units have a preferred set of identification codes that are established while a connection/registration is made between the two units.
- The push-buttons on the RCD would also generate different codes that would trigger the HLP to set to a particular configuration (e.g. armed mode).
- The MCUs/ASICs on both the HLP and the RCD units involve a certain program/code that helps them run the entire process of hardware execution as mentioned above.
- In addition to the above point, the software loaded into both the units (i.e. HLP and RCD) will enable them to operate in ultra-low power modes as and when necessary.
- The software execution would also allow both the units to track the battery level so as to make the user aware of a needed replacement.
- In addition to all the above points, special security measures would have been taken in the software written for the units that an intruder is not able to read the contents or access the code memory of the units.

Power requirements and product life-span

Power requirements is one of the most essential part of an industrial IoT product. The WSDCAM alarm system is a very tightly power constrained product. The RCD uses a 27A 12V alkaline battery that provides a 2 year battery life-span for the RCD assuming that every day, there are no more than 5 triggering or button presses. The HLP on the other hand provides a 2-year life span provided that the magnetic field sensor triggering takes place for no more than 5 times a day.

The HLP unit is designed in a fashion that it enters the ultra-low power mode whenever the HLP unit is configured into the disarmed mode. On the other hand, the RCD unit is designed such that it would consume low power at all times except whenever a push button interrupt occurs.

The product physical life-span is based on the environmental conditions that it operates upon. The product is expected to work in an atmosphere where humidity is less than 80% and the working temperature lies between -10 and 60 degree Celsius while the storage conditions range between -20 and 70 degree Celsius.

Bill of Materials

The bill of materials includes all the essential tear-down information on the components that were used to produce the product. All the elements (1-14) that were presented in the block diagram have been included in the bill of materials. Wherever reliable information was unavailable, appropriate assumptions have been made and they have been added with an asterisk (*).

Security Concerns

Security and safety is at the centre of the goals and objectives of the industrial IoT product that this paper focuses upon. However, the safety and security of the product itself is at the core importance. If a security system is compromised, the safety and security of the entire system associated with the product is compromised.

The WSDCAM alarm system allows a connection of up to eight RCD units with one HLP unit. On the other hand, one RCD unit can connect with multiple HLP units. This fashion of connection itself opens a space of compromise. While it is true that once an RCD unit is registered with one HLP unit, only the RCD unit that is registered has the capability to withdraw/cancel its registration on a HLP unit. This implies that if a registered RCD unit is lost, the user security and safety is compromised because the lost RCD unit allows an intruder to gain an unprivileged access.

In addition to the above security concern, it is true that the HLP MCU/ASIC stores important codes and information in the external EEPROM available on the HLP unit. If an intruder gains an unfair access to the user's HLP unit, the HLP device can be compromised as the intruder can physically damage or attack the HLP unit and thus the EEPROM in two different ways:

1. The intruder can steal the information in the EEPROM available on the HLP through methods of physical attack
2. The intruder can even replace or change the contents of the EEPROM with his/her RCD unit so that the HLP remains under the impression that the intruder's RCD unit is registered and authorized to gain an access.

While there are abundant possibilities that a security system can be compromised, companies and organizations are coming up with better and stronger standards and technologies that can reduce the chances of a security compromise.

Concluding Remarks

To conclude, this paper relates the essential elements that were taught in the class with the technologies that are being used outside the class. Through this paper, I have learnt how a typical industrial IoT system is manufactured keeping in mind the points that go into building an industrial IoT product. Some of the key learnings that I had pertaining to an industrial IoT product/system with this paper are as below:

1. Limited form-factor
2. Limited power supply
3. Limited hardware-software complexity
4. Application specific design
5. User-friendly execution architecture
6. Secure and safe products/systems
7. Products/systems with high operational efficiencies
8. Products/systems with reliable service
9. Real-time response to the user
10. Near fail-proof systems

Questionnaire based on the paper guidelines:

Could the device be improved?

Yes. The device can be improved by reducing the existing complexities and loopholes that allow an intruder to access the system and by which the security of the system and the user is compromised.

Could it be expanded to hit other markets?

Yes. This could be expanded to hit other markets and companies like Telit and Cisco are already putting in huge efforts. Some of these markets could be data privacy in the cryptocurrency sector. Cryptocurrency security is one of the rising concerns and this device implementation can be expanded such markets.

How has this case study related to the course?

This case study has specially focussed on the key concepts that go into the design of any embedded system. The key concepts have been presented in the beginning of the concluding remarks.

Has this investigation inspired you in any way?

This investigation has in particular inspired me on an entrepreneurial journey to devise my own products/systems that can address the existing challenges in the society.

How easy/hard was it for you to understand the technical parameters of the device?

It required a bit of work since this project has been the first of its kind in my life. However, once I gained some pace, it was no longer challenging.

How hard was it to find technical information on the device?

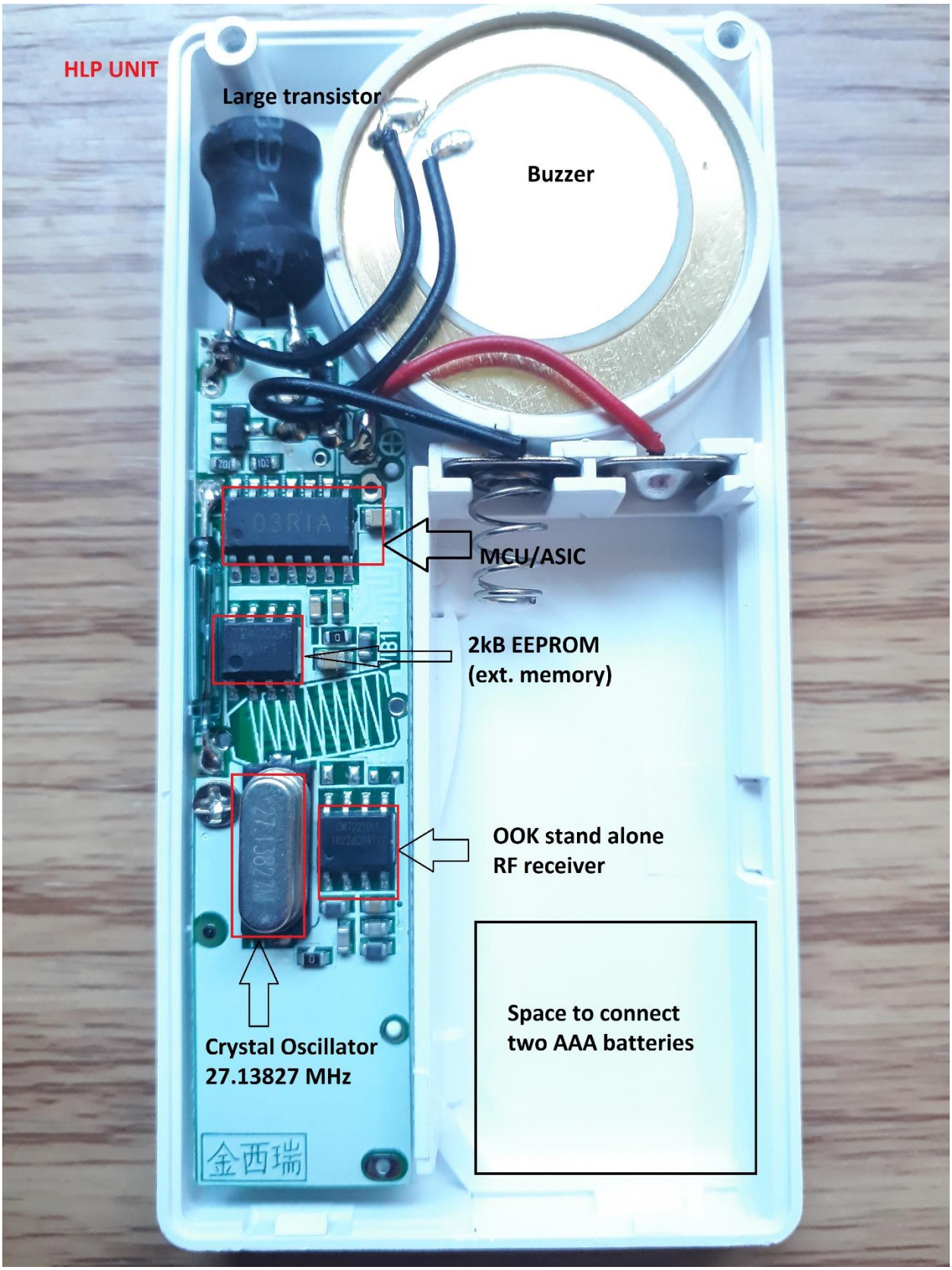
While I was required to make appropriate assumptions at certain places, it was hard to find all the technical information on the device. Partly this was because the product is using Chinese components which are unavailable on the internet and partly because some of the components may have been prepared solely by the company selling the product.

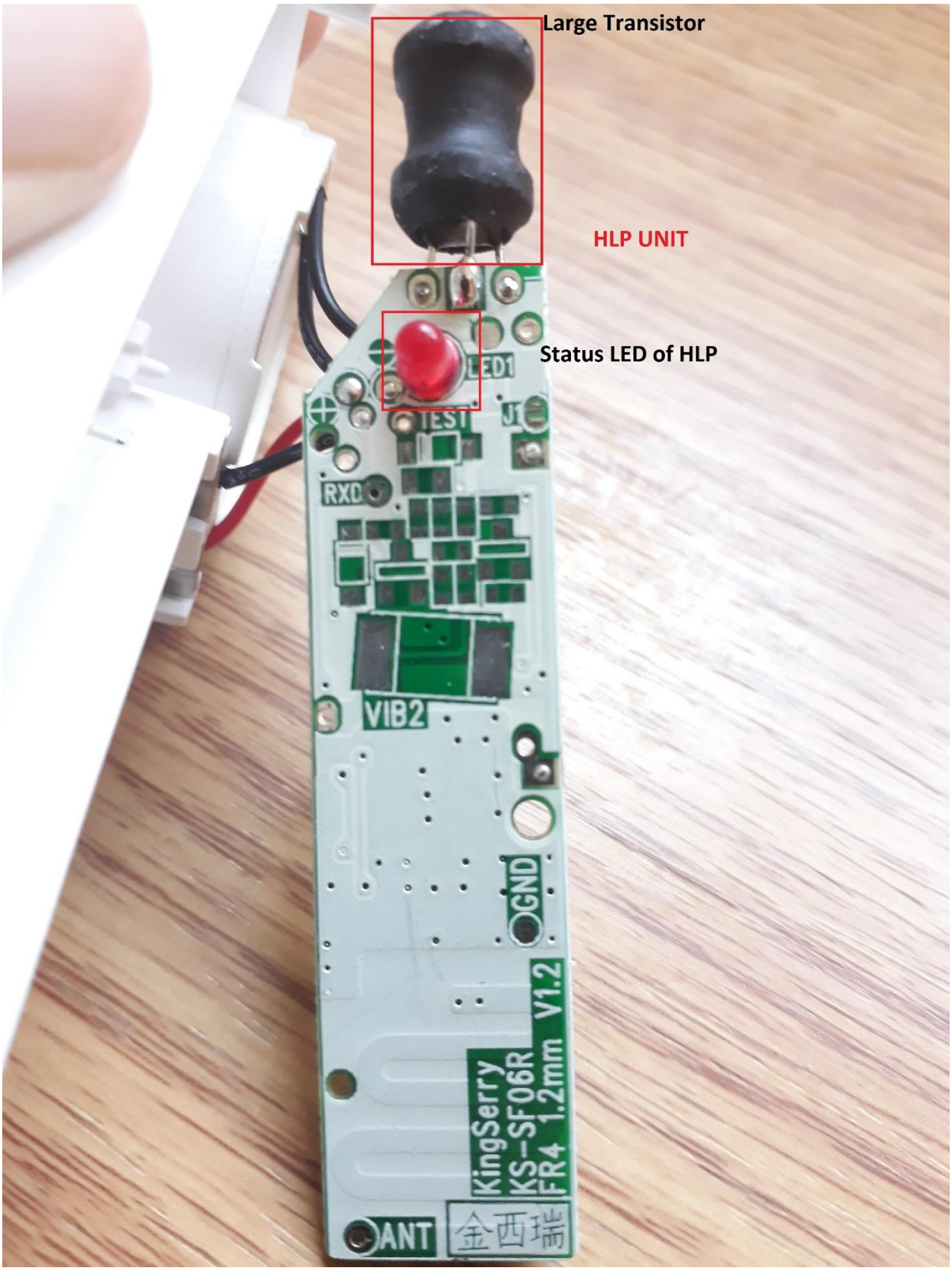
After what you learned in the course, did you have any intuitive feel for how the hardware and software system operated?

Yes. Whatever, I learned through this case study only makes more sense given what I have learnt and experienced so far in the Embedded Systems Engineering domain.

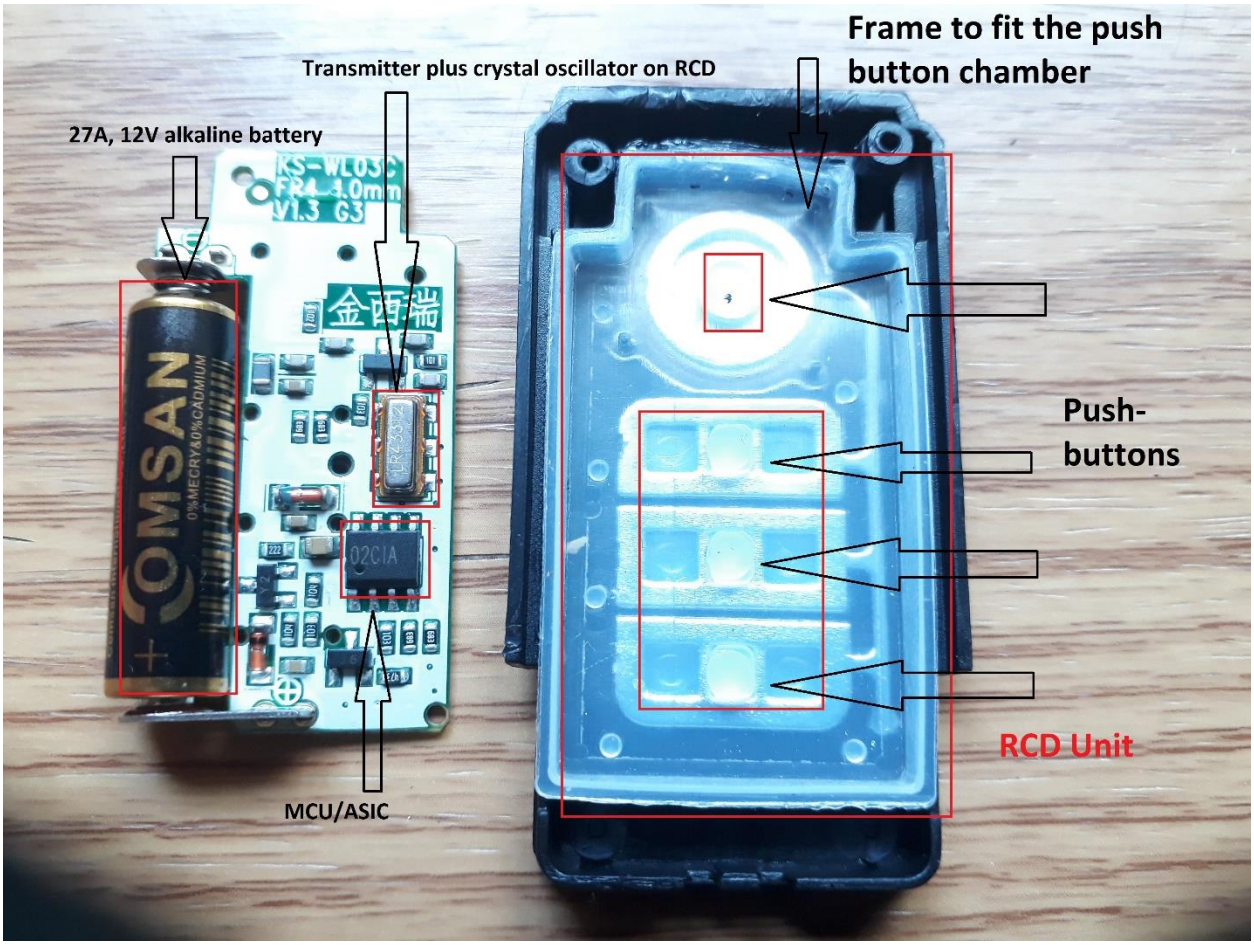
APPENDIX

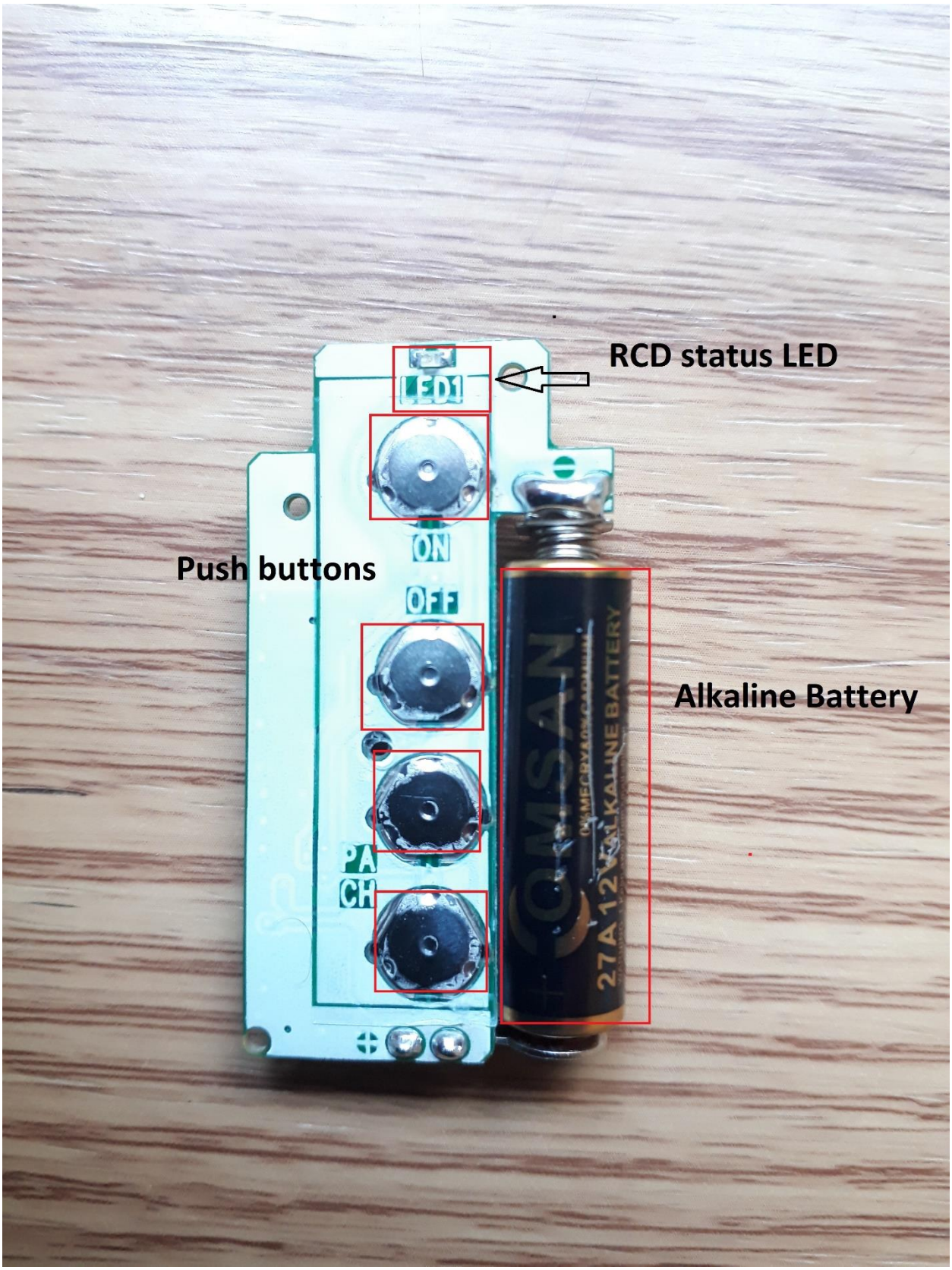
HLP (Host Locking Platform) Unit


HLP UNIT
Large transistor
Buzzer
MCU/ASIC
2kB EEPROM
(ext. memory)
OOK stand alone
RF receiver
Space to connect
two AAA batteries
Crystal Oscillator
27.13827 MHz

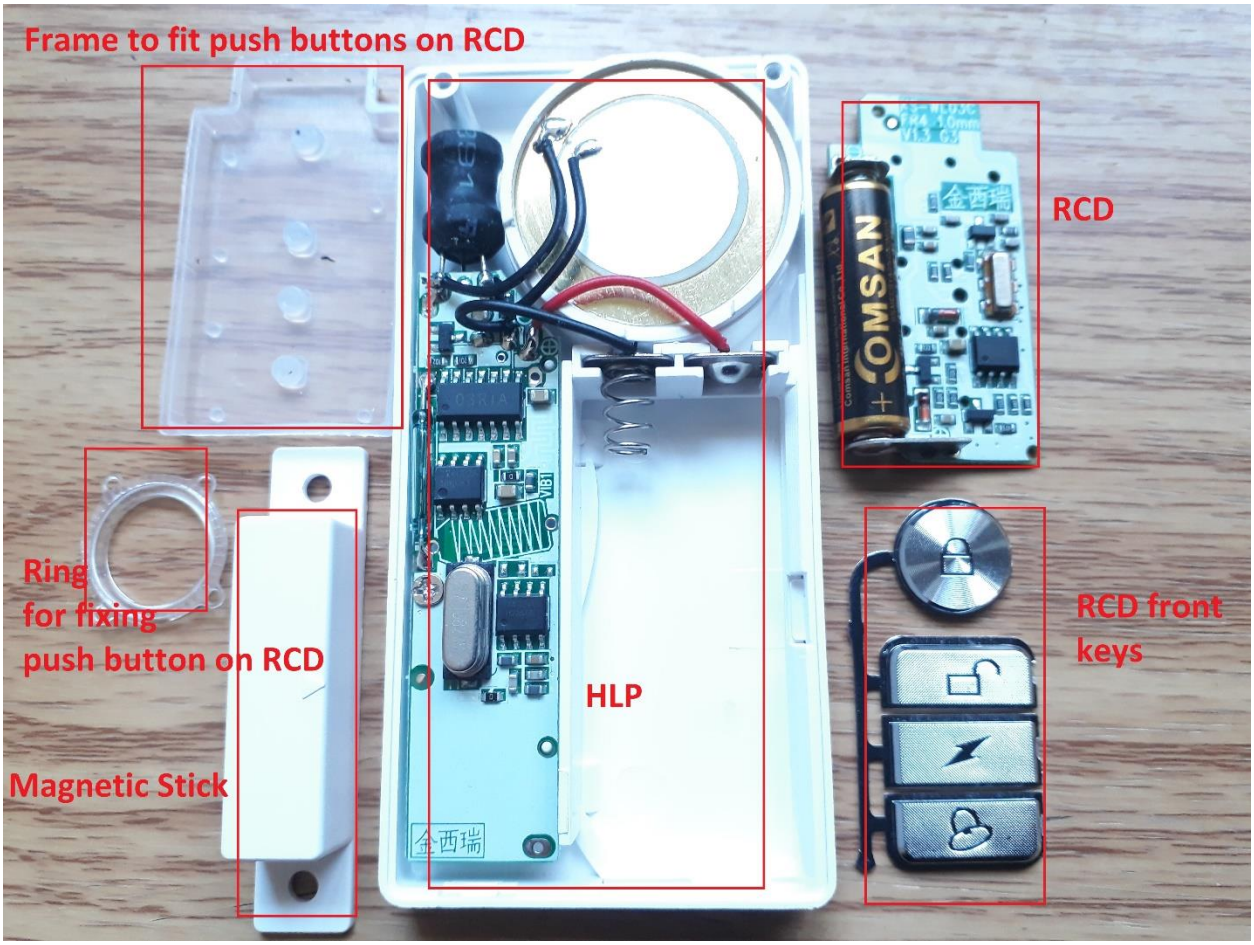

Large Transistor
HLP UNIT
Status LED of HLP
LED1
TEST
J1
RXD
VIB2
GND
KingSerry
KS-SF06R
FR4 1.2mm V1.2
ANT
金西瑞

RCD (Remote Control Device) Unit




RCD status LED
LED1
Push buttons
ON
OFF
PA
CH
Alkaline Battery
COMSAN
27A 12V ALKALINE BATTERY

Magnetic Stick and all components



Citations

[1] - Nubo
[2] - Forbes
[3] - Cisco
[4] - Medium