RFID In-Flight Security Seal

By

HENNA TAN SHEN PO

FINAL PROJECT REPORT

Submitted to the Department of Electrical & Electronic Engineering
in Partial Fulfillment of the Requirements
for the Degree
Bachelor of Engineering (Hons)
(Electrical & Electronic Engineering)

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

RFID IN-FLIGHT SECURITY SEAL

by

Henna Tan Shen Po

A project dissertation submitted to the
Department of Electrical & Electronic Engineering
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
Bachelor of Engineering (Hons)
(Electrical & Electronic Engineering)

Approved:

____

Mr. Abu Bakar Sayuti Bin Hj Mohd Saman
Project Supervisor

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK

September 2013

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

Henna Tan Shen Po

ABSTRACT

In the airline industry, on board sales are often faced with issue of pilferages. It is difficult to determine which party is involved in this issue as no strong evidence can be used to prove it. Plastic security seals are commonly used to secure contents of the airline trolleys for on board sales have proven to be easily compromised. This project proposes a solution to this issue by developing a prototype of an electronic seal through the use of semi-passive Radio Frequency Identification (RFID) technology. Semi-passive RFID technology does not interfere with the avionic control system, which make it an ideal choice to be implemented on board. This project is essentially a system integration of semi-passive RFID, active RFID and microcontroller which involves the development of firmware programming with power aware computing technique. Tampering the electronic seal triggers the system and wakes up the microcontroller. The microcontroller stores events in memory and returns to sleep mode. During investigation, data of the electronic seal can be read or downloaded. Further analysis of the data could be carried out to ensure the time stamp is tally with the personnel scheduling. In conclusion, the author proposes a concept solution to this serious issue of pilferages in the airline industry by developing an electronic seal which is avionic approved.

ACKNOWLEDGEMENTS

1. Gratefulness and glory be to God, who brought me here and made all things possible.
2. My supervisor, Mr. Abu Bakar Sayuti Bin Hj Mohd Saman for the supervisions, advices and patience.
3. My sponsor, Envotech Network Sdn. Bhd. for the materials.
4. My family and friends for their continuous moral and emotional supports.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

RFID – Radio Frequency Identification

IoT – Internet of Things

CHAPTER 1
INTRODUCTION

1.1 Background of Study

RFID is short for Radio Frequency Identification, is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. A RFID device consists of a chip and an antenna and the chip usually has a capacity of 2 kilo bytes of data [1].

The advent of radio technology brings in the RFID technology. In 1901, Guglielmo Marconi first transmitted radio signals across the Atlantic. Since then, radio waves have been an important medium for data transmission [2]. In 1935, Scottish physicist Sir Robert Alexandar Watson-Watt invented the radar system that could locate planes at a distance by beaming radio waves at them. The reflected waves received are used to calculate the distance of the plane by elapsed time [3]. His invention was used during the World War II but the problem was there was no way to identify if the plane detected belonged to the enemy or the country's own pilots returning from a mission.

The Scottish physicist then headed the project to develop the first active Identify Friend or Foe (IFF) system. The British placed a transmitter on their own plane and when the transmitter received signals from radar stations on the ground, it began to broadcast a signal. The signal is then received on ground and used to identify as friend or foe [4].

A RFID system is based on the IFF concept. It comprised of three main components:

- RFID Tag
- RFID Reader
- Data Processing System

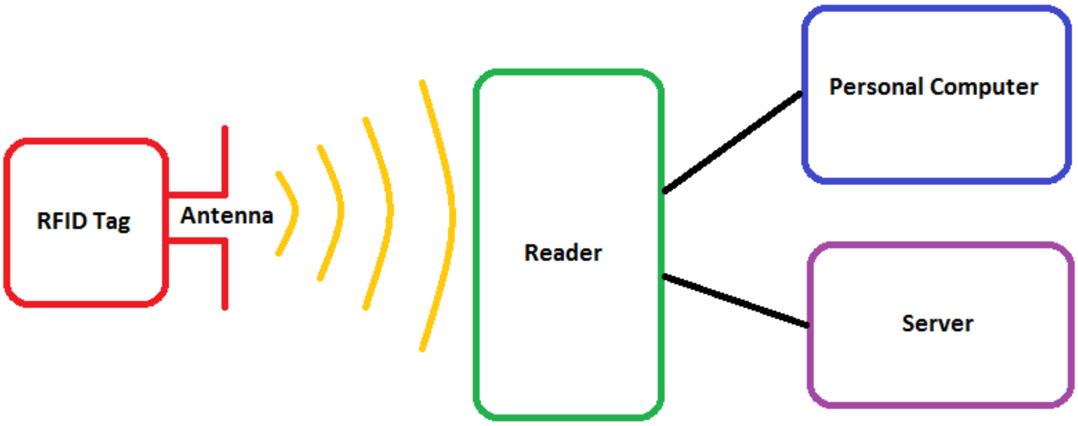


Figure 1.0 – A RFID System

As portrayed in Figure 1.0, RFID tag is the transponder of the system. It is a tag located on the object to be identified. It contains data required for processing. In the current market, there are three types of RFID tag, mainly the active RFID, passive RFID and battery assisted RFID. An active RFID tag has an integrated power supply and actively sends RF signals. A passive RFID tag receives power supply from the frequency signal of the RFID reader and sends data encoded in the tag's memory. A battery assisted RFID is the latest innovation. It has an integrated power supply to power up, run the chip and the memory, transmit and receive data over greater distances. It uses the power of the RFID reader to identify that reading is in progress.

A RFID reader is the transceiver of the system. It is a handheld device used to interrogate with a RFID tag. It transmits a frequency signal to the RFID tag and receives data from the tag. A reader converts radio waves into digital information for further processing [5].

A Data Processing System is a database that collects the data received by the reader. This is important for tracking purposes as it enable remote monitor of the objects with RFID tag. It may be a personal computer connected to the reader or a remote server where data is transferred over the air by the reader.

1.2 Problem Statement

Active RFID has proven to be effective in security and supply chain industry [6]. The improvement of RFID tags over bar codes offers a better way to track merchandise because of their ability to store data efficiently. However, this application has yet to be extended to aviation industry. This is due to the factor that the aviation industry communicates using radio frequency. The use of active RFID for security purposes may interfere with the aviation control system.

Airline on board sales supply chain has been facing issue of pilferages. The journey of transporting the airline trolleys for on board sales from land side to air side involves three private parties. Therefore, it is difficult to determine which party is involved in the issue of pilferages as no strong evidence can be used to prove it. Plastic security seals are commonly used to secure contents of the airline trolleys for on board sales. Unfortunately, plastic security seals have proven to be easily compromised.

1.3 Objective and Scope of the Study

The objectives of this project are:

1. To develop a prototype of an avionic approved electronics seal for airline industry.
2. To demonstrate a proof of concept for a solution to the issue of pilferages in airline in-flight supply chain.

The scope of the study of this project is to develop the hardware and firmware to demonstrate a proof of concept for the solution to the issue of pilferages in airline in-flight supply chain.

CHAPTER 2
LITERATURE REVIEW / THEORY

2.1 RFID and Barcoding

RFID technology and barcoding technology both use labels and scanners to read the labels. They also rely on an IT system to identify the object in a database system. However, to apply it in a real time situation, the advantages of RFID over barcoding make RFID technology a better option. The major advantages of RFID over barcoding are as follow: [7]

- Do not require line of sight
- Multiple parallel reads
- Individual items instead of an item class can be identified
- Read or write capability

Consider a real time situation where a box of various goods is received in a warehouse. Each individual goods need to be recorded to acknowledge receipt. If barcode technology is used, a worker needs to open the box and scan each product. This is time consuming and error-prone. The flow of goods into the warehouse will not be efficient. However, by using RFID technology, each product will have a RFID tag attached to it. Just by installing a RFID reader portal in the warehouse, all products in the box would be identified without tampering the box. Furthermore, it can achieve significant labor savings, reduced data-related errors and improve product availability. Besides, multiple products could be identified in one read. The data collected could then be stored in a database for further use.

The read or write capability of the RFID technology adds on to why RFID technology is a better option than barcoding technology. An example of the application of this capability of RFID tag is the military. The military make heavy use of read or write tags [7].

2.2 RFID Applications

Today, RFID has become a major technology for tracking goods and assets around the world [8]. It is found in automated data collection, identification and location systems. This technology uses radio signals to track and identify objects, animals, people, vehicles, goods and assets without the need for direct contact or line of sight contact [9]. RFID identifies the target automatically and in real time. It also provides increased levels of product and asset visibility for the supply chain industry. RFID technology tracks the status of the target using the concept of Internet of Things (IoT).

2.2.1 Internet of Things

Internet of Things is a vision that is being built in this 21st century [10]. It is a technological revolution that creates a layer of digital connectivity with things and people. The Internet of Things is a world where everything can be analogue and digitally communicate through the use of RFID technology [11].

RFID technology has been widely used for various industries [12]. The applications of RFID are as follow:

- Access Management
- Tracking of Goods
- Tracking of Persons and Animals
- Contactless Payment
- Machine readable travel documents
- Logistics
- Retails

2.2.2 RFID Applications in Security and Supply Chain

In the supply chain industry, RFID can be used to monitor the movement of products. RFID tags can be attached directly to each of the products or to the containers that carry them [13]. Almost any item and any container can be tagged. Readers can then be placed at certain place to monitor the movement and location of inventory. The readers can provide real time data which can be stored in a server for further analysis.

Using RFID tags on products also enable more accurate inventory counts. It has been proven that using RFID technology for inventory counts save labour cost and time. At the same time, it will be able to increase the productivity of a company.

RFID applications in fleet management have a significant return of investment (ROI). It is able to effectively track the containers and cargo globally. Besides, this reliable tracking of cargo and inventory assets is cost effective and is able to increase the security of transporting them too. Moreover, companies are able to gain visibility of their inventory assets and cargos by tracking them using RFID technology.

2.3 Types of RFID Tags

RFID tags come in three varieties: active, passive and semi-passive which is also known as battery assisted. Each of them has their own characteristic and functionality.

2.3.1 Active RFID Tag

Active RFID tag is powered by a battery internally [14]. It broadcast radio signals actively to the reader at a time internal which is defined beforehand. Many active RFID operates at fixed intervals as this could economize the power consumption. Besides, it has the ability to store additional information sent by the transmitter [15].

Active RFID tag has been actively used in the security and chain supply industry. It has proven to be effective and efficient. However, active RFID tag is not avionic approved due to its active characteristic. Table 1.0 shows the features of an active RFID tag [15].

Type of RFID	Active
Battery	Integrated in chip
Characteristic	Active transmitter and receiver
Shelf Life	Life of battery, usually 5 years
Range of Signals	Typically up to 100 meters
Cost	High

Table 1.0 –Active RFID Tag

2.3.2 Passive RFID Tag

Passive RFID tag has no internal power supply [14]. It only powers up when a reader at presence energized the chip through radio signals. The current induced in the antenna provides just enough power for the integrated circuit in the tag to transmit a response. Passive RFID tag is avionic approved. However, it is unable to provide the security needs of the airline in-flight trolley. Table 2.0 shows the features of a passive RFID tag.

Type of RFID	Passive
Battery	No Battery
Characteristic	Transmit radio signals only when the chip is energized by a reader
Shelf Life	Very high, ideally does not expire over a lifetime
Range of Signals	Range covered by a reader, typically 3 meters
Cost	Very low

Table 2.0 –Passive RFID Tag

2.3.3 Semi-Passive RFID Tag

Semi-passive RFID tags also known as battery assisted RFID tags are similar to passive RFID tag but has an internal power source [14]. However, the internal power source does not power the broadcasting of radio signals. When a reader is present and is transmitting radio signals to the antenna of the tag, it energized the semi-passive RFID chip and hence, prompting the chip to transmit radio signals back to the reader. This characteristic of the semi-passive RFID tag enable it to be deployed into security tracking system.

Type of RFID	Semi-Passive
Battery	Integrated in chip
Characteristic	When energized by reader, the tag identify that reading is in progress Uses on board battery to power up and store data in memory
Shelf Life	Life of battery, usually 5 years, after which, it behaves as passive RFID tag
Range of Signals	Typically up to 20 meters
Cost	Low

Table 3.0 – Semi-Passive RFID Tag

2.4 Why Semi-Passive RFID?

The author chose to make use of semi-passive RFID to develop a prototype of an electronic seal. The reason semi-passive RFID is chosen because it has a unique characteristic. It uses on board battery to power up and store data in memory. It does not transmit data unless it is energized by a reader. This characteristic of semi-passive RFID makes it avionic approved and thus an ideal choice for this project.

The life span of a semi-passive RFID tag is quite long. It depends on the on board battery to act as semi-passive. After the battery runs out, it behaves like a passive RFID tag. The signals are able to transmit to a distance of about 20 meters. Moreover, the cost of a semi-passive RFID is low as compared to active RFID. The cost-effectiveness made it an ideal prototype for real time usage.

2.5 Semi-Passive RFID Applications

Semi-passive RFID has not been a popular choice as it was not being further exploited as compared to active RFID. Nevertheless, there are applications in the industry that are making use of semi-passive RFID.

2.5.1 Semi-Passive RFID in Automation

Semi-Passive RFID has been used by German automaker Audi in expanding their existing use of RFID in their manufacturing operations [16]. Audi incorporates semi-passive tags into the assembly process for their Audi TT sport cars due to its ability to withstand high temperatures.

Audi utilizes an OIS-P RFID system by Identec Solutions to make sure that assembly instructions are tally and also to ensure that the accuracy of robots positioning parts can be increased. According to Gerhard Schedler, president and CEO of Identec Solutions, "The automotive line is very complex, and you always have to know what is where, and which step is occurring, such as which color is needed. It is a work in process. Now the skid is intelligent and can tell the manufacturing machines what to do. It gives the car a voice."

2.5.2 Semi-Passive RFID in Retail

Another application of semi-passive RFID is in the case of a US retailer who has asked not to be named [17]. The semi-passive RFID tags are attached to employee identification cards as employee IDs. The workers can then be tracked and identified at which facility there were in. Integrated readers are installed in the ceiling to read the RFID tags. By tracking the movements of the staff, the company is able to collect data indicating whether the employees are at the appropriate areas at the particular time.

2.5.3 Semi-Passive RFID in School

In India, an Indian private grammar school implemented the semi-passive RFID tags onto the ID card of each student [17]. Readers are also installed on the ceilings of classrooms. The school used the ID card to track its students and to obtain the locations of each student. The school also hopes to install a reader in every classroom in future, so that they are able to identify in real time, which students are in which classroom.

CHAPTER 3
METHODOLOGY

3.1 Workflow of Transporting Trolley in Airline Industry

The journey of transporting goods for on board sales involved three parties – Duty Free Supplier, Transporter and the Air Crews. The typical workflow of transporting the goods for on board sales is as shown in Figure 2.0.

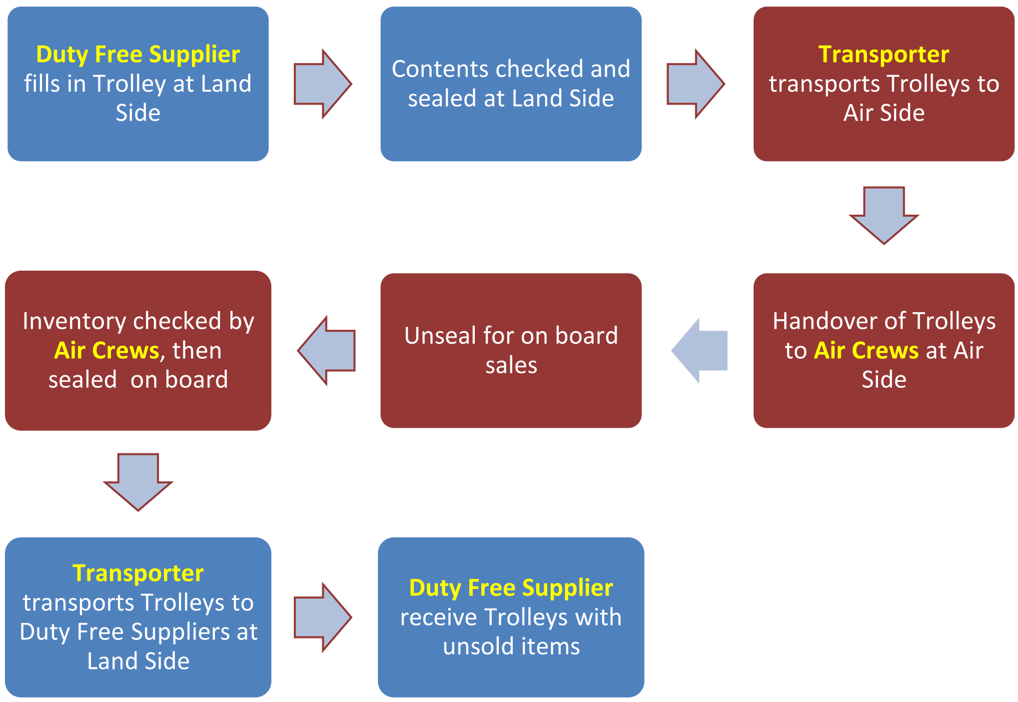


Figure 2.0 – Typical Workflow of Transporting Goods

At Land Side Warehouse, Duty Free Supplier fills in the trolleys with goods for on board sales. After contents were checked, the suppliers sealed the trolleys. A second party, the Transporter will transport the sealed trolleys into the Air Side. The Transporter will then hand over the trolleys to the Air Crews at Air Side. Trolleys were unsealed on board for sales.

After the last call of the sales, the inventory is checked and recorded by Air Crews. The trolleys are then sealed on board. After the plane landed, the Transporter will transport the trolleys back to the Duty Free Suppliers at Land Side. The Duty Free Suppliers will check the unsold items with the records provided by the Air Crews. Often, the records are not tally.

3.2 Proposed Concept of Solution

This project proposes to use the semi-passive RFID tag to develop an electronic seal. There will be three Event Types that will trigger the electronic seal – Sealing Event, Tamper Event and Read Event. Figure 3.0 shows the finite-state machine of the concept of the electronic seal.

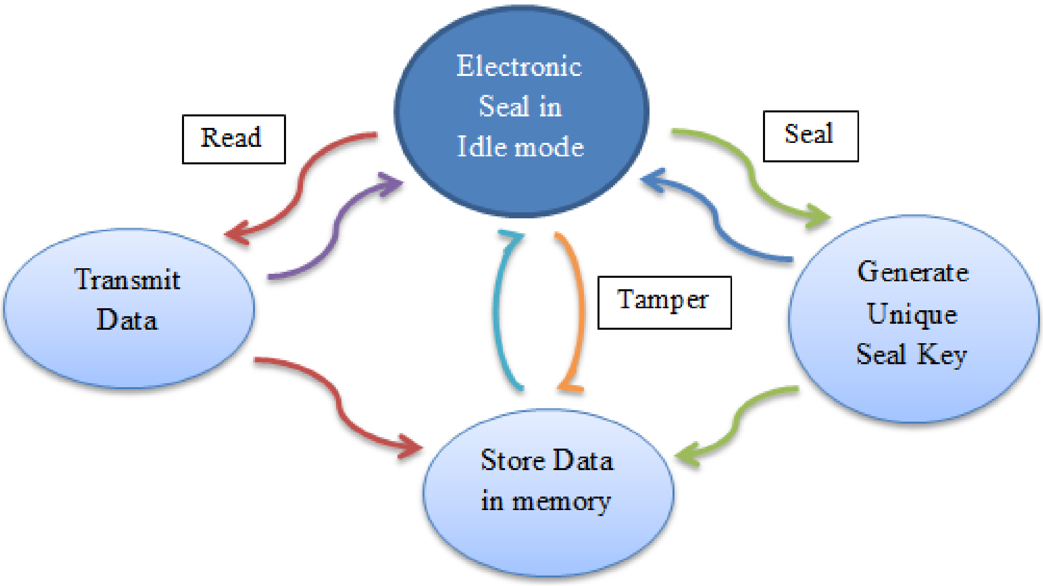


Figure 3.0 – Concept of the Electronic Seal

The electronic seal will generate a unique 4 digit seal key upon each sealing event. It will then store the Sealing Event, Event Date and Time and Current Seal Key in cache. Upon each tamper event, the electronic seal will store the Tamper Event, Event Date and Time and the Current Seal Key. No data is transmitting over the air during the Sealing Event and the Tamper Event. This is to ensure that the electronic seal does not interfere with aviation control system.

The Read Event occurs when a Reader transmits radio signal to the semi-passive RFID tag. The electronic seal will then transmit the data stored in cache to the Reader. It will also store the Read Event, Event Date and Time, Reader ID and Current Seal Key in cache. Table 4.0 shows an example of data that can be stored.

Date / Time	Event	Seal Key	Reader
280103 1128	Seal	1234	Duty Free Suppliers
280103 1230	Read	1234	Transporter
280103 1300	Read	1234	Air Crew
280103 1400	Tamper	1234	
280103 1700	Seal	2233	
280103 2100	Read	2233	Transporter
280103 2200	Read	2233	Duty Free Suppliers

Table 4.0 – Example of Data for an Ideal Case

The example in Table 4.0 shows the data of an electronic seal that is not compromised. Since three parties are involved in the workflow of transporting the trolley, each party should have a reader to check for data. If Seal Key is not tally before the on board sales, it means that the trolley has been compromised. The Event Date and Time will eventually bring justice to the parties involved.

3.3 Proposed Electronic Seal

The proposed electronic seal is a system integration of a semi-passive RFID chip, nRF24LE1 module, a microcontroller and an antenna which also involves the development of firmware programming. Its special characteristic of activating RF module only when a reader is present makes it an avionic approved device. A UHF Reader is not allowed on board as it may interfere with the avionic control system.

3.3.1 Hardware

3.3.1.1 nRF24LE1

nRF24LE1 is an ultra-low power wireless system on-chip solution. It has a 2.4 GHz transceiver with embedded microcontroller and a 16kB program memory on-chip flash. The combination of processing power, memory, low power oscillators, real-time counter, AES encryption accelerator, random generator and a range of power saving modes provides an ideal platform for implementation of the proposed

Electronic Seal in this paper. The nRF24LE1 also offers a rich set of peripherals including SPI, 2-wire, UART, 6 to 12 bit ADC, PWM and an ultra-low power analogue comparator for voltage level system wake-up [18]. Figure 4.0 shows the nRF24LE1 (credits: www.goodluckbuy.com).

Figure 4.0 – nRF24LE1 Hardware (credits: www.goodluckbuy.com)

3.3.2 Firmware

The firmware is written in C Programming Language using uKeil compiler. The hex file is loaded into the hardware so that the hardware could work as desired. The firmware tells the microcontroller when to allow the RFID chip to transmit data through radio signals as actively transmitting radio signals are not avionic approved.

There are three events that will trigger the integrated system, specifically the tamper event, read event and seal event. Each event is described briefly in Figure 5.0, Figure 6.0 and Figure 7.0 respectively. The firmware will also ensure that tamper event and sealing event is recorded and stored in the cache.

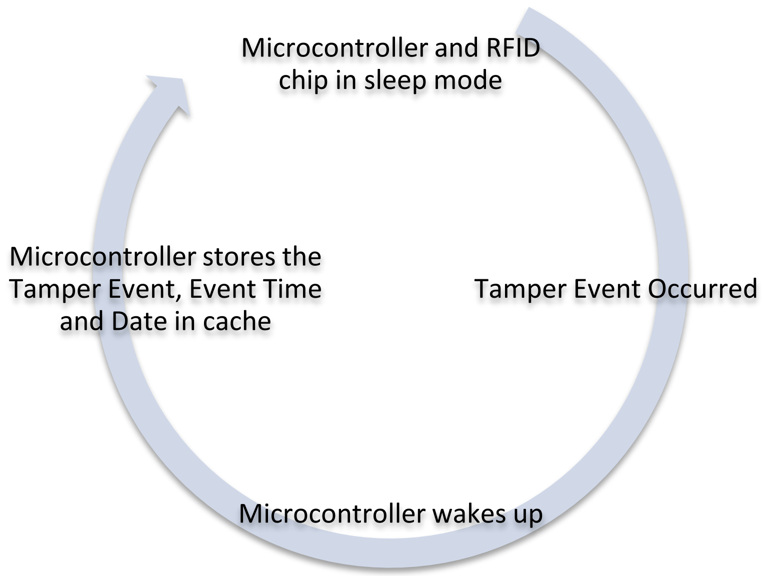


Figure 5.0 – Tamper Event

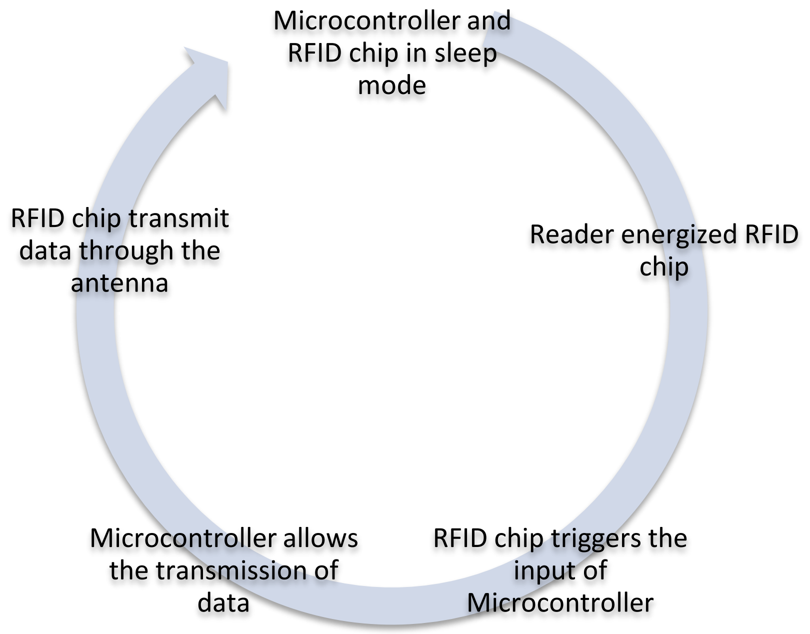


Figure 6.0 –Read Event

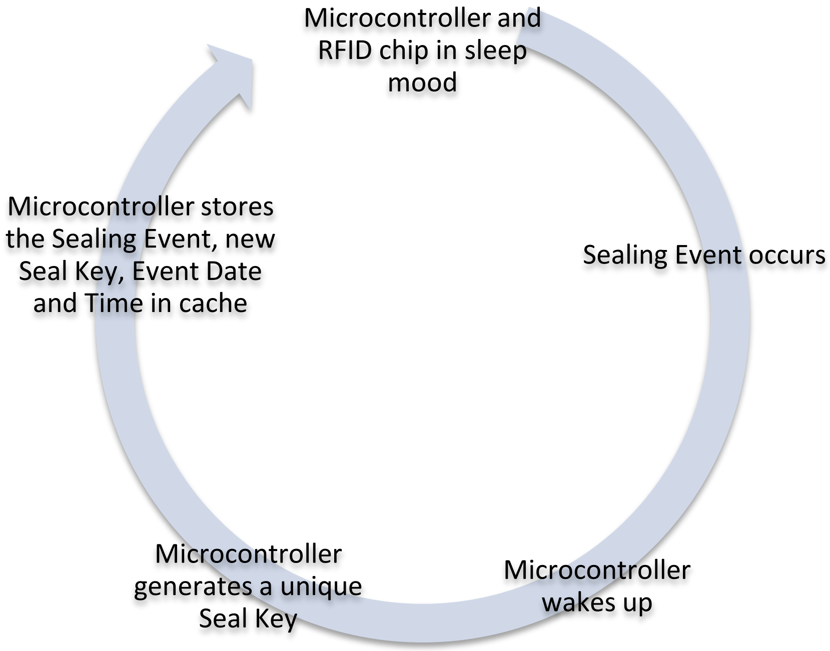


Figure 7.0 – Seal Event

3.4 Project Activities

3.4.1 Project Proposal

A research was done regarding the issue of pilferages in avionic industry and a proposed solution was given by the author. The author gathered adequate materials and proposed the solution to her supervisor.

3.4.2 Project Charter / Draft

To begin the detailed research of the project, the author needs to understand how a RFID system works. The author needs to do a research on which microcontroller to use. Besides, the author needs to learn to write a firmware using Programming in C in uKeil Vision. In addition, the author needs to know how to load the firmware into the hardware.

3.4.3 Project Closed Out

The project will be completed when the prototype is able to generate a unique seal key each time a sealing occurs and store them in cache. The project will be presented and defended by the author.

3.5 Key Milestone

This project is a system integration of various hardware, software and firmware. Each area has a key milestone that the author wants to achieve.

The hardware will mainly consist of a semi-passive RFID chip, antenna, nRF24LE1 and a microcontroller. The semi-passive RFID chip wakes up the microcontroller when a reader energizes it. The microcontroller then allows nRF24LE1 to transmit data to a reader. Upon sealing, the microcontroller ensures that a unique seal key is generated. The antenna will be the receiver and transmitter of frequency between the semi-passive RFID chip and the reader.

3.6 Gantt Chart

Table 5.0 shows the Gantt Chart of the Project.

Project Activities	**Week No**													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Acquire equipment and uKeil compiler														
Testing of nRF24LE1 with compiler														
Testing on RF transmission														
Testing on Power Down and Wake Up Mode														
Progress report														
Testing on Seal Key, Date and Time														
Structure of Firmware														
EDX														
Final Report														
Oral Presentation														

Table 5.0 – Gantt Chart

3.7 Tools

The tools that are used for this project are as follow.

Language	• Programming in C
Software	• Keil uVision4 • nRFFlasher
Hardware	• nRF24LE1 System on chip • antenna • switch
Others	• Internet Connection

Table 6.0 – Tools Used

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 Project Workstation

The nRF24LE1 uses 2.4GHz GFSK RF transceiver with embedded protocol engine. The embedded protocol engine enables data packet communication and supports various modes from manual operation to advanced autonomous protocol operation [18].

To begin developing this project, required software such as Keil uVision4 and nRFFlasher are downloaded and installed. Figure 8.0 and Figure 9.0 shows the workplace of Keil uVision4 and nRFFlasher respectively.

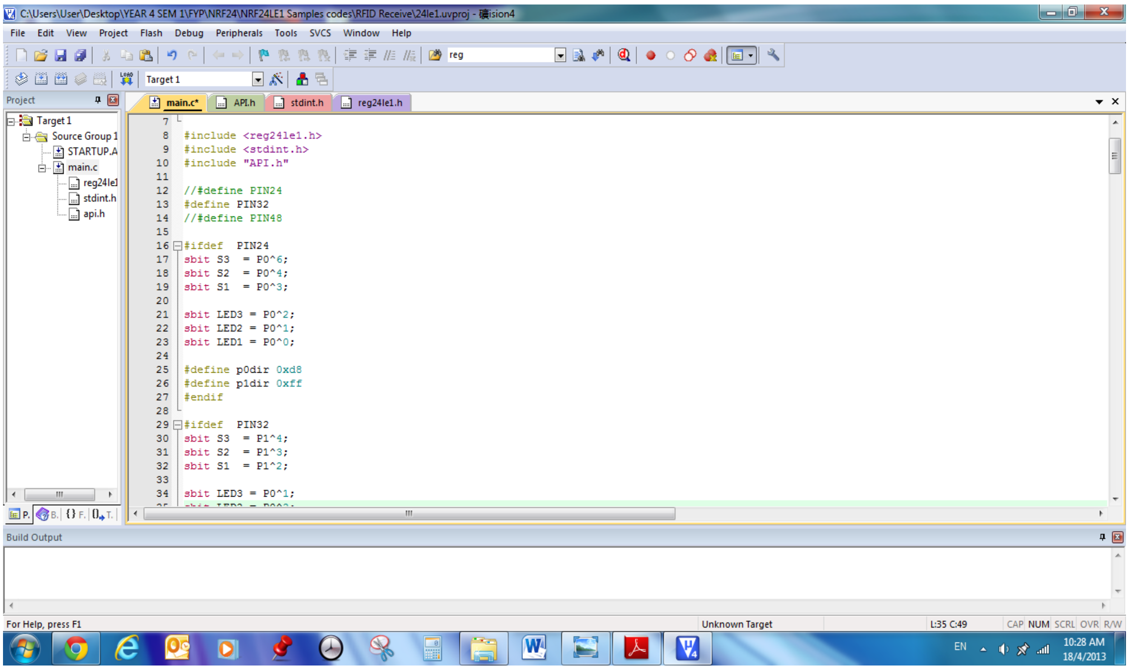


Figure 8.0 – Keil uVision 4 workplace

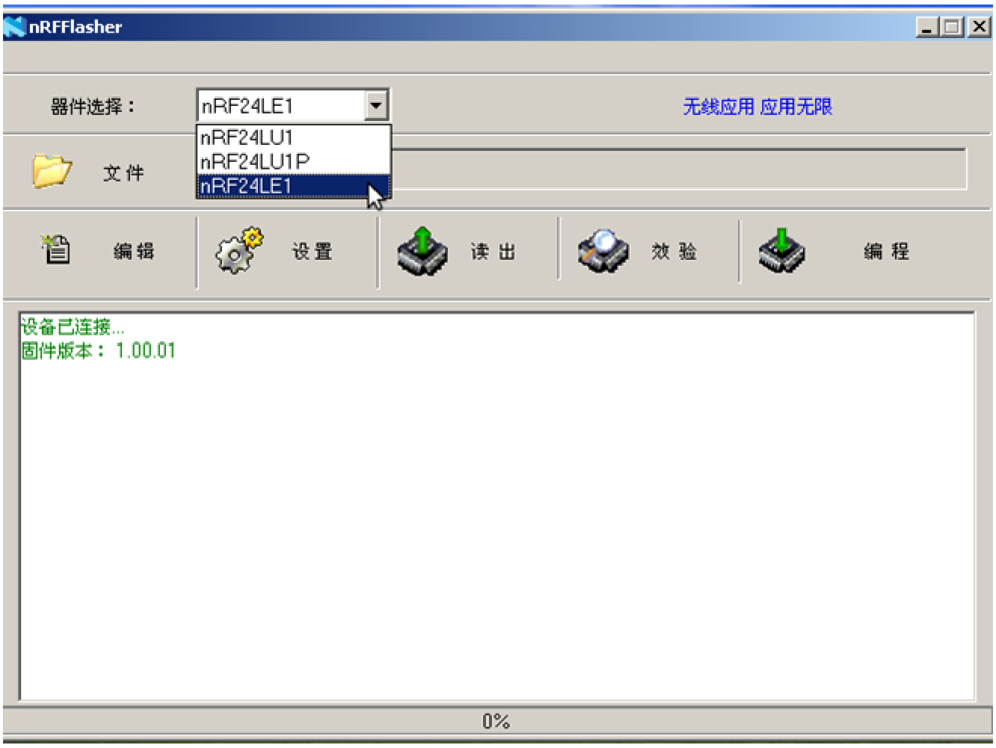


Figure 9.0 – nRFFlasher

4.2 Results and Discussion of Prototype

The development of the hardware and firmware of the prototype yield results that will be discussed in this section.

4.2.1 Transmit Mode

To enable the hardware to transmit data through RFID, a firmware must be developed. A test program is developed to ensure the transmitting function of the hardware is properly developed. The test program is able to transmit a string of characters when activated.

The test program is further developed into the actual firmware. The prototype successfully transmits the seal key stored in the memory when prompted. This function is being verified with a receiver module that will be discussed in 4.3.2.

The nRF24LE1 uses the 2.4GHz GFSK RF transceiver with embedded protocol engine. The RF transceiver module is configured and operated through the RF transceiver map. This register map is accessed by the MCU through a dedicated on-chip Serial Peripheral interface (SPI) [18].

To begin transmitting, the nRF24LE1's RF module needs to be initialized. The flowchart in Figure 10.0 shows the brief workflow of the transmitting mode.

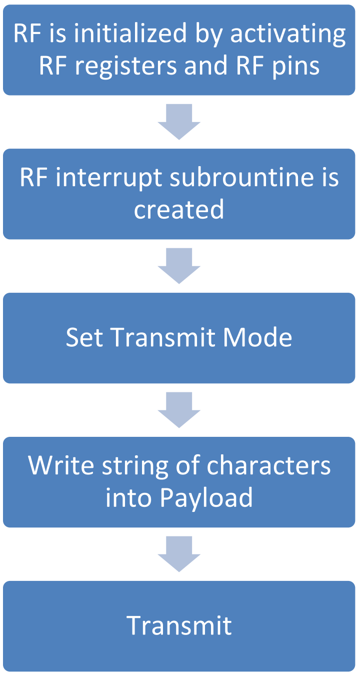


Figure 10.0 – Flowchart for Transmit Mode

In transmitting mode, the nRF24LE1 transmits a string of characters. When the string of characters are transmitted and successfully received by the second party, the nRF24LE1 will be notified by acknowledgement (ACK). In debugging mode, it sends a UART command "Send OK". Figure 11.0 shows a short snippet of the code while Figure 12.0 shows the output of the transmit mode. The transmitter device sends a string of characters to the receiver.

```
L01_Init( );                           //Initialize the internal 24L01P
L01_SetTXMode( );                      //Set as TX mode
L01_FlushTX( );
L01_FlushRX( );
L01_WriteTXPayload_Ack( ( INT8U* )"HENNA 2013\r\n", 12 );
RFCE = 1;
delay_ms(2000);
while( rf_flag == 0 );

if( rf_flag & ( 1<<2 ) )
{
    P0 ^= ( 1<<2 ) | ( 1<<1 );
    UART0_SendStr( "Send OK!\r\n" );
    //send_flag = 1;
}
if( rf_flag & ( 1<<3 ) )
{
    UART0_SendStr( "Send Error!\r\n" );
    //send_flag = 0;
}
RFCE = 0;
rf_flag = 0;
```

Figure 11.0 – Code Snippet for Transmit Mode

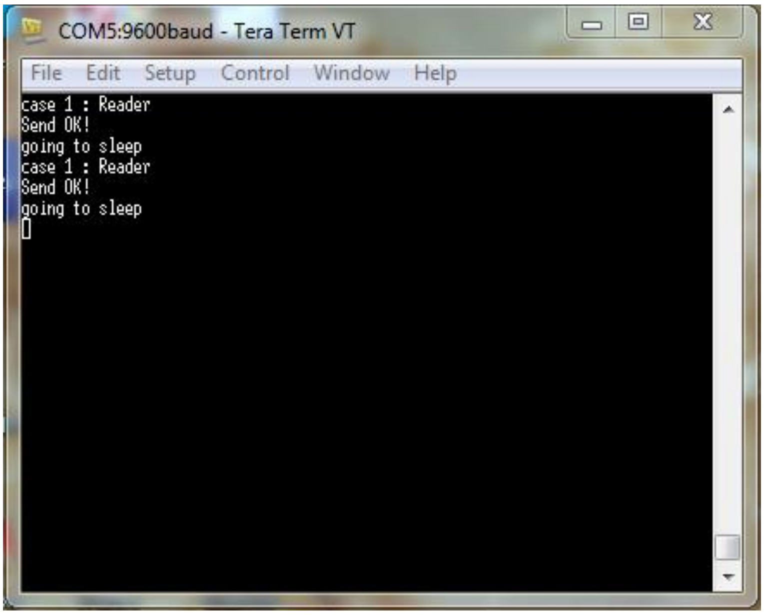


Figure 12.0 – UART Window of Transmit Mode

4.2.2 Receiver Mode

In receiver mode, the RF transceiver is used as a receiver. The receiver demodulates the signals from the RF channel, constantly presenting the demodulated data to the baseband protocol engine. The baseband protocol engine constantly searches for a valid packet. If a valid packet is found (by a matching address and a valid CRC) the payload of the packet is presented in a vacant slot in the RX FIFOs. If the RX FIFOs are full, the received packet is discarded [18].

In this project, another nRF24LE1 module is being loaded with receiving mode firmware. This module will act as a reader to receive data transmitted by the prototype. To begin receiving, the nRF24LE1's RF module needs to be initialized. The flowchart in Figure 13.0 shows the brief workflow of the receiving mode.

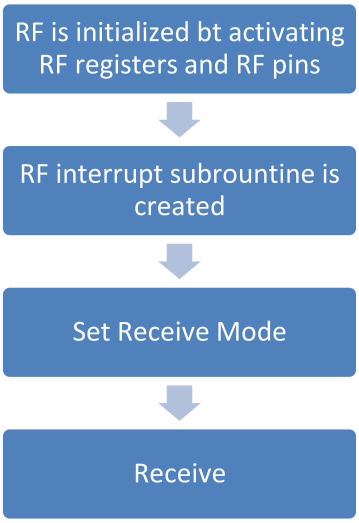


Figure 13.0 – Flowchart for Receiving Mode

In receiving mode, the nRF24LE1 receives the string of characters transmitted. Once it receives the string of characters, it sends an acknowledgement (ACK) back to the transmitter. In debugging mode, it sends a UART command of the strings of characters received. Figure 14.0 shows the code snippet of the receiving mode while Figure 15.0 shows the output of the receiving device. The device received a string of characters from the transmitter and prints it on the UART window.

```
CLKCTRL = ( CLKCTRL | 0x80 ) & ~0x08;
P0DIR = 0;
UART_Init( 3 );                    //9600, 8, N, 1

RFCON = 0x07;
RFCE = 0;
RFCKEN = 1;                                        //
RF = 1;                                              //
for( itmp = 0; itmp < 30000; itmp ++ );

L01_Init( );                    //Initialize the internal 24L01P
L01_SetRXMode( );                 //Set as RX mode
L01_FlushTX( );
L01_FlushRX( );
L01_ClearIRQ( IRQ_ALL );

RFCE = 1;
P0 |= ( 1<<0 );

EA = 1;
UART0_SendStr( "nRF24LE1 RX test start!\r\n" );
```

Figure 14.0 – Code Snippet for Receive Mode

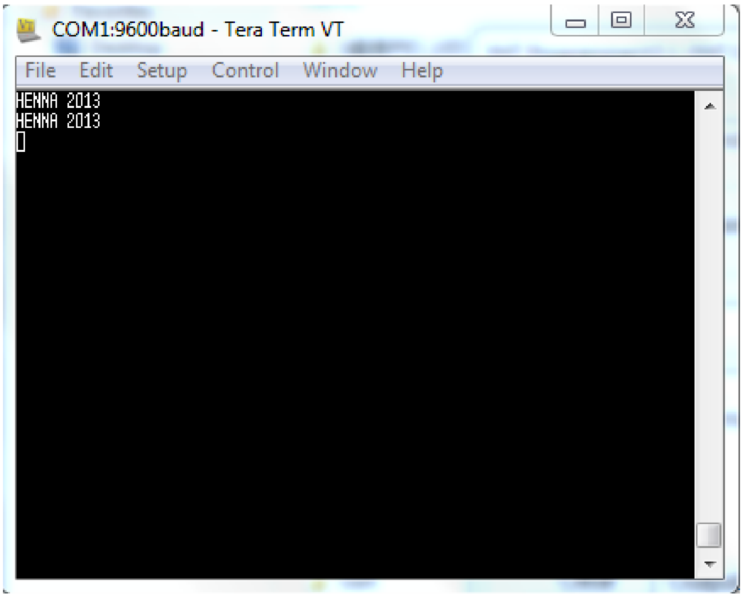


Figure 15.0 – UART Window for Receive Mode

4.2.3 Power Down Mode

The nRF24LE1 has a power down control function that supports four types of power saving modes: [19]

- Deep Sleep

- Memory Retention, Timers Off
- Memory Retention, Timers On
- Register Retention

The deep sleep mode will cause a system reset when executed. This mode uses the least amount of power consumption. The only wakeup source is wakeup from pin. The memory retention mode will cause a system reset. However, part of the RAM will retain data, but all register values are lost. The memory retention mode can be useful to keep data for the application. This mode uses less power as compared to register retention mode.

The register retention mode will not cause a system reset on wakeup. All registers and RAM retain data as before the power down. After wakeup, the program continues to run from where it was put to sleep, in addition the wakeup interrupt will execute if enabled.

The prototype uses Register Retention mode because it fits the criteria of the project. The flowchart in Figure 16.0 shows the brief workflow of power down the module.

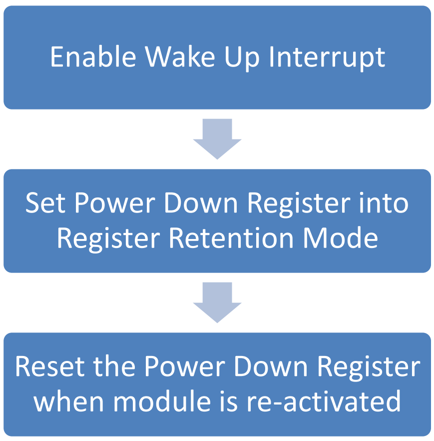


Figure 16.0 – Flowchart for Power Down Mode

To power down the module into register retention mode, a command is sent to the power down register. Figure 17.0 shows the code snippet of the power down mode.

```
wake_init();
UART0_SendStr( "going to sleep\r\n" );
PWRDWN = 0x04;
PWRDWN = 0x00;        // when awake
```

Figure 17.0 – Code Snippet for Register Retention Mode

4.2.4 Wake Up Mode

When the prototype is in register retention mode, a wake up mode is configured to wake up the module. The wake up mode is triggered by an external input pin. A 3.3V is required to wake up the module. Figure 18.0 shows the flowchart of the wake up mode.

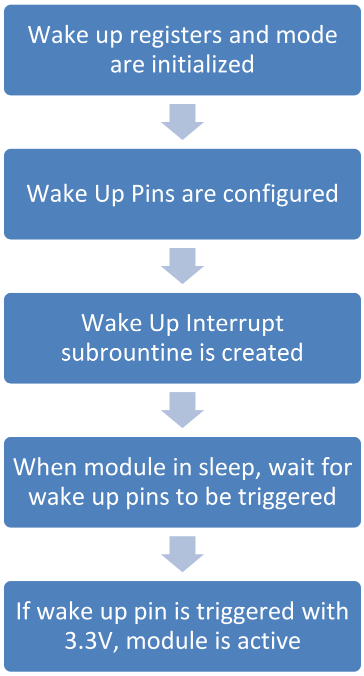


Figure 18.0 – Flowchart for Wake Up Mode

4.2.5 Seal Event

When seal event occurs, the microcontroller wakes up and records the event. The microcontroller generates a unique four digit seal key for each seal event that occurs. The seal key is recorded and kept in memory. The RF module is not activated to ensure that there is no interference with the avionic control system when seal event occurs on board.

With a unique seal key generated upon each seal event, authorities will be able to track and detect if a seal event is valid and authorized. Figure 19.0 shows the seal key generated on the prototype when a seal event occurs.

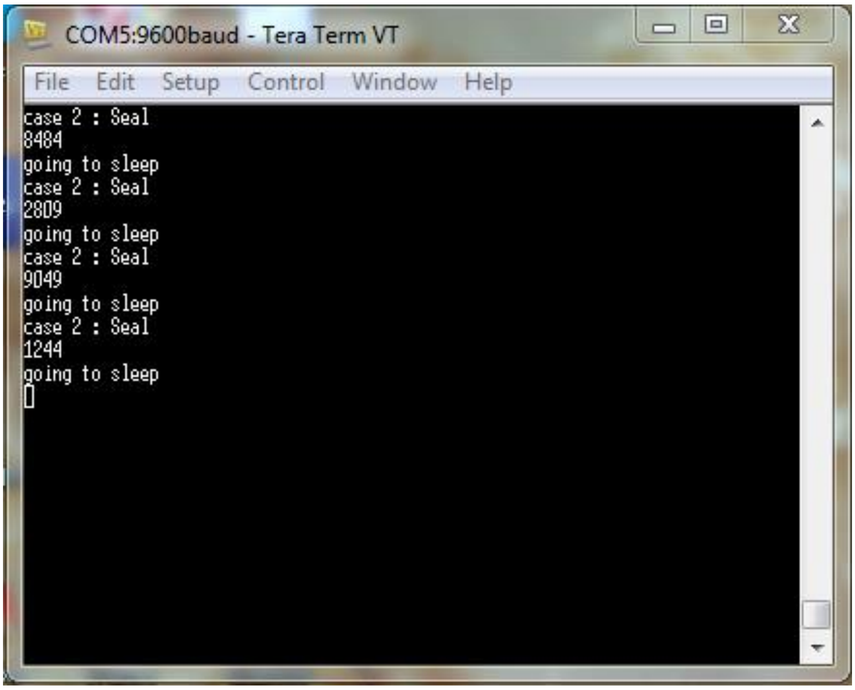


Figure 19.0 – Seal Key generated on Seal Event

In Figure 19.0, the first seal key generated when a seal event occurs is 8484. The second seal key generated when a second seal event occurs is 2809. From the data obtained, the seal keys generated are unique and does not repeat.

4.2.6 Read Event

When a reader's signal triggers the RF input pin of the prototype, a read event occurs. In this project, the reader is represented by another nRF24LE1 module which is loaded with firmware that receives data transmitted by RFID.

Figure 20.0 shows the seal key generated while a seal event occurs and when a reader triggers the prototype, its RF module is activated and data being transmitted. The seal key generated is 7454. After it sends the data, the prototype goes back to register retention mode.

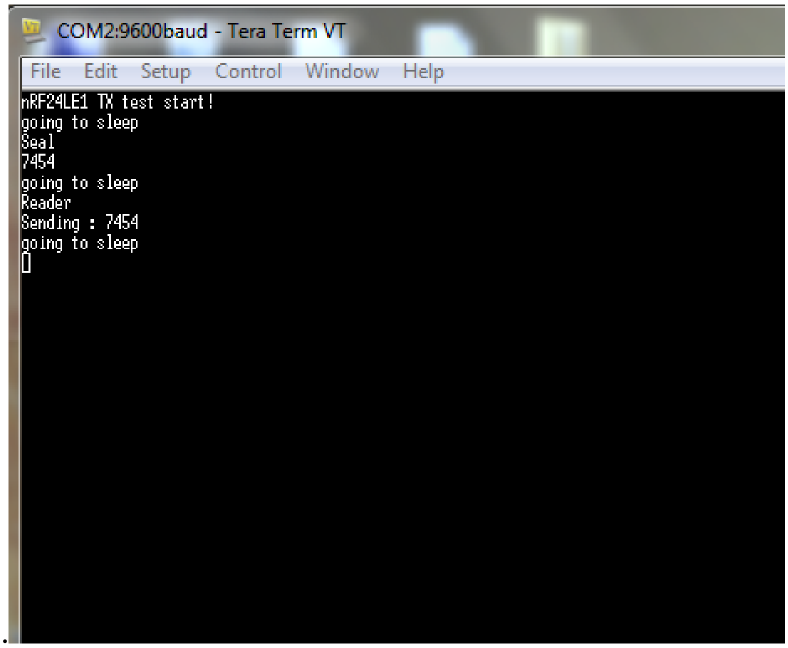


Figure 20.0 – Sending of Data

In this project, the reader is signified by another nRF24LE1 that is loaded with receiving mode firmware. The receiving mode firmware is discussed in section 4.1.2. Figure 21.0 shows the receiving of data when the prototype sends data.

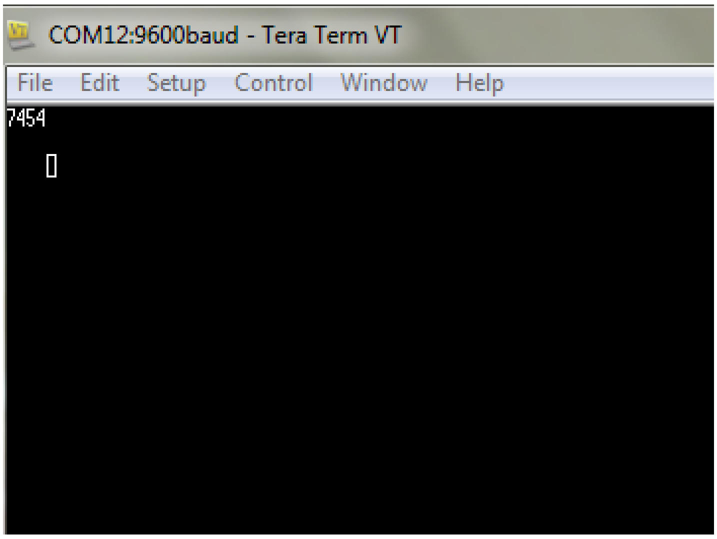


Figure 21.0 – Receiving of Data

4.2.7 Tamper Event

Tamper event occurs when unsealing of the prototype is triggered. The event is recorded by the microcontroller. This event doesn’t generate anything. The timestamp of this event is important in investigating the issue of pilferages for airline on board sales. Figure 22.0 shows the Tamper event.

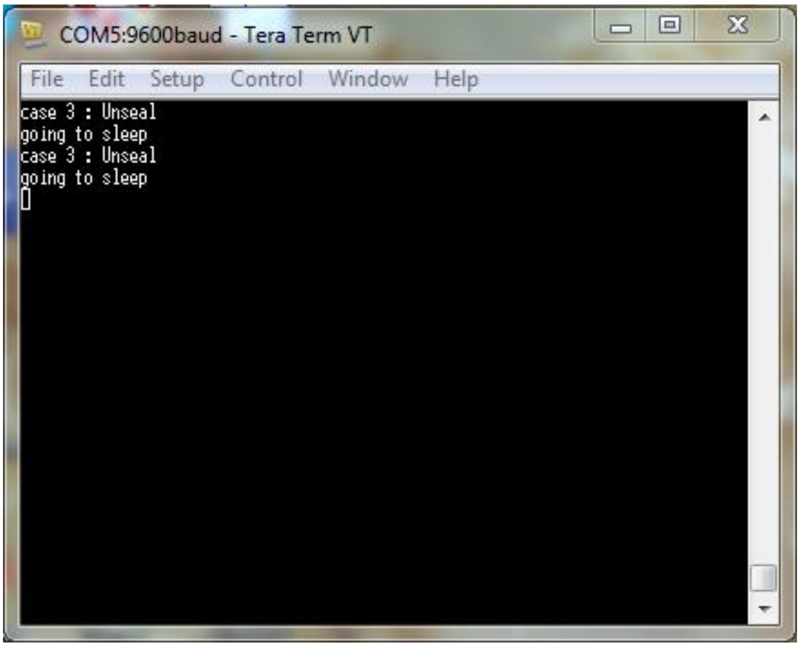


Figure 22.0 – Tamper Event

4.3 Challenges Faced

The development of the firmware of the prototype is challenging. This section relates the challenges faced while developing the project.

4.3.1 UKeil Vision Compiler

uKeil Vision compiler is a subset of C compiler, thus has a limited library. For example, it does not have the time.h library. In uKeil, rand() function generates a pseudo-random number. However, in C programming, rand() function is generated based on a variable eg. time or date. This is to avoid generating the same number pattern after reset. The time.h provides the time variable eg. rand(time).

4.3.2 Hardware

4.3.2.1 Wake Up Pin

When the nRF24LE1 is put into register retention mode, it is inactive. To re-activate it, an external wake up pin is required. The testing and writing of the firmware for this function is difficult as resources are limited.

The wake up pin is unstable and inconsistent. It does not always function as desired. This is due to the hardware sensitivity. The wake up pin is active high. When an external source of 3.3V is given to the wake up pin, the module is activated. However, hardware testing often has a certain percentage error as compared to theoretical findings.

4.3.2.2 UART

The UART often displays inappropriate characters when it was activated to send a string of characters. This is caused by the sensitivity of the hardware. The UART cable is very fragile and often has connection problem. Moving the cable while the UART is transmitting data gives a different output.

4.3.3 Firmware

4.3.3.1 Real Time Clock

Time stamp is an important feature in tracking the events of the electronic seal. The real time clock generates the current date and time of the events. In this project, the author faces difficulties incorporating the real time clock function when the device is in register retention mode. Further testing and development could be done in this matter to produce a time stamp for each event.

4.4 Cost Effective

The issue of pilferages for on board sales is a daily event for airlines. An average airline operates 250 to 300 flights daily. Each flight has an average of 3 trolleys for short journey flights. Items that are usually reported to be stolen are high end products, liquor, cigarette, cosmetics and jewelry. According to a local airline company, 25% of flights suffered from the issue of pilferages for on board sales and a fully stuffed trolley can cost up to USD 10, 000. The loss of goods usually mounted up to 30% of the products in the trolley. The loss is not merely the value of goods; the management time cost is also high.

When cases of pilferages are reported, the company has to investigate and interrogate the parties involved, mainly the ground staffs, air crews and contractors. The whole process of interrogation takes a lot of effort and time. Each case of interrogation takes at least an hour to complete. Considering an average management time cost of USD 60 per man-hour, a ball park figure of USD 100 per case can be concluded.

The proposed solution uses a nRF24LE1 module that costs only USD 8. The mechanical development is given an estimate of USD 20 per device. The total cost of the proposed device gives an estimate of USD 28. Table 7.0 shows the cost of loss while Table 8.0 shows the cost of solution.

Loss per Trolley	Cost (USD)
Products (30%)	3, 000
Man-Hour	100
Total	**3, 100**

Table 7.0 – Cost of Loss

Parts per Device	Cost (USD)
Electronics	8
Mechanical	20
Total	**28**

Table 8.0 – Cost of Solution

Currently, plastic seals are being used to secure the airline trolleys. Given that the price of one plastic seal is 1 USD and assuming the case of one trolley per flight. The total cost of using plastic seals per month is calculated as shown in Table 9.0. The proposed electronic seal is reusable. The total cost of using an electronic seal per month is calculated as shown in Table 9.0. From the table, the proposed electronic seal offers an effective yet low cost solution to the problem faced by the airline on board sales industry.

Plastic Seal	Proposed Electronic Seal
2 seals X 30 days = 60 seals Price per plastic seal = 1 USD	1 seal (reusable) Price per seal = 28 USD
Total cost per month = 60 seals X 1 USD = 60 USD	Total cost per month = 1 seal X 28 USD 28 USD

Table 9.0 – Cost of Plastic Seal vs Cost of Proposed Electronic Seal

4.5 Impacts on Society

Currently, the issues of pilferages of airline on board sales are usually being point to the air crews of which the air crews denied of such actions. Interrogation that is carried out has proven to be inefficient as no strong evidence can be produced. Inefficient interrogation may results in innocent party being put to blame.

Blaming the innocent party will result in deterioration of the relationship between employer and employee. The employee may feel pressured to keep his job while harboring unfavorable opinions about his boss, while the boss wonders if the employee is working to the best of his ability. When an employee has a record of involving in issue of pilferages, employers will be concerned about the morale of the employee and will eventually lead to expensive issues with turnover or low productivity.

CHAPTER 5
CONCLUSION

Airline on board sales supply chain has been facing issue of pilferages and has been creating a hassle in the industry. The loss of duty free items in the airline on board sales supply chain brings forth damages to the airline industry. Insufficient interrogation may results in wrong judgment. This will eventually betray the trust between employers and employees.

Active RFID has proven to be efficient and effective in security and supply chain industry. It has been providing solutions for security and supply chain industry without fail. However, active RFID technology has yet to be implemented in the airline on board sales supply chain. Active RFID actively transmit signals over the air. This characteristic of an active RFID results in the fear of interference with the airline control system which could affect the safety of the passengers.

Safety of the passengers should always be a priority. Fortunately, with the technology available today, the incorporation of a semi-passive RFID and an active RFID as proposed is the solution. This incorporation will result in a device which is a system integration of firmware and hardware. The device transmits signals only when prompted by an external device such as the reader. The device will act as a semi-passive RFID on board and act as an active RFID off board. This integration will ultimately be the solution to the issue of pilferages in the airline on board sales supplies chain and yet ensuring that there will be no interference with the airline control system.

The nRF24LE1 is a member of the low-cost, high-performance family of intelligent 2.4 GHz RF transceivers with embedded microcontrollers [18]. Its ability to power down and wake up by an external source makes it an ideal choice for this project.

In conclusion, the proposed electronic seal is an ideal solution to the issue of pilferages in the airline on board sales supply chain industry. Its unique seal key generation upon each sealing makes it possible for involving parties to track and safeguard their goods.

CHAPTER 6
RECOMMENDATION

In this demonstration prototype, the reader is signified by a switch. Further improvement can be done by purchasing a UHF Reader. A UHF reader will be able to communicate with the semi passive RFID chip which will be connected to the wake up pin of nRF24LE1 module.

A Graphical User Interface (GUI) can also be developed for the reader. The GUI will show the data received from the nRF24LE1 module in a user friendly way. This will be easier for users to use and interface with a reader.

The seal key generated on each sealing is a four digit unique number. Further improvements can be made to generate hexadecimals number or even 8 digits of seal key. This way, it can increase the security level of the seal key.

In this prototype, the author has not been able to generate real time clock. Further development in generating a real time clock would bring the project one step ahead.

REFERENCES

[1] A. Osman and Teddy Mantoro "A User Profile for Information Filtering Using RFID-SIM Card in Pervasive Network," Faculty of Information and Communication Technology, International Islamic University Malaysia, Malaysia, 2010.

[2] J. Landt. (2001, Oct. 1) *Shrouds of Time: The History of RFID* [Online]. Available: www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

[3] Mark Roberti. (2001, Dec. 20) *The History of RFID Technology* [Online]. Available: http://www.rfidjournal.com/article/view/1338

[4] Dean Boys. (2005, Dec. 20) *Identification Friend or Foe IFF Systems:IFF Questions & Answers* [Online] Available: www.dean-boys.com/extras/iff/iffqa.html

[5] S. Ahson. M. Ilyas "RFID Handbook Applications, Technology, Security, and Privacy," CRC Press Taylor & Francis Group, 2008.

[6] Scheer, "Optimising supply chains using traceability systems," in *Improving Traceability in Food Processing and Distribution, Cambridge*, 1st ed. I. Smith and A. Furness, England: Woodhead publishing Limited, 2006, pp.52–64.

[7] Gary M. Gaukler, Ralf W. Seifert "Applications of RFID in Supply Chains" in *Trends in Supply Chain Design and Management: Technologies and Methodologies*, 1st ed. Hosang Jung, F. Frank Chen, and BongjuJeong, Texas: Springer-Verlag London Ltd, 2007.

[8] InfoSec. (2008, Feb) *RFID Security* [Online] Available: http://www.infosec.gov.hk/english/technical/files/rfid.pdf

[9] Thing Magic. (2010) *RFID and The Internet of Things* [Online] Available: http://rfid.thingmagic.com/rfid-blog/bid/28549/RFID-and-The-Internet-of-Things

[10] Amy Rogers Nazarov. (2009, May 9) *Internet of Things* [Online] Available: http://www.internetevolution.com/document.asp?doc_id=181268

[11] RFID Journal. *RFID Business Applications* [Online]. Available: http://www.rfidjournal.com/article/view/1334

[12] DATAMARS. (2010) *Types of RFID tags* [Online]. Available: http://www.datamars.com/default.aspx?menuitemid=258&menusubid=14&AspxAutoDetectCookieSupport=1

[13] VIZINEX RFID. *RFID Applications in Supply Chain Management* [Online]. Available: http://www.vizinexrfid.com/rfid-applications-in-supply-chain-management/592/

[14] The Corporate Machine. *RFID Types* [Online]. Available: http://www.tcm-s.com/Assets/Product/RFID/RFID%20Basic/Types%20of%20RFID.htm

[15] Pierre-Jean Benghozi, *RFID Solutions (FMSH Editions)* [Online]. Available: http://editionsmsh.revues.org/97

[16] Beth Bacheldor. (2007, Jan. 29)*Audi Uses Semi-Passive Tags to Make TTs* [Online]. Available: http://www.rfidjournal.com/article/view/3002

[17] Claire Swedberg. (2012, Dec. 12) *Pilots of CSL's Battery-Assisted Passive UHF RFID Card Underway* [Online]. Available: http://www.rfidjournal.com/article/view/10223/2

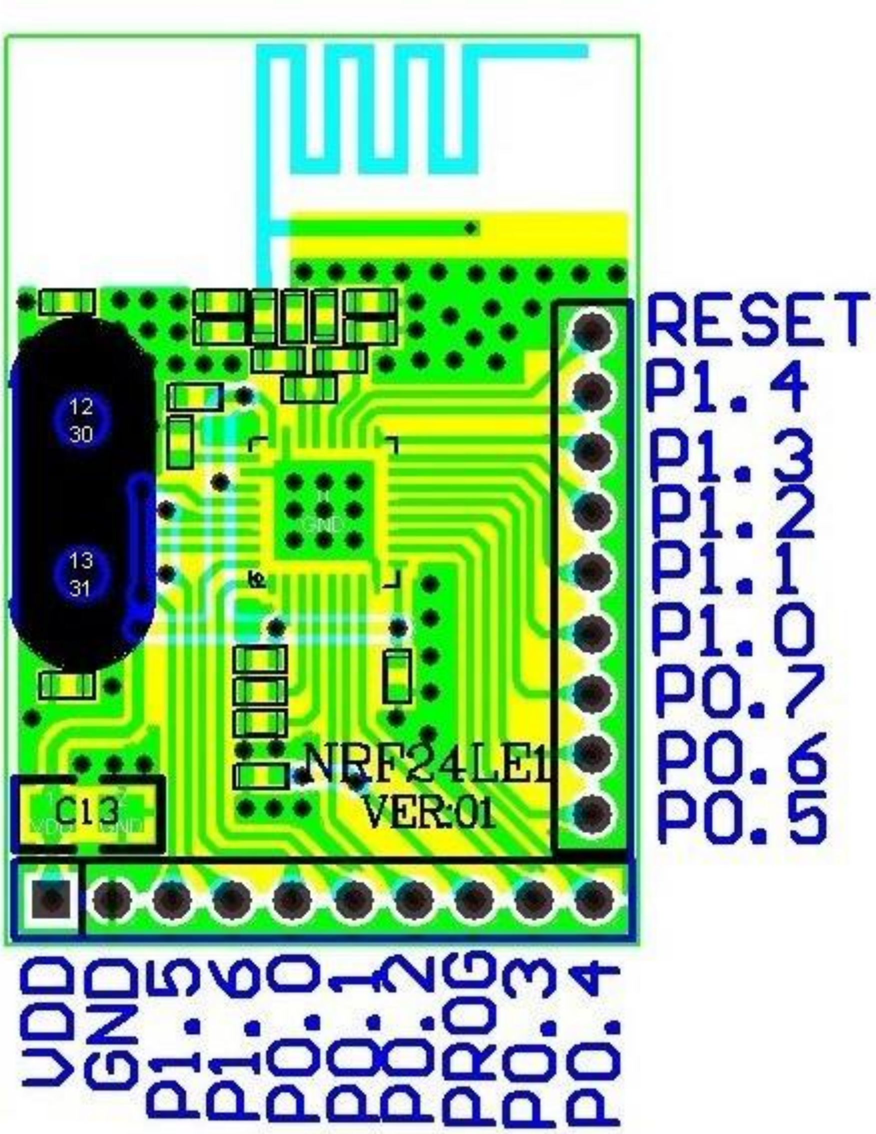
[18] *nRF24LE1 Product Specification*, 1.6th ed, Nordic Semiconductor ASA, Norway, 2010.

[19] NORDIC SEMICONDUCTOR. *Which power down mode should I use with the nRF24LE1* [Online]. Available: http://www.nordicsemi.com/chi/layout/set/print/Nordic-FAQ/Silicon-Products/nRF24LE1-OTP/Which-power-down-mode-should-I-use-with-the-nRF24LE1

APPENDICES

APPENDIX A

PINS OF NRF24LE1



APPENDIX B

NRF24LE1 SYSTEM ON CHIP

NORDIC SEMICONDUCTOR

nRF24LE1

Ultra-low Power Wireless System On-Chip Solution

Product Specification v1.6

Key Features

- nRF24L01+ 2.4 GHz transceiver (250 kbps, 1 Mbps and 2 Mbps air data rates)
- Fast microcontroller (8051 compatible)
- 16 kB program memory (on-chip Flash)
- 1 kB data memory (on-chip RAM)
- 1 kB NV data memory
- 512 bytes NV data memory (extended endurance)
- AES encryption HW accelerator
- 16-32bit multiplication/division co-processor (MDU)
- 6-12 bit ADC
- High flexibility IOs
- Serves a set of power modes from ultra low power to a power efficient active mode
- Several versions in various QFN packages:
    - 4×4mm QFN24
    - 5×5mm QFN32
    - 7×7mm QFN48
- Support for HW debugger
- HW support for firmware upgrade

Applications

- Computer peripherals
    - Mouse
    - Keyboard
    - Remote control
    - Gaming
- Advanced remote controls
    - Audio/Video
    - Entertainment centers
    - Home appliances
- Goods tracking and monitoring:
    - Active RFID
    - Sensor networks
- Security systems
    - Payment
    - Alarm
    - Access control
- Health, wellness and sports
    - Watches
    - Mini computers
    - Sensors
- Remote control toys

APPENDIX C

AIRLINE TROLLEY AND PLASTIC SEAL