# INTERNET OF THINGS

A RFID Temperature Smartsensor

**Abdulakeem Odunmbaku**

Bachelor's Thesis

___.___.______ _______________________________

**SAVONIA UNIVERSITY OF APPLIED SCIENCES** **THESIS**
**Abstract**

| Field of Study<br>Technology, Communication and Transport | | | |
|---|---|---|---|
| Degree Programme<br>Information Technology | | | |
| Author(s)<br>Odunmbaku AbdulAkeem Adeoye | | | |
| Title of Thesis<br>RFID Temperature Smartsensor | | | |
| Date | 8th June, 2012 | Pages/Appendices | 45/ 7 |
| Supervisor(s)<br>Mr. Arto Toppinen | | | |
| Client Organization/Partners | | | |


Abstract

This project was about the technology of the Internet of Things (IOT). It was used to achieve the aim of building a smart sensor. The IOT was implemented by integrating RFID technology and smarts sensor technology. These sensors used were mostly Micro-electromechanical Systems (MEMs). The sensors are small since they are micro systems, which is enough to build a relative small device

In this project, a custom made “G2iL+” chip was used to build the RFID tag. A temperature sensor switch was also used. An antenna was built on a PCB board to achieve an RFID tag with the chip. The tag is passive so it gets its power from the reader.

At the end of this project, it was possible to make the connection between the RFID tag and the temperature switch. The temperature of surroundings can be measured by using a special reader for the RFID tag. This device can be embedded on any surface without any notice of its presence on the surface.



Keywords
RFID tag, smart sensor, temperature switch

**SAVONIA - AMMATTIKORKEAKOULU** **OPINNÄYTETYÖ**
**Tiivistelmä**

| |
|---|
| Koulutusala<br>Tekniikan ja liikenteen ala |
| Koulutusohjelma<br>Informaatioteknologia |
| Työn tekijä<br>Odunmbaku AbdulAkeem Adeoye |
| Työn nimi<br>RFID Lämpötilaälyanturi |

| | | | |
|---|---|---|---|
| Päiväys | 08.6.2012 | Sivumäärä/ Liitteet | 45/ 7 |

| |
|---|
| Ohjaaja (t)<br>Arto Toppinen |
| Toimeksiantaja/ yhteistyökumppani(t) |

Tiivistelmä


Tämän työn aiheena oli Internet of Things (IOT). Sitä käytettiin älyanturin rakentamiseksi. IOT toteutettiin integroimalla RFID-teknologia ja älyanturiteknologia. Käytetyt anturit olivat pääasiassa Mikrosysteemejä (MEMs). Mikrosysteemien pienen koon vuoksi oli mahdollista rakentaa vastaava pieni laite.

Tässä työssä mittatilaustyönä tehtyä G2iL +" sirua käytettiin RFID-tunnisteen rakentamiseksi. Myös lämpötila-anturin kytkintä käytettiin. Antenni rakennettiin PCB-taululle, jotta saataisiin aikaan RFID- tunniste sirun kanssa. Tunniste on passiivinen, joten se saa energiansa lukijasta.

Projektin lopussa oli mahdollista löytää yhteys RFID- tunnisteen ja lämpötilakytkimen välillä. Ympäristön lämpötila voidaan mitata käyttämällä RFID- tunnisteen erityistä lukijaa. Tämä laite voidaan upottaa mihin tahansa pintaan huomaamatta sen läsnäoloa kyseisellä pinnalla.



Avainsanat
IOT, RFID - tunniste, älyanturi, lämpötilakytkin

Acknowledgement

My acknowledgement goes firstly to the Finnish government for giving me this great opportunity to explore and experience their nearly perfect educational system, and acquire more knowledge in this great field of information technology. I also recognize my prestige institution (Savonia University of applied Sciences), staffs, teachers, students for taking me as one of them and staying and studying together for the past four years.

My acknowledgement also goes to my thesis supervisor, Mr. Arto Toppinen, who with his professional skills helped, me in completing my thesis. Also, to the whole department of information technology as the shared knowledge between the teachers, and student has greatly influenced my skills and ability in the world of information technology.

Lastly, my gratitude goes out to my family, friend and loved ones, who have helped me in staying in a balanced state of mind in order to achieve my goal during the entire period of my studies at Savonia University of Applied Sciences. They have stood by me in thick and thin, mentally and physical, moral and spiritually and without them I would not be right where I am today.

Odunmbaku AbdulAkeem A.
30th April, 2012
Kuopio, Finland

## Glossary

dB - Decibel

dBi – Decibel Isotropic

EPC – Electronic Product Code

ERP -Electronic Road Pricing

ETSI - European Telecommunications Standards Institute

HF – High Frequency

IC – Integrated Circuit

ISO- International Organization for Standardization

kph – Kilometer Per Hour

LF – Low Frequency

mW – Milliwatt

RF600A – Simatic RFID Antenna

RF600R – Simatic RFID Reader

RFID – Radio Frequency Identification

RF-Manager – Simatic RFID Host Application Developer Software

RF – Radio Frequency

TCP – Transmission Control Protocol

IP - Internet Protocol

TR - Receive

TX – Transmit

UHF – Ultra High Frequency

USB – Universal Serial Bus

WR – Read Write (reprogrammable)

IOT – Internet of Things

MEMs – Micro-electromechanical Systems

TABLE OF CONTENTS

## INTRODUCTION

In the past, temperature sensors were usually big and it was easy to read, then its measurement requires actually calibration using the human eyes. It also requires mathematical skills to read the measurement and it can be measured wrongly if the human reader has no enough skills to use it. They can be accurate to few millimeters measurement, and can be used only around large environment like the human body, an environment temperature or a large device temperature. Figure 1 shows the example of this kind of thermometer.

FIGURE 1. A mercury Thermometer (Genesis of Temperature sensor) (youarenowaware 2012)

As technology grew, more accurate temperature devices were built, they measure temperature to more accurate readings, and they only require the ability to read to use the thermometer. This can also be regarded as the beginning of smart sensors. This involves the use of electronic devices to sense the temperature of an object or area. The thermometer takes a value from a body, compares it to a specific internal value of the thermometer, calculates it and displays its result on a digital screen. This type of thermometer can also be called a digital thermometer. The electronic component present in the thermometer is usually a passive component that is used in the sensing of the temperature. Figure 2 and 3 shows an example of a digital thermometer and passive temperature sensor respectively.


FIGURE 2. A digital Thermometer (basaldigitalthermometer 2012)

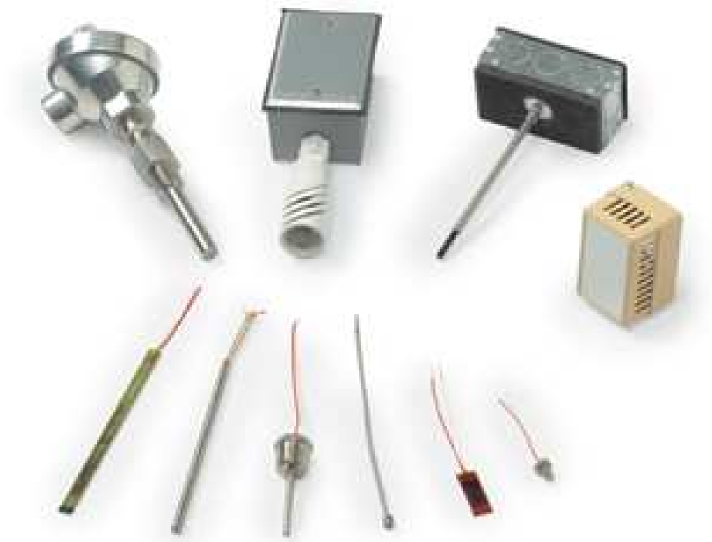


FIGURE 3. Passive temperature sensor (Minco 2012)

As technology developed, temperature sensors were employed in other areas of life. It was implemented in building construction, phone technology and other areas of life. The implementation hereby leads to the development of the RFID smart sensor. It involves the use of passive RFID tags and combining it with a smart temperature sensor.

This thesis is based on the use of RFID technology and smart sensor technology. The purposed of this thesis is to implement a temperature smart sensor and an RFID tag. The finished device can read the temperature of a particular region such as the roof of buildings and important machinery parts. The RFID tag will be built using a G2iL+ chip. This chip is manufactured by NXP semiconductors. The temperature smart sensor usually acts like a switch component. It uses a specific temperature as the midpoint to act as the switch. If the temperature goes over the temperature, it closes its circuit and allows the content of the RFID tag to be read and when it is below the specific temperature, it opens its circuit and the content of the RFID tag cannot be read.

# 2. RFID technology

RFID (radio-frequency identification) technology means the use of wireless radio frequency to identify different objects. RFID is an improved form of bar coding. Bar coding on the other hand is a machine readable representation in form of bars. Bar codes help in keeping track of items and inventory. A RFID tag is used with other devices to implement the RFID technology, each RFID tag transmits on its own radio frequency. Also, each RFID tag has its own unique identifier. This unique identifier is transmitted via the radio frequency of the RFID tag. An RFID tag consists of three main components (Yu 2011).

- The transponder
- The interrogator
- The middleware

The transponder is that part of the RFID tag that deals with the physical entity of RFID technology; it includes a RFID chip, and an antenna for the chip. An interrogator is a reader that reads the information in the RFID tag. The middleware part of the RFID technology is a system that deals with the filtering of data that passes through the RFID tag reader.

## 2.1. Types of RFID tags

RFID tags are classified according to their functions. This function mainly is focused on how they are been powered. There are two major types, active and passive RFID tags.

### 2.1.1 Active RFID Tag

Active RFID tags are RFID tags that are powered by self implanted batteries. Their characteristics include long read range, short detecting time, large memory space and a data logging function. This is possible because each RFID tag is equipped with its own batteries (Huang, Han, Zhang, Chen, Wu, 2011). Figure 4 shows an example of an active RFID tag.

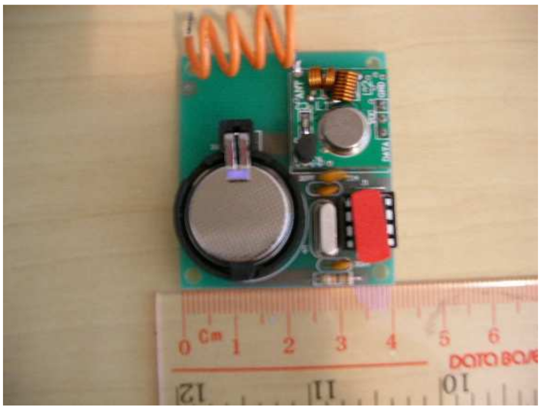


FIGURE 4. Example of active RFID tag (Ananiahelectronics 2012)

### 2.1.2. Passive RFID tag

On the other hand, passive RFID tag is not equipped with its own batteries like the active RFID tag. Instead, it powers itself from the interaction of radio waves between itself and the RFID receiver (Huang et al. 2011). The antenna of a passive RFID tag forms a magnetic field; thereby it draws power from the receiver, energizes the tag circuit and powers itself. Figure 5 shows a passive RFID tag.

FIGURE 5. A passive RFID and it circuitry (Anomicofficedrone 2012)

## 2.2. Frequency of RFID Tag

RFID systems are differentiated by the use of different frequency by different RFID tags. The use of these frequencies also determines the protocol used to communicate between the source RFID tag and the reader.

These frequencies can range from 100 KHz to over 5 GHz. The classification of the frequencies is presented in table 1.

TABLE 1. RFID frequency table (Hunt, Puglia & Puglia, 2007 and Klaus 2010)

| Frequency Band Range | Name (Frequency) | System name (RFID) |
|---|---|---|
| 125Khz – 134KHz | Low Frequency | LF Systems |
| About 13.56MHz | High Frequency | HF Systems |
| 860MHz – 960MHz | Ultra high Frequency | UHF Systems |
| 2.4GHz – 2.45GHz | Microwave | Microwave Systems |

## 2.3. RFID Reader

RFID tags are meant to be read. To read, a RFID tag require a reader in order for this aim to be achieved. A RFID reader on the other hand communicates with the RFID tags using radio frequency. A RFID reader must possess one or more antennas to communicate with a RFID tag.

A RFID reader must have logical components. This logical component includes a reader API, communication, event management and antenna subsystem (Glover & Bhatt, 2006).

- **Reader API**

Reader API allows RFID reader to request tag inventories, control configuration settings of the reader, and monitoring the health of the reader.

- **Communication**

Communication handles the details of communication of transport protocols of the reader and the middleware.

- **Event management**

Event management can also be called “observation”. When two or more observation occurs, it is called an event. The event management defines the kind of observation good enough to be called an event and interesting enough to communicate with.

- **Antenna subsystem**

Antenna subsystem consists of the interfaces and logic that enable the reader to interrogate RFID tags and also control the physical antennas.

FIGURE 6. Different types of RFID reader (GAO Tek Inc 2008)

## 2.4. Standards of RFID tags

In modern technology, the needs for standardization are necessary for application of the inventory. In RFID technology also, application standards are important so that improvements can be carried out on previous standards and better products can be manufactured. The standards of RFID tag also are based on application purposes. The use of an RFID tag can biased with the application function it is to be used for, example of application includes (Glover & Bhatt 2006 and Wolfram, Gampl & Gabriel 2010).

### 2.4.1. Privacy

RFID standards can be based on privacy and data protection of a tag. A tag can be used in an application and can include the privacy of the user.

### 2.4.2. Security

A RFID tag may be used in tracking and tracing of goods and it possess the security function, by not allowing tampering or stealing of the goods.

Different standards of RFID tags that includes one or more different measure such as memory locking, unique identifier, random identifier, data covering, authentication and encryption, are as follows (Wolfman et al. 2010);

- ISO 14443
- ISO 15693
- ISO 18000-6c
- EPC Gen2
- EPC HF

# 3. Internet of Things

In this thesis, the main idea is to implement the technology behind Internet of thing (IOT) to build a smart sensor. IOT on the other hand, is the uniqueness in the identification of objects/ things in a virtual representation and internet-like way. In the present world, human interaction is needed in completing most part of production process or in the operation of simple machines. The idea of IOT was introduced to reduce the dependence of humans by machine and monitoring of activities would be much easier.

The RFID technology was seen as the ideal technology to implement the IOT technology, where all object (things) will be equipped with radio tags and can be identified by smart reader and computers. With this way, monitoring of things all around our daily life will be easily monitored. Goods will be easily tracked, inventories can be easily monitored, temperature along the supply chain, companies would know exact amount of goods and services needed to avoid waste, e.t.c (Commission of the European Communities, 2009).

## 3.1. Features of Internet of Things

The working principle of IOT is similar to that of internet application, but slightly different. This form of sharing information is divided into three main parts: information uploading, information transmitting and information downloading. The difference between IOT and other internet application is that, the information is termed as the object of the sentence. The three main features are analyzed in details below (Yinghui& Guanyu, 2010).

### 3.1.1. Service: Only Thing’s Information

The normal internet application such as web services could also mean a thing’s information and some other some other information when uploading data. In IOT, term “thing” in the internet of things is just used for a single thing’s information. The thing’s information is specially orientated for IOT, it intelligently process the information and globalize the thing’s information to increase the human welfare.

### 3.1.2 Expression: Standard Code

In IOT, efficiency is very important, so information uploading and transmitting is being completed automatically. For this procedure to be achieved, a standard expression of information uploading is necessary. Organizations such as ISO/IEC are responsible for IOT standardization of information items for IOT. Electronic tag used for IOT must contain name, content and format of information items. In the present stage of standardization, the major achievements made are the RFID coding, UID (recommended by the Japanese) and thee Electronic product code (EPC).

### 3.1.3. Storage: Electronic tag

The thing entity in IOT is solely circulating around human production, consumption and goods exchange. The need for information about this thing became a necessity to attach information about the product to each product. The characteristics of bearer of information on the product should be;

- Light and small physical form in other not to add to the weight of the product.
- Simple in design and easy to read the information it holds.

An electronic tag was chosen as the appropriate option. That simply shows how a RFID tag is introduced into IOT. It small in size and shape, can record information in it and can be embedded into a body with ease.

### 3.1.4. Uploading: Non-contact Machine Reading

In the real world, uploading of information is done manually by a user. In IOT, information of a thing is not done by anybody, but is to be read by a reader. The reader obtains the information from the “thing” entity. Present technology suggest that, RFID readers read by a non contact scanning of an IOT device information is been expressed with electronic signal of the RFID tag. The advantage of non contacting reading is that, it shortens the time of uploading the “thing’s” information unto the internet. Figure 7 shows the communication dimension of IOT.

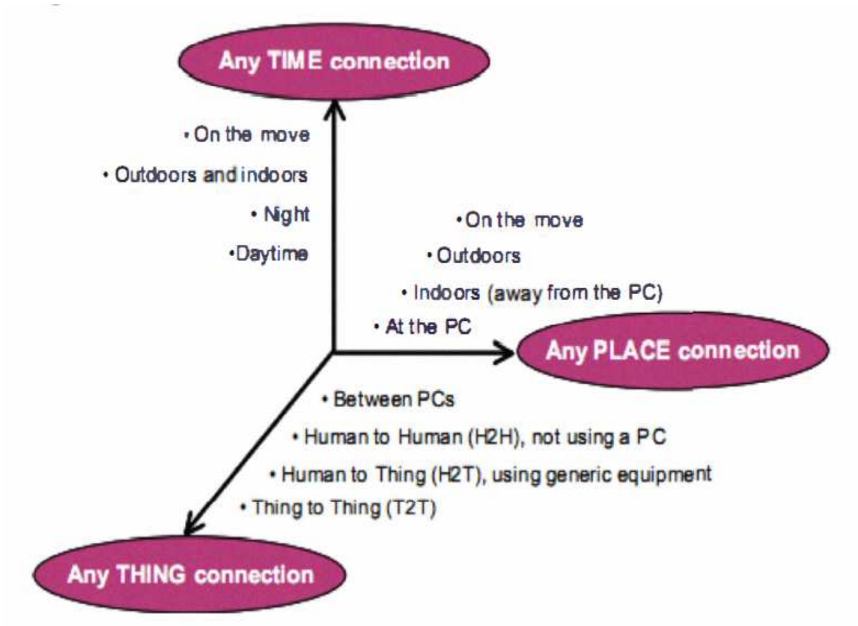



FIGURE 7. Communication Dimension of IOT (Tan, Wang. 2010)

### 3.2. Technology of IOT

This is the combination of different technologies. Their intelligences are combined to form the unique technology of IOT. The key technology used in the implementation of IOT is mainly focused around the sensing areas of IOT. This technology discussed in this thesis is solely concentrated on the development of IOT combined with RFID Technology. The features of the technology are discussed as follow (Handong, Lin. 2011);

#### 3.2.1. RFID Technology

As discussed early in this paper, Radio frequency identification (RFID) technology is an emerging technology that can realize a non-contacting information transmission by recognition of radio frequency signals. In IOT, a thing is associated with a RFID tag, and it works with the principle of “one thing, one code”. With this principle, goods (things) can be properly managed and a real-time tracing can be achieved.

### 3.2.2. Sensor Technology

Sensor technology is responsible for the acquiring and recognition of the “thing” in IOT. The technology is developed so as to acquire the information of the environment around objects. It also the scope used by the RFID technology in recognition of frequency. The main idea of the sensor technology part of IOT is to provide the most original information of the object.

### 3.2.3. Embedded Technology

An IOT system is built as an embedded system so as to provide intelligent features. An IOT system is also built so as to recognize each object and interact with them. This makes each object an intelligent object. During communication with each object, information and physical distribution flow synchronize intelligently to provide a quick and efficient network platform for the sharing of objects information. The main purpose of this technology in IOT is to make objects in IOT to have a certain degree of intelligence.

### 3.2.4. Nanotechnology

IOT systems are built to be compatible with other technologies such as nanotechnology. It can interact with objects with smaller volume, connect with them and decrease the consumption of the system. Figure 8 shows the technology of IOT.

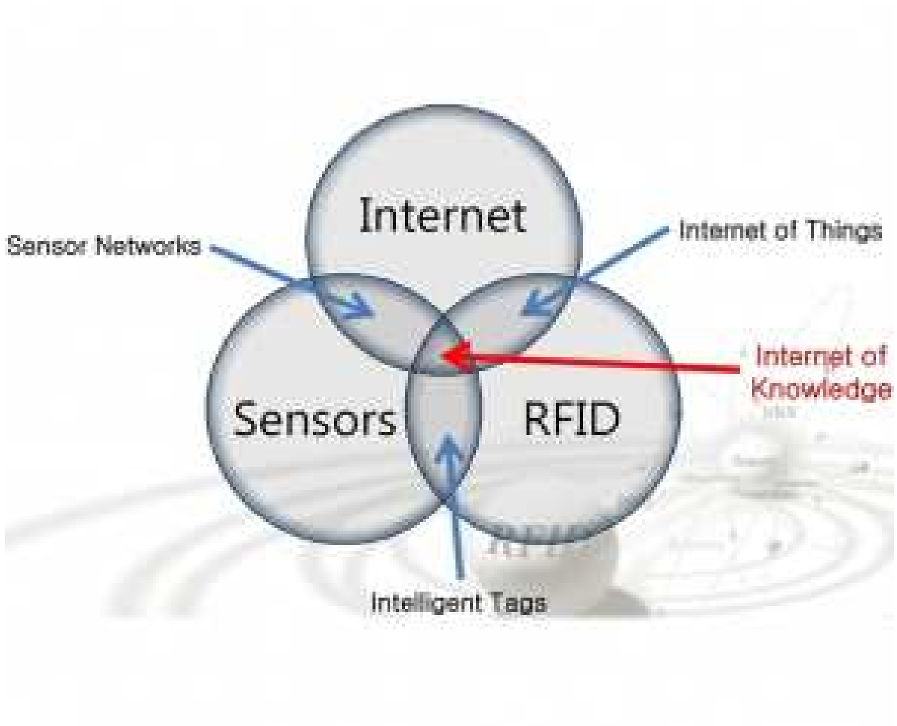



FIGURE 8. Technology behind IOT (bit-tech 2012)

### 3.3. Architecture of IOT

In IOT, numerous objects are connected, numbering up to billions sometimes. Because of this huge number, a large traffic will be created and more data storage will be needed. Rather than using today's internet structure, challenges such as security, a conclusion was arrived at to develop a new architecture for IOT. Various considerations such as the following were taken when talking about the architecture of IOT;

- Every object is connected, and they can exchange information by themselves.
- Traffic and storage of network increases rapidly
- In the future, can different objects in IOT communicate with each other?

There have been IOT applications such as the EPC Global, smart hospital already, but the development of a standard architecture of IOT is imminent. The lack of global standards, which gives rise of different standards and technologies, gives an inter-operable problem between different types of IOT. The ideal architecture should have a unified structure which can identify and process every application system (Tan, Wang. 2010).

Existing architectures of IOT are written in UID or EPC code. These codes are embedded in an RFID tag. With this, a RFID reader can read the objects information from the tag in a non-contacting form. Figure 9 shows an example of IOT architecture.

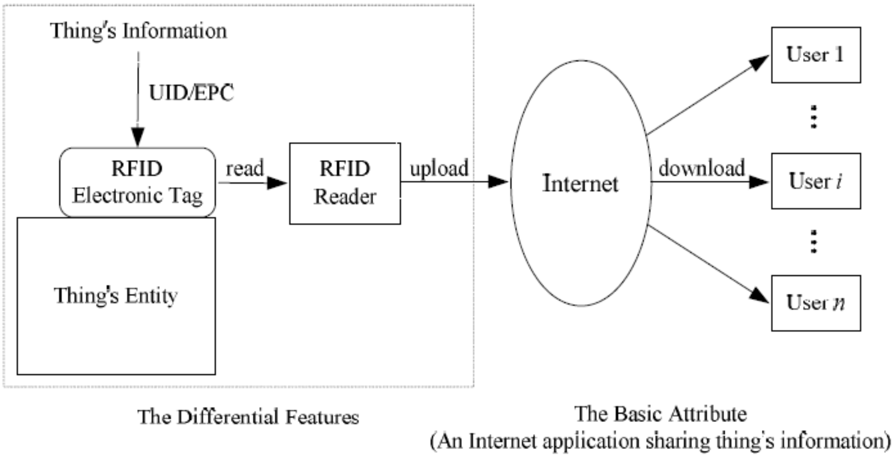



FIGURE 9. An example of an IOT architecture (Yinghui& Guanyu, 2010).

## 4. Smart sensor

Smart sensors are Micro-Electromechanical Systems (MEMs) devices with more embedded features than ordinary sensors. They are smaller, cost effective and consume less power, they are aimed to detect and report information in unusual and extreme situations. The information got from the smart sensor is shared with an end user; the sensing detention is done in different hierarchical processes. One of the main properties of a smart sensor is sharing information among neighbors with over lapping sensing areas. Smart sensors with signal conditioning and embedded function are more adopted in the market and the trend toward pervasive sensor. These smart sensors are facing basic sensors out like smart phones facing out mobile phones (Gervais-Ducouret, 2011 and Bruckner, Velik & Zucker. 2008).

### 4.1. Generations of Smart Sensor

The call for new type of sensors emerged when older types of sensors began to prove they are prone to errors and also fail in unfavorable conditions like weather and temperature conditions. The strategy of implementing expert knowledge from previous technology to a framework of new architecture that supports smaller and smarter sensor was deployed. The intention is to enable sensor manufacturing to be more flexible and dynamically configurable (Loganantharaj, Palm & Ali, 2000).

In recent years, the increase in the area of nanotechnology has produced interesting materials which provides more opportunity for the development of sensing transduction technology. Older generations of sensors are built on to produce improved performance and extension of its functional capabilities. This development has been achieved through the implementation of structural designs. The technology behind this improvement makes use of advanced calculation, algorithm and signal processing. Example of these includes characteristic functions, weight functions, inferential calculation of soft sensors with the sensor having its own advanced self adaptive method for frequency-to-digital conversion (Yurish & Gomes, 2005 and Wilson 2005).

The generation of smart sensor can be categorized into three generations Wilson 2005,

#### 4.1.1. First generation

The first generation can be classified according to its receptor. The sensor receptor is trapped in the base sensor. The electronics part of the sensor is usually fused with the transducer.

#### 4.1.2. Second generation

This is based on the individuality of component making up the sensor. The electronic element and the sensor node of the sensor are separate in the sensor.

#### 4.1.3. Third generation

In this generation of smart sensor, the electronic element and the sensing node of the sensors are fused together on a single chip, and are relatively small and portable.

### 4.2. Types of smart sensor

There are different types of smart sensors. These smart sensors are mostly MEMs systems, and they are of great interest in many fields of the industry like, biomedical application, control systems, security systems etc. These Microsystems combine sensing, accuracy and signal processing in a microscopic scale. Examples of smart sensors include (Yurish & Gomes, 2000),

- Temperature sensors
- Pressure sensors
- Accelerometer sensors
- Optical sensors
- Humidity sensors
- Gas sensors
- Chemical sensors
- Biosensor sensors e.t.c.

### 4.3. Uses of smart sensor

The names of smart sensors literally define their uses. As stated above, the name of each smart sensor defines what each one is used for. For example, Temperature smart sensor for measuring temperature, pressure smart sensor for measuring sensor, accelerometer for measuring acceleration. Figure 10 shows examples of smart sensors

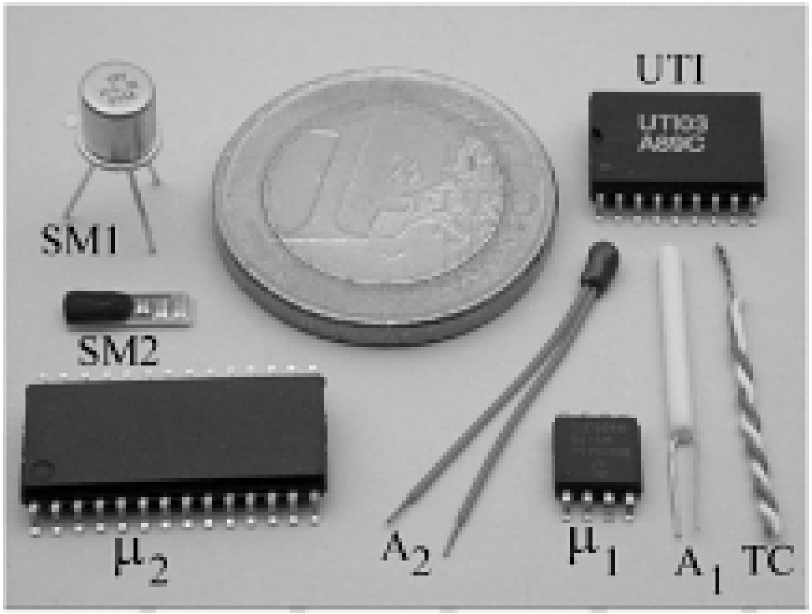



FIGURE 10. Different Temperature smart sensor (Gerard Meijer, 2008)

# 5. RFID smart sensor

The implementation of a sensor is to monitor and collect sensorial data with the issues of data transmission, costs, enabling enhanced technology. The large quantity of data collecting gave birth to the development of smart sensors. On the other hand, data transmission must be processed, identified and placed as context information for the end user. RFID technology is hereby used to transmit the information gotten from the sensor and can as well be read by a compatible tag reader (Catarinucci, Colella, Esposito, Tarricone & Zappatore, 2009).

The RFID smart sensor includes both the hardware and the software infrastructure which as to be versatile, configurable and easy adjustable to different topologies. The main point of the RFID smart sensor is the selection of a suitable technology for the collection and transmission of specific sensorial data (Catarinucci et al. 2009). This key technology should have the following characteristics:

1. Simple to use in different application domain.
2. Low-cost and low power consumption. The implementation of this gives way to high numbers of sensorial nodes.
3. The RFID sensor system should be operable with any kind of sensor.

RFID tags with generic smart sensors can lead to the realization of a sophisticated smart-sensor system. Smart sensors are relatively cheap just as same as RFID tags, so building a cheap system is practically possible.

## 5.1. Smart transducer interface for sensor and actuator

A smart transducer interface for sensors and actuator is a specific standard that specify set of features that will allow a smart transducer to communicate with an outside world. This technique is employed in RFID systems so as to ease the communication between the interfaces (IEEE, 2010) . The following shows the design elements that are essential in all smart transducers, which forms this smart transducer standard.

### 5.1.1. Communication protocol

In embedded communication systems, communications are maintained by communication protocols. These protocols are complex because of the synchronization of the system (Yang, 2005). Embedded operating systems are used in transducer interface and protocols are needs for transportation of information.

### 5.1.2. Command structure

Command structure is the language of communication that is used to control the action of the smart transducer. A command structure should support all communication protocol that will be used when designing a smart transducer interface. A transducer interface must also be able to retrieve data available to multiple sensors.

### 5.1.3. Transducer electronic data sheet (TEDS)

The transducer electronic data sheet consist of the configuration information of the smart transducer interface, it also show the capability of the interface for each smart transducer. Basically, the TEDS contain all the characteristics of a transducer interface.

### 5.1.4. Transducer data

The transducer data consist of the smart sensor result measurements. This is also the final stage in the communication process of the smart transducer interface communication. The transducer interface handles the measurement measured by the sensor according to the specification of the TEDS and passes it out for a reader to display (IEEE, 2010).

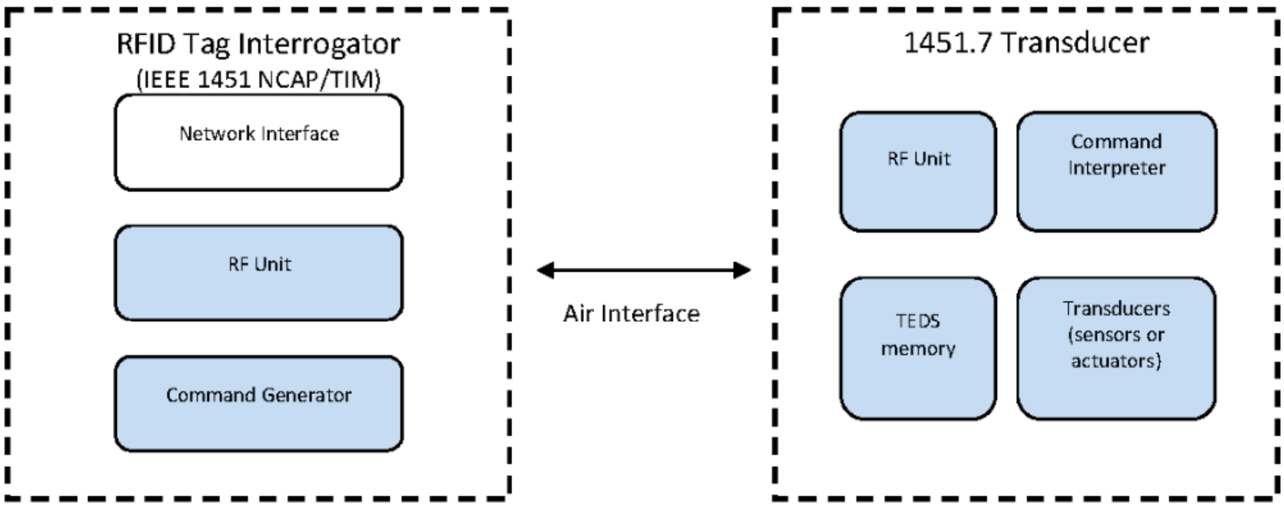



FIGURE 11. A RFID System with Smart transducer interface (IEEE 2010)

## 5.2. IEEE 1451.7 Standards

IEEE is an organisation responsible for creating standards for smart sensors and actuator. IEEE 1451 standards are set of standards for smart sensors networks, this unifies the data acquisition and control systems spanning through numerous transducers (Bela & Halit, 2011). Therefore, IEEE 1451.7 is the standards set for sensors and actuator that are associated with RFID systems. Over the past years, the IEEE organisation has set numerous standards used for sensor communication before arriving at 1451.7 standards (Prasad, 2010).

These IEEE 1451 standards are designed to allow interconnection of variety of sensors and actuator transducer in a network, wireless or wired, with different configuration. This can be configured as point to point, distributed multi drop, or mixed mode (IEEE, 2010). The family of the 1451 standard are as follows and their year of standardization;

1. 1451.0- 2007: Is an IEEE standard for a smart transducer interface for sensors and actuator. With common functions, communication protocol and TEDS formats.
2. 1451.1- 1999: Is an IEEE standard for a smart transducer interface for sensors and actuator. It is also known as Network capable application processor (NCAP) information model.
3. 1451.3- 1997: Is an IEEE standard for a smart transducer interface for sensors and actuator. It as a transducer to microprocessor communication protocols and a TEDS format.

4. 1451.4- 2003: Is an IEEE standard for a smart transducer interface for sensors and actuator. It has digital communication and TEDS format for a distributed multi drop systems.
5. 1451.5- 2004: Is an IEEE standard for a smart transducer interface for sensors and actuator. Comes with a mixed-mode communication protocols and a TEDS formats.
6. 1451.5- 2007: Is an IEEE standard for a smart transducer interface for sensors and actuator. Contains wireless communication protocols and TEDS formats.
7. 1451.7- 2010: Is an IEEE standard for a smart transducer interface for sensors and actuator. Is the present one that contains transducers to RFID systems communication protocols and TEDS formats.

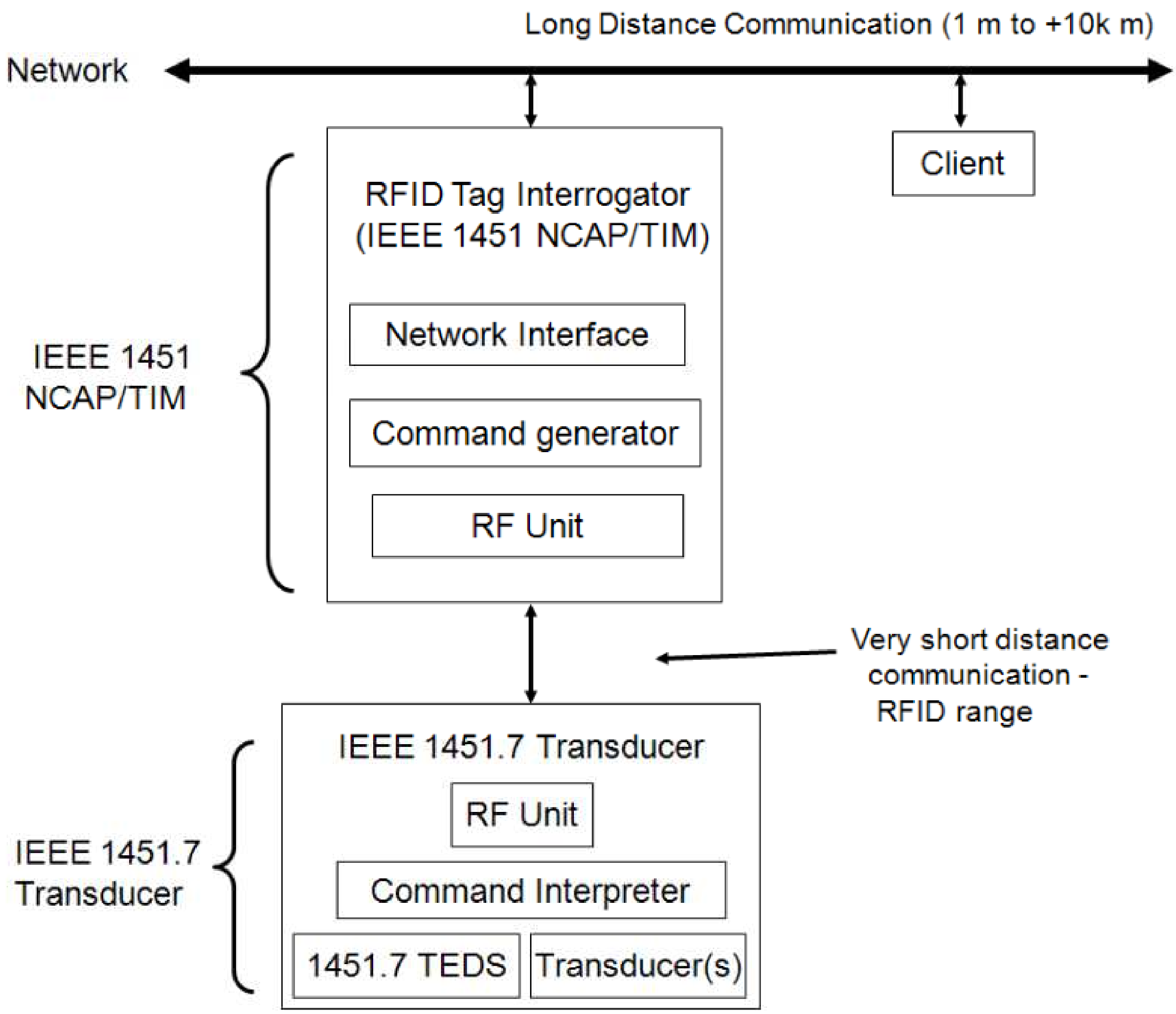



FIGURE 12. separate IEEE 1451.1 (NCAP) and TIM modules with an IEEE 1451.7 transducer in a network (IEEE 2010)

## 6. RFID Chip

In RFID tag, a tag cannot be achieved without the use of a chip. In this thesis, a chip was used. With this chip, a RFID tag can be formed. With a RFID chip, the IOT, which is the idea of this thesis, can be achieved.

### 6.1. UCODE G2iL+ Chip

UCODE G2iL+ is a chip made by NXP semiconductor. This chip has the ability to work with a designed antenna to form an RFID tag. The UCODE G2iL+ is an upgrade product for the UCODE G2iL chip. The G2iL chip series produced by NXP has the capability to be used as RFID tag, but they all have different characteristics (NXP, 2012). Figure 13 shows the chip used to build the RFID tag.


FIGURE 13. The G2iL+ Chip (newsblaze 2012).

#### 6.1.1. Characteristics if G2iL+

The lists below are the characteristics of the chip used in this project.

1. Generation: This chip is an UHF RFID tag of EPC global v1.2.0. This can also be said to a EPC Gen2 tag.
2. Memory: It has a 128 bit of EPC memory. From the memory, 64-bit is the TAG identifier (TID) which 32-bit of it is factory locked with unique serial number.

3. Memory Read protection: It has a 32-bit kill password for permanent disable of the tag and a 32-bit access password.
4. Function: The tag as a default factory setting just to act as an identifier, but different functions such as tamper alarm, digital switch, data transfer mode.
5. Read and Write: The chip as a read and write function which can allow a user to activate different feature into the tag.
6. Power: The chip is a passive semiconductor, so it gains its power from a reader. That means that is uses an external power supply.
7. Data Memory: It as data memory retention for up to 20 years.
8. Read Range: The chip offers a long read and write range due to its low power design. Figure 14 showing the switch circuit created by tamper alarm.

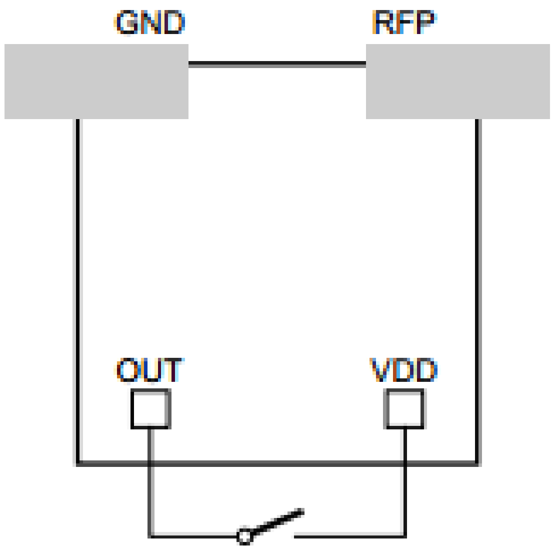



FIGURE 14. An Example of the Chip Function Connection (Tamper alarm) (NXP, 2012)

#### 6.1.2. Operation

1. Operating Frequency: The chip is operating on an international input frequency between 840 MHz and 960 MHz.
2. Input Power: The read function sensitivity of the chip make it to work at a typical -18 dBm of input power.
3. Power supply: The supply voltage and supply current received by the chip from the reader is 1.8v and 7µA respectively. Figure 15 showing how the chip looks from the back.

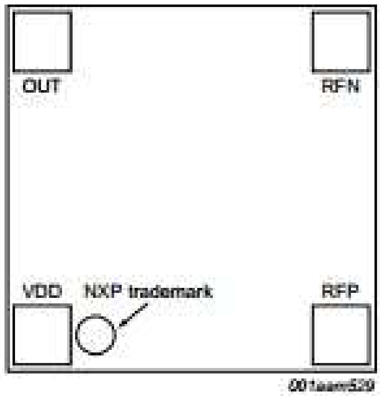



FIGURE 15. Back View of the Chip (Pin bearing) (NXP 2012).

## 6.2. Antenna Design

To achieve a RFID tag, the two main parts needed are the chip and an antenna. I have discussed the chip used earlier in this thesis. To get an antenna for the chip, a PCD board is needed and a suitable design to accommodate the pins of the chip accurately.

In this thesis, the slot antenna design was used. A plain PCB board if used and the dimensions of the chip are cut into the board according to a specific European standard. The chip is then placed between the cut dimensions and soldered according to the pin configuration. Figure 16 and 17 showing the antenna design and picture of the RFID tag used.

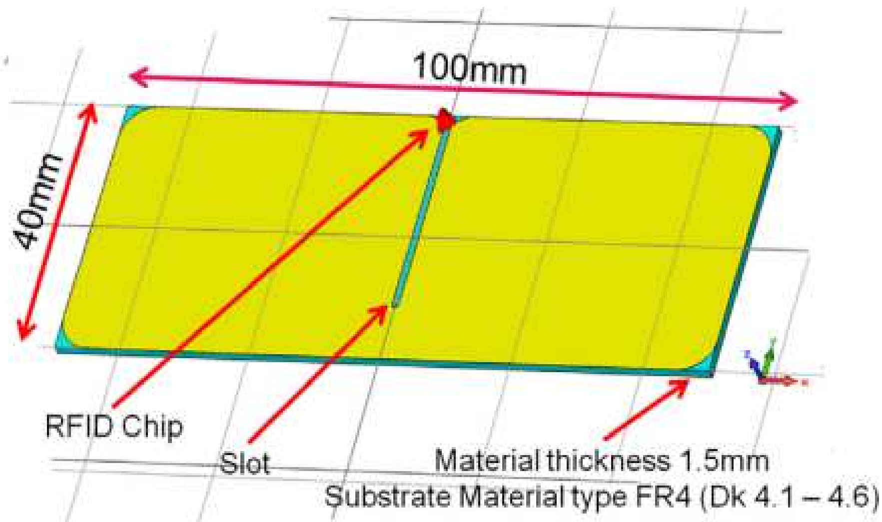



FIGURE 16. Slot PCB board design of an Antenna (NXP, 2010)

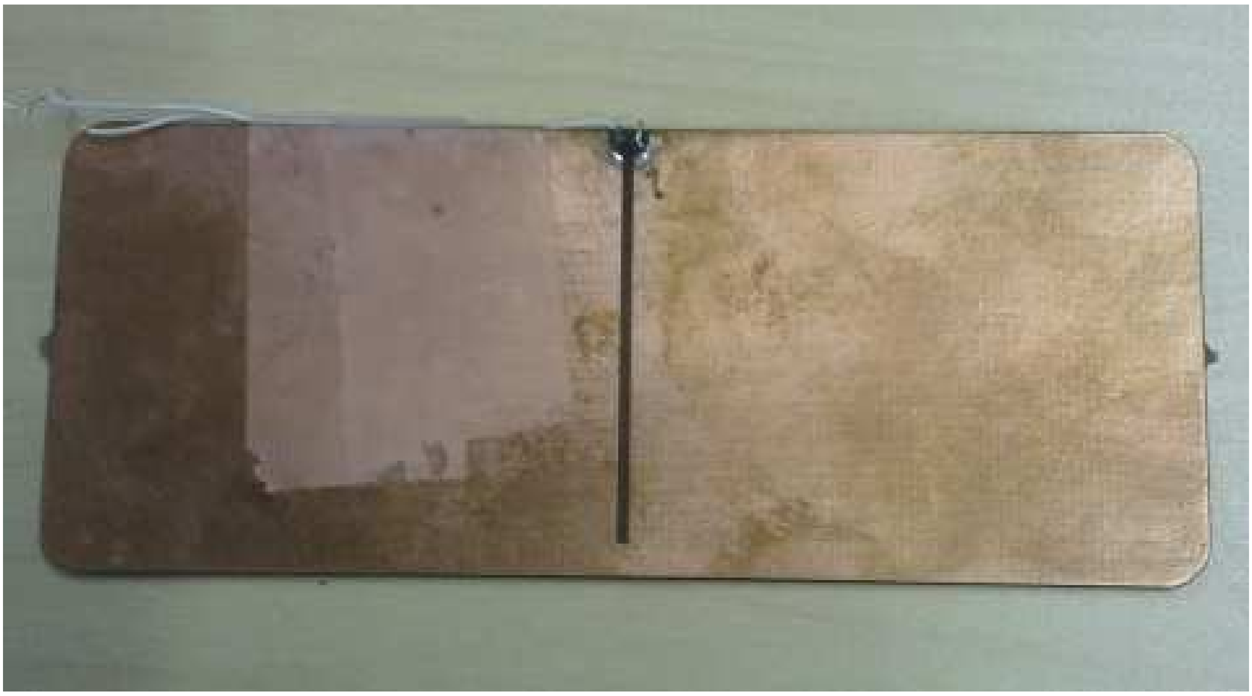


FIGURE 17. Real time RFID tag used.

## 6.3. Testing of RFID tag

After the RFID tag had been built, a Siemens RF660 RFID system was used to test it. Figure 19 shows the interface of the RF660 system and the tag ID of the chip. Figure 18 also shows the picture of the information in the RFID tag.

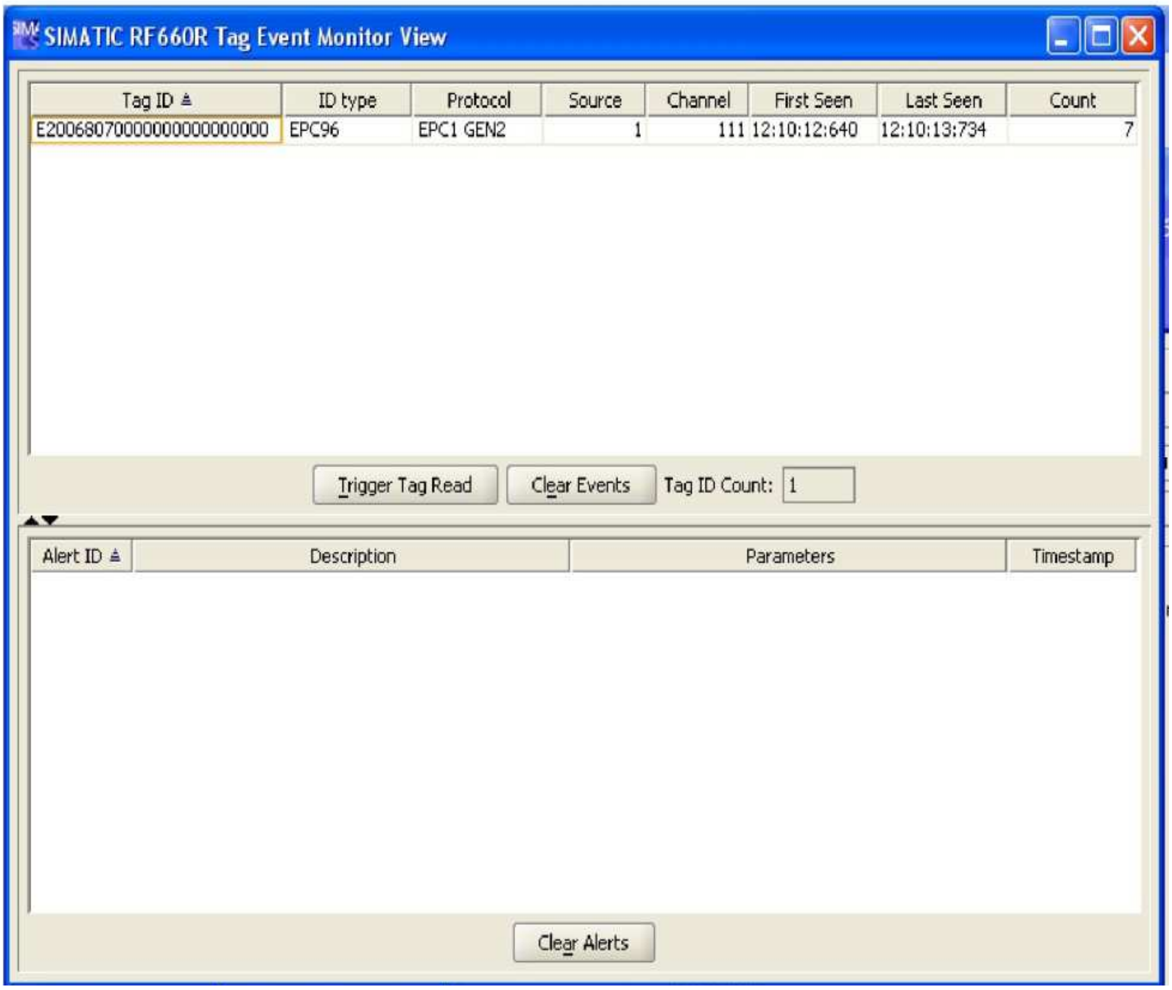



FIGURE 18. RF660 RFID reader

### 6.4. Perimeter of RFID tag ID memory

The RFID tag ID memory is divided into different section. The following are the perimeters of the RFID tag memory:

- Class ID
- Mask designer ID
- Model number

For this tag, the ID is E20068070000000000000000. The perimeter is as follows;

- Class ID: E2h
- Mask Designer ID: 006h
- Model Number: 807h

## 7. Temperature Smart Sensors

### 7.1. Temperature Switch

A temperature switch can also be called a thermo switch. In thermo switches, temperature changes activated the switch. The behavior of the switch depends on the value of temperature which the thermo switch has been configured with. In this final work, an ELFA UP62 thermo switch is used. In previous projects, the use of thermo switch has been without any smart embedded unit. In this project, the implementation of IOT gave the idea of adding an embedded unit to make the use of thermo stat more efficient. Figure 19 shows the temperature switch used.


FIGURE 19. ELFA UP62 thermo switch (www.elfaelektroniikka.fi)

The thermo switch works in such a way that when the configured temperature value of the switch is reached, it caused a break or activates certain part of a machine by supplying a breached voltage.

### 7.2. Operation

The small size of ELFA UP62 gives it a fast reaction to temperature changes. It works with a fixed temperature of 90 ˚C. When this temperature is reached, it performs specific actions according to its implementation in the area of use. Figure 20 shows the dimension of the thermo switch used in this work.

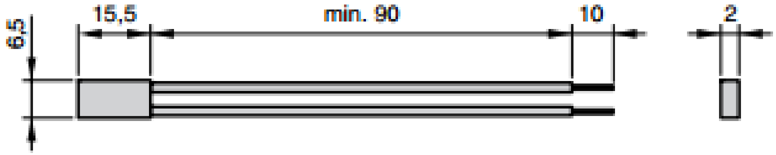



FIGURE 20. Dimension of ELFA UP62 in millimeters. (elfaelektroniikka 2012)

### 7.3. Connection

When the thermo switch is set to be used, the side with nothing printed on it should be used. The unprinted side should be placed on the surface that needs to be monitored. Figure 21 showing how the thermo switch should be used.

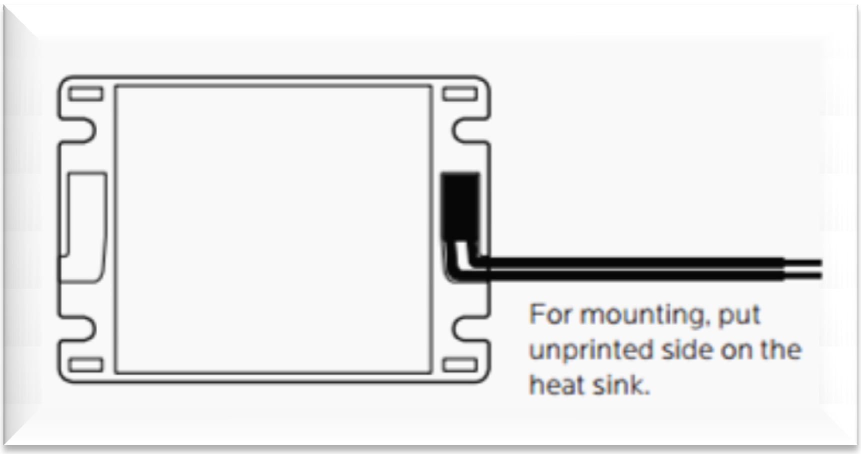



FIGURE 21. Mounting the Switch with its unprinted side (elfaelektroniikka 2012)

## 8. RFID Temperature Smart sensor

The RFID in this sub-topic serves as the embedded part of the system. This thereby makes the system smart. In IOT, the result of a sensor is to be able to read and documented if needed. When a temperature sensor senses its object temperature, it does not have the ability to display it on its own.

The RFID is added to the sensor, so as to receive the information provided by the temperature sensor, computes it and readily allows the measurement to be shown when read. Figure 22 shows an example of a smart temperature sensor.


FIGURE 22. A RFID Temperature Smart Sensor (dhl-innovation 2012)

### 8.1. Construction of the Smart Sensor

Discussed earlier in the thesis are the RFID technology, and the RFID tag that has been built for this project. Also available, are the temperature sensor and the thermo switch to be used in this project. When this two component are connected together, I realized a temperature smart sensor. The RFID is first read with a Siemens RF600 system, and then a tamper alarm function is written into it. The tamper alarm function makes the RFID tag act as a switch.

After the tamper alarm function is been activated on the tag, the thermo switch is then connected to the VDD and the OUT pin of the RFID tag. In the RFID tag, the antenna is connected to the ground pin of the RFID chip. The ground serving antenna gives the whole smart sensor a ground connection. Figure 23 shows the connection of the thermo switch and the RFID tag.

FIGURE 23. The Constructed Smart Sensor.

### 8.2. Operation of the Smart Sensor

The operation of smart sensors are based on its operation frequency, working voltage and the temperature it can measure. The characteristic are as follows;

- Frequency: It’s operating at 915MHz
- Voltage: Its input voltage is 1.85v
- Temperature: Measure temperature of 90 ˚C

# 9. System Testing

## 9.1. Application of RFID Temperature Smart Sensor

The application of this kind of smart sensor is used in industries such as food industry, courier services, and industry machine e.t.c. They are used in temperature sensitive areas of the industry. For example, they are used on parcels to be delivered and should maintain a specific temperature so as not to get destroyed. The smart sensor is placed on the parcel and can be read from time to time as mode of transportation can cause a rise or A drop in temperature.

Also, in food industry, smart tag sensors are added to strategic places along the production line. As know, little increase over a temperature threshold can cause a serious damage in the production process. The addition of this smart sensor can stop the serious damage and increase the production process. Figure 24 showing an example of where a temperature smart sensor can be used.

FIGURE 24. RFID Temperature smart sensor in a vent (Rfid.thingmagic 2012)

## 9.2. Uses of RFID Temperature Smart Sensor

After the conclusion of the project, the ideal testing position is the heating system in a building. Also when the RFID tag is used with a smaller temperature value, it can be used under a temperature sensitive roof. It will be placed just beneath the roof and it can be read easily because of the long range measurement ability of the tag.

## 10. Conclusion

In this work, the idea of how IOT works was explained. I have had a chance to learn and read more about it and work on it during this project. The IOT has made the interaction of things with our real world look simpler than we thought it would be.

The chapters about smart sensor also explain lot about new systems that can be developed using this new technology. Smart sensors are so easy to build and very cost effective. They also consume less power compared to other basic sensors.

The RFID smart sensor has proven to go a long way as it already has been in used in big companies and has really made goods production more efficient and cost savings. In the future, more efficient RFID smart sensor systems can be built and all things can interact with each other. This would lead to less dependency on humans in dealing with things.

**References:**

Ananiahelectronics 2012. http://www.ananiahelectronics.com/RF8315T.htm [Accessed 14th May 2012]

Anomicofficedrone 2012. http://anomicofficedrone.com/2011/11/15/lets-destroy-some-rfid-tags/ [Accessed 14th May 2012]

basaldigitalthermometer 2012. http://www.basaldigitalthermometer.com/images/basal_digital_thermometer.jpg [Accessed 14th May 2012]

Béla G. Lipták, Halit Eren. 2011. Instrument Engineers' Handbook: Process Software and Digital Networks. CRC Press 2012. Volume 3

Bil Glover and Himanshu Bhatt. 2006. RFID Essentials. Mary O'Reilly January 2006

Bit-tech 2012. http://www.bit-tech.net/news/bits/2012/01/13/internet-of-things-government-cash/1 [Accessed 22nd May 2012]

Commission of the European Communities (18.6.2009). Internet of Things — An action plan for Europe. 2009.

Commission of the European Communities (18.6.2009). Internet of Things — An action plan for Europe. 2009.

Dhl-innovation 2012. http://dsi.dhl-innovation.com/en/products/smartsensor/smartsensor_rfid [Accessed 24rd may 2012]

Dietmar Bruckner, Rosemarie Velik, Gerhard Zucker. 2008. Network of Cooperating Smart Sensors for Global-View Generation in Surveillance Applications. 6th IEEE International on Industrial Informatics, INDIN 2008. 13- 16th July 2008.

Elfaelektroniikka 2012. https://www.elfaelektroniikka.fi/elfa3~fi_fi/elfa/init.do?item=37-440-86&toc=0 [Accessed 24rd may 2012]

GAO Tek Inc 2008. http://www.gaotek.com/index.php?main_page=index&cPath=63_96 [Accessed 14th May 2012]

Gerard C. M. Meijer. 2008. Smart Sensor Systems. John Wiley & sons 2008. Volume 10

Gerd Wolfram, Birgit Gampl, Peter Gabriel. 2010. The RFID Roadmap: The Next Steps for Europe. Springer- Verlag Berlin Heidelberg, 2008.

Huang Jingyuan, Han Jiale, Zhang Zheming, Chen Haibin, Wu Jingshen. 2011. Reliability Optimization for Multilayer Active RFID Tags on Rigid and Flexible Substrates. Electronic Packaging Technology and High Density Packaging (ICEPT-HDP), 2011 12th International Conference on, 8th – 11th August 2011.

IEEE standard for A Smart Transducer Interface for Sensors And Actuators- Transducer to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats. 2010. IEEE 2010.

Jon S. Wilson. 2005. Sensor Technology Handbook. Elsevier Inc, 2005.

Klaus Finkenzeller. 2010. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. 3rd edition. John Wiley & sons ltd 2010.

Laurence Tianruo Yang. 2005. Embedded Software and Systems. Second international Conference China, December 2005. Springer- Verlag Berlin Heidelberg 2005.

Luca Catarinucci, Riccardo Colella, Alessandra Esposito, Luciano Tarricone, Marco Zappatore. 2009. A Context-Aware Smart Infrastructure based on RFID Sensor-Tags and its Application to the Health-Care Domain. IEEE Conference on Emerging Technology and Factory Automation, 22- 25th September 2009

Lu Tan, Neng Wang. 2010 3rd International Conference on Advanced Theory and Engineering. 2010

Minco 2012. http://www.minco.com/products/sensors.aspx [Accessed 14th May 2012]

Newsblaze 2012. http://newsblaze.com/story/2010040707000000001.mwir/topstory.html [Accessed 23rd may 2012]

NXP Datasheet, 2012. http://www.nxp.com/documents/data_sheet/SL3S1203_1213.pdf [Accessed 23rd may 2012]

NXP Products Identification References, 2010. http://www.nxp.com/documents/application_note/Application_Note_1715__PCB_reference_antenna_design_v3.pdf [Accessed 23rd may 2012]

Ramjee Prasad. 2010. Future Trends and Challenges for Ict Standardization. Rivers Publishers, 2010.

Rasiah Loganantharaj, Günther Palm, Moonis Ali. 2000. Intelligent Problem Solving: Methodologies and Approaches. 13th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems New Orleans, Louisiana, USA, 19- 22th June 2000.

Sergey Y. Yurish, Maria Teresa S.R Gomes. 2005. Smart sensors and MEMs. Proceedings of the NATO Adavanced Study Institute on Smart Sensors and Mems, Povoa De Varzim, Portugal. 8- 19th September 2005

Stéphane Gervais-Ducouret, 2011. Next Smart sensors Generation Sensors applications Symposium (SAS), 2011 IEEE Conference, 22- 24th February 2011.

V. Daniel Hunt, Albert Puglia, Mike Puglia. 2007. RFID – A Guide to Radio Frequency Identification. Wiley-Interscience, 2007.

Yinghui Huang, Guanyu Li. 2010. Descriptive Models for Internet of Things International Conference on Intelligent Control and Information Processing, China. August 2010.

Youarenowaware 2012. http://www.youarenowaware.com/tag/thermometer/ [Accessed 14th May 2012]

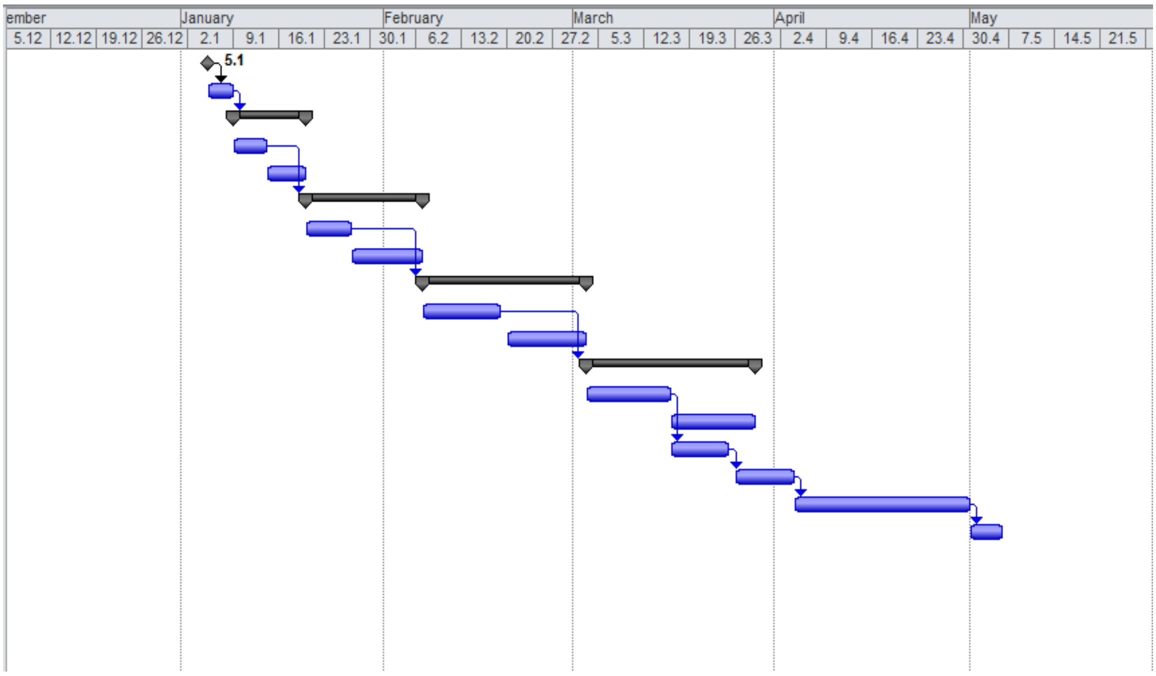
Yu Chen. 2011. Understanding Technology Adoption through System Dynamics Approach: A Case Study of RFID Technology. 2011 Ninth IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.

# Appendix 1

## 1. Thesis Plan

| | | Task Name | Duration | Start | Finish | Predecessors |
|---|---|---|---|---|---|---|
| 1 | | Start | 0 days | Thu 5.1.12 | Thu 5.1.12 | |
| 2 | | Choosing of topic | 3 days | Thu 5.1.12 | Sun 8.1.12 | 1 |
| 3 | | **Project description** | **11 days** | **Mon 9.1.12** | **Thu 19.1.12** | **2** |
| 4 | | Idea gathering | 5 days | Mon 9.1.12 | Fri 13.1.12 | |
| 5 | | Topic filtering | 6 days | Sat 14.1.12 | Thu 19.1.12 | |
| 6 | | **Thesis material compilation** | **14 days** | **Fri 20.1.12** | **Mon 6.2.12** | **4** |
| 7 | | Library search | 7 days | Fri 20.1.12 | Thu 26.1.12 | |
| 8 | | Online search | 7 days | Fri 27.1.12 | Mon 6.2.12 | |
| 9 | | **Search and gathering of mate** | **20 days** | **Tue 7.2.12** | **Fri 2.3.12** | **7** |
| 10 | | Search for chip | 10 days | Tue 7.2.12 | Sat 18.2.12 | |
| 11 | | Temperature switch search | 10 days | Mon 20.2.12 | Fri 2.3.12 | |
| 12 | | **Design of project part** | **20 days** | **Sat 3.3.12** | **Wed 28.3.12** | **10** |
| 13 | | RFID antenna design | 10 days | Sat 3.3.12 | Thu 15.3.12 | |
| 14 | | Finalizing of device | 10 days | Fri 16.3.12 | Wed 28.3.12 | |
| 15 | | Testing of parts | 7 days | Fri 16.3.12 | Sat 24.3.12 | 13 |
| 16 | | Finalizing of work | 7 days | Mon 26.3.12 | Tue 3.4.12 | 15 |
| 17 | | Thesis writing | 20 days | Wed 4.4.12 | Mon 30.4.12 | 16 |
| 18 | | Finalizing thesis | 5 days | Tue 1.5.12 | Sat 5.5.12 | 17 |

## 2. Gantt Chart

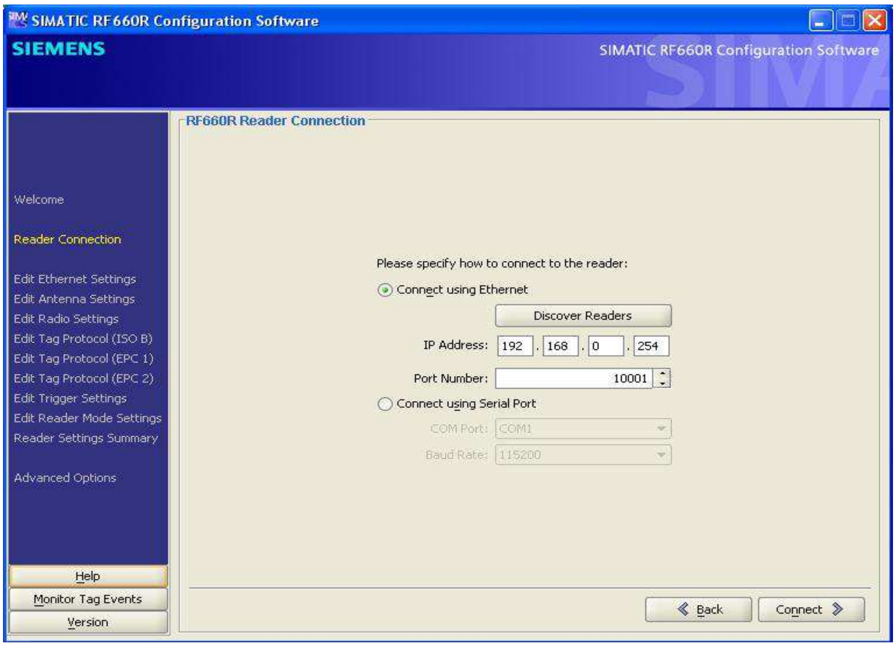


## Appendix 2

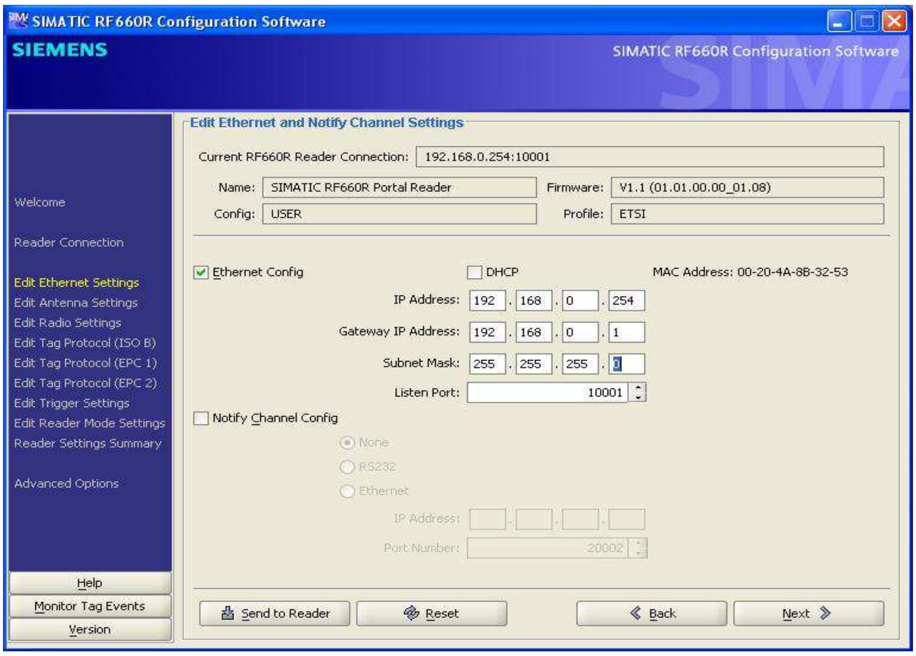
### RFID Monitoring System

How to create a template on Simatic RF 660R for reading of RFID tags.The following is a step by step picture guide for creating the reader template settings;

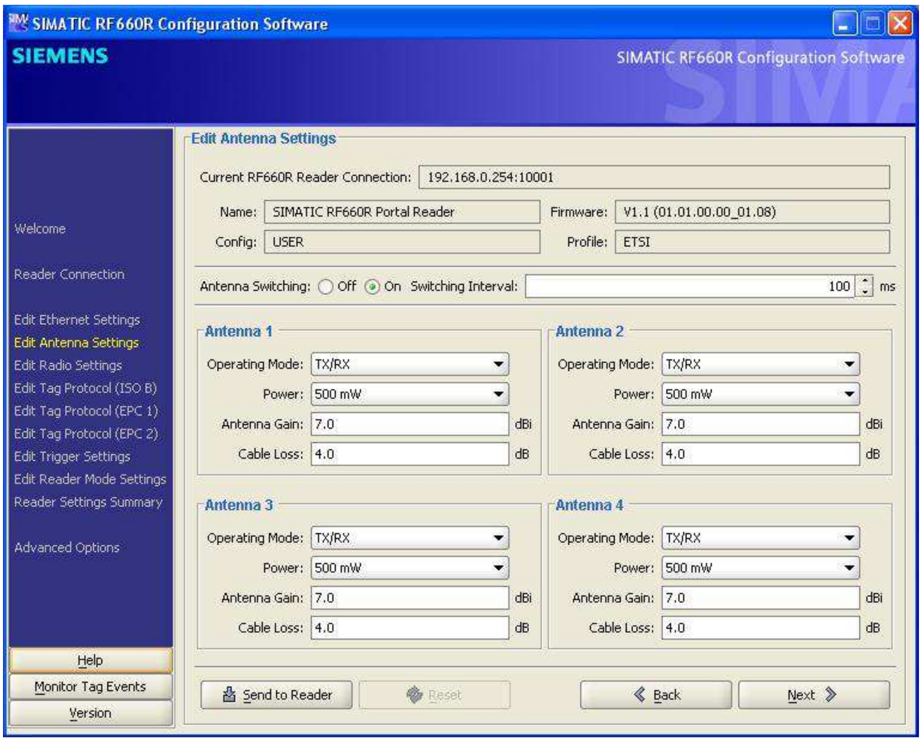
1. Picture showing the reader connection. It could be either Ethernet or Serial port



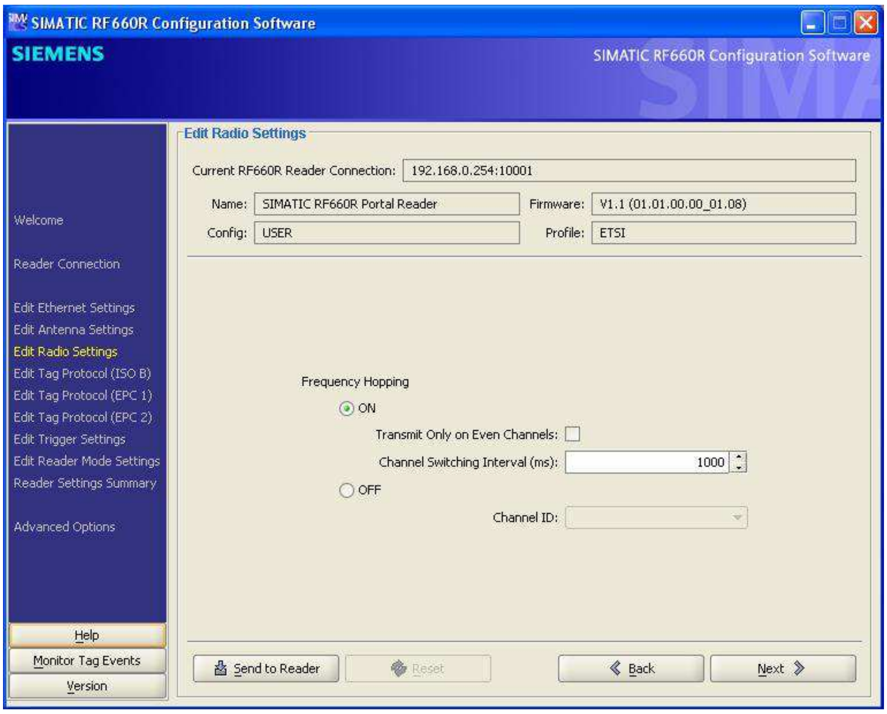

2. Ethernet or Channel configuration which tag events are sent



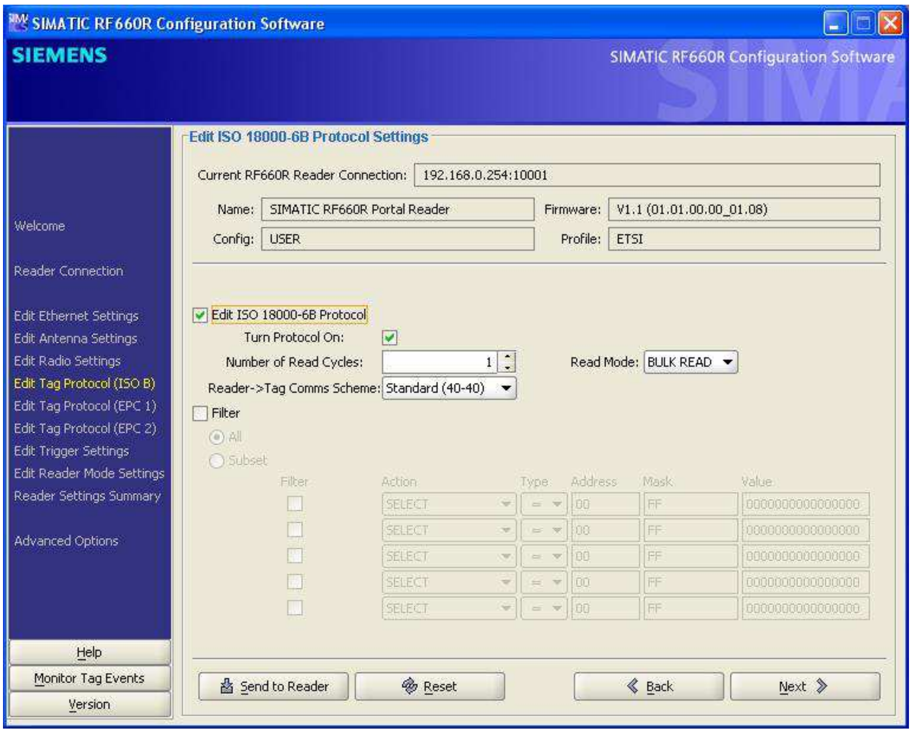
3. This shows the antenna settings of the reader, it has the capacity of up to four antenna



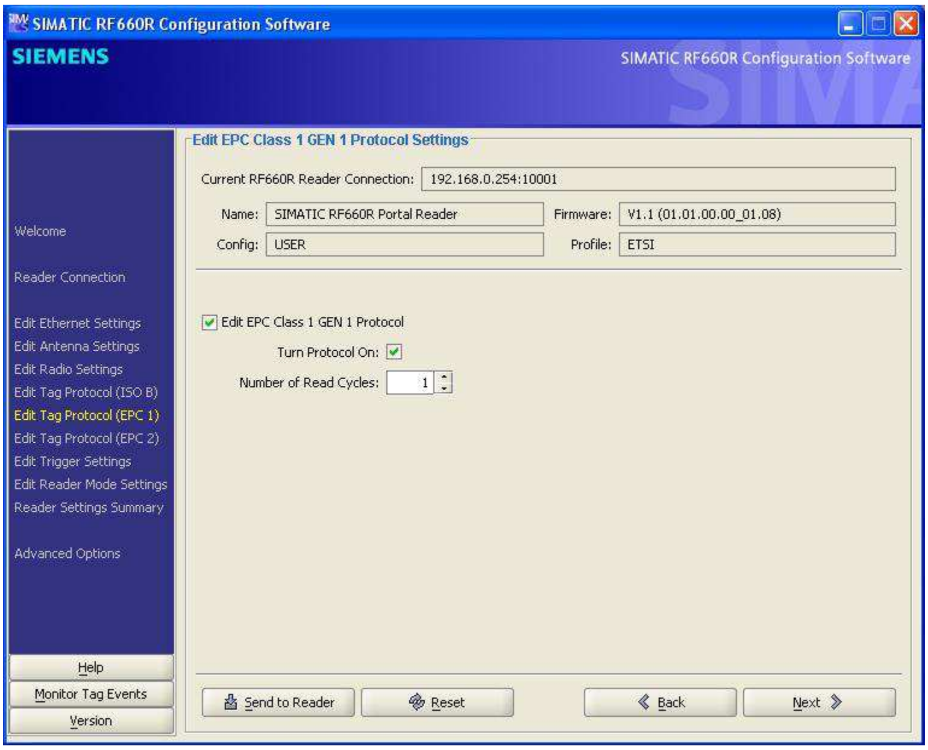

4. This is the frequency setting of the system



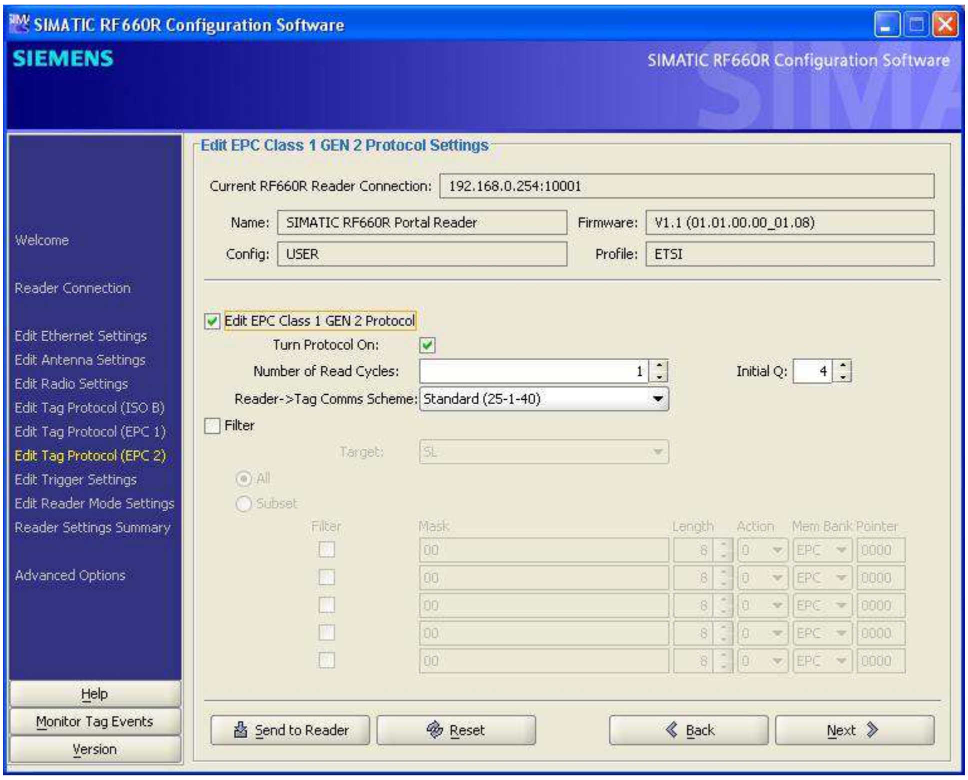
5. Settings allowing ISO 18000B RFID tags



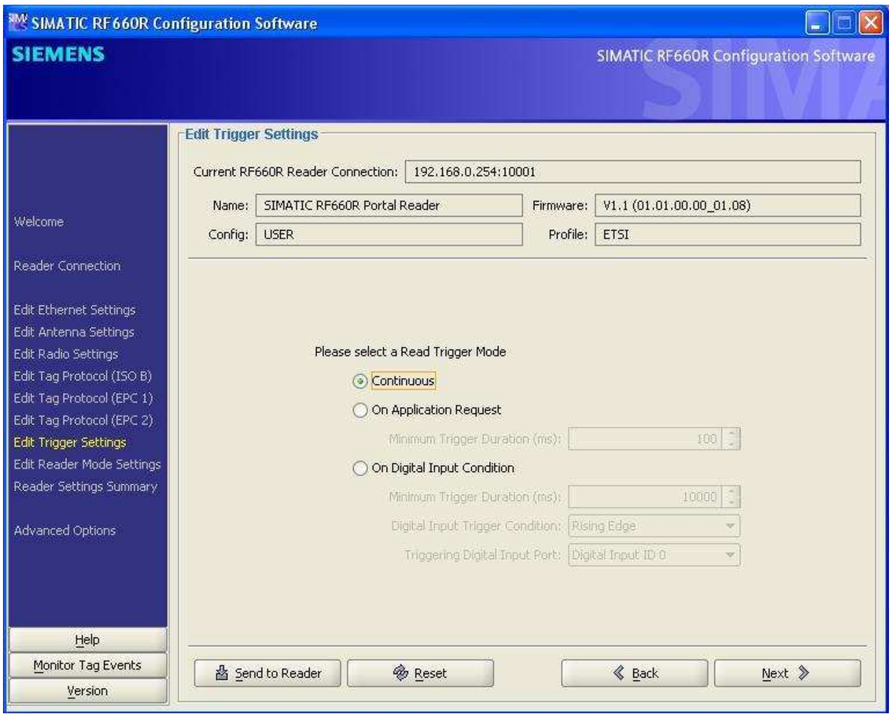

6. Settings allowing the reader to detect EPC class 1 generation 1 RFID tags



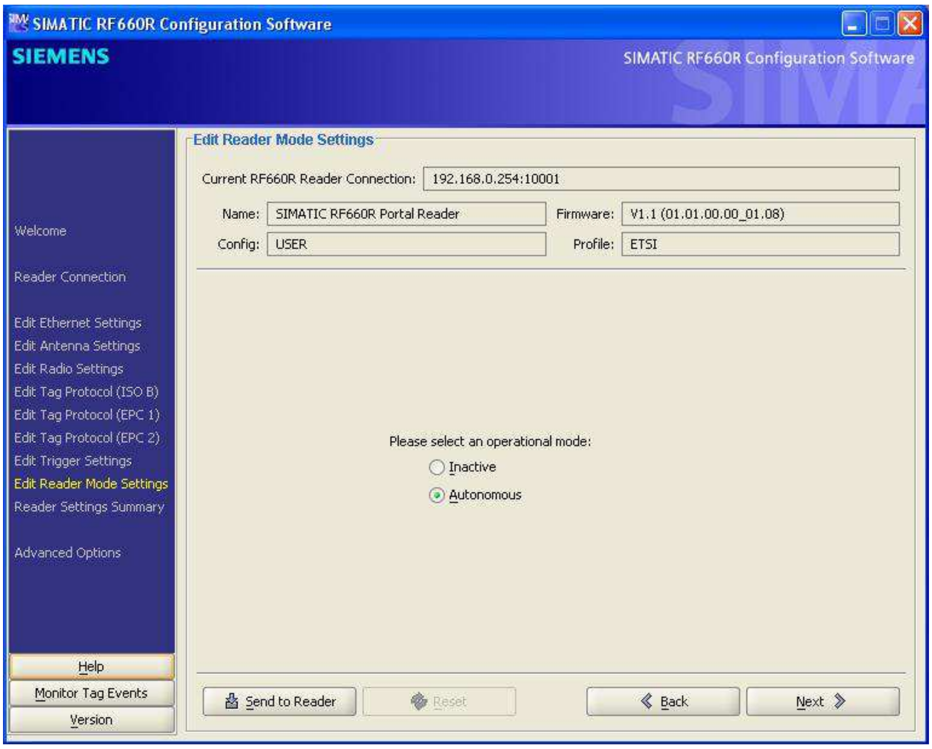
7. Setting allowing the reader to detect EPC  class 1 generation 2 RFID tags



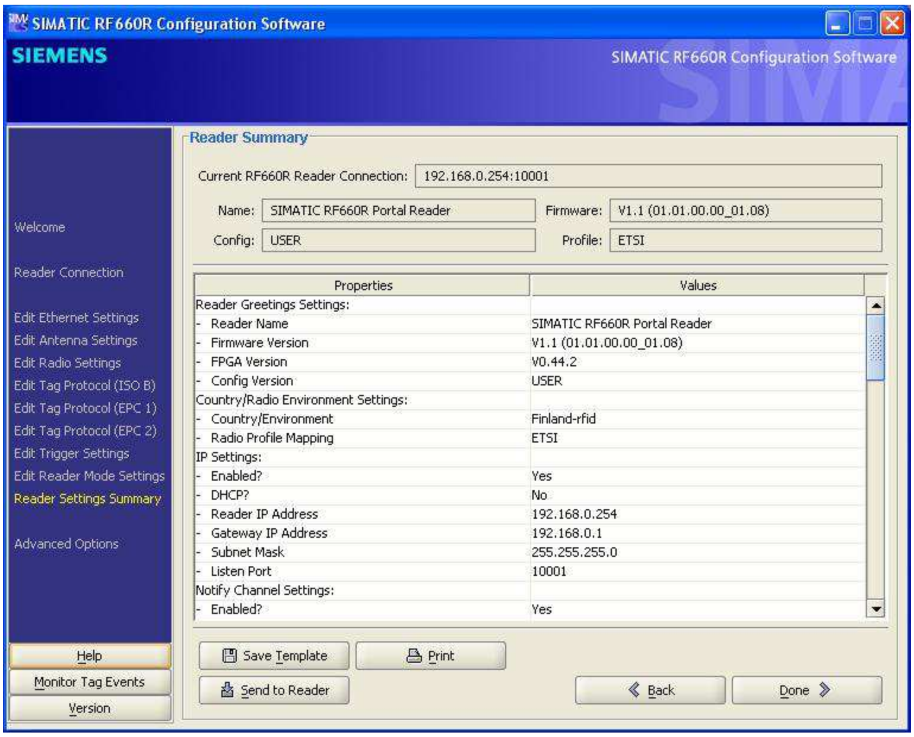

8. The next picture allows continuous trigger settings. Allows the reader to perform continuous RFID tag reading.



9. Configuring the reader mode of system




10. Summary of step-by-step of setting up of the template



11. Testing of the created template with RFID tags