Lappeenranta University of technology
Faculty of technology management
Department of information technology

Bachelor's thesis

Jesse Keränen

Design of RFID-system for industrial after-sale service

Examiner: Professor Kari Smolander

Supervisor: Professor Kari Smolander

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
Teknillistaloudellinen tiedekunta
Tietotekniikan koulutusohjelma

Jesse Keränen

Design of RFID-system for industrial after-sale service

Kandidaatintyö

2011

44 sivua, 11 kuvaa, 6 taulukkoa, 1 liite.

Työn tarkastaja: Professori Kari Smolander

Hakusanat: aidc, huoltopalvelu, RFID, tunnistus
Keywords: after-sale service, aidc, identification, rfid,

RFID-tekniikka on radiotaajuudella toimivaa etätunnistusta, jossa hyödynnetään RFID-tunnisteiksi kutsuttuja tageja, sekä RFID-lukijoita. RFID-tekniikan käyttökohteet ovat erittäin laajat. Tässä kandidaatintyössä tutkitaan RFID-tekniikan hyödyntämismahdollisuuksia teollisuuden huoltopalvelusuhteessa. Työ keskittyy huollettavien laitteiden etätunnistamiseen mobiileja RFID-lukijoita hyödyntäen. Laitteiden tiedot noudetaan olemassa olevasta tietokannasta web-käyttöliittymän kautta. Koska laitteet koostuvat pääosin metallista, joudutaan tunnistetyyppien valintaa pohtimaan tarkasti. Metallipinnat sekä nesteet vaikuttavat erittäin negatiivisesti useiden tunnisteiden lukuetäisyyteen. Työssä keskitytään vaadittavan järjestelmän suunnittelemiseen aikaisempia tutkimuksia hyödyntäen, mutta itse järjestelmän toteutus ei kuulu tähän kandidaatintyöhön. Lopussa järjestelmän alustava suunnitelma esitellään.

ABSTRACT

Lappeenranta University Of Technology
Faculty of Technology Management
Degree Program in Information Technology

Jesse Keränen

Design of RFID-system for industrial after-sale service

Bachelor’s Thesis

2011

44 pages, 11 figures, 6 tables, 1 appendix.

Examiner: Professor Kari Smolander

Keywords: after-sale service, aidc, identification, rfid

RFID-technology is an automatic identification technique using radio waves to exchange data between RFID tags and RFID readers. RFID technology is used in wide area of applications. In this bachelor’s thesis, the utilization possibilities of RFID technology in industrial after-sale service are analyzed. The thesis focuses on identifying serviced machines by using mobile RFID readers. The data associated with the machines is retrieved from current database using web user interface. Comparison between different tag types must be made because the machines consist mostly of metal. The effect of conductive materials such as metal and liquids to the read-range of tags is highly negative. The study focuses on the design of such system using current research but the actual implementation of such system is not part of this study. In the end, preliminary design of the system is presented.

ACKNOWLEDGEMENTS

I wish to express my gratitude to the Lappeenranta University of Technology for the possibility of doing this bachelor’s thesis. I also want to thank Sulzer Pumps Finland for providing me the research subject and guidance during the process.

I would like to thank my instructor and supervisor Prof. Kari Smolander from Lappeenranta University of Technology, and Matti Outinen and Pekka Salmi from Sulzer Pumps who made this research possible.

Finally, I would like to give special thanks to Jarkko Kemppainen from Sulzer Pumps who initially guided me to the path leading to this research.

TABLE OF CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

AIDC	Automatic Identification and Data Capture
AIP	Air Interface Protocol
CEPT	European Conference of Postal and Telecommunications Administrations
DOS	Denial Of Service
EPC	Electronic Product Code
ERO	European Radiocommunications Office
ETSI	European Telecommunications Standards Institute
Gen1	Generation 1
Gen2	Generation 2
HF	High Frequency
IEC	International Electrotechnical Commission
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standards
IT	Information Technology
LF	Low Frequency
MAC	Media Access Code
PDF	Portable Document Format
PHP	PHP: Hypertext Preprocessor
RF	Radio Frequency
RFID	Radio Frequency Identification
ROI	Return of Investment
RS-232	Recommended Standard 232
SQL	Structured Query Language
UHF	Ultra High Frequency
UII	Unique Item Identifier
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WORM	Write Once, Read Many

1 INTRODUCTION

This chapter describes the background and context of the thesis; defines the problem and key objectives; discusses the scope and limitations of the study and outlines the structure of this bachelor’s thesis.

1.1 Background

The use of different kinds of AIDC-methods (Automatic Identification and Data Capture) in industries world-wide has risen considerably over the past decade. Especially different types of barcodes and RFID-technology (Radio Frequency Identification) have stabilized their position not only in faster and more efficient stock and process control but also in maintenance management. Large retailers such as Wal-Mart, Target and Albertsons already began implementing RFID-systems in their warehouses and distribution centers back in 2006, in order to improve inventory accuracy and inventory [1]. In conjunction, global software suppliers such as Oracle, SAP, Microsoft and IBM are accelerating efforts in order to play a higher role in the RFID business. This network effect is driving the use of RFID-technology forward and the more people use it, the more valuable it becomes. That encourages even more people to use it, creating exponential growth. One advantage of RFID-technology when compared with barcodes or other code carriers is the ability to store multiple pieces of information on the small RFID-tag and this information can still be modified or extended [2]. RFID also has the advantage of bulk reading and high resistance to hostile environments including dust, dirt or vibration [3].

This bachelor’s thesis focuses on the utilization of suitable AIDC-methods in Sulzer Pump Finland’s customer targets as a part of after-sale service and on integration with the current identification system. The new system will make use of mobile readers, using either WLAN (Wireless Local Area Network) or cellular network. RFID will be the identification technology of choice in this thesis, but other identification methods (such as barcodes) will be weighed in and considered as well from the usability and economic efficiency viewpoints. The primary aim of using RFID technology is to reduce the transaction cost of operational processes at the interface between the real worlds and the virtual world [4]. Limitations and drawbacks of RFID will be presented also.

Current internal research and documentation from Sulzer Pumps Finland will be used in conjunction with more recent researches and solutions. Both customer and supplier side's needs will be taken into consideration when producing the requirements specification, since the final solution has to please both parties.

1.2 Goals and limitations

The main goal of this thesis is to create a new, mobile identification solution for Sulzer Pumps Finland's after-sale service targets. No present mobile system exists, although the current database holding all the needed device information will be used with the new system. The system should include identification of device or object via mobile reader, fetching the data from the existing database based on serial number and execution of certain commands straight from the mobile reader (such as viewing the maintenance history). No additional information will be stored into to tag, since it leaves an opportunity for clandestine tracking and inventorying [5] and there is no real benefit for replicated information being held in the tag in this project.

The present system consists of serial number attached to the device or object in question and inputting that to a terminal, which connects to the database and outputs the current information on that particular device or object. Since there is no mobility in this current system, information collection tends to be tedious and inconvenient which in turn costs money. The new solution should consist of a mobile reader, connected to the middleware which in turn is connected to the main database via WLAN or cellular connection. RFID middleware processes the streams of tag or sensor data from the readers. [6]. Tag type may vary from location to location, depending on the information required. Passive tags are ideal when only the static information on device or object is needed, and semi-passive tags or active tags are used when real-time information is needed. Because RFID tag acts as a certain type of sensor (identity sensor) it is possible to integrate more sensors into the chip, such as temperature and acceleration sensors [7]. Unique authentication for customers must be implemented and data retrieved from the database must be filtered in such way that only relevant data is presented through the mobile reader to the customer.

The challenges and demands set by the present system must be taken into account and possible development areas are to be outlined. Data retrieval methods and the actual identification method and devices must be weighed against other possible options.

This thesis only covers the design of such system, not the actual implementation. The design will include the definition of demands, basic architecture plan and a suggestive estimate of cost.

1.3 Structure of the study

The first chapter acts as an introduction, giving background information on the thesis and lists goals and the scope of this study. It also reveals the structure of the thesis which is illustrated in table 1. In the second chapter, RFID technology and affiliated concepts are explained. Security issues concerning RFID technology and system in design are discussed in chapter three, along with possible attacks and threats. In chapter four the design of RFID-system is presented. Basic architecture of an RFID system is shown along with the proposed architecture plan for the designed system. The main system components and users are also revealed.

Results of this study and further development areas are discussed in chapter five and finally, a summary of the research is presented in chapter six.

Table 1. Structure of the study.

Chapter #	**Theme**
Chapter 1 Introduction	Research setting Purpose and scope of the study
Chapter 2 RFID Overview	RFID technology and affiliated concepts explained
Chapter 3 Security	Security questions concerning an RFID system
Chapter 4 System Design	The design of an RFID system for target environment
Chapter 5 Discussion and Conclusions	Findings of the study and future development
Chapter 6 Summary	Summary of the findings and conclusions

2 RFID OVERVIEW

RFID is rooted in discoveries made by Faraday during the mid-nineteenth century and discoveries made between 1900 1940 in radio and radar technologies [8]. It is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders [9]. The technology can be used for identification of humans, animals or objects. Unlike many other identification methods used (such as barcodes) RFID-identification does not require straight visual contact between the tag and the remote reader. High-inventory speeds are also a benefit of RFID-system, since multiple tagged items can be scanned at the same time.

In RFID-system, an antenna emits radio waves generating voltage in the inductor of the passive tag or triggering the active tag to send data. The transponder chip starts working with this voltage, uses the inductor as antenna, and sends its ID to the reader antenna in bit-serial form [2]. Tags can also have their own power source which they use for transmitting data or for other functions. Tags relying solely on their own power source are called active tags and tags relying partially on their own power source are called semi-active or semi-passive tags. The typical RFID data capture architecture using fixed reader can be seen in figure 1.

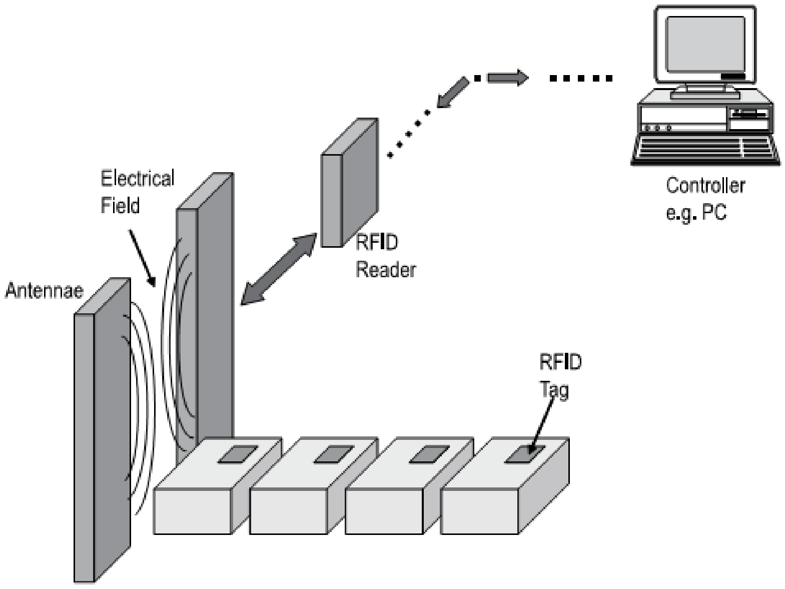

Figure 1. Typical RFID data capture architecture with fixed reader. [2]

2.1 Radio frequencies

Different RFID systems operate at variety of radio frequencies. Each range of frequencies offers its own operating range, power requirements and performance. Different ranges may be subject to different regulations or restrictions that limit what applications they can be used for [10].

Different frequency ranges used with RFID applications can be seen in table 2. The typical maximum read range for specific frequency range can be seen in table 3.

Table 2. RFID frequency ranges. [11]

Name	Frequency range	ISM frequencies
LF	30300 kHz	< 135 kHZ
HF	330 MHz	6,72 MHz, 13,56 MHz, 27,125 MHz, 46,680 MHz
UHF	300 MHz – 3 GHz	433,920 MHz, 869 MHz, 915 MHz
Microwave	> 3 GHz	2,45 GHz, 5,8 GHz, 24,125 GHz

Table 3. RFID read range by frequency. [11]

Frequency	Typical max. read range for passive tags	Some typical applications
LF	50 cm	Pet identification
HF	3 m	Building access control
UHF	9 m	Boxes and pallets
Microwave	> 10 m	Vehicle identification of all sorts

2.1.1 LF (Low Frequency)

Low-frequency systems have proven to be sufficient in certain applications despite their limited read range. Successful implementations exist in manufacturing, assembly, logistics and access control [2]. LF tags are usually not expensive. However, LF tags do not allow bulk reading.

2.1.2 HF (High Frequency)

High-frequency systems allow several transponders to be read at the same time and usually represent a good compromise between cost and benefit. HF tags are not very resistant to adverse mechanical and thermal conditions [2] and are significantly affected by conductive materials [3].

2.1.3 UHF (Ultra High Frequency)

Passive tags using UHF technology reach read ranges up to 9 meters in Gen1 (First Generation) tags, and over 10m in Gen2 (Second Generation) tags. Main downsides with UHF tags are problems with absorption, reflection and refraction [3]. Whereas Gen1 tags did not work reasonably well with metal, Gen2 UHF tags have overcome this issue. The biggest disadvantage for using UHF tags is the relatively high price.

2.2 Tag types

RFID transponders are either active or passive. Passive RFID transponders do not have their own power supply; the tiny electrical current induced in the antenna by the incoming RF (Radio Frequency) signal provides enough power for the transponder to send response [3]. Active RFID transponders, in contrast to that, have their own power source, and may have longer ranges and larger memories than passive transponders, as well as the ability to store additional information sent by the transceiver [9]. There also exists a hybrid form, i.e. semi-active or semi-passive tag. Semi-active tags have their own power supply for the microchip, but communicate using the power of the field of the reader. [3]. Comparison between active, passive and semi-active tags can be seen in table 4.

Table 4. Comparison of Passive, Semi-active and Active tags. [10]

Tag Type	Power Source	Communication	Max. Range	Relative Cost
Passive	Harvesting RF energy	Response only	10 m	Least expensive
Semi-active	Battery	Response only	> 100 m	More expensive
Active	Battery	Respond or initiate	> 100 m	Most expensive

2.2.1 Passive

Passive tags are the cheapest type of tag considering it from the power supply aspect. They do not contain a battery or other power source and therefore they must wait for a signal from a reader [6]. They obtain power from the reader using an electromagnetic property known as the near field. In order to work, the antenna and the tag must be in close proximity to the reader due to lack of internal power source. The near field takes advantage of electromagnetic properties and generates a small, short-lived electrical pulse with the passive tag that can power tag long enough for it to respond [6].

Mostly because they are the cheapest, they also have the highest market value. Their disadvantages are a rather limited read range (better with Gen2 tags) and limited functionality. [3] On the other hand since their economic lifetime is not restricted by the battery life it allows long-lasting service.

2.2.2 Semi-active

Semi-active tags are a hybrid between passive and active tags. They have their own power source, but they do not rely on it solely. The battery provided power can for example be used for extra functionality like sensors, while the actual transmission of data between reader and tag uses the energy harvested from the reader’s signal. By conserving its internal power, the tag’s battery life can be greatly extended.

2.2.3 Active

Active tags have their own power source, usually an internal battery. Since they have their own power source, they can actively transmit and receive on their own, without the near field of the reader's antenna [6]. Active tags can communicate over longer distances and can have more functionality, but have limited lifetime, higher weight and higher price. As in semi-active tags, additional sensors can be attached.

Comparison between active, passive and semi-active tags can be seen in figure 2.

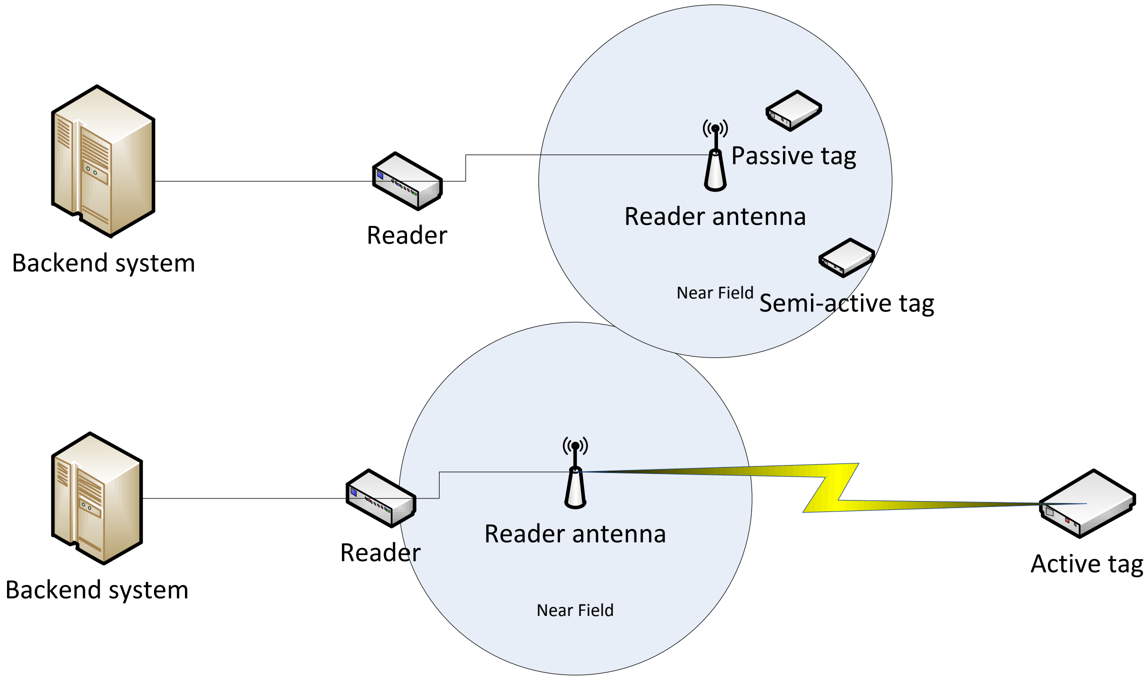

Figure 2. Tag processes.

2.3 Memory

The size of memory of RFID tags can range between single-bit memory up to several kilobytes.. A very common memory size is 96 bit for storing an EPC (Electronic Product Code) [3]. Memory technologies in RFID tags can be broken down to four categories.

2.3.1 Single-bit, read only

The simplest type of tag stores exactly one bit and does not contain a chip [4]. Single-bit tags can only signal their existence; hence they are used mostly in anti-theft systems where the sudden disappearance of a tag can cause an alarm. The tags are removed at the point of sale after transaction.

2.3.2 Read-only with UII (Unique Item Identifier)

The tags with UII are assigned unique multibit serial numbers during manufacturing [4]. The serial number is fixed, and cannot be altered after manufacturing. Usually, a database is used to associate the item number with the tag ID. Because of the flexible association method and low price, they can be reused and are the most economical tags.

2.3.3 WORM (Write Once, Read Many)

Tags with WORM type of memory are not programmed by the manufacturer, but can be written once by the user with proper equipment and read over 100 000 times [4]. Once the data is written into the tag, it cannot be erased. If there is free space available after the data insertion, usually more data can be added later. Usually they are used to store item and serial number.

2.3.4 Read/write

Read/write tags have individually writeable storage areas where data can be written and modified. [4]. User data, handling instructions or process data can be stored in these tags. Read/write tags also allow data encryption in the tag. As opposed to WORM tags, where incorrect data entry usually means discarding the tag, read/write tags rewritten multiple times, thus any errors can be corrected. It is also possible to lock certain areas of the tag’s memory so that it cannot be erased.

2.4 RFID Readers

The second component in basic RFID system is the interrogator or reader. Technically reader units are transceivers (transmitter and receiver) [6]. RFID readers send and receive data to and from tags. They consist of an antenna along with the required electronic for communication, a microprocessor for controlling the device, and an interface for forwarding the data to processing backend system [3]. The antenna can be an integral part of the reader, or it can be a separate device [6]. RFID readers can be broken down to two main categories: stationary readers and mobile readers. Stationary readers have a fixed location and permanent network connection can be presumed [3]. The antenna in stationary reader is usually separate from the reader, while mobile readers are a combination or reader and antenna [6]. Mobile readers, in contrast, can be moved around and they can work without network connection as long as the data is uploaded to backend system at some point (via docking station or when network connection can be established). Readers usually contain a system interface, such as an RS-232 (Recommended Standard 232) serial port or Ethernet jack; cryptographic encoding and decoding circuitry; a power supply or battery; and communications control circuits [6].

2.5 Middleware

All the data read from tags need to be processed and while some readers possess the capability for doing this, usually another component is brought into the system: the middleware. Middleware acts between the backend system and readers, aggregating and filtering data and providing an open and neutral interface towards the applications [3]. Using middleware, applications can easily cope with older tag and reader technology. The backend can be a standard commercial database accessed by using SQL (Structured Query Language), such as MySQL, Oracle, PostgresSQL or similar product [6].

2.6 Complete system

RFID-system usually consists of tag(s), reader(s), middleware and backend-system. The system can be modified to some extent, such as reader and middleware being in the same physical device, or backend system not being even present. In essence, the term “RFID-system” represents all the hardware and software related to the system.

A minimal system needs a single tag, reader and a computer or similar smart device with appropriate software. This kind of system is only the bare minimum and is usually not practical, since any new piece of information must be written to the tag directly. Depending on the application, security issues may arise, since all the relevant information is stored into the tag itself.

More practical solution is to implement a backend-system consisting of Web-server and database. A fictional RFID-system can be seen in figure 4. The RFID reader communicates with the backend-system via Wi-Fi interface. The access to database can be for example via internet-browser. A simple way is to implement the interface with PHP (PHP: Hypertext Preprocessor) which handles the information stored in the database. The system can be done without browser access and PHP (or similar programming language) but in this thesis it is the most practical one, since same data must be accessed from different locations, outside local network.

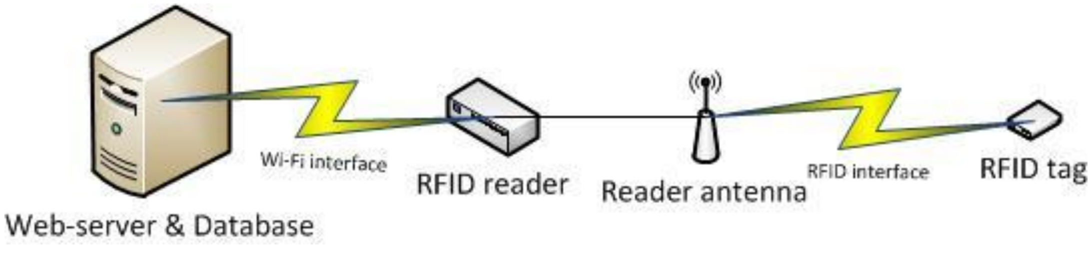

Figure 4. A sample RFID-system.

2.7 Standardization

Regulatory standards are useful to all types of business organizations and for governments. Standards generally can ensure the minimum level of product characteristics such as quality, interoperability, reliability and safety for the user community. Standards are developed and issued by standard organizations and international standards are available for use worldwide.

The RFID system includes many standards and does not yet have a single universally accepted standard. Most of the existing and proposed standards deal with the air interface protocol (such as ISO 18000 series and EPC), data content, conformance and applications. Standardization also ensures interoperability between devices of different vendors [3].

There is a variety of groups defining those standards and regulating the use of RFID technology. Most well-known are ISO (International Organization for Standardization), IEC (International Electrotechnical Commission) and EPCglobal. The main bodies governing frequency allocation in Europe are ERO (European Radiocommunications Office), CEPT (European Conference of Postal and Telecommunications Administrations), ETSI (European Telecommunications Standards Institute) and national administrations.

Standardization of tags is not very important to system operation because flexible software can easily deal with different kinds of tags. However, with standardized equipment no additional software is required for dealing with different kinds of tags and overall architectural simplicity with standardized products leads to lower costs.

3 SECURITY

Attention must be given to data protection and security in RFID applications. Generally, consumer protection should also be considered, but in this project the labeled objects remain stationary inside the tag owner's premises. Systems should always be designed with security in mind, i.e. security should not be an afterthought but an important design goal [3]. There are five common security goals in security and privacy respecting RFID systems, which can be seen in figure 3: maintaining data security, preventing counterfeiting, preventing illegitimate access, preventing unwanted recognition and tracking, and coping with denial of service [3].

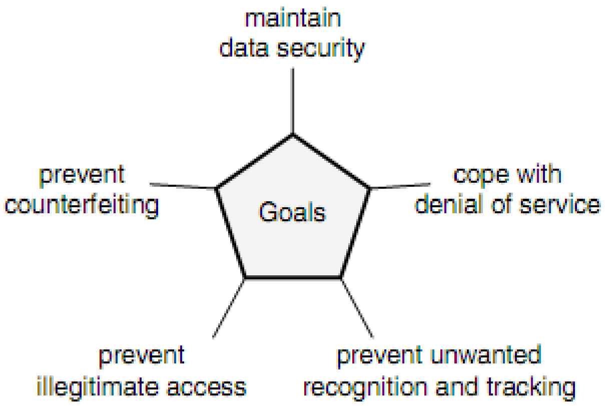

Figure 3. Goals for security and privacy respecting RFID systems [3].

Maintaining data security: "Illegitimate reading of data must be prevented in RFID systems because the data must be treated confidentially since it may be privacy sensitive" [3].

Maintaining data security can be achieved by storing data within the backend infrastructure rather than on the tag directly whenever possible. Using tags as identification purposes only and retrieving the associated information from the backend infrastructure gives more flexibility since the resource constraints are not as tight as in the tags. This enables the use of more secure and proven standard security protocols [3]. The only data left on the tag is the UII or serial number which is useless without the associated data.

Prevent counterfeiting: An identifier (such as barcode and simple RFID tag emitting its signal) can be cloned relatively easily. For RFID systems this may cause damage in some scenarios where counterfeit products are masked as genuine or where an RFID keycard is cloned, giving the cloned card the same privileges as the real one. In this project the possible threat of counterfeiting is minimal but could arise as replacing another tag with a different cloned tag, giving the reader and user false information. Since the factories are well guarded and only guided tours are allowed, switching securely mounted tags is hardly a threat.

Prevent illegitimate access: Preventing illegitimate access is closely related to maintaining data security. Access to stored data should be controlled to ensure data integrity and privacy. This can be achieved by securing the communication between middleware and backend system, and requiring authentication before giving access to the stored data. Restricting modifications to stored data by end-users help to maintain the data integrity.

Prevent unwanted recognition and tracking: Recognition and tracking of objects are core functionalities of RFID systems. However, when human beings get involved, this functionality usually becomes an unwanted one for privacy reasons. In this project the tags stay stationary and mounted on the objects, so this is not an issue.

Cope with DOS (Denial of Service): This goal focuses on the availability of the RFID system. In ideal case the system should keep running even when attackers try to bring the service down. However, as it is not possible to prevent all kinds of DOS attacks, the system should at least provide means to cope with them [3].

Before analyzing possible attacks, potential targets must be recognized [6]. Target can be the system as a whole, or just a section of it. In general aspect, damage can be caused even if the underlying database is not affected by manipulating tag data or duplicating the tag. Objectives of an attack scenario help to determine the type of attack. Attacker could, as an example, place misinformation into a competitor's database so it's rendered useless.

One of the simplest ways to attack an RFID system is to prevent the tag on an object from being detected and read by a reader. Since many metals can block RF signals, all that is needed to defeat a given RFID system is to wrap the item in aluminum foil. This can be used as a protection measure to guard an electronic passport, or to trick security gates from detecting a product with RFID tag. Attacks over the air-interface on tags and readers typically fall into one of five types of attacks: eavesdropping, spoofing, insert, replay and DOS. There are a multitude of attack types concerning encrypted systems and physical mischief, but since the tags used in this system are physically guarded by fences, walls and factory personnel and the tags themselves store no vital information from security or privacy perspective, the associated attack types are left out. General classification of different attacks on RFID systems can be seen in figure 5.

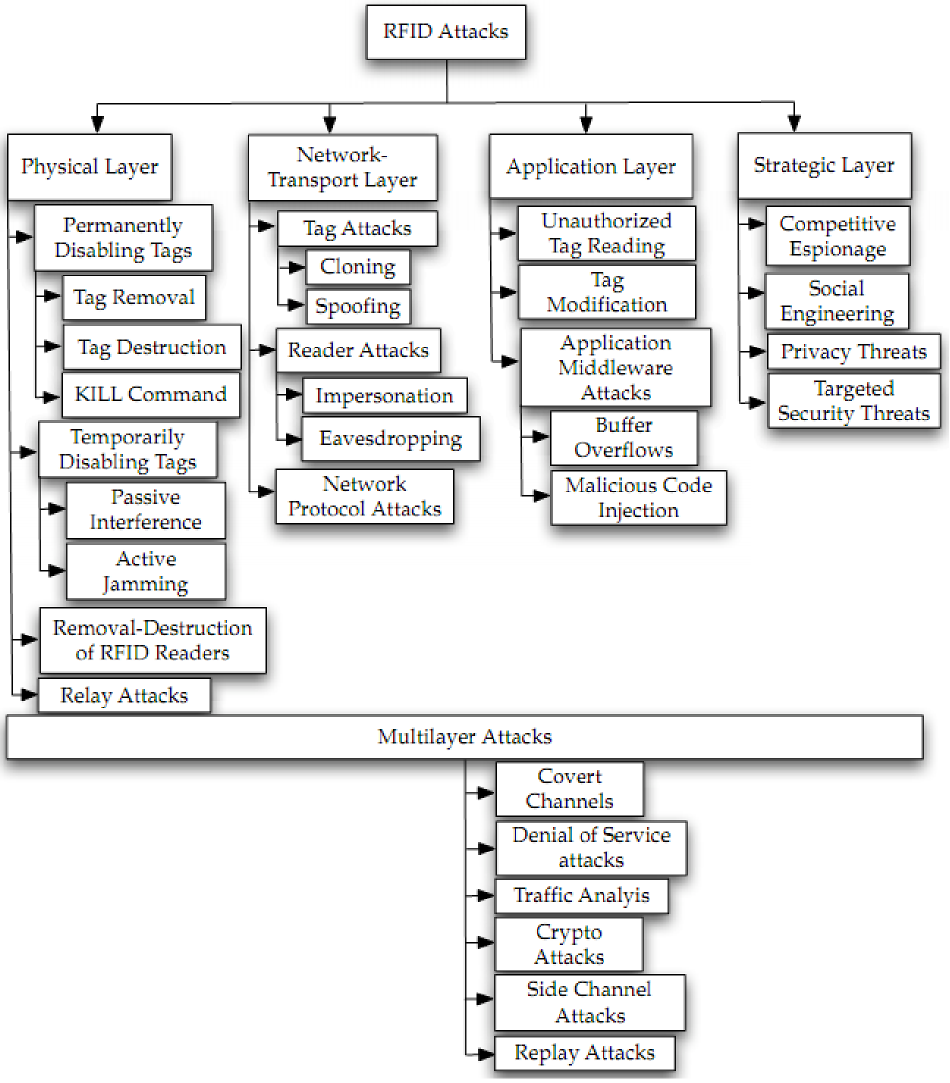

Figure 5. Classification of RFID attacks [12].

As previously mentioned, the attacks on physical layer can be left out, as long as their existence is still acknowledged. Attacks on physical layer require great effort and create minimal damage on the system in design. The strategic layer includes attacks that target the organization and business applications in order to help competitors gain valuable information. Since the tags remain stationary and contain only the serial number or UII, no tracking of goods can take place and even if competitors could acquire the data stored in the tags, they would only acquire the serial number or UII.

3.1 Eavesdropping & Replay

The wireless nature of RFID makes eavesdropping one of the most serious and widely deployed threats. The unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers. Eavesdropping can be performed both ways: reader-to-tag and tag-to-reader. The recorded information may be used later as part of more sophisticated attacks.

Replay attack is closely related to eavesdropping, but the distance has to be much shorter. A valid RFID signal is intercepted and its data is recorded; this data is later transmitted to a reader where it is “played back”. Because the data appears valid, the system accepts it. This kind of attack can be used against smart cards, since they usually transmit the signal when they get close to the reader. The perpetrator could for example use the attack for copying the message on remote car key in order to unlock the doors or turn the ignition on. However, this can usually be circumvented by using security tokens or other authentication methods between the card and the reader. The most relevant attacks on network transport layer and application layer are presented.

3.2 Spoofing & Cloning

Spoofing attacks supply false information that looks legitimate so the system accepts it. Typical spoofing attacks may involve a fake domain name, IP address or MAC (Media Access Code). An example of spoofing is an RFID system broadcasting an incorrect EPC number over the air when a valid number was expected [6].

An alternative to spoofing is cloning, where the entire tag is cloned by copying an unprotected tags ID and any associated data to the clone-tag. Once fully cloned, the tag will seem legitimate to the system.

3.3 Insert

Insert or malicious code injection attacks insert system commands where data is normally expected. These attacks work because it is assumed that the data is always entered in a particular area, and little to no validation takes place. Insert attacks are common on Web sites, where malicious code is injected into a Web-based application. A typical use for this type of attack is to inject an SQL command into a database. This same principle can be applied in an RFID situation, by having a tag carry a system command instead of valid data in its storage area.

3.4 Denial of Service

DOS attacks, also known as flood attacks, take place when a signal is flooded with more data than it can handle. They are well known because several large DOS attacks have impacted major corporations such as Microsoft and Yahoo [6]. The DOS attacks aim at interrupting the communication between an RFID reader and an RFID transponder. A variation on this is RF jamming, which is well known in the radio world, and occurs when the RF is filled with a noisy signal [6]. In either case, the result is the same; the system is denied the ability to correctly deal with the incoming data. Either variation can be used to defeat RFID systems.

4 SYSTEM DESIGN

Requirements analysis forms the basis for the following stages and is thus critical for the success of the project. It essentially consists of process analysis, environment analysis, object analysis and IT infrastructure analysis [4.] These aspects should be evaluated together, as they represent different views of the same situation. Ideally, requirements analysis should be preceded by an analysis of the current situation and its weaknesses. In most cases, there are prior solutions for RFID systems, so it is generally necessary to answer questions regarding integration into existing systems and transition from one system to another [4]. Stage model for RFID implementation is shown in figure 6.

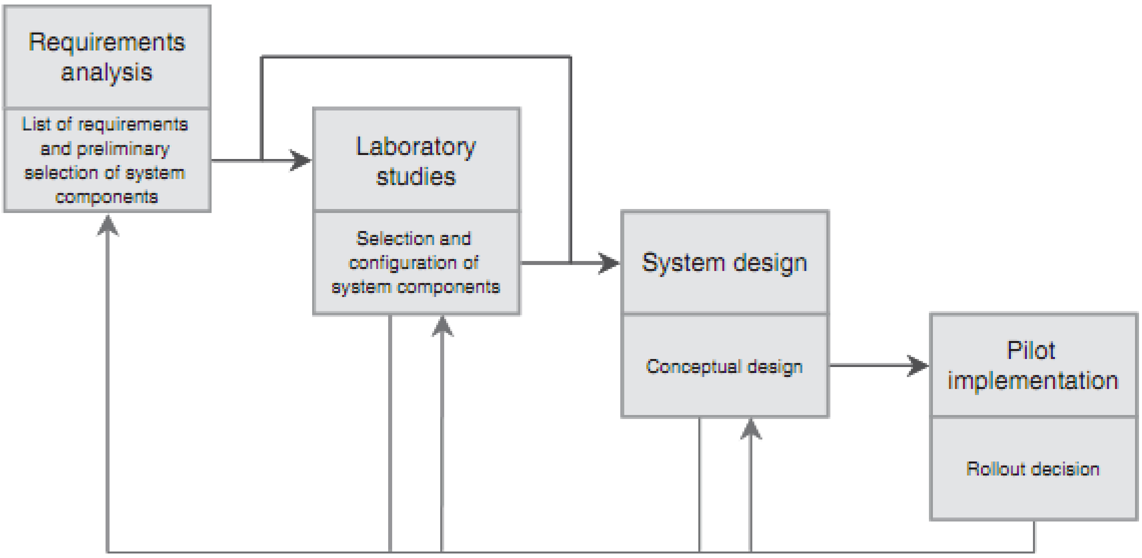
Requirements analysis
List of requirements and preliminary selection of system components
Laboratory studies
Selection and configuration of system components
System design
Conceptual design
Pilot implementation
Rollout decision

Figure 6. Stage model for RFID implementation [4].

4.1 System overview

This thesis is done in collaboration with Sulzer Pumps Finland Oy. The focus on this thesis was to find a suitable method for identifying machinery in customer targets, as part of after-sale service. During the initial phase of requirement outlining, RFID-technology was the identification technology of choice. Other identification methods, such as barcodes, magnetic stripes or optical recognition were unpractical for the task, mostly due to the extreme and harsh conditions of the identification environment.

In essence, the task was to design an RFID-system for identifying individual machines in different customer target locations. The system should be efficient and faster than the current method which is manual identification by the serial number attached to the machine. The serial number plates are also subject to the harsh environment and due to dust, dirt and temperature changes degrade in time, becoming less and less readable. The serial plates are kept in place, since there is no serial number written on the outside of RFID tag.

Since the factories and customer target locations have a lot of conductive materials around, it limits the choice of possible RFID tags. HF tags and Gen1 UHF tags work around conductive materials but read-ranges drop dramatically when brought closer to the material and eventually drop to zero. This is because the electrical coupling between the tag's antenna and the material causes an impedance change that reduces the power coupled into the tag. It is possible to add dielectric materials to the antenna to alleviate a trade-off between free-space and direct attach performance [13]. Gen2 UHF tags on the other hand work with conductive materials around and possess the ability to work both near- and far-field [14]. What further limits the choice of tags is the fact that the machines themselves consist mostly of metal, meaning that the mounting surface will be conductive. This affects the communication between tag and reader severely. When metal is close to tag antenna, it reader's magnetic field causes an eddy current and cancels the magnetic field necessary for communication [15]. However, when ferroelectric material is placed between the tag and the metal surface it cancels the effect. The effects of this can be seen in figure 7.

The main purpose for designing an RFID-system is to decrease the time it takes to retrieve device information without AIDC methods. It also makes a firm base for future development and possibilities of an RFID system go beyond object detection and identification. RFID system gives also a competitive edge, since due to the novelty of RFID technology and lack of metal-compliant tags it hasn't been taken into use widely in this particular field of industry.

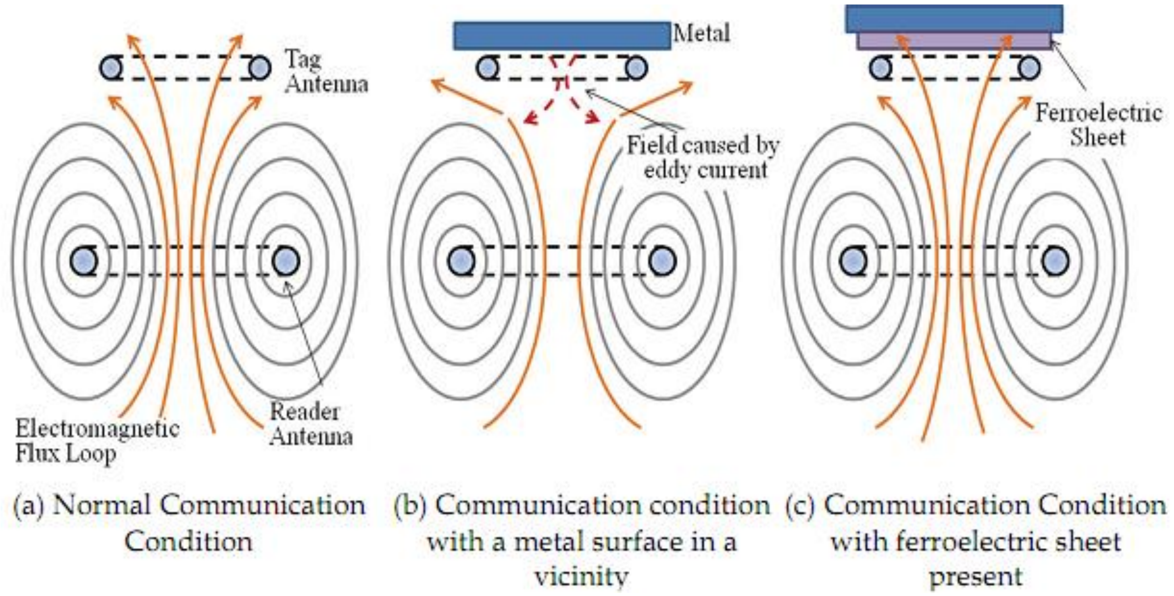
Tag Antenna
Metal
Field caused by eddy current
Ferroelectric Sheet
Electromagnetic Flux Loop
Reader Antenna
(a) Normal Communication Condition
(b) Communication condition with a metal surface in a vicinity
(c) Communication Condition with ferroelectric sheet present

Figure 7. Basic principle of metal tag [15].

4.2 Architecture

The basic architecture of the design in process is shown in figure 8. The RFID tag placed on the machine is identified by mobile RFID-reader. The reader is connected to the user's laptop, which is acting as middleware. The laptop connects to the Web-server which shows the machine's information to the user. A database with all the machines' information already exists, but the request form has to be made.

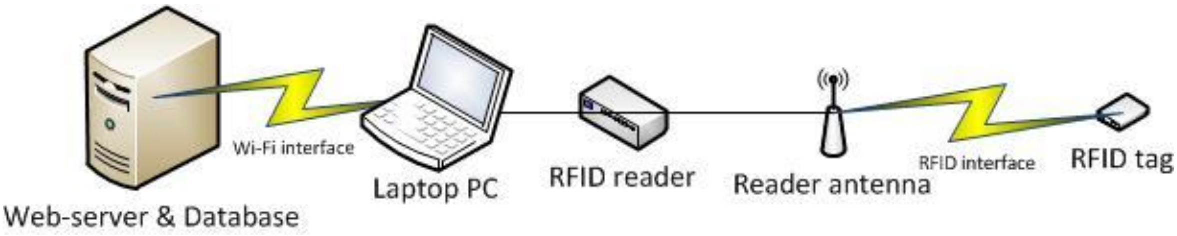

Figure 8. Basic architecture.

When the serial number is read from the RFID tag, the reader sends it to a form open in laptop's browser. The browser requests a new document from the Web-server, showing the machine's part list. A user authentication is done, and the Web-server shows a document containing the machine's information or an error message. The data retrieval phases can be seen in figure 9. The system has a Web user interface and therefore no additional programs are needed for data retrieval; a simple modern browser will be sufficient. Since tagged elements remain stationary and additional elements after initial setup are added seldom, adding and editing data in the database is left out from the RFID system. This also helps keeping the system secure from several attacks.

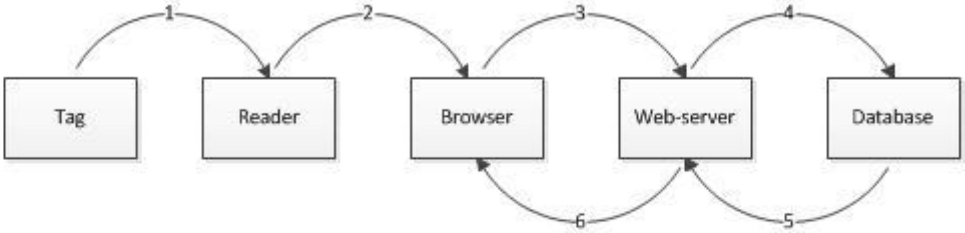

Figure 9. Data retrieval phases.

1. Tag is recognized and data stored in it is retrieved by the RFID reader.
2. The reader sends the data (serial number) to the laptop's browser.
3. The browser sends a request to the Web-server.
4. The Web-server runs a PHP-script and sends a request for the database.
5. The Database sends the correct PDF-document (Portable Document Format) to the Web-server.
6. The Web-server returns the document to the browser.

4.3 Security & Privacy

RFID technology raises two main concerns for users: clandestine tracking and inventorying. Since RFID tags respond to reader interrogation without alerting their owners or bearers, clandestine scanning of tags becomes a plausible threat. Even tags that use cryptographic algorithms usually still emit unique identifiers [16]. Since tags carry only serial numbers and are not connected to a single user in any way user privacy is not an issue.

Even when the nominal reading range of an RFID tag would be low, rogue scanners with their own powerful antennas or antenna arrays can exceed the nominal reading range. Rogue reader can be even configured to out limit legal power limits. This means that in theory it would be possible in some scenarios to eavesdrop on reader-tag communication outside the industrial plant. An attacker could also walk along a guided tour scanning everything within read-range. In either case, the eavesdropper would only acquire a serial number attached to certain machine, without any additional information. Physical attacks to tags or mobile readers are unlikely; since no visitors are allowed to enter the plant without a guide (access to premises is usually controlled as well).

4.4 System components

Since the tags have to be attached machines consisting mostly of metal, it severely limits the range of options for different tag types. The read-range of a tag attached to the machine should be at least approximately one meter. So far only Gen2 UHF tags possess these characteristics and are the choice of tag type in this project. The main downside of Gen2 UHF tags that are compatible with metal surfaces compared to generic label- or inlay-tag is the cost. Tags for metal surfaces can cost over ten times than normal inlay-tags, although this depends on the exact tag type. On-metal tags are usually capsulated in protective cover and can thus survive extreme environments. They can usually be attached to the tracked object by screws, welding or by adhesive applicants. Since passive Gen2 UHF tags possess superior qualities over the other types of tags for this particular application they are the suggested choice for this project.

Maintenance personnel are assigned a reader and laptop for maintenance and identification work. Each person or team are given one reader and one laptop but there may be multiple persons or teams with multiple readers at the same area. Another solution was considered, where only readers would be handed over to maintenance personnel and the laptops would be replaced with one or several central computers acting as middleware. This would become cheaper, but the screen size on handheld readers is impractical for viewing large lists and schematics. Maintenance personnel also have to make reports on their work orders and these can now be done on-site.

The mobile RFID-reader is connected to the laptop, which acts as a middleware, by USB-(Universal Serial Bus) or RS-232-connection or even wirelessly, depending on the reader capabilities. The laptop connects either to the local network via WLAN-connection or uses mobile connection to reach a cellular tower in order to connect to the internet in order to retrieve the information from the backend-system. The architecture of this system is illustrated in figure 10.

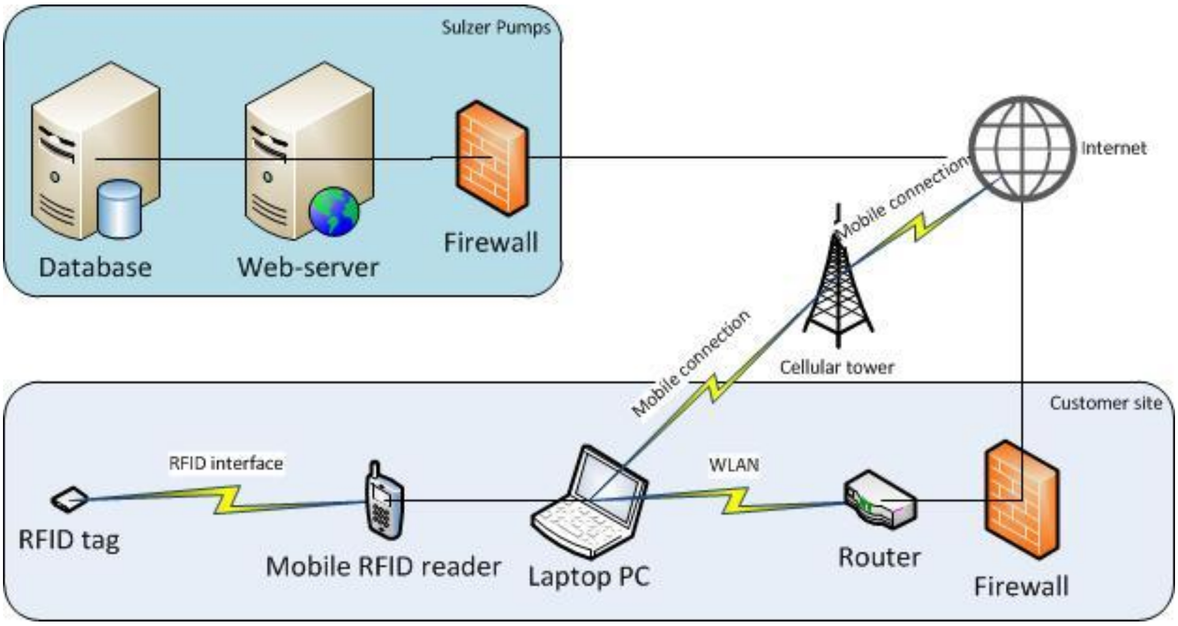

Figure 10. System architecture.

4.5 Users

The system has two main end-users: the maintenance personnel who read the tags and the system administrator who manages the linking between tag entities and machines. The system administrator also handles the adding, deleting or editing of existing tag data. If either user’s actions lead into an error, a sufficient error message will be shown, describing the problem at hand. Figure 11 shows the use-case diagram for the RFID-system. Both users use predefined login information to authenticate themselves and working network connection is assumed. Use-cases 1 and 2 are shown respectively in tables 5 and 6. The system administrator can be working either inside the Sulzer Pumps’ local network or remotely, but the maintenance personnel is assumed to be working off-site, connecting to the server remotely.

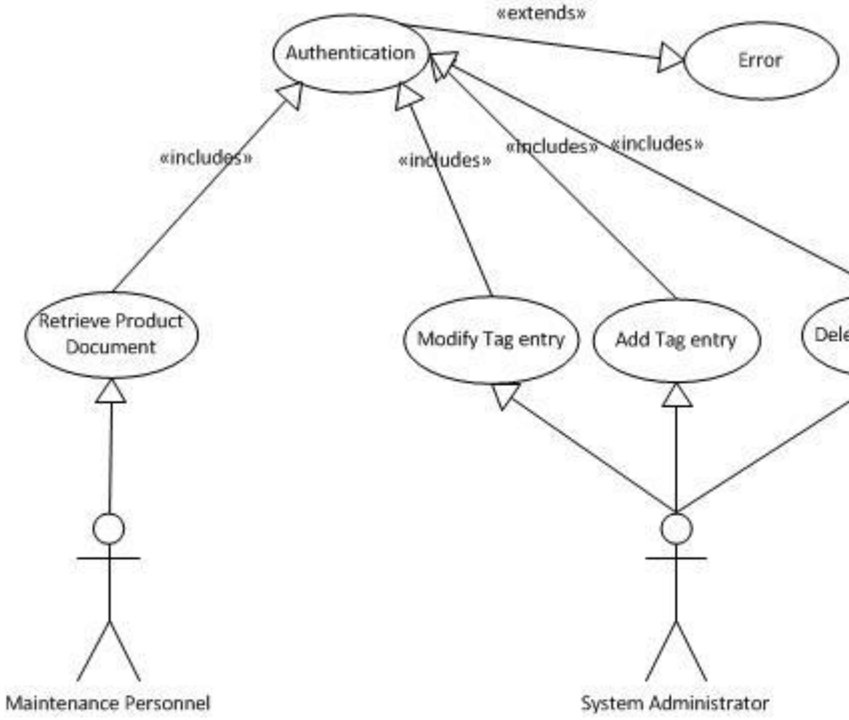

Figure 11. Use-case diagram of the system.

Table 5. Use case 1.

ID	UC-1
Name and version	Data retrieval v. 1.0
Actors	Maintenance personnel
Precondition	User has a laptop PC, RFID reader, network connection and login information to the service.
Description	User reads an RFID tag from an object in order to retrieve object-specific documentation from the database.
Basic flow	User reads an RFID tag and enters the serial number from the tag into a form open in user's laptop browser. User authentication is done and user receives object-specific documentation to the screen.
Exceptions	Authentication fails. Network connection fails. RFID signal weak or missing.

Table 6. Use case 2.

ID	UC-2
Name and version	Tag binding and modification v. 1.0
Actors	System administrator
Precondition	User has login information to the service. User is has a computer with network connection to access the service.
Description	User logs in the service in order to add, delete or modify tag data bound to real object data.
Basic flow	User logs in, adds, deletes or modifies data.
Exceptions	Authentication fails. Network connection fails.

5 DISCUSSION AND CONCLUSIONS

The main goal of this thesis is to create a new, mobile identification solution for Sulzer Pumps Finland's after-sale service targets. The system design includes reading the inspected machine's information via mobile reader. An RFID tag is placed on the machine storing its serial number or the UII only, leaving all other details in the database. This makes the system more secure, and easier to update the machine's information. The reader uses radio waves to communicate with the tag, and WLAN or cellular connection is used to communicate with the server.

After preliminary study on using RFID technology near and with conductive materials, such as metals it became clear that normal, first generation RFID tags would not work adequately enough in the environment. Read-ranges would be severely limited and in some cases non-existent due to the industrial environment, where steel and other metals are present. However, second generation UHF tags have been shown to work near and with conductive materials and even when attached directly to the metal (sometimes an additional spacer is needed between the tag and the metal surface).

The suitability of an RFID system in an environment full of metal objects needs to be further analyzed with proper testing of equipment. Different kinds of tags need to be tested with different readers to get accurate read-range estimates. Because special tags' (such as those designed to work especially with metal) prices vary a lot depending on the manufacturer, supplier and exact specifications of the tag, it is hard to estimate the real cost of the system at this point. The cost estimate also depends heavily on the amount of tags needed and readers deployed. Training costs and system integration have to be also considered. Once different equipment from different vendors has been tested, those that pass the requirements (adequate read-ranges, sufficient read-rate, and environmental compatibility) can be further compared in order to choose the most cost-efficient solution. There is no need to pay extra for unneeded features.

The ROI (Return of Investment) can be estimated and calculated when the initial screening of equipment has been done. The ROI analysis is commonly utilized to justify capital investments in costly systems [17]. However, not all organizations are looking for short- or long-term ROI on their investment, but are rather concerned with being compliant with their customers in order to continue doing business with them. With the given specification at this point, the system cannot be considered to turn profit on itself. However, it saves valuable time and gives a firm base for further development. It also binds the customers more to the service, since it's harder to jump to competitor's service when a working automated system is at hand.

Further research must be done if such system is to be implemented. The next step is to look into different vendors and test different equipment in appropriate environment. After laboratory testing, the system can be tested in real environment, still keeping the original data system intact. If the results are positive, then a small scale pilot can be launched where the system is used in real environment using the actual database. If the pilot is successful, then the system can be implemented properly. It's important to note that when proper equipment has been found, it needs to be tested thoroughly with the backend-system in order to scope out any areas in need of development. If there is no existing WLAN coverage at the maintenance site, the signal reception for mobile connections needs to be inspected. If there is no reception, then either WLAN access points must be deployed in order to achieve network connection at the maintenance site or possible offline database stored on the laptop needs to be created.

The initial focus is on the basic functionality of the system i.e. retrieval of the product specification document and after that has been proven to work; the focus can be shifted towards additional features. It is still important to acknowledge the future development areas so they can be easily implemented in the later versions of the system.

Future development of the system can include new functionalities for the system, such as ordering parts directly from the system or adding extra sensors (temperature, voltage, etc.). Wider use of the whole system can be also considered in the future. The Sulzer Pumps supplies the machines in question to the customers and said machines can be tagged at their origin and thus their movement between their departure and arrival can be tracked.

Requirements specification considering the system was produced in the process and it includes the main parts of the design. Exact specifics of certain parts of the system are left out due to privacy and confidentiality reasons.

The field of RFID technology is rapidly evolving area which constantly brings new solutions for existing (and new) applications. The RFID is not, however, solution for everything and doesn’t replace older identification methods altogether. RFID has its advantages in certain applications and it possesses qualities and features which other AIDC methods don’t (e.g. bulk reading, unique identifiers and large data storage). RFID system is usually still far more expensive than widely used barcodes and thus, the organization wishing to implement the technology has to compare the benefits of such system to the overall costs and ROI.

6 SUMMARY

The goal of this thesis was to design a mobile identification system for Sulzer Pumps Finland to be used in customer target locations as part of after-sale service. This was done using RFID technology as the identification method. After initial research, the focus shifted from Gen1 HF and UHF tags to Gen2 UHF tags due to the nature of the environment and capabilities of the said tag types. The system can be implemented in small scale relatively easily, but further research must be done regarding the tags, since read-ranges and prices vary greatly amongst Gen2 metal-compliant tags. When appropriate hardware has been discovered an overall cost estimate and ROI must be calculated in order to evaluate the cost-effectiveness of the whole system.

With metal-compliant tags, the system is possible implemented and requirement specification for such system was produced as part of the thesis. However, the cost of such system is not clear yet, since hardware testing and selection hasn't been done. Compatibility of the backend-system has to be also tested before actual implementation. Since the readers communicate directly with laptop PCs rather than remote middleware the backend-system needs only little improvements for basic functionality since it is already accessed by normal desktop- and laptop PCs.

The system was designed with focus on basic functionality in mind, which was to retrieve a product specification document from the database and show it to the user. Additional features are not included in the first version of the system, but are acknowledged so they can be later implemented without unnecessary re-design.

There already exist applications where RFID technology is used in conjunction with metal objects, so the technology should be suitable for this application. Further research and testing must still be done before system if fully deployed.

REFERENCES

1. Gonzalez, H., Han, J,. Li, X., Klabjan, D., Warehousing and Analyzing Massive RFID Data Sets. University of Illinois at Urbana-Champaign, 2007.
2. Günther, O., Kletti, W., Kubach, U., RFID in Manufacturing. Springer, Germany 2007.
3. Henrici, D., RFID Security and Privacy: Concepts, Protocols, and Architectures. Germany: Springer, 2008.
4. Hansen, W-R., Gillert, F., RFID for the Optimization of Business Processes, John Wiley and Sons, Germany, 2008.
5. Li, H., Development and Implementation of RFID technology. In: Turcu, C. ed., Development and Implementation of RFID technology, I-Tech Education and Publishing, Croatia, 2009, pp. 1-12.
6. Thornton F., Haines, B,. Das, A.M. Bhargava, H., Campbell, A., Kleinschmidt, J., RFID Security. Syngress, Canada, 2006.
7. Min, H., RFID tag performance optimization: a chip perspective. In: Miles, S.B. Sarma, S.E., Williams, J.R. eds., RFID Technology and Applications, Cambridge University Press, UK, 2008, pp. 33-46.
8. Mickle, M., Mats, L. and Hawrylak, P., Physics and Geometry of RFID. In: Ahson, S. and Ilyas, M. eds., RFID Handbook: Applications, Technology, Security and Privacy, CRC Press, USA, 2008, pp. 3-17.
9. Curty, J-P. Declercq, M. Dehollain, C., Joehl, N,. Design and Optimization of Passive UHF RFID Systems, Springer, Switzerland, 2007.
10. Weis., S., RFID Technical Considerations. In Bidgoli, H. ed., The Handbook of Technology Management: Supply Chain Management, Marketing and Advertising, and Global Management. John Wiley and Sons, 2010, pp. 220-231.
11. Bhatt, H. and Glover, B., RFID essentials. O'Reilly, USA, 2006.
12. Mitrokotsa, A., Rieback, M.R. and Tanenbaum, A.S, Classifying RFID Attacks and Defenses, Information Systems Frontiers, Volume 12, Number 5, 491-505.
13. Bridelall, R. and Hande, A., Performance Metrics and Operational Parameters of RFID Systems, In: Bolic, M., Simplot-Ryl, D. and Stojmenovic, I. eds., RFID

Systems: Research Trends and Challenges, John Wiley and Sons, UK, 2010, pp. 23-56.

14. Demystifying UHF Gen 2 RFID, HF RFID, EE Times, Design, Industrial Control, http://www.eetimes.com/design/industrial-control/4019123/Demystifying-UHF-Gen-2-RFID-HF-RFID/.

15. Kim, M., Song, B., Ju, D., Choi, E. and Cho, B., Development of Metallic Coil Identification System based on RFID. In: Turcu, C. ed., Radio Frequency Identification Fundamentals and Applications, Design Methods and Solutions, Intech, Croatia, 2010, pp. 198-214.

16. Juels, A., RFID Security and Privacy: A Research Survey. Journal of Selected Areas in Communication (J-SAC), 24(2):381-395, RSA Laboratories, 2006.

17. Jones, C. and Chung, C., RFID in Logistics: A Practical Introduction. CRC Press, USA, 2008.

APPENDIX 1. Requirement specification

1 PURPOSE AND OVERVIEW

The RFID-system is designed for Sulzer Pumps in order to access maintenance data more conveniently. The system will be used by the maintenance personnel in customer target locations.

2 BUSINESS OBJECTIVES

ID	Date	Requirement	Requirement description	Notes
G1	13.4.11	Faster data retrieval	Object’s data retrieval time should decrease greatly	
G2	13.4.11	Customer reliance	Customers are more dependent on provided services	

3 RESTRICTIONS

ID	Date	Restriction	Restriction description	Notes
RE-1	8.3.11	System must be separate from the SAP	The identification system should not be integrated with present SAP R/3 system.	
RE-2	8.3.11	The system should use the present database.	An interface is created to access and view data from current database.	No modifications allowed.
RE-3	8.3.11	Web-based user interface	System should have web-based user interface for interoperability and easy access.	
RE-4	8.3.11	Tag contains only essential information	No unnecessary information is stored into the tag (only serial number).	
RE-5	13.4.11	Tags are read-only	Once the serial number is written on the tag, it cannot be removed or modified.	Minimizing security risks.
RE-6	8.3.11	Only relevant information is shown to user	Data from server is filtered so only relevant information regarding the customer's products is shown.	
RE-7	8.3.11	User authentication	Users need to be authenticated.	
RE-8	8.3.11	Multi-device	Should work with multiple device configurations (readers/middleware)	
RE-9	8.3.11	Minimal offline support	System needs an internet connection.	No additional data stored offline.
RE-10	13.4.11	Hardware	System should use existing hardware as much as possible.	

(continues)

APPENDIX 1. (continues)

4 INTEREST GROUPS

ID	Date	Interest group	Interest group description and role	Notes
I-1	8.3.11	Designers	Designing of the system	
I-2	8.3.11	IT Manager		
I-3	8.3.11	Director of Customer Support Services		
I-4	8.3.11	System admin	Maintenance for the system	
I-5	13.4.11	End-users	End-users of the designed system	
I-6	13.4.11	Developers	Coding, testing, documenting	
I-7	13.4.11	Customers	Group receiving the service	Service deployed at customer sites

5 USER GROUPS

ID	Date	User group	User group description and role	Notes
U-1	8.3.11	Maintenance personnel	End-user of the system	
U-2	8.3.11	System administrator	Maintenance and updating of the system	

(continues)

6 USE-CASE DIAGRAM

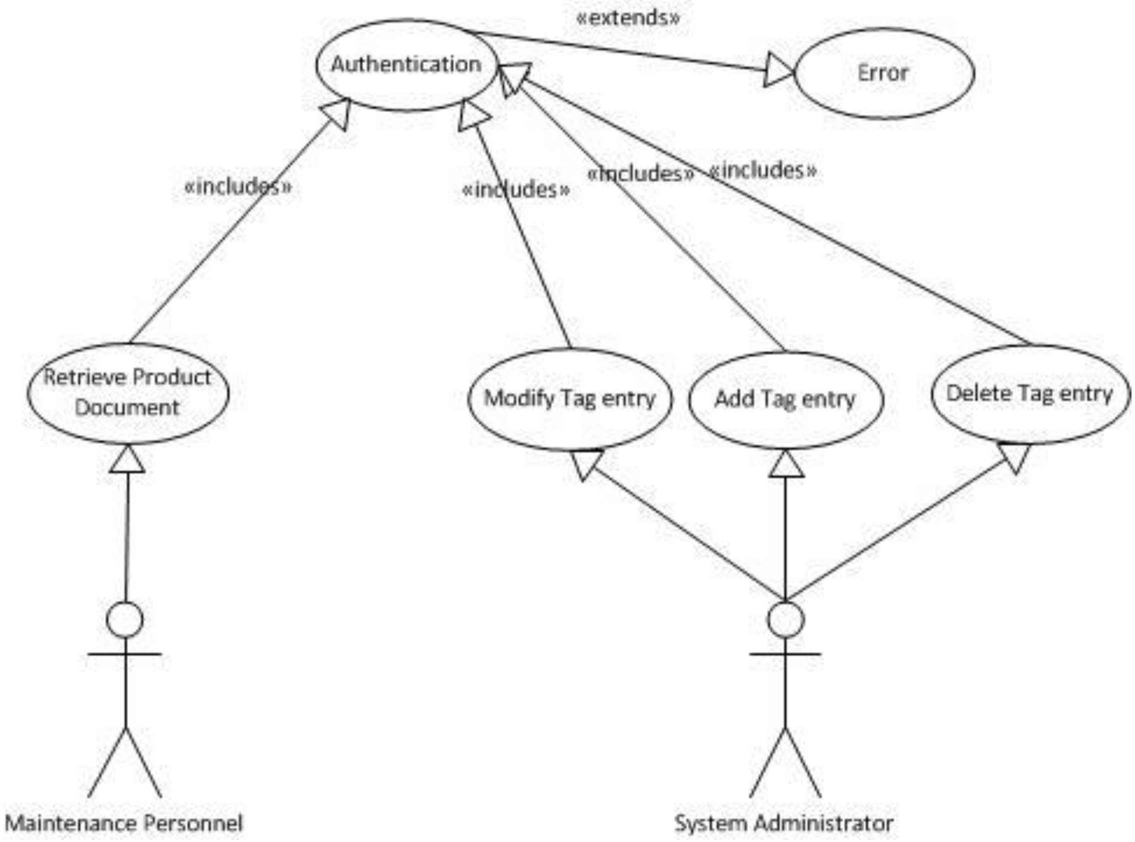

Figure 1. Use-case diagram

7 ASSUMPTIONS

The user uses generic laptop with 8”-15,4” screen with Windows XP or Windows 7 as operating system. End-users are assumed to know how to operate computers but are not expected to know the technology in-depth. Users are provided with a short training for the system.

(continues)

8 REQUIREMENTS

ID	Date	Requirement	Requirement description	Priority
FR-1	13.4.11	Integration with PumpsOnline	System uses PO as backend.	High
FR-2	17.4.11	User authentication	Users need to be authenticated in order to access the service	High
FR-3	13.4.11	Unique user accounts	User/customer specific user accounts.	High
FR-4	13.4.11	Device documentation	Retrieval of device documentation from the database.	High
FR-5	13.4.11	Default language English	System's main language is English.	High
FR-6	17.4.11	Additional languages	System supports additional languages	Low
FR-7	13.4.11	Maintenance reports	Users can create reports on-site.	Normal
FR-8	13.4.11	Operating system	Must work with Windows XP and 7	High
FR-9	13.4.11	Maintenance history	Users can view maintenance history.	Normal
FR-10	13.4.11	Printing	Users can print documents from printers in the same network.	Normal
FR-11	13.4.11	Sensors	System should be made so extra sensors can be attached in future.	Normal
FR-12	17.4.11	Order tracking	Orders made in PO can be tracked	Low
NR-1	13.4.11	Feedback	System must provide sufficient feedback on status of procedure.	High
NR-2	17.4.11	Error reporting	Error reporting has to be clear and specific describing the exact error.	High
NR-3	13.4.11	Simple user interface	User interface should be bare and minimal.	Normal
NR-4	13.4.11	Easy navigation	Navigation should be easy and logical.	High
NR-5	13.4.11	User groups	System should be designed for existing and new customers.	High
NR-6	13.4.11	Easily deployed	Once ready, the system should be easily deployed to customer sites.	Normal

9 USE CASES

Use case 1

ID	UC-1
Name and version	Data retrieval v. 1.0
Actors	Maintenance personnel
Precondition	User has a laptop PC, RFID reader, network connection and login information to the service.
Description	User reads an RFID tag from an object in order to retrieve object-specific documentation from the database.
Basic flow	User reads an RFID tag and enters the serial number from the tag into a form open in user's laptop browser. User authentication is done and user receives object-specific documentation to the screen.
Exceptions	Authentication fails. Network connection fails. RFID signal weak or missing.

(continues)

Use case 2

ID	UC-2
Name and version	Tag binding and modification v. 1.0
Actors	System administrator
Precondition	User has login information to the service. User is has a computer with network connection to access the service.
Description	User logs in the service in order to add, delete or modify tag data bound to real object data.
Basic flow	User logs in, adds, deletes or modifies data.
Exceptions	Authentication fails. Network connection fails.

10 ARCHITECTURE

The basic architecture of the design in process is shown in figure 1. The RFID tag placed on the machine is identified by mobile RFID-reader. The reader is connected to the user's laptop, which is acting as middleware. The laptop connects to the Web-server, using either WLAN connection or mobile connection, which shows the machine's information to the user. A database with all the machines' information already exists, but the request form has to be made. Multiple readers can be reading tags in the same area at the same time.

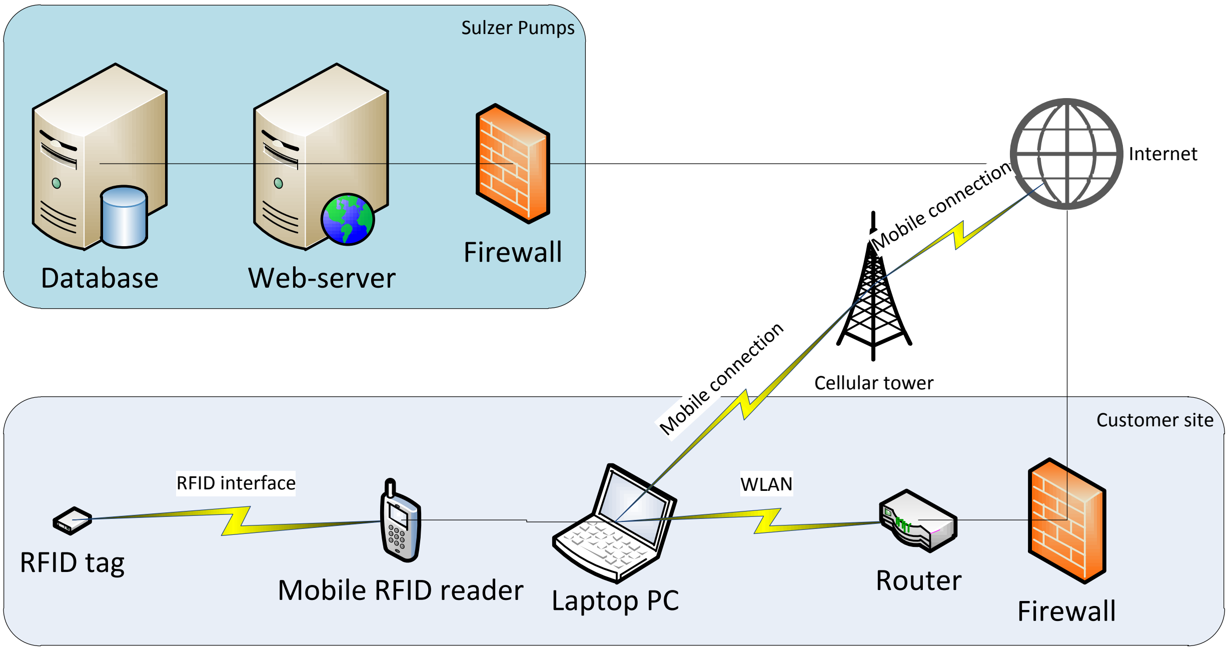

Figure 2. General system architecture

(continues)

APPENDIX 1. (continues)

When the serial number is read from the RFID tag, the reader sends it to a form open in laptop's browser. The browser requests a new document from the Web-server, showing the machine's part list. A user authentication is done, and the Web-server shows a document containing the machine's information or an error message. The data retrieval phases can be seen in figure 3. The system has a Web user interface and therefore no additional programs are needed for data retrieval; a simple modern browser will be sufficient. Since tagged elements remain stationary and additional elements after initial setup are added seldom, adding and editing data in the database is left out from the RFID system. This also helps keeping the system secure from several attacks.

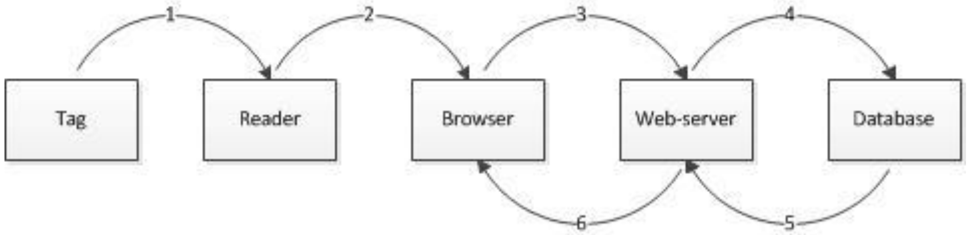

Figure 3. Data retrieval phases.

1. Tag is recognized and data stored in it is retrieved by the RFID reader.
2. The reader sends the data (serial number) to the laptop's browser.
3. The browser sends a request to the Web-server.
4. The Web-server runs a PHP-script and sends a request for the database.
5. The Database sends the correct PDF-document to the Web-server.
6. The Web-server returns the document to the browser.