SToP Tampering of Products in Aviation Industry

Design a practical guideline for choosing an appropriate RFID system for anti-counterfeiting in the aviation industry

Sara Kheiravar
**SToP Tampering of Products in Aviation Industry**  
(Design a practical guideline for choosing an appropriate RFID system for anti-counterfeiting in the aviation industry)

Sara Kheiravar

Master Thesis  
Subject category: Technology  
Series and Number: Logistics 12/2008

University College of Borås  
School of Engineering  
SE-501 90 BORÅS  
Telephone +46 033 435 4640

Examiner: Maria Fredriksson  
Supervisors: Håkan Torstensson (UCB), Herman Schmidt Schieferstein (Airbus), Andreas Pfeil (T-Systems)  
Client: Airbus-Hamburg  
Date: 1st of Feb. 2008  
Keywords: SToP Project, Aviation Industry, RFID technology, Anti-counterfeiting, SUP, LRU
Abstract

Controlling the authenticity of a product in the supply chain has been a struggle for manufacturers, and increasing complexity of the chains intensifies the imitation and counterfeiting threats. Indeed, counterfeiting is absent from effective control in supply chain and manufacturers are looking for a technology to supply this control. The ability of RFID to provide a tagged item with unique electronic code, it’s characteristic to hold some historical data about the item and supply automatic, immediate and accurate data about the tagged item attracts manufacturers to use RFID technology to provide the effective control throughout the supply chain. In line with this issue, SToP (Stop Tampering of Products), an EU founded project, aimed at developing an anti-counterfeiting solution based on auto-identification technologies for consortium companies concerned with or affected by fake products. SToP is committed to establish the business cases, do research and at the end issue application guidelines for using RFID technology against counterfeiting in particular business contexts. Under SToP’s umbrella, this master thesis is initiated with the purpose to design a practical guideline for choosing an appropriate RFID system for anti-counterfeiting in the aviation industry that is one of the affected industries.

The conclusion of the thesis consists of a number of sections, which altogether fulfill the purpose of the thesis. The thesis forms a base for continues challenge of implementing RFID as an anti-counterfeiting device focusing on the aviation industry, proposes solution scenarios based on RFID technology, suggests applicable standards and proposes a secure RFID method to prevent counterfeiting specially in the aviation industry. Jointly, these sections from guidelines as a foundation for decision-making for kind of RFID system for anti-counterfeiting application in the aviation industry.

Keywords: SToP Project, Aviation Industry, RFID technology, Anti-counterfeiting, SUP, LRU

1 The SToP project aims at developing ambient intelligence-based and network-oriented systems for the efficient and secure authentication of products. It thereby helps to reduce the problems imposed by counterfeiting and product privacy. (http://www.stop-project.eu/)
Acknowledgments

This master thesis is the final part of the Master program in Logistics at University College of Borås, Sweden. The thesis was initiated by Airbus, special projects in Hamburg and carried out from 1st of April 2006 till 30th of October 2006. Throughout the thesis I received strong support from my supervisors in Airbus and T-systems, Herman Schmidt Schieferstein and Andreas Pfeil. Their helpful and insightful feedbacks have facilitated the analysis and given me valuable experience in Aviation industry and RFID technology. Furthermore my supervisor Håkan Torstensson form school of engineering in UCB has contributed with valuable support, directions and improvements of the thesis work. I also like to express my gratitude to everyone I have been in contact with or interviewed, SToP project partners and specially Harald Vogt the coordinator of SToP project from SAP Research. Without their input this thesis would not have been possible. Finally I heartily thank my parents who have been a great support during whole my study.

Sara Kheiravar
Borås, February 2008
Table of Contents

1. Introduction ................................................................................................................. 1
  1.2. Background ............................................................................................................. 1
  1.3. Problem definitions ................................................................................................. 2
  1.4. Purpose .................................................................................................................... 3
  1.5. Delimitations ........................................................................................................... 3
  1.6. Target groups and Reading Suggestions .................................................................. 3
      1.6.1. Airbus ............................................................................................................... 4
      1.6.2. University ......................................................................................................... 4
      1.6.3. SToP project partners ....................................................................................... 4

2. Extended Background ................................................................................................. 5
  2.1. Airbus ..................................................................................................................... 5
  2.2. SToP, Stop Tampering of Products ........................................................................ 5
      2.2.1. Main Scientific and Technological objectives of SToP .................................. 6
      2.2.2. Members of the Project Consortium and Their Role .................................... 6
  2.3. Airbus and RFID ..................................................................................................... 8
      2.3.1. RFID tagging Operational- Polaris ................................................................. 8
      2.3.2. Stop Tampering of Products by means of RFID-SToP ................................... 9
  2.4. Introduction to RFID Technology .......................................................................... 10
      2.4.1. What is RFID? ............................................................................................... 11
      2.4.2. RFID system components .............................................................................. 11
  3. Methodology .............................................................................................................. 14
    3.1. Type of study ........................................................................................................ 14
    3.2. Research methods ................................................................................................. 14
        3.2.1. First step ......................................................................................................... 14
        3.2.2. Second step ..................................................................................................... 14
        3.2.3. Third step ....................................................................................................... 15
  4. Validity and Reliability ............................................................................................... 15
  4.1. Counterfeiting ......................................................................................................... 17
      4.1.1. Counterfeiting in aviation industry ................................................................. 18
    4.2. Clarification of terms ............................................................................................ 19
    4.3. SUPs’ points of presence, Points of counterfeiting in Aircraft part’s lifecycle ...... 21
        4.3.1. Source of SUPs in MRO phase ...................................................................... 22
    4.4. Dangers (risks) and examples from the past ....................................................... 24
    4.5. Current countermeasure for SUPs problem ......................................................... 26
  4.6. Future Solution (electronic authentication of aircraft parts, SToP project) ............ 27
      4.6.1. Approach 1: (master-slave, active-passive RFID tagging) ............................ 28
      4.6.2. Approach 2 (Passive RFID tagging) .............................................................. 28
      4.6.3. RFID (on which parts) .................................................................................... 30
  5. Regulations and Standards of RFID for Aviation Industry ....................................... 32
    5.1. General overview ................................................................................................. 32
    5.2. Airworthiness ....................................................................................................... 32
5.2.1. RFID and Airworthiness Procedure ................................................................. 33
5.3. Standardization .................................................................................................. 35
  5.3.1. Types of Standards for RFID ................................................................. 35
  5.3.2. Standard organizations for RFID ......................................................... 36
5.4. Adhering to a standard ..................................................................................... 41
  5.4.1. Recommended RFID standards for authentication application .......... 42
6. Authentication of RFID tag .................................................................................. 44
  6.1. Security threats to RFID tags in aviation industry ........................................ 44
    6.1.1. Data Security Threats ............................................................................ 44
    6.1.2. Hardware Security Threats ................................................................. 45
  6.2. Data Content Security ..................................................................................... 45
    6.2.1. Security approach for in transmit data between reader and tag .......... 45
    6.2.2. Security approaches for data on the tag .............................................. 45
  6.3. Hardware security .......................................................................................... 46
  6.4. Cryptography Standard for RFID ................................................................. 48
    6.4.1. PKI technology ..................................................................................... 48
    6.4.2. PKI Standard ........................................................................................ 48
  6.5. Recommended Security Solution” Aviation industry needs highly secure crypto HF RFID” .......................................................... 49
7. Conclusion and Recommendations ................................................................. 50
  7.1. Conclusions .................................................................................................... 50
    7.1.1. Layered architecture against SUPs ....................................................... 50
  7.2. Recommendation (Internet of Parts) ............................................................. 51
    7.2.1. Scenario of Internet of Parts ............................................................... 51
    7.2.2. Future challenges ................................................................................. 52
Table of Figures
Figure 1: Overview of SToP Consortium and Partners Involvement (Nochta 2005,26) ..........7
Figure 2: Polaris – Data architecture principle (Airbus) .......................................................... 9
Figure 3: overview of Auto ID and Data Capture (AIDC) technologies ............................... 11
Figure 4: RF subsystem (Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Philips 2007) ........................................................................................................... 12
Figure 5: RFID system components ...................................................................................... 13
Figure 6: Chart showing counterfeit products seized in 2005 by U.S. Customs and Border Patrol ........................................................................................................ 18
Figure 7: Aircraft Lifecycle ..................................................................................................... 22
Figure 8: aircraft engine master-slave tagging ..................................................................... 28
Figure 9: Aircraft Lifecycle Surveillance ............................................................................... 29
Figure 10: Lifecycle of an LRU (Jens Muller_SToP) ............................................................... 31
Figure 11: EPC Code schema ................................................................................................ 37
Figure 12: EPCglobal Standards Overview ............................................................................. 38
Figure 13: ATA Aviation market place ..................................................................................... 39
Figure 14: SPEC2000, Traceability database ........................................................................ 40
Figure 15: memory description of high memory RFID (Polkinghorne 2007) ......................... 41
Figure 16: RFID Standards for Aviation Industry ................................................................... 42
Figure 17: MicoWire ................................................................................................................ 47
Figure 18: RFID based network ............................................................................................... 52

List of Tables
Table 1: Mechanism of illicit trade, Aviation industry (SToP) .................................................. 24
Table 2: Boeing and Airbus Simplified View of Standards Activity ...................................... 42
Table 3: PKI Scenario ................................................................................................................ 48
Table 4: RFID Transponder: Aviation Selection Criteria ....................................................... 49

Appendices
Appendix A: Qualitative Study ................................................................................................. 56
Appendix B: Standard Organizations ........................................................................................ 58
Appendix C: EPC Network Architecture-inside the Enterprise ............................................... 59
1. Introduction

This chapter introduces a background for a better understanding of the problem domain. Furthermore problem definitions, purpose and delimitation of the thesis are defined. In order to facilitate different interested parties, reading suggestions and an overview of the disposition of the thesis is provided.

1.2. Background

Fast growing supply chains coupled with rapidly growing globalized markets create very long and complex supply chains representing very large areas of exposure that provide potential market predators with unlimited opportunities for counterfeiting.

Controlling the legitimacy and the brand integrity of a product in the supply chain has been a struggle for manufacturers, and increasing complexity of the chains intensifies the problem. Indeed, counterfeiting is absent from effective controls in supply chain and at first glance the solution is clear: Imposing severe penalties for counterfeiters, increasing the integrity of supply chain, tracking and tracing products through their travel in chain, having accurate and immediate data of products anywhere / anytime in the chain, authentication of all components in the supply chain, etc. But the main challenge is how to realize these solutions. Is it possible to control and track a supply and demand chain, which starts from USA and goes through Europe and ends in China with hundreds of nodes, in accordance with the existing technologies? Is there reliable technological infrastructure available to guaranty this control?

The characteristics that attract the manufacturers to think about RFID as a potential solution for anti-counterfeiting is the ability of RFID to provide a tagged item with unique electronic code, it’s characteristic to hold some historical data about the item and supply automatic, immediate and accurate data about the tagged item. There are many ongoing research projects in industries and universities about cost features, implementation requirements and feasibility of realizing the use of RFID as an anti-counterfeiting device.

SToP\(^2\) (Stop Tampering of Products) is an EU subsidized project aimed at developing an anti-counterfeiting solution based on auto-identification technologies for consortium companies concerned with or affected by fake products including luxury goods, pharmaceutical, and aviation manufacturers. Participants in this project include SAP (project coordinator), University St.Gallen (academic support), Novartis (pharmaceutical company), Richmond (luxury goods), Oria computers (software company), Space code (RFID hardware), Bundesdruckerei (printing company) and Airbus (aircraft manufacturer). (Nochta 2005)

\(^2\) The SToP project aims at developing ambient intelligence-based and network-oriented systems for the efficient and secure authentication of products. It thereby helps to reduce the problems imposed by counterfeiting and product privacy. (http://www.stop-project.eu/)
Because of high risk of tampered products in aviation industry, this industry is one of the main victims of such products. All components in this industry are keen to find a solution to increase the quality of current authentication process. Introducing RFID as solution has caught the attention of aircraft manufacturers, but it is one of the most complex industries concerning regulations, specifications, and standardization and security issues. When it comes to deployment of RFID, questions come up that must be completely clarified. Airbus as one the key components of the aviation industry has been involved in the SToP project to analyze the possibility of the SToP objectives in the aviation industry and to pave the way for implementing RFID in aircraft parts as an automatic anti-counterfeiting device.

This thesis work will form a base for continues challenge of implementing RFID as an anti-counterfeiting device focusing on the aviation industry. It will take a look at the size and most common means of counterfeiting in the aviation industry today, and also the replacement market products for aircrafts. It will then explain how an RFID system works and proposes a range of increasingly secure methods of using RFID to prevent some of the different types of counterfeiting specially in the aviation industry.

1.3. Problem definitions

To introduce the purpose of the thesis a discussion follows of the problem domain. The focus of the discussion concerns both technical and business related issues.

Problem definition 1
In average, each aircraft is made up over 4 million parts. To present RFID technology as solution for anti-counterfeiting, tagging all individual parts is infeasible. The parts that are more in danger of counterfeiting have to get defined and tagged.

Which parts are more vulnerable to get tampered and have to be tagged?

Problem definition 2
Due to the regulations in the aviation industry, all parts used or aimed to be used in an aircraft are obliged to follow predefined specifications. RFID also as a part in an aircraft has to follow particular standards, protocols and regulations defined by responsible organization.

What are the rules, specifications and protocols for RFID in the aviation industry?
Is there any standardized RFID tag that could fulfill the aviation requirements?

Problem definition 3
Considering the materials used in an aircraft and the operation environment of it, different kinds of RFID tags must be used. Existence of many RF devices as well as metal devices in an aircraft brings difficulties to find a tag operating properly without interfering in the operability of other parts.

Which RFID tag technology could be used without compromising safety of an aircraft?
**Problem definition 4**
To use the RFID tag as an anti-counterfeiting device, some historical and event data is needed to be stored in the tag supporting the tracing process. Today RFID tag’s memory size is very limited and an optimistic data structure is vital. In addition, adhering to a common structure of data for the whole aviation industry is a must. On the other hand, as RFID is a data capturing device, appropriate data architecture is needed.

*What is the data structure of a tag?*

**Problem definition 5**
Data security has been always an important issue in RFID, but it is even more important when it comes to usability of RFID in authentication. By implanting RFID, manufacturers want to greatly increase the confidence a customer or user that a product is authenticated. The necessity condition to ensure the authenticity of a tagged item is ensuring the authenticity of the tag and tag data.

*How the tag and tag data could be secured?*

### 1.4. Purpose

Based upon knowledge within Airbus as well as existing technologies about RFID the purpose of this thesis is to design a practical guideline for choosing an appropriate RFID system for anti-counterfeiting usability in the aviation industry.

### 1.5. Delimitations

Due to the time limitation, it is necessary to delimitate the scope of this thesis to achieve the final result.

There are different solutions available for the counterfeiting problem. However, this thesis will focus on applying the RFID technology as a solution. The work is done based on requirements of the aviation industry, so the results will just cover those of the aviation industry.

The thesis work will cover the RFID application in counterfeiting and its requirements in the aviation industry and there will be no account for analyzing Technical aspects of RFID system components (RF Subsystem, Enterprise Subsystem, Inter-Enterprise subsystem) as it will not fulfill the purpose of this thesis.

However, this thesis work is paving the way for new platform investigation; Investigation of the new platform and future techniques is out of scope of this thesis.

### 1.6. Target groups and Reading Suggestions

The thesis is written for three target groups Airbus, University and Stop project partners, so readers probably have different interests. This part contains some reading suggestions for the identified target groups.
1.6.1. Airbus

The thesis work is principally aimed for Airbus where the thesis has been initiated and performed. In order to achieve a clear picture of the thesis content and what outcome to expect the reader should thoroughly study the problem definitions presented in 1.2. It is recommended to perspicuously read chapter 4 to get an overview of counterfeiting problem in aviation industry as well as RFID usage in the aircraft lifecycle. Chapter 5 gives information on regulations and standards for RFID in the aviation industry. Chapter 6 is interesting for those affected with RFID’s security features. Chapter 7 is highly interesting as it presents the results of the thesis work.

1.6.2. University

Thesis work is also aimed at university students wishing to achieve knowledge of RFID and its counterfeiting application in the aviation industry. It is likely that these readers find most interest in chapter 2 and 4, where it is possible to get information about the project, RFID technology, the counterfeiting problem in aviation industry and how RFID can help to handle the problem. Chapters 5, 6 and 7 are interesting in order to understand the requirements of an RFID technology that is appropriate in aviation industry.

1.6.3. SToP project partners

As this thesis work has been done in line with participation of Airbus in the SToP project, a considerable part of it could also be of interest for SToP project partners. These readers are assumed to be able to draw their own parallels to their organizations.
2. Extended Background

In order to complement the background and the purpose presented in first chapter, this chapter follows the presentation of Airbus and SToP project. Thereafter the involvement of Airbus in SToP project is presented. A brief introduction of RFID technology concludes the chapter.

2.1. Airbus

Airbus, an EADS\(^3\) company, is one of the world’s leading aircraft manufacturers. The company produces about half of the world’s civil aircrafts. Airbus is founded in 1970 and for over 37 years, it has been offering state-of-the-art passenger aircrafts supported with the highest quality of service.

The Airbus product line comprises of 4 civil aircraft families—A320, A300/A310, A330/A340, and A380—from 100 seat single-aisle A320 family to 555-seat double-deck A380 family which is the largest civil aircraft available in the market. The Airbus aircraft families offer the highest degree of commonality, comfort, technology and innovation. Airbus has always been the pioneer in recognizing and implementing groundbreaking technologies as well as incremental in its aircrafts. And its ability to make a good balance between innovation and economics, operational reliability and flexibility makes Airbus the most advanced on the market.

Introducing first twin-engine wide-body aircraft, first twin-aisle aircraft with a two-crew cockpit using latest digital technology, electronically-managed fly-by-wire flight control system, first carbon-fibre keel beam and the last product-A380-containing advanced aerodynamics, high-pressure hydraulics and the increased use of carbon fibre reinforced plastic are all re-approvals of Airbus’s tradition of innovation.

Airbus’ approach is to be at the cutting edge, continuously pushing the boundaries to develop new and better ways to apply technology for the continuous improvement of its business, products and services. (Airbus n.d.)

2.2. SToP, Stop Tampering of Products

SToP is an EU financed project that aims at developing ambient intelligence-based and network oriented systems for the efficient and secure authentication of products- affected by fakes- at any stage of their entire lifecycle.

---

\(^3\) The European Aeronautic Defense and Space Company EADS N.V. (EADS), EADS is a global leader in aerospace, defense and related services. The Group includes the aircraft manufacturer Airbus, the world's largest helicopter supplier Eurocopter and EADS Astrium, the European leader in space programmes from Ariane to Galileo. (www.eads.com)
SToP’s main goal is to apply ambient intelligence technologies (like RFID) in the real world and in cyberspace, for the secure authentication of smart products and of easily distinguishing genuine and fake products. In order to achieve this goal, SToP is evaluating and developing technologies and approaches that could eventually remove the fake products and illicit trades.

2.2.1. Main Scientific and Technological objectives of SToP

1. “Analysis of the structure and mechanisms of the illicit market as well as an in-depth investigation of the supply- and demand-side drivers of trade with counterfeit products.

2. Development of a clear business case framework, especially helping small and medium sized organizations to evaluate the financial impact of illicit trade on brand name and revenue.

3. Development of a distributed and network-oriented system, enabling enterprises and end-users to efficiently manufacture, deliver and purchase secure and authentic products. This includes the development and extension of existing smart tagging technologies as well as the design of suitable, collaborative software components as part of a comprehensive network infrastructure. Underlying issues such as security, scalability, interoperability, robustness of the system, and the development of potential standards will be given due consideration.

4. Development of integration concepts, helping organizations to seamlessly integrate the approaches into existing business environments and enterprise software systems, e.g. in ERP and Supply Chain Management tools.

5. Real-world application trials to assess and verify the applicability of the approved solutions.” (Nochta 2005,8-9)

It is of great importance to develop a solution which is scaleable and accessible for a wide variety of potential users. Thus, SToP has started with different partners from different industries.

2.2.2. Members of the Project Consortium and Their Role

The SToP consortium brings together eight partners from five different European countries, namely France, Germany, Liechtenstein, Slovenia, and Switzerland. Research, development and business competencies of the partners cover all issues that are significant for the achievement of the objectives of SToP. These broad ranges of partners from different industries make a wide-spread technology and knowledge transfer possible, and thus help solving product authentication problems in a broad range of scenarios. Following are a list of the partners participating in this project.
Figure 1: Overview of SToP Consortium and Partners Involvement (Nocha 2005,26)

“Partner’s role in the project:

- **University of St. Gallen (HSG):** S&T Research, Economics, Architecture Design, Business Applications. Definition of Generic Requirements that resulting solutions should fulfill, in order to be accepted by various business communities. Contribution to application trials (mobile devices to verify product authenticity with main focus on user friendliness and interoperability).

- **SAP (SAP):** Collection of generic requirements on a back-end infrastructure that keeps track of product related data during the product’s whole lifecycle. Integration aspects of the resulting systems into existing and future enterprise software systems. Development and implementation of security mechanisms that ensure that only authorized parties can change data related to products’ authenticity verification. Thereby an important issue is that products or product parts continuously change their owners, which will be addressed by the development of adequate delegation mechanisms.

- **Airbus (AB):** Provider of specific application trials, related to the secure authentication of aircraft spare parts during service and maintenance operations, to increase aircrafts’ safety. Integration into the related systems and processes.

- **Montblanc (MB):** Provider of specific application trials, related to the secure authentication of pens and fine leather articles, which are heavily affected by product forgers and illicit trade.
• **Swarovski (SWA):** Provider of specific application trials, related to the secure authentication of crystal articles, a target of illicit/grey markets. Enhancement of Production environment by means of smart packaging but also article tagging.

• **Bundesdruckerei (BDR):** S&T Research: Secure Data on secure tags, Secure Readers, Verifier Components

• **SPACECODE:** S&T Research: Hardware related problems, integration of smart tags into products under specific conditions, such as; Architecture Design to make sure that different kind of smart tags are handled by the back-end infrastructure in a portable way.

• **ORIA:** S&T Research on the development of adequate models,” (Nochta 2005,27-28)

### 2.3.  **Airbus and RFID**

As mentioned in section 2.1, Airbus has had a long reputation in implementing ground breaking technologies. Airbus is investing continuously in ambient intelligence, internet of things and ubiquitous computing technologies to fill information gaps all over the industry that if realized, could make a revelation in Aviation Industry.

In 1999 for the first time ever, Airbus implemented the RFID technology to improve its tool management processes. Now all tools and tool boxes in Airbus are equipped with RFID tags that contain historical information of tools offering electronic support for loan, location and repair management of tools. (Airbus applies RFID technology to supply of aircraft spare parts 2003)

Currently Airbus is investing in RFID technology for spare parts of aircraft. Equipping spare parts with RFID tags will considerably help in simplifying spare part management processes-inventory and repair management of spare parts. Furthermore, since authentication of parts has always been a big headache for Airbus- considering 6 million parts made in as many as 33 countries; Airbus is deeply interested in developing a proper RFID system to ensure authenticity of spare parts during their whole lifecycle, which can significantly reduce the risk of counterfeit parts and consequently improve aircraft safety. (Airbus applies RFID technology to supply of aircraft spare parts 2003) (Violino 2004)

To develop such an RFID system, Airbus has launched or involved in some relevant research projects. Projects including RFID tagging in Simulation-HLSTR, RFID tagging Operational-Polaris, and Stop tampering of products by means of RFID are running in System and Equipment Standardization (special RFID projects) - Airbus. (Schmidt-Schieferstein 2007)

#### 2.3.1.  **RFID tagging Operational- Polaris**

Polaris is an RFID test project that has been launched to elaborate RFID basics and to demonstrate its applicability in aircraft environment, and to verify RFID tag / transponder usage under all aircraft operational circumstances and developing basis for equipment Configuration Management by means of RFID.
In this project the “High Lift System Test Rig” in Airbus-Bremen is used as ground based test bed to earn experience on installation criteria and RFID transponder operational behaviors. The “Canadian Air Force (CAF) A310 Polaris” is used as an airborne test bed to sample RFID transponder operational behaviors under airborne environmental criteria to introduce RFID on aircraft equipment in civil and military aviation operation environment. Kortenburg Inc⁴, / MSG⁵ / MacSema Inc⁶, / Silverstroke⁷ are hardware and software sample providers. (Airbus, RFID on MRTT POLARIS n.d.)

Tests have been accomplished by CAF under Airbus supervision and with support of hardware and software providers.

2.3.2. Stop Tampering of Products by means of RFID-SToP

Equipment used in aviation, on-board of aircraft and for its operation, must be tested and certified according to airworthiness standards. The behavior and condition of these equipments must be traceable throughout theirs life cycle without the danger of falsification. Billions of dollars of damage occur every year by bogus parts’ supply market and high amount of documentation, and to ensure recognition of bogus parts in aircraft documentations’ processing is required today. Smart/intelligent devices (like RFID) attached to the respective

---

Footnotes:

⁴ www.kortenburg-rfid.com
⁵ www.msg.de
⁶ www.macsema.com
⁷ www.silverstroke.com
equipment with adequate software are sought to distinguish proper certificated items from uncertified (SUPs), to ease today’s high documentation efforts for equipment authentication. Airbus has involved itself in SToP project to realize this vision.

**Airbus tasks in SToP:**

- **Delivery of recommended Unique ID methods for aviation**
  Research to update unique identification methods, applicable for aviation operation and filter their usability for SToP - elaborate, define and provide “aviation standard” data format, data safety and data content for practical preparation on products with smart device hardware

- **Delivery of cost analysis of bogus parts in Aviation market**
  Research on aviation data to visualize lost of values and material by use of bogus parts.

- **Delivery of hardware classification and recommendation**
  Research to update knowledge on RFID technological constrains applicable for aviation operation. Classify and filter hardware technologies usability for aviation industry.

- **Delivery of test descriptions and test results.**
  Definition of integrated lab trials, which will be followed by the development and implementation of real-world application trials that will demonstrate solutions in work
  ✓ investigate and conduct methods and procedures for smart hardware devices hardware installation
  ✓ conduct practical operational testing of smart device tagged specimen covering readability, repeatability, data security, hardware airworthiness(Airbus contribution to SToP 2006)

### 2.4. Introduction to RFID

In recent years automatic identification technologies have become more popular. The ubiquitous barcode labels that caused a revolution in auto identification technology have been becoming insufficient in many cases. The fact that they can not be programmed and have to be read from short distance as well as having low memory capacity caused industries to move toward a new technology-RFID- that can fill such gaps.

---

8 RFID stands for Radio Frequency Identification
2.4.1. What is RFID?

RFID system is an Automatic Identification and Data Capture (AIDC) system using radio waves to transmit information. RFID technology has great advantages to work over greater distances\(^9\), at great speeds and with relatively good storage capacity in comparison to other AIDC technologies. (e.g. Finkenzeller 2006)

A simple RFID tag provides tagged item with unique ID; its ability to communicate over distances reduces human involvement and respectively human errors and work loads. So each tagged item is able to announce its presence everywhere and every time that is needed. The ability to obtain some additional features like rewritable memory, security and environmental sensors (temperature, shock, humidity, pressure, vibration and altitude) intensifies its capabilities so in addition to presence, a tagged item can announce its location, source and happened events.

Where ever there is a need to mark, tack or trace an item, RFID is a good solution; today most common RFID applications are supply chain management and logistics, asset management, product authentication and process control.

2.4.2. RFID system components

A simple RFID system is formed of two main subsystems:

---

\(^9\) Some tags depends on radio frequency used in tag can be read several meters away even beyond the line of sight.
• RF subsystem is the hardware part of the system and is responsible to store and retrieve identification information using radio waves. The RF system includes two components RFID tags and RFID readers. A RFID tag is an electronic device-microchip-equipped with an RF antenna, containing unique identifier that is attached to a certain item. A RFID reader is a device that communicates wirelessly with RFID tag. RFID reader sends radio frequency signals to RFID tag and the tag picks up signals by its antenna and sends back unique identifier by backward signals and it is caused to identification of a tagged item.

![Wireless Communication](image)

**Figure 4**: RF subsystem (Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Philips 2007)

• Enterprise subsystem is a computer system that contains RFID software (device management, data management) and enterprise applications (business process management) to collect, analyze, and process data provided by RF subsystem. Enterprise subsystem makes the data attained from RF subsystem useful for business process management. (Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Philips 2007)

---

10 Also is called RFID transponders

11 Sometimes a RFID tag contains additional features like memory for additional data and environmental sensors
Figure 5: RFID system components
3. Methodology

This chapter describes the accomplishments of this thesis. First the methods used for collecting data and data sources are discussed. Further it contains the validity and reliability concepts of the thesis that is the reflection on the quality of chosen research methods.

3.1. Type of study

Based upon the purpose of the thesis to design a practical guideline for choosing an appropriate RFID system for anti-counterfeiting (in the aviation industry), and considering Creswell’s advices\(^\text{12}\), the qualitative study is recognized as the most appropriate method for collecting data. The qualitative method versus quantitative is primarily based on information gathering from personal interviews, observations and documentations.\(^\text{13}\) Qualitative study has more focused on gathering specific data to achieve a deep knowledge of the studied area. The goal of this method is to discover patterns which emerge after close observation, careful documentation, and thoughtful analysis of the research topic\(^\text{14}\). In this research the data collected from personal experiences (interviews and meetings) as well as reliable academic achievements form the foundation of the results and recommendations.

3.2. Research methods

The thesis work has been made in three steps. Since the aim of research is to design a practical guideline based on theoretical studies, both theoretical and empirical research approaches are followed during the work.

3.2.1. First step

In the first step the theoretical approach has been followed. The thesis started by intensive literature review and investigation in the scope of project. Different Books, recent scientific articles, reliable reports of previous researches and company files and reports have been reviewed to get information for constructing the foundation knowledge of critical concepts in the project.

3.2.2. Second step

The thesis work was proceeding by empirical research approach. After gaining enough theoretical knowledge about the problem, the practical part of thesis was started by working as an active member of SToP project group in Airbus. Performing the research in the Airbus facilitated the data collection process; Informal conversations with other employees, interviews and meetings have made a better understanding of problem scope.

Due to the undefined scope of counterfeiting problem in aviation industry, finding the accumulated and organized source of information is so difficult. So it is decided to collect some data by making interviews. Making structured and unstructured interviews with

---

\(^{12}\) Appendix A

\(^{13}\) Merriam (1994)

\(^{14}\) Dublin City University- School of Computing
professionals helped to get a better understanding of counterfeiting problem in aviation industry. Attending in relevant meetings is also a way for collecting information. Being involved in meetings, SToP project meetings and other official meetings, made the data collecting process faster.

In line and parallel with empirical work and data collecting process, three case studies were carried out; a case study is characterized by a deep investigation of a few subjects\(^{15}\). The interviews have been conducted in case studies.

- **Evaluate the counterfeiting problem in aviation industry**
  The first case study focuses on the scope of counterfeiting problem in aviation industry to emerge the need for countermeasure solutions. The case study has been done by use of interviews and internal Airbus documentations as well as available statistical reports about tampered parts in aviation industry.

- **Evaluate practical usage of RFID hardware, covering the operational area in aviation**
  The purpose of second case study was to enlighten the usage issues of RFID considering aviation requirements. This part has been done by reviewing Airbus internal documents and relevant articles.

- **Investigation and elaboration of applicable data security methods**
  The third case study was about investigation of security aspects of RFID. This case study has been performed by using documentation of earlier research projects (internal-Airbus and SToP or external) as well as reviewing relevant theoretical books and articles.

**3.2.3. Third step**

The last part focuses on conclusions and recommendations. This part is based on knowledge gained in theoretical and empirical research work. The data collected from empirical work was interpreted and analysed to make a reliable conclusions. A continuous study was going hand to hand with all steps; profound knowledge gained during the thesis was the base for conclusions.

**4 Validity and Reliability**

It is so important for a qualitative research work to be evaluated for its validity and reliability. Validity of study is the degree of correctness of the result; the correspondence of what research method was intended to measure and what currently measures. Different measuring instruments are used in this thesis, e.g. interviews, supervisions and literature review. These measuring instruments are able to measure the intended purpose. A continuous data verification process has been done during the thesis work; the purpose is to keep the quality of gathered data. This validation is carried out by iterative consulting with supervisors and interviewees.

\(^{15}\) Wiedersheim-Paul & Eriksson, 1991
Reliability of study is the degree of stability of the experimental result; repeating the experience within predefined bounds reproduces the same result. A reliable method is independent of the investigators and interviewees. For a reliable result of an interview the questions should be completely clear and organized to avoid misunderstanding, otherwise the answer to a same question could be different with different persons. Repeating questions in interviews, asking for more explanation, arranging structured interviews, asking attendance questions and overall trying to follow professional interviewing rules helped to reach high reliability in this thesis work.

Overall, in order to get a good result, first of all a pre-study about the current situation of RFID in aviation industry has been made. Then the data has been collected from those who had wide experience in the field of this study. Finally, based on the empirical data collection from Airbus and T-Systems in combination with theoretical work, the result has been reached. The result of this thesis can help making strategic decisions in the study area.
4. Part Authentication (Anti counterfeiting)

This chapter presents the scope of counterfeiting in aviation industry, such as its meaning, terms, dangers, points of presence and current countermeasures. And then will provide a solution in line with making use of potential of RFID technology to counter the problem of counterfeiting.

4.1. Counterfeiting

**Definition:** Counterfeiting is crime of manufacturing and distribution an unauthorized imitation of a genuine product to deceive the customer.

Counterfeiting has become a worldwide problem as it is one of the fastest growing industries. Like other industries technological developments leverage its rate of growth. Just in America, In addition to the elimination of more than 750,000 jobs, American businesses lose more than $200 billion in revenues every year (DNA technologies, The 21st Century Solution to Counterfeiting, Forgery & Diversion 2005). European Union Commissioner, László Kovács, in press conference held in 8 Feb 2005, points out that in 2003 alone, EU Customs seized about 100 million faked item which represents a 900 percent increase within four years; and even though these seizures are considered to correspond to more than 1 billion Euros. With tracking into account all counterfeiting activities all over the globe, it reaches up to five to eight percent of the total world trade, which is quite considerable and alerting.

“The global economy for illicit goods is massive, but by definition impossible to measure. What we do know is that it is getting bigger. The number of counterfeit items seized at EU borders has increased by more than 1000% rising from 10 million in 1998 to over 103 million in 2004” (Peter Mandelson, EU commissioner for External trade, at the EU-US summit in Vienna in 2006.)

The most prolific abuse is the counterfeited product at the item level, for example brand name apparel, electronics, pharmaceutical products aircraft part. (Figure 6) The growing counterfeiting industry pushes affected industries to find an adequate solution to save their industries investing new technologies like hologram, microware, Auto-Id and DNA based technologies.
One portion of above-mentioned figure is allocated for pharmaceutical industry; seemingly it has the least proportion but highest risk as it has been identified as a threat to the public health by Food and Drug administration (FDA). In 2004, the FDA reported 58 counterfeit drug cases, significant increase from the 30 cases in 2003. (FDA 2005) further more, In China it was estimated that in one year a total of 192,000 Chinese patients died from fake drugs while in Nigeria, almost 2,500 people were killed through injecting a supposed anti-meningitis drug during an international vaccination campaign. (Pearson 2006)

Another portion in black market that is very discussionable from commercial point of view is captured by consumer electronics and computer’s hardware. Peripheral electronics and replaceable computer devices are parts that manufacturer usually earns the highest margin for a system from them. Counterfeit peripherals can impact manufacturer’s profitability as well as the quality and operational performance of the system.

4.1.1. Counterfeiting in aviation industry

Nowadays you cannot imagine everyday life of the industrial society without the aircraft. A third of the world trade of industrial products, measured by its value, is carried out by aircraft. The tourism, as an important branch of industry, is increasingly dependent on air traffic as a shuttle for the passengers. And the development cooperation, as it is carried out these days, would hardly be conceivable without aircraft.
But unfortunately counterfeiting in aviation industry is not taken into account in Figure 6 and there is no reliable statistical data on hand about the share of this industry in black market. However the risk of counterfeiting in aviation industry is considerably higher than other industries and even small counterfeits cause large problems. Billion dollar damage occurs every year by bogus parts supply market and a high amount of documentation and documentation processing is required today to ensure that a part is genuine or not.

This risk and damage increases as aviation industry’s growing rate increases. According to Airbus prognosis the number of passenger aircrafts will be more than double in the next 20 years. Since the year 2000 the demand for an available amount of seats from new operators, partly low fare carriers, and due to the strong growth of the economic globalisation within the world economy has increased about 30%. According to Airbus this trend will continue, as the Asia-Pacific-Region grows on and up to the year 2025 will claim a third of the world market. The leader of the French department of aviation security warns about more aircraft incidents: "In the year of 2020 there is the danger of an aircraft incident ever week".

The subject of counterfeit parts (unapproved parts) concerns a branch of industry where valuable goods are deployed, containing the costs corresponding their quality. The serious price struggle within the aircraft sector leads however increasingly to the necessity for the aircraft companies to lower the costs within the maintenance and repair fields, the temptation to use "low-quality-parts" increases. It is already proved that such "low-quality-parts", that are spare parts, which do not fulfil the quality requirements of the manufacturers, were used. Even in "Air Force aircraft", the aircraft of the US-President, such parts were found. A few years ago a whole Italian dealer chain, which had specialised in selling such non-certified components, was busted.

During the last years Chinese companies of different industrial sectors have been blamed for non-compliance of copyright and property rights and it is to fear that Chinese companies increasingly will offer copies of certified original components".

Within such a complex product as an aircraft there are far more dangers than only the copy of components. As complex as an aircraft, is also the problem of the "unapproved parts". Despite of strict checks there have been so far two crashes in Europe which can be attributed to parts not airworthy\textsuperscript{16}.

There are special terms and definitions for condition of aeronautical parts defined by authorized organizations. Previous to find a solution for tampering aeronautical parts, the scope of problem, kinds of counterfeiting and definition of counterfeiting in aviation industry should be clarified.

\subsection*{4.2. Clarification of terms}

According Civil Aviation advisory publication (CAAP) 2002 and Civil Aviation Regulations (CAR) 1998:

\textsuperscript{16}Airworthy: Being in fit condition to fly
Approved Part: A part which is produced in accordance with the means outlined in Civil Aviation Regulations, maintained in accordance with the applicable regulations, and meets applicable design standards is called Approved part. Approved parts are identified as parts which have met applicable regulations, standardizations and specifications of authorized organizations.

Counterfeit Part: A part made or modified so as to imitate or resemble an ‘approved part’ without authority or right, and with the intent to mislead or defraud by passing the imitation as original or genuine.

Suspected Unapproved Part (SUP): A part, component, or material that is suspected of not meeting the requirements of an approved part; a part, for any reason, may not be ‘approved’. Reasons may include findings such as a different finish, size, colour, falsified or altered identification, incomplete or altered paperwork and poor material standard.

Unapproved Part: A part that does not meet the requirements of an ‘approved part’. This term also includes parts which have been improperly returned to service (contrary to the applicable regulations) and/or parts which may fall under one or more of the following categories:

1. Parts shipped directly to the user by a manufacturer, supplier, or distributor, where the parts were not produced under the authority of, and in accordance with a production approval issued by an NAA (National Airworthiness Authority) for the part. For example, production overruns where the parts did not pass through an approved quality system.

2. New parts which have passed through a PAH’s (Production approval Holder) quality system which are found not to conform to the approved design data.

3. Parts that have been maintained, modified, overhauled, or approved for return to service by persons or facilities not authorized to carry out such services under regulations of an NAA.

The following parts, while they do not comply with the regulations, are not intended to be investigated under the SUP program:

• An approved part which is used in the wrong application
• A part manufactured or maintained by an approved source which is determined to depart from the type design, i.e. part which departs or escapes from the manufacturing or maintenance facility’s quality system

These parts may be considered as Defect parts.

This includes parts shipped to an end user by a Production Approval Holder supplier who does not have direct ship authority from the PAH.
4. Parts that have been maintained, modified, overhauled, or approved for return to service which are subsequently found not to conform to approved/acceptable data\textsuperscript{19}.

5. Counterfeit parts.” (Detecting and Reporting Suspected Unapproved parts 2002)

Due to the similarity of unapproved parts’ characteristics to those of approved parts, immediate identification of unapproved parts is often difficult. The international official language of civil aviation authorities (CAAs) has agreed to use “Suspected Unapproved Parts” phrase for counterfeited or unapproved parts because of their unknown statues or insufficient information at the time of discovery.

4.3. SUPs’ points of presence, Points of counterfeiting in Aircraft part’s lifecycle

To combat with SUPs in aircraft lifecycle, first, potential points of presence should be found, where we have to look for SUPs?

Finding potential places where SUPs find their way to aircraft lifecycle requires taking into account the complete aircraft life cycle, from Design and Production, through its operational period, and into maintenance, repair and replacement of parts with newer equipment. The brief aircraft life cycle includes Design, Production, Operation, and MRO (Maintenance, Repair, and Overhaul) phases.

There are limited numbers of aircraft manufacturers responsible for design and production of aircrafts worldwide; the significant part of civil aircraft market is shared by Boeing and Airbus. All part suppliers for these companies are under intensive inspection to follow applicable regulation and standardization defined by NAAs, though the problem of SUPs in design and production phases is almost not applicable and it is granted that a new aircraft fresh out of manufacturer is completely safe and airworthy. The problem reveals when an aircraft comes to operation and maintenance phase.

It is hard to get a satisfying answer if you want to estimate the damages for the firms confronted with SUP's. Basically all firms which collaborate on aircraft are affected including manufacturers, dealers, service and maintenance companies, airlines, suppliers, customers and the aircraft producers themselves.

\textsuperscript{19} (a) This would include parts produced by an owner/operator for the purpose of maintaining or modifying their own product, which have been approved for return to service, and found not to conform to approved data.

(b) This does not include parts currently in the inspection or repair process, such as parts removed for maintenance. Parts in this status may be considered not acceptable for installation.
Often, it is service and maintenance companies confronted with the matter of SUP's, as they must, owing to an extreme pressure of competition, put up with the strain of hard financial and time wise pressure. The airlines and so the aircraft producers carry the consequential loss. Aspects as security, quality and product liability have priority for the aircraft producers and can leave serious damage to their image when an accident happens.

4.3.1. Source of SUPs in MRO phase

The longest phases of aircraft lifecycle are operation and MRO. The product aircraft has operation life of 20 to 40 years if its appliances and parts are serviced, repaired or changed in fixed intervals. Indeed an aircraft requires maintenance and support for decades. The possibility of replacing or adding a SUP starts in the first maintenance station of the aircraft life and it increases as aircraft sees more maintenance stations. Following is the source of SUPs in MRO phase.

The range of the SUP's is large, and different kinds of SUP's could be used in MRO phase.

- **Parts without documents:**
  Documents are important to prove the origin of a part. An airworthiness certificate is a confirmation that the part is produced and serviced according to the specifications. A part may not be used without accompanying documents.

- **Unauthorized parts:**
  Parts, which are not qualified to be installed in aircraft are considered as parts without authorization and may not be used in aircraft. It is possible that conventional components with equal or rather similar measurements are produced by mistake or ignorance. Apart from mistake and ignorance is resolution, producing components without authorization with forged documents by purpose of counterfeiting. Furthermore parts lose their authorization if they are not kept in good condition according to maintenance documents. This can happen during overhaul or service activities for example by false treatment or refinement.

- **Parts from overproduction:**
  The overproduced parts are kept in the stock and are sent; these parts can be stolen easily. These parts do not fulfil the airworthiness requirements as they have not been tested and hence have no documents.
• **Parts from Scraped aircrafts:**
Visible defects can often be corrected with simple means, as for example a conventional numeric controlled machine. With faked accompanying documents you cannot recognize the part is a scrap part and so it is an enormous security risk on the market. Particularly closed down or crashed planes are cannibalized and their parts are reused.

• **Parts which should not be deployed any more:**
All parts of an aircraft have a limited lifecycle. Depending on purpose the life time can be longer or shorter. When the life time has expired the danger is that some parts are not airworthy anymore and can fail. In the overhaul station these parts are replaced with new parts and are thrown away. It can happen that these parts get cosmetic corrections and/or faked documents (shorter operating hours declared) and so enters once more to operation cycle.

• **Changed parts:**
Originally approved parts, which were changed by somebody not authorized.

• **Forged parts:**
Forged parts are mostly made out of inferior material deviating from the definition and are substandard spare parts. Simple production processes, not accomplished tests and forged documents are properties of forged parts. These are mostly visually perfect and cheaper that genuine parts. The great resemblance of the forged parts to the original parts makes clear identification difficult, if not impossible. The identification of all parts is possible in time and with expensive test procedures but when the part arrives shortly before it is used; it is even for an experienced mechanic almost impossible to recognize if the part is an original.

• **Parts from military aircraft:**
Parts from military production have other standards and rules as parts for the civilian air traffic. Military surplus parts (defined as parts which have been originally released as surplus by the military, even if subsequently resold by manufacturers, owners/operators, maintenance organizations, or any other suppliers of parts) may not qualified to be used in civil aircrafts. Because of this one must be very cautious to use parts from military production into civilian aircraft.
Table 1: Mechanism of illicit trade, Aviation industry (SToP)

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Significance in aerospace industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-quality fakes</td>
<td>Repairable parts upgraded by use of polished scrapped parts</td>
</tr>
<tr>
<td>Forgery of overt and covert security features</td>
<td>Falsifying of airworthiness certification documents</td>
</tr>
<tr>
<td>Non-perceptive counterfeiting</td>
<td>Minor or not applicable</td>
</tr>
<tr>
<td>Low-quality fakes</td>
<td>Probability in bulk production e.g. bolts, screws, nuts, sheet metal etc.</td>
</tr>
<tr>
<td>Perceptive counterfeiting</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Parallel trade / Product diversion</td>
<td>Minor or not applicable</td>
</tr>
<tr>
<td>Theft</td>
<td>Desirable but not frequently</td>
</tr>
<tr>
<td>Factory overrun</td>
<td>Minor or not applicable</td>
</tr>
</tbody>
</table>

4.4. **Dangers (risks) and examples from the past**

Observations in the near past shows that the organized criminality has always accompanied the aircraft industry.

Up to 80% of the aircraft accidents are based on human errors and are therefore the most frequent reason for aircraft accidents. Not only the crew but also the flight controllers, the maintenance personnel and the managers of airlines belong to the "human errors". Among all these details the amount of "unapproved parts", built into an aircraft, is not given. For these components there are no official figures; however unofficial estimates talk about 10% of unapproved (not certified) components in an aircraft.

The Italian company "Panavigation" was supposed to have supplied firms all over the world with unauthorized manipulated aircraft parts or rather parts with forged documents. After the firm was blown with its deals, civil servants found over 40,000 aircraft parts that had not been stored according to prevailing storage instructions. Next to parts fit for the scrapheap a small
metal workshop was found where parts were being polished. Panaviation could not draw up airworthiness certificates for the parts, as it was not an approved maintenance company. That is why Panaviation kept the origin of the polished parts (for example from crashed aircraft) and let a specialized company draw up the certificates. Computer prints of the customer lists of Panaviation prove that even many renowned airline companies as Austrian Airlines or Lufthansa have bought spare parts from Panaviation. All together there are hints of over 50 airlines and hundreds of maintenance companies.

The danger of the SUPs is clear with this example as even airlines, maintenance companies and aircraft producers cannot identify the SUPs. The second danger is that there are no laws and applications against spare part brokers in Europe. Perpetrators, who end up in court, mostly get a base small sentence of punishment. The sentences are mostly smaller than those for drug dealers, and so there are criminals who have changed from the drug scene to the "aircraft line of business".

To own and to sell aircraft parts you do not need a state authorization or licence and you do not need any training. As you see, anybody can deal with aircraft parts because the admission barriers are low and the competitors mostly more expensive. Apart from the danger that spare part brokers deliberately sell SUPs, the costs are also a danger for the finding of SUPs. As an example we can take Lufthansa, who could not understand any more which parts were suspicious and which not, after they had learnt about the case of Panaviation. The German Federal Airworthiness Authority in Braunschweig (LBA) obliged Lufthansa to change all the suspected parts in 150 engines, but the question is how Lufthansa has to recognize this parts and how much money and time this recognition process costs.

The extent dimension of the built in SUPs can immediately, but as well years later have devastating consequences. The dangers are not calculable, because once brought in SUPs into the logistic system of airlines, maintenance companies or producers are difficult to identify. Faulty parts are extremely dangerous if they are nonetheless built into an aircraft. Anytime a disaster can happen, as the following examples show.

Investigators found in the USA a compressor disc from a jet engine, which is used in the DC-9 /MD 80 commercial jet airplanes series. The compressor disc had two documents, one original document and one forged document. The forged one showed that the part is overhauled by the Spanish Iberia and is ready to be used. But the original document showed that the part is worn-out, outside of the permissible tolerance and really fit for the scrap heap.

1995 a compressor disc broke in the engine of a fully occupied MD-80 of the low-cost airline ValuJet. The aircraft taxied just to start in Atlanta and was fortunately not yet air-borne. The parts hit, sped up to 30,000 revs per minute, with the force of shell fire (splinter) through the passenger cabin and injured seven people seriously. The aircraft caught fire and the passengers saved themselves over the emergency slides. If this had happened in the air, there would be a catastrophe.

In the second example the passengers didn’t have any luck. A Convair 580 from Partnair was on its way from Oslo to Hamburg in September 1989, as the machine disappeared from the
radar and fell into the sea. On board were two pilots, one stewardess, one mechanic and about 50 passengers. How could this accident happen and which part did the SUP role?

The crash was caused by the support of the auxiliary power unit (APU) in the aircraft tail, which did not fulfill the specifications of the producer. The faulty support, which let the APU have a loose stand, produced un-damped vibrations, which put the whole aircraft fuselage in vibration. In addition to the faulty support, the bolts and their cases which connect the vertical stabilizer to the fuselage were not original parts. Due to the heavy vibrations these bolts finally broke and the empennage broke off. The aircraft disappeared in the height of about 6000 to 7000 meter from the radar and crashed. The charter company, Partnair, went out of business, and the origin of the parts was never determined.

4.5. Current countermeasure for SUPs problem

The Aviation industry has been threatened by SUPs since its birth. This threat increases as the market increases. In the past decade, aviation industry suffered more with SUPs and consequently gets more serious to combat unapproved aircraft parts and those individuals who profit form their manufacture and/or sale. On November 15, 1995, the Suspected Unapproved Parts (SUP) Program Office (AVR-20) opened in FAA\(^\text{20}\). This office was responsible for promoting a cohesive, consistent, aggressive approach to SUPs to identify unapproved parts and remove them from the aviation system. The program included the investigative process of SUPs and detailed definition of airworthiness and SUPs. This office shut down in July 2007 and the office’s responsibilities were realigned to the Flight Standards Service (AFS) and the Aircraft Certification Service (AIR) of FAA. (Scalone 2001)

According FAA program for SUPs, there are specially trained inspectors who are responsible to inspect suspected parts. The inspection starts just when a notification about suspected part is received from every component in aviation industry. Special report forms for SUPs and hotlines are available for all organizations and individuals to make notification easily.

A notification about SUPs is a trigger for inspection; as long as there is no SUP report there is no investigation and processing of Sup reports. There are many people including parts’ suppliers, distributors, owners/operators who are not enough aware of the importance of installing only approved parts and consequently importance of investigating and reporting SUPs to responsible agencies. Furthermore with today's competition in the aircraft industry there are signs that the airlines are not very keen to report SUPs to the authorities. Parts with flaws, which are reported to the authorities are taken away without reimbursement of expenses. So it is conceivable that the airlines recycle the parts and so get their purchase price back.

Succeeding of this program depends on increasing of public awareness of SUPs and taken better policies and operation guarantee. In the other word the entire industry must continuously be proactive in identifying and removing SUPs. But how the integration of an industry could be guaranteed?

\(^{20}\) Federal Aviation Administration
In case that people do understand the importance of reporting SUPs, it is not easy for them to recognize a part as a SUP because of lack of immediate and accurate data about part. Being realistic, with current countermeasure, there is still considerable risk of SPUs in aircraft threatened aircraft safety.

4.6. Future Solution (electronic authentication of aircraft parts, SToP project)

Because of the inherent danger of unapproved aircraft parts, more force is needed to keep them out of the system and off the aircraft. Additionally, we must stop those individuals who attempt to profit from the intentional manufacture and/or sale of unapproved parts. Their priorities are not safety first.

As mentioned above, lack of accurate and immediate data in addition to absence of industry and document integration makes the current countermeasure insufficient. The truth is that the handling of airplane parts over the years without aiding new technologies is impossible.

Solution:” Using RFID technology to establish an electronic pedigree to secure the aircraft parts against SUPs problem”

RFID technology can provide automate accurate and immediate data of a part and in combination with ERP guarantees the intensive integration of industry. Item level tagging provides aircraft parts with embedded electronic security markers that are automatically read in parts lifecycle. An electronic security marker is a unique data code that, by itself or in conjunction with a network, can distinguish the product as genuine. This marker is unique for each part and cannot be easily altered, providing an enhanced level of security. Also the ability of RFID tag to store some crucial historical data of part in its memory makes the authentication process easier; it is easy to find the information about originality of a tagged part and in the case of suspicion, data on tag as a pointer to data in ERP leads the workers to find more information about the part. This electronic pedigree Coupled with the paper pedigree system to fill in the authentication gaps can grant 100% reliable authentication process. Therefore, by tagging parts, there is sufficient information about the part, and then no need for using SUP term, because the part has just only statues : approved or unapproved.

With implementing electronic pedigree solution, tampering parts’ documents demands considerable effort. To tamper a part, part documents should also be tampered. Imitation of electronic documents with some security features is not as easy as paper documents. And furthermore one has to change electronic data on tag, as well as data on the ERP and paper documents. Complexity and difficulty of process decreases the motivation to tamper.

Electronic authentication can be effective with the active participation of manufacturers and suppliers, maintenance stations and airlines. The participation of all trading partners at this early stage is encouraged and will lead to the migration to a robust electronic pedigree system as design features can be piloted at the same time that improved protection of the aviation supply is being realized. Implementing a fully operational RFID track and trace system in aviation industry needs initial requirements that would be analyzed in next chapters.
4.6.1. **Approach 1: (master-slave, active-passive RFID tagging)**

Tagging subparts of a main critical part of an aircraft with passive tags (slave tags) and equipping the main part by an active tag (master tag) during aircraft production phase, could be a solution to insure that authenticate subparts are used with the host part during maintenance phase. Usually a main part has longest lifecycle than its subparts; and when some parts is being changed because of mal-functionality or expiration with new parts, an RFID reader chip built into aircraft equipment will read new subpart tag as they are connected. And then the host processor authenticates that genuine parts are installed or not.

![Master Tag-main part](image)

![Slave Tags- Subparts](image)

**Figure 8: aircraft engine master-slave tagging**

4.6.2. **Approach 2 (Passive RFID tagging)**

Equipping parts by passive RFID tags to the certain level during production phase and equipping MRO workers with a reader and handheld could be the other solution for authenticating parts during their lifecycle. The part manufacturer writes initial and birth data on tag and additional data would be added updated in each MRO stop during the part lifecycle. The data on tag is readable/writable with a reader connected to a mobile handheld. As the handheld connects to ERP’s database the data would be synchronized. The data on tag is master data. This model insures the track ability
and tractability of parts. The tag would include a digital signature that would be authenticated directly by RFID readers prior to being operated. In addition, MRO technicians can have access to some historical data useful for part configuration.

Advantages of tagging aircraft parts by RFID:

- Aircraft safety
- Automatic calibration
- Automatic authentication
- Difficulty of data mitigation
- Set up information in various aircraft equipments
  (For example whole story of engine in its lifecycle could be found)
4.6.3. **RFID (on which parts)**

**Deciding which items should be tagged:**

First step to implement the above-mentioned solution is tagging parts by RFID, but the question is which tens of thousands of parts on an aircraft should be tagged. The most important factors for deciding which parts should be tagged include:

- the cost of a part
- a part's criticality in aircraft operations, and
- The relative ease of a part's repair and/or replacement.
- The genus of part (because of the high metal content of aircraft, plastic and other composite parts in the cabin will be easier to tag.)

**LRUs**

Closed groups of aviation parts which during the lifecycle of an aircraft have to be replaced are called Line Replaceable Units (LRU). Computers, electronic appliances as well as doors and flaps belong to the group of LRUs. The aviation industry has the vision to start solving SUPs problem on the level of LRU. Tagging removable parts and critical parts that have short life-cycles and are more in danger, such as the plane's brakes, which typically must be overhauled after every 1,000 landings. The question is why especially LRU's are endangered.

Generally it is regarded that all components are affected and can as SUPs be brought into circulation, but especially components with a certain financial effort or a longer order time, are more frequently affected. Airlines with an old fleet or with some old aircraft models must sometimes fight for spare parts, as they are no longer produced or the price is relatively high. The old Airbus A300B is out of production but there are still airlines, which use this type of aircraft. The consequence is that the aircraft gets older and need appropriate spare parts. It gets more difficult obtaining them and the prices for the spare parts rise as well. In Europe and the USA you seldom find old fleet but there are countries next which are affected. Especially countries where the industry grows fast and the age of the fleet is high are endangered.

As an example we can name Russia after the fall of the Soviet Union, whose former state airline Aeroflot had very old machines. Aeroflot had divided up into smaller companies, which had taken over the partly more than 25 years old aircraft. The spare parts industry could not cope with the demand and so other aircraft were cannibalised, that is for example that two damaged aircraft were taken apart to keep a third one in working order. This "cannibalising-cycle" of the own fleet caused already several aircraft accidents and holds the danger that there are still SUP's in some machines in Russia. The Russian, who have tried hard in later times to spread out the feeling of security in their aircraft industry, could be followed for example by the Chinese. So the LRU’s hide the biggest danger to be affected and the goal of the industry is to have an electronic pedigree for each LRU that documents its origin and its lifecycle.
Figure 10: Lifecycle of an LRU (Jens Muller-SToP)
5. Regulations and Standards of RFID for Aviation Industry

Following airworthiness regulations is a must for each part in aircraft; RFID affixed to an aircraft part also needs to follow respective airworthiness regulations; which is briefly presented in this chapter. Standardization concept, types of RFID standards and some standardization organization especially for RFID and aviation industry are introduced. This chapter concludes standardization discussion with proposing an application standard for RFID in whole aviation industry.

5.1. General overview

Implementing RFID in Aviation industry needs more challenge than others. Because of high risk of failure: Risk = Probability × Consequences of harm

Consequence of harm in a failure/crash of an aircraft is a matter of life or death. Then even with low probability, risk is really high. And even if probability tends towards zero and risk gets closer and closer to zero, it is still considerable. If and only if probability approaches zero the value of risk would be zero. Therefore, there are always more inspections, regulations, standardization for each part of aircraft\(^{21}\) to approach zero probability of risk for aircraft. Consequently, implementing RFID in board of aircraft means meeting all requirements of responsible agencies\(^{22}\) certifying aircraft parts and approving their safety in aircraft.

To implement the RFID technology as a solution for combat with SUPs and Before Airbus can use tags on airplane parts for planes flown internationally, however, it needs to get approval from other regulatory agencies around the world. Such mandatory regulations and standardizations delimitate circle of options and force us to consider some technical requirements which a tag has to meet before be used in aircraft. Following presents the boundaries that such rules built and consequently provides the list of requirements for an RFID tag in aviation industry.

5.2. Airworthiness

An Aircraft must be airworthy and each part on and in the aircraft must be in accordance with airworthiness regulations. Airworthiness is a term to dictate whether an aircraft is worthy of safe flight. To be in a condition for safe flight, all parts, one by one, must operate and also cooperate with other parts in a 100% safe and proper way, in other words the necessary and sufficient condition for airworthiness of an aircraft is using all airworthy parts. It is a must that each aircraft obtains its airworthiness certificate before first flight from the responsible agencies. Each country has its own aviation authority\(^{23}\) basically with its own regulation but

\(^{21}\) Even small parts like bolts and screws have to follow standardization rules to be applicable in aircraft.

\(^{22}\) FAA, EASA, CAA$s$, ATA…

\(^{23}\) national aviation safety agencies; The most leading aviation safety agencies are:

FAA, Federal Aviation Administration is responsible to authorize operation of an aircraft in United States airspace.

EASA, European Aviation Safety Agency is the centrepiece of the European Union’s strategy for aviation safety. Its mission is to promote the highest common standards of safety and environmental protection in civil aviation for all European national aviation safety agencies. This Agency is also responsible for type-certification, i.e. the
usually harmonized in mutual acknowledgment agreements between all countries around world.

5.2.1. RFID and Airworthiness Procedure

Parts before being used as a part of an airworthy aircraft are certified and authenticated by a program of authorized inspectors. RFID also as a part of aircraft must meet some technical requirements to be certified in accordance with airworthiness standards.

Airworthiness criteria for RF devices is defined by RTCA\textsuperscript{24}; RTCA criteria describe the required resistance of any equipment installed on aircrafts to vibration, power input, radio frequency susceptibility\textsuperscript{25}, lightning, and electrostatic discharge. The airworthiness procedure for RFID tag includes:

1. Testing the environmental conditions according to RTCA, document DO-160E
   All tags attached to aircraft parts should meet the RTCA DO 160 airworthiness criteria about environmental conditions and test procedures for airborne equipment\textsuperscript{26}. (RTCA, DO-160E, Environmental Conditions and Test Procedure for Airborne Equipment. 2004)

2. Software (if applicable) DO-178B, Software Considerations in Airborne Systems and Equipment Certification. DO-178B provides guidance for determining, in a consistent manner and with an acceptable level of confidence that the software aspects of airborne systems and equipment comply with airworthiness requirements\textsuperscript{27}. (RTCA, DO-178B, Environmental Conditions and Test Procedure for Airborne Equipment. 2004)

Furthermore, to bring an airworthy tag on the board of aircraft modification document is required; documentation that dictates the kind of modification must be followed for installation the RFID tag within the aircraft for example which kind of glue is needed, where in the part it must be glued and etc. These documents are foundation of an aircraft design, production and modification.

\textsuperscript{24} Radio Technical Commission for Aeronautics
\textsuperscript{25} There are many RF devices in board of aircraft (Navigation Systems ……); RFID devices must work in a manner that would not interfere with such equipment on the airplane necessary for continued safe flight
\textsuperscript{26} RTCA, DO-160E, Environmental Conditions and Test Procedure for Airborne Equipment. 2004
\textsuperscript{27} RTCA, DO-178B, Environmental Conditions and Test Procedure for Airborne Equipment. 2004
In addition to above-mentioned items, RFID tags should be able to sustain in high temperature, function properly in metal, contact with chemical liquids and increased humidity to be proper to install in an aircraft part.

To help identifying which RFID tag technology could be used without exposing safety of aircraft, FAA has released a memo\textsuperscript{28} according to airworthiness criteria and based on examination/test of the current RFID technology for “passive-only” tags in Boeing and FedEx airplanes. Saying that there is no safety risk to use passive RFID tags in aircraft, under the following conditions:

A unit used to express relative difference in power or intensity, usually between two acoustic or electric signals, equal to ten times the common logarithm of the ratio of the two levels.

- “The tags must operate in the "passive-only" mode.

- The RFID devices must not radiate (back-scatter) characteristics with harmonics below a level of 35 dBuV/m\textsuperscript{29}. This is to make sure that the tags don't pick up energy emitted by the engines or other devices, reflect it back and possibly interfere with aircraft systems\textsuperscript{30}.

- The frequency used by the tags needs to be outside the published aviation frequency bands to prevent interference with aircraft systems.(The most common RFID frequencies—2.45 MHz, 915 MHz and 13.56 MHz—do not overlap with any frequencies used in aviation and are acceptable for tagging parts.)

- The generation of harmonic frequencies from the RFID tags will be maintained such that the fundamental through the 4th harmonic frequencies do not impinge upon any assigned aviation communication or navigation frequency

- The use of passive-only devices is restricted to ground operations only, i.e., aircraft not-in-motion, where the intended interrogation of any passive RFID device is not conducted while the aircraft is positioned on an active taxiway or runway

- The RFID devices must meet the requirements of Federal Aviation Regulations\textsuperscript{31} for example each item of installed equipment must--function properly when installed.

- The passive-only RFID devices must be of high integrity, i.e., be designed to operate in an aircraft operational environment with robust radio frequency stability.” (Policy for Passive-Only Radio Frequency Identification (RFID) Devices 2005)

\textsuperscript{28} FAA policy memorandum for “Passive-Only” RFID devices
\textsuperscript{29} dBuV = decibel ratio of Volts to one microvolt
  
  dBuV/m = decibel ratio referenced to a microvolt per meter = Field Strength
\textsuperscript{30} It is established in RTCA/DO-160, Section 21, Category M for radiated interference to ensure tag harmonics are less than 35 dBuV/m
\textsuperscript{31} Federal Aviation Regulations 23, 25, 27, and 29.1301
The FAA has not yet cleared RFID policy for applications in flight because of concerns that its signals could interfere with avionics. The FAA RFID team's next step will be to develop guidelines for the use of active and battery-assisted RFID devices on aircraft. It was expected that research and studies to implement a guideline for these devices would be completed by early 2006, but there is just a certification for one type of active RFID tag for use on a limited number of aircraft types.

Kortenburg Master Tag is the first airworthy tag that certified by LBA\textsuperscript{32} and Airbus is considering using and testing it in the Canadian MRTT / Polaris project mentioned in section 2.3.1.

\section*{5.3. Standardization}

\textbf{Definition:} “Standardization is the process of establishing by common agreement engineering criteria, terms, principles, practices, materials, items, processes, and equipment parts and components”. (McGraw-Hill 2003) A Standard is an outcome published document that sets out specifications and procedures designed to ensure that a material, product, method, or service meets its purpose and consistently performs to its intended use. (IEEE\textsuperscript{33} Standards Association)

In today’s networked world, the initiative factor of success in a globally used product is interoperability; standardization means set up universally agreed set of guidelines for interoperability. Standards usually are used voluntarily unless safety concerns exist. In such cases standards can be released as regulations.

All components of aviation industry have to follow standards issued by official standardization organizations\textsuperscript{34}. Following such standards is a prerequisite for survive in the chain. So standards in aviation industry are more imposed through regulation.

In RFID concept, standardization refers to approaches for increasing commonality of a part, process and information. Non-standard RFID does not make sense at all. The main usability of RFID is providing a product with a unique code, and what does unique mean if there is no unique universal coding system for RFID; So RFID and standardization are two inseparable concepts.

\subsection*{5.3.1. Types of Standards for RFID}

There are four main types of standards for RFID technology (Harmon 2007)

\textsuperscript{32} LBA (Luftfahrt-Bundes-Amts) is German Aviation Authority that on its own responsibility or in supports of the EASA responsible for airworthiness certificate actions

\textsuperscript{33} Institute of Electrical and Electronics Engineers

\texttt{http://standards.ieee.org/stdsdev/index.html}

\textsuperscript{34} ATA, ISO, IEC...
• **Technology standards**
  Standards for technical features of RFID including air interface communications format and data exchange protocol to ensure the compatible technique of tag-reader communication

• **Data Standards**
  Standards for data structure and format in RFID tag to ensure compatible data transmission

• **Conformance Standards**
  Standards for qualification and verification of RFID device design and manufacturing to ensure the conformity with a standard including Proposed guidelines for the qualification of design and manufacture and Test Specifications

• **Application Standards**
  Standards for usability of RFID tag in a certain application\(^{35}\) to ensure the compatibility of used systems by anyone involved in the application; application standards may include technical, data, and conformance standards.

5.3.2. **Standard organizations for RFID**

Error! Reference source not found. Appendix B illustrates all standard organizations for RFID; the main standard organizations in this case for aviation industry are ISO/IEC\(^{36}\), GS1, EPCglobal and the most important one, ATA\(^{37}\), that is especially developing standards for RFID in aviation industry. ISO/IEC is more active in developing technology standards. GS1/EPCglobal is developing standards for supply chain management applications including asset management and counterfeiting applications. ATA is industry level standard organization which develops standards for applications applicable in aviation industry.

**GS1 (Global Specification No.1)**

GS1 is a national and industrial level standard organization and its main activity is the development of the GS1 System, a series of standards designed to improve supply chain management by providing efficiency and visibility of chain. The GS1 System is an integrated system of global standards that provides for accurate identification and communication of information regarding products, assets, services and locations. (GS1 n.d.)

**GS1/EPCglobal**

EPCglobal is one of the key product areas of GS1 system offering industrial driven global standards for EPC\(^{38}\)/ RFID technologies to enable immediate, accurate and automatic identification and tracking of an item through the whole supply chain to increase supply chain effectiveness. EPCglobal network consists of EPC code, EPC tag and reader, EPC discovery

---

\(^{35}\) Freight container, Ship Label, Product Package, Product Mark/Tag, e-Seal, e-Authentication

\(^{36}\) Joint technical committee of International Organization for Standardization (ISO) and International Electro-technical Commission (IEC), IEC is more active in providing technology standards for RFID (Appendix …)

\(^{37}\) Air Transport Association of America (Industry level standard organization)

\(^{38}\) Electronic Product Code
service (Object Name Service (ONS), EPC Information Services (EPCIS)). Defining standards facilitates data sharing of electronic product code related information within and between industries i.e. events of RFID readers and product information of tagged products.

EPC Code is an identification schema for EPC tag that provides a tagged object with unique electronic identification code. EPC Code is a bridge between an object and its relevant information in ERP. To enable unique identification, EPC Code has four main elements: header, EPC manager number, object class, and serial number of the object.39

Figure 11: EPC Code schema

EPCglobal has developed standards for different tag classes and readers. It provides a list of different options for user to choose the tag that fits with expected functionality and cost. In addition, by availability of standard tags and readers, user has more options of suppliers.

EPC discovery services (i.e. ONS, EPCIS) are offering services to simplify the data exchange process. EPC discovery services consist of a database and a set of web service interfaces that if are connected to internet can be invoked by any authorized computer in the internet. Object Name Service is based on Domain Name Service (DNS) idea for the internet. In the EPCglobal network, ONS encodes a EPCCode to an Internet Protocol (IP) address and uses the existing DNS infrastructure to retrieve all EPCIS that store the information refered to a EPC Code embeded in the respective RFID tag. EPCIS is the event information of a tagged object stored in EPCIS servers. (EPCglobal n.d.)

39 Appendix....
ATA

ATA is the Air Transport Association of America, the first and only trade organization for the major U.S. airlines. ATA performs a variety of services for its members, including promotion of the industry, and the safety, cost-effectiveness and technological advancement of its operations. The ATA initiated 20 years ago ATA Aviation Marketplace as a means of standardizing the exchange of parts pricing availability information between original equipment manufacturers (OEMs), suppliers and major airlines, known as a spec2000. It has since evolved to E-commerce standards, File Standards, Traceability Standards for worldwide aviation industry. So, ATA is pointed as an industry-level standard organization for RFID. The technical aspects of spec 2000 are established and maintained by the spec 2000 International Coordinating Group, consisting of representatives from the major airline, manufacturer, supplier and repair associations from around the world. (ATA-Spec2000 n.d.) (Air Transport Association of America n.d.)

40 http://www.epcglobalinc.org/standards/
Spec2000, chapter 9 (Traceability Standards)
ATA Spec 2000 Chapter 9, AIDC (Automatic Identification and Data Capture) is a data standard and an e-business standard, contains industrial guidelines for aircraft parts traceability. AIDC includes standards such as bar-coding, 2D Data Matrix and RFID, which are used to mark and identify products and/or store information which can be read in an automated manner. The model for this specification was the license plate concept for automobile registration. License plates are simply pointers to a database of unlimited fields of tracked information. Similarly, the part number and serial number uniquely identify aircraft parts and become the pointer. Chapter 9 has recently added a section which helps companies determine what steps and data are necessary to allow cradle-to-grave parts traceability. This is not yet a "data exchange" standard. (Traceability Standards 2002)

What is a CAGE Code?
A CAGE Code (Commercial and Government Entity) is a five-position alphanumeric code that identifies U.S. companies doing business with the U.S. government. The NSCM Code (NATO Supply Code for Manufacturers) is the corresponding code for non-U.S. companies. Spec 2000 has adopted the CAGE/NSCM codes as a standardized way to identify Spec 2000 users. In Spec 2000, CAGE/NSCM Codes are used to identify Manufacturers, Suppliers and Repair Agencies. Both CAGE and NSCM codes are assigned by the Defense Logistics Services Center (DLSC). Consequently, a part should be uniquely identified using MFR (CAG/NSCM) +SER Nr., this information must be static and marked on the part once, at the beginning of its lifecycle, and not change even after, so that the part can be traced effectively throughout its lifecycle.

RFID on aircraft parts specification
The RFID project team (RFID on parts) in ATA e-business program is working on developing RFID application standards for whole aviation industry (i.e. data standards and technology standards). ATA specifications are base on ISO/IEC and EPCglobal standards. Anti-counterfeiting and part authentication applications need more RFID memory. So, project team RFID on parts has prepared High Memory RFID (64 Kbit RFID tag) Specification; it is specification of part identity and other information on hi-memory RFID tags. This follows the identified data format, permanent bar code parts identification, for a universal serial Nr that provides “social security number” (Figure 14) to uniquely identify of the part throughout its lifecycle.

---

lifecycle. The 64 bit memory is designed to hold information that is needed according RFID applications in aviation industry.

![Graphical Memory Description](image)

**Figure 15: memory description of high memory RFID** (Polkinghorne 2007)

Current data record contains some information about the part that currently is important but can change over time. Mechanic comment area is open for mechanics to write helpful information for the next mechanic installing, removing or diagnosing the component. With some security features this block can help in authentication process. Part history record contains information about important maintenance events, for example if a modification is done against the component it will be recorded in part history blocks. These history records enable different components in aviation industry to track the maintenance and repair history of parts using AIDC coded parts. (Polkinghorne 2007)

5.4. Adhering to a standard

To realize the deployment of part-level (LRU level) tagging through the aviation supply chain for authentication application, as a first step all components involved in a parts’ lifecycle including aircraft manufacturers, airlines, MRO centers, GEMs and other aviation must stick on universal rules, specifications and methods of deployment to ensure the safety and
commonality. Within the aviation industry, collective standards provide an accurate, easy and inexpensive method of data entry and data storage for the tracking and traceability of aircraft parts. Also an intelligence-based and network oriented RFID system that will be used across multiple components of aviation industry should contain standard identifier format; using a standard identifier format makes it easier to decode identifiers in the tag. When a reader reads a standard identifier, it can parse the identifier and decode its fields. When the database is distributed across several components and many servers, a standard identifier format with specified fields greatly facilitates the look up process.

Airbus and Boeing as the aviation industry leaders have agreed to use the Air Transport Association's (ATA) SPEC2000 e-business specification for AIDC as the basis for their directive, As well as taking advantages from ISO/IEC and EPC standards. SPEC2000 spells out how individual RFID tags need to be constructed.

<table>
<thead>
<tr>
<th>Mark It</th>
<th>Track It.</th>
<th>Share It.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Frequency Identification of Tools and Parts</td>
<td>Automated Data Capture and Management</td>
<td>Aircraft Reliability and Maintenance Data Exchange Web Data Transmission</td>
</tr>
<tr>
<td>ATA SPEC 2000 Chapter 9</td>
<td>ATA SPEC 2000 Chapter 15</td>
<td>ATA SPEC 2000 Chapter 11</td>
</tr>
</tbody>
</table>

Table 2: Boeing and Airbus Simplified View of Standards Activity

**5.4.1. Recommended RFID standards for authentication application**

The following standards are recommended based on airworthiness regulations, e-authentication application requirements and ATA standards in line with Airbus vision.

![Figure 16: RFID Standards for Aviation Industry](image)

- ISO/IEC
- EPC
- ATA Spec2000

**Figure 16: RFID Standards for Aviation Industry**

---

43 Part authentication RFID application is product Item-level tagging. The recommended technology for product tagging is (860-960 MHz with trading partner agreement) or (13.56MHz with trading partner agreement) ISO17367(product tagging)
Technical standards:
- ISO 15693 Passive, read-write operating at 13.56 MHz
- ISO/IEC 18000-3 (parameters for air interface operating at 13.56 MHz) RFID for item identification air interface
- ISO/IEC DTR 24729, Information technology- RF system implementation guidelines for item-level tagging

Conformance standard:
- ISO17367 –supply chain applications of RFID for item level tagging-Proposed guidelines for the verification and qualification of design and manufacture for RFID tags

Data standard:
- Spec2000 chapter 9, memory description for high memory RFID (64kbit) + Unique ID: SSN (Social Security Number)
6. Authentication of RFID tag

This chapter starts by describing possible security threats to an RFID tag, and then discusses about different security approaches to mitigate these threats. The chapter concludes with proposing a security solution for RFID tag in aviation industry, particularly in anti-counterfeiting application.

6.1. Security threats to RFID tags in aviation industry

However, RFID solution for controlling authenticity and legitimacy of products may end the headache of SUPs. There are still some security issues about RFID on which realizing the RFID solution depends addressing such issues. A threat and risk analysis is performing to determine how the safety of aircrafts might be compromised by tag data being either read or changed by unauthorized people. Just an authentic RFID tag can ensure that a tagged part is authentic. RFID technology provides a tool to deal with SUPs problem; in the solution scenario, RFID plays the role of a security marker that holds some crucial data about originality of part and escorts a part in its lifecycle. So some sensitive data are usually available on RFID. Therefore serious consideration must be given to the security aspects of such RFID application. Otherwise not only RFID can not be an effective solution for counterfeiting but also can leverage counterfeiting. “An escort must be the most reliable person to trust”.

On the other hand, criminal efforts to read, change, or manufacture tag copies are naturally dependent on the direct or indirect value of the data saved in the RFID tags or on the value of the tagged parts. Criminal efforts to imitate parts depend on the value of parts; therefore, using RFID as an anti-counterfeiting tool means tagging valuable goods with valuable data. The more motivation the more risk.

A good security solution needs to ensure that an RFID tag, data and accordingly tagged part is authenticated. Often, achieving “perfect security” is technically or economically infeasible; the optimal solution must provide “enough” security that supports a tradeoff between risk, cost and benefits. There are already some solutions like implementing encryption algorithms, software-based access control to protect information on the tag chip or to prevent interception communications between the tag and reader, and using killing commands or additional hardware like hologram and microware to prevent tag changing or copying the tag.

6.1.1. Data Security Threats

As RFID is wireless-based and network-oriented technology, all security threats, it inheritances from wireless and network based technologies. The wireless character of RFID technology lets data to be transmitted over the air. It makes RFID systems vulnerable to attack. Data can be eavesdropped or/and tampered during its travel between tag and reader or reader and network. There are different cryptography-based solutions with different security levels for different wireless applications, but there is no definite and invincible solution. Data on the tag also can be accessed and tampered and spoofed with unauthorized reader.
6.1.2. Hardware Security Threats

The tag itself is threatened by Cloning, Deactivation, Destruction and Detaching. A tag can be cloned to be installed on a fake part or exchanged with the original tag in the original part. All these hardware threats must be considered when a security approach is going to be taken.

6.2. Data Content Security

To set a proper security level for data content in an RFID system some factors should be taken into account, the technical restrictions of available RFID tags, the application that tag will be used in, the risk involved and the trade off between all these factors and security cost. Different applications need different security levels. The mission is providing a 64kbit (High memory) 13.56MHz passive tag with appropriate security level for authentication application in aviation industry. There is Minimum security measures taking into account minimum security needs identified in such tags. For example the very nature of RFID that is the unique number stored in tag’s memory forms the basis for a number of security concepts. But this level of security is not sufficient in RFID application for anti-counterfeiting.

In general, data security is about protecting confidentiality, integrity and availability of data. Data confidentiality is protected by setting limits on who can get what kind of data. Data integrity is protected by preventing unauthorized modification of intended state of data. Data availability is protected by preventing any interrupt that destroys timely access to data. To claim a secure RFID system, the data in transmit between reader and tag and the data on tags must be protected from unauthorized access and unauthorized modification (Data tampering).

6.2.1. Security approach for in transmit data between reader and tag

Choosing a certain type of RFID system can ease security risks. A passive 13.56MHz High Frequency solution can potentially offer a considerable level of security for RF communication between reader and the tag. According the nature of HF the tags need to be close to readers to be read. Furthermore, HF technology combined with high memory and consequently additional data on tag needs either closer distance or more sophisticated readers to be read. The short communication distance of HF devices with additional memory capacity decreases security risks by increasing attack effort. The most often communication security threat is called eavesdropping that almost is not applicable for HF devices.

**Benefits:** compatible for aviation industry, High memory, High security

**Weaknesses:** readable from short distance

6.2.2. Security approaches for data on the tag

**Access rights**

It refers to setting access rights for ATA memory blocks that contain confidential data. Rights can have the “read and write data”, “only read data” and “neither write nor read data” attributes. ISO/IEC 18000-3-2 standard supports both read and write protecting with a 48-bit memory access password can be set by the tag user (Password protected read/write commands). In addition this standard offers an additional feature called lock pointer, which is

44 Additional features like high memory or additional computations require sophisticated tags.
a memory address that all addresses less than the address stored in lock pointer is overwrite protected. A user can manage memory access right by setting lock commands for different memory blocks. The passive 64Kbit 13.56 MHz RFID tag complies with ISO/IEC 18000-3-2; this security feature can be applied to provide data confidentiality. In addition with high memory capacity (64Kbit) longer passwords can be defined that supports higher security.

**Benefits:** preventing of data tampering by write-protect lock command and preventing of unauthorized reading for confidential data by read-protect lock command

**Weaknesses:** needs password management system

---

### Data encryption

It refers to storing encrypted data in an RFID tag to protect the data. The data encryption process is performing with the reader or the enterprise subsystem. If it is performing by enterprise system then for reading data on the tag a connection to enterprise system is needed (on-network)\(^4\). If the encryption process can be handled by reader (off-network) then the data on the tag can be read without any connection to enterprise that is the proper way in authentication and anti-counterfeiting tags. When there is not access possibility to backend network the mobile reader can do encryption and decryption process and as there is a possibility for network connection the reader forward the decrypted data to the network.

**Benefits:** Part data that is encrypted in the tag can be decrypted just by a reader with the corresponding cryptographic software. So the data is protected from unauthorized access.

**Weaknesses:** needs password management system, deploying encryption system needs more memory on the tag and also reader

---

### Disabling the tag_ Kill feature

It refers to equipping the tag with a kill command. This command is used for fully disabling the tags functionality when its use is no longer required; at first, this feature was designed in EPCglobal tags to protect consumer privacy. When one wants to detach the tag from product for example at the end of product lifecycle, the tag should be destroyed to be protected from subsequent unauthorised access and data abuse. A tag will be dead as it remotely receives a kill command that means the tag will be deactivated to send or receive data and can never be reactivated. EPCglobal tags are the only standards-based tags that support a kill feature.

**Benefits:** prevents a tag from being reused improperly, prevents a tag data to be abused.

**Weaknesses:** The kill command can just disable the tag from wirelessly data send and receive and the data will remain in tag’s memory even after kill command. So the tag data is accessible by a professional. The kill command is also managed by passwords; it needs password management system. Although kill command can be a tool for data security, at the same time it can be a security threat; if an unauthorized person finds the kill command password then the tag can be deactivated when it has to operate.

---

### 6.3. Hardware security

Despite the data security features, physical security features could verify the authentication of the tag and consequently part without the reader.

\(^4\)\text{For example EPC network architecture _Appendix C}
Tamer resistance
It refers to RFID tags that any attempt for altering or tampering could be physically recognised. Such tags are usually produced from frangible antenna; with any try for removing the tag, the antenna breaks. These kinds of tags are good in applications that the tagged part is travelling the long way through the chain and is out of the implanting organisation control; consequently it is not possible to be permanently monitored.

**Benefits:** discouraging the adversary from detaching the tag  
**Weaknesses:** sophisticated adversary may be able to repair a frangible antenna (Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, Ted Philips 2007)

Equipped with additional physical security tools –microwire, Hologram
Additional physical security features can be considered in item-level tagging. RFID tags with microwire or hologram.
A hologram is a flat surface that, under proper illumination, appears to contain a three-dimensional image. They are made from metal readable by machine or human eye. Because they cannot be copied by ordinary means, holograms are widely used to prevent counterfeiting of documents such as credit cards, driver's licenses, and admission tickets. (How products are made n.d.) An RFID tag with hologram will create an extra security level. By Hologram, it could be possible to recognize that the RFID tag itself is original or fake.
A microwire is an N-component alloy generating a well distinguished voltage pulse in a detector when the microwire is exposed to an alternating magnetic field. Any mix of metals in microwire is capable of generating a unique voltage pulse in a detector when the microwire is exposed to an alternating magnetic field. A micowire is a security maker for an RFID tag for its authentication.

**Benefits:** discouraging the criminal by adding an extra security marker  
**Weaknesses:** enforce more expenses by adding an extra security marker

![Figure 17: Micowire](image-url)
6.4. Cryptography Standard for RFID

6.4.1. PKI technology

Data-encryption is one of the security approaches for data on the tag. There are different cryptography methods; the commonly used encryption method today is public/private key infrastructure (PKI\textsuperscript{46}). PKI uses a pair of mathematically related keys, public key and private key. The public key is freely distributed but the corresponding private key is unique for anyone and has to be kept secret.

Public key infrastructure architecture consists of software (client software, server software), hardware (e.g. RFID) and PKI technologies. The server software is a certificate authority responsible for issuing user’s certificates. A user can digitally sign a message using his/her private key and the receiver can verify the message by using the corresponded public key in the user’s certificate. The PKI architecture could be used in encryption and authentication of messages between the RFID tag and reader or reader and enterprise system as well as verification and authentication of users in RFID applications to ensure the authenticate access to data.

<table>
<thead>
<tr>
<th>Sender</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send an encrypted message using receiver’s public key</td>
<td>Decrypt an encrypted message using his private key</td>
</tr>
<tr>
<td>Send an encrypted signature using his private key</td>
<td>Decrypt an encrypted signature to authenticate the sender using sender’s public key</td>
</tr>
</tbody>
</table>

Table 3: PKI Scenario

6.4.2. PKI Standard

To support the interoperability concepts, the standardized cryptography method shall be chosen. Public key cryptography standard is introduced by IEEE\textsuperscript{47}, standard 1363a Elliptic Curve Cryptographic (ECC) algorithm. For RFID applications, ECC enables very fast signature creation. The IEEE Standard 1363a ECC algorithm provides the same level of security as previous algorithms\textsuperscript{48}, but uses 75 percent less tag memory for a digital signature. One of the primary advantages of ECC RFID Security is that it provides a high level of security without increasing computing power, complexity or cost. To use ECC standard the ATA work group for ATA specification 2000 could consider adapting the IEEE Standard

\textsuperscript{46} Public Key Infrastructure  
\textsuperscript{47} Institute of Electrical and Electronic Engineers  
\textsuperscript{48} 1,024-bit RSA encryption
1363a ECC algorithm and ask for hardware (readers and tags) incorporate with the IEEE 1363a ECC standard. (Harold F.Tipton 2001) (Pearson 2006)

**6.5. Recommended Security Solution**

Aviation industry needs highly secure crypto HF RFID

As mentioned above there are different tools and approaches to deploy a secure RFID system. Considering pros and cons of each one and based on knowledge from chapter 4 and 5, recommended secure RFID tag in aviation anti-counterfeiting application is a **Secure and Unique RFID Tag and Reader Specially Created for Aviation Industry** specified as following:

1. 64kbit (high memory) HF RFID tag operating in 13.56 MHz –passive mode complying ISO/IEC 18000, ISO/IEC 18000-3-2, ISO/IEC DTR 24729, ISO17367, ISO 15693 and ATA Spec2000 chapter 9 Standards and Authenticated PKI-enabled RFID reader

2. Equipped with kill command and microwire, and digital signatures complying the IEEE’s PKI encryption standard.

<table>
<thead>
<tr>
<th>Frequency Application</th>
<th>HF 64 Kb 13.56 MHz</th>
<th>UHF 64 Kb 868 MHz</th>
<th>UHF 2Kb 868 MHz</th>
<th>EPC Gen 2 868 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto ID</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Event Marking</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data Security</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Parts Security</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>ATA Compatibility</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Airworthy DO 160E</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Table 4: RFID Transponder: Aviation Selection Criteria**
7. Conclusion and Recommendations

The final chapter is based on analysis in previous chapters. The chapter presents conclusion regarding the problems defined in section 1.2. and recommended approaches presented in sections 4.6, 5.4, 6.5. At the end recommendations for future research are presented.

7.1. Conclusions

There is a widespread agreement that radio frequency identification is the best solution for counterfeiting problem. RFID tags give the character of uniqueness to their hosts and are traveling with them from one entity in the supply chain to the other providing a great tracing system across the supply chain. The RFID-based tracing system assures the integrity of supply chain the way that even finding a gap to enter an unapproved part is so difficult. However to apply appropriate RFID technology is a big challenge and inquires guidelines considering requirements and characteristics of the host industry and presenting those of the RFID technology. Previous chapters are trying to pave a way to design a guideline for choosing appropriate RFID technology considering the characteristics and requirements of the Aviation industry. In line with this purpose:

Chapter 4, giving the foundation in order to understand counterfeiting problem in aviation industry as well as proposing solution scenarios based on RFID technology, the answer to problem definition 1.
Chapter 5, studying the regulations and standardization requirements of the aviation industry for RFID systems and analyzing applicable standards as well as summing up with the results, the answer for problem definition 2, 3, 4.
Chapter 6, introducing the possible security threats for RFID technology as well as mitigation approaches and concludes with proposing a security solution proper for aviation industry, the answer for problem definition 5.

7.1.1. Layered architecture against SUPs

Based upon the results gained from previous chapters and inspired of the current pharmaceutical industry solution which has already started to use RFID technology in anti-counterfeiting applications (pearson 2005) as well as the idea of “Internet of Things”, the following architecture is recommended as a practical guideline for implementing RFID systems in aviation industry as a solution against SUPs. Architecture is combination of hardware and service layers to provide multiple layers of security against SUPs.

1. Secure and unique tags specially created for Aviation Industry

The first layer of security approach is the airworthy RFID transponder compliance with ISO 15693 passive, ISO/IEC 18000-3, ISO/IEC DTR 24729 and ISO 17367, read-write operating at 13.56 MHz. The transponder manufacturer programs the 64 Kbit tag memory according Spec2000 chapter 9 memory description and locks UID in the tag as well as Product Manufacture Number (PMN). (Detailed information about data in tag is described in Figure 15) (Kortenburg Master Tag is currently the only tag available according these specifications).
2. **Digital signing of tags**
   Generating and locking digital signatures in tags’ memory while tagging LRUs. The size of signature depends on the demanded level of security; bigger signatures need more memory space, pharmaceutical anti-counterfeiting application uses 1,024 bit digit signature (key size). The authenticated RFID reader is equipped with a Public key to read the signature and though validate the authenticity of the tag and pursuantly authenticity of tagged LRU during its lifecycle.

3. **Chain of custody event validation**
   After checking the authenticity of tag’s digital signature, the authenticated RFID reader creates event validation information both in the tag and backend data network. At the first step the LRU manufacturer writes production data in the network and some in the tag then associates that data to the tag via UID. As a LRU starts its lifecycle, each event could be record in the tag as an event marker as well as backend network by the authenticated reader. Comparing the event data stored in the tag with corresponding event data in a data network provides an additional level of security.

7.2. **Recommendation (Internet of Parts)**

Following the above-mentioned architecture, RFID technology can provide a good confidence in authenticity of aircraft parts. RFID technology, joined with a reliable security level and data infrastructure standards, guarantees both part authenticity and pedigree. This functionality of RFID technology supports an Idea of “Internet of parts”.

The prerequisite to realize the idea of implementing RFID technology against SUPs is the support of all partners in the aviation industry, creating a comprehensive network of all components (aircraft parts manufacturers and suppliers, Aircraft manufacturers, Airlines, MRO stations, Aircraft Scrapping stations) to create comprehensive tracing system across whole supply chain.

RFID technology makes the infrastructure ready to connect all Aircraft parts (LRUs) to large databases and networks. Only in this way data can collected and processed to realize the vision of fully interactive and responsive network environment.

7.2.1. **Scenario of Internet of Parts**

Each part of aircraft is uniquely identified by an RFID tag. Each individual working directly with parts is equipped with a handheld reader mobilized with a middleware. Each partner in the supply chain has an enterprise system to store and process the data retrieved from tags and all partners are connected to an inter-enterprise system. One who is dealing directly with parts store and retrieve data (UID and historical data) using Public key infrastructure, with their handheld readers. Afterward the data in the handheld would transmit to a local database in a local enterprise system. Data exchange among supply chain partners is supported by the ONS (Object Name Service) infrastructure.
Each partner can make a query for the earlier actions in the part made by other partners and see the history record. These data combined with internal traceability information provides a great traceability system. Consequently, any potential problems and product recalls can be effectively and efficiently managed. Besides, the authenticity of products is ensured through digitally signed electronic documents that accompany each part. In this way, companies in the aviation industry achieve full traceability of parts across the supply chain and prevent the circulation of unapproved parts in it.

![Figure 18: RFID based network](image)

### 7.2.2. Future challenges

Giving birth to the idea of “Internet of Things” is so challengeable; in the first step convincing the components in aviation industry to share their data with other parts is so difficult. On the other hand managing the security features of such network is so complicated (defining different level of viewing rights, coding system to ensure that only authorized users can access the certain data, providing sophisticated internet security features). Researchers and studies about the prerequisites of the implementation of the idea “Internet of Things”, analysis the
current technologies and tools in line with the implementation of such idea and researching about the deployment challenges, all could be a subject for future researches.
References


Airbus. "RFID on MRTT POLARIS." RFID on MRTT POLARIS -RFID in Aircraft operational Environment. Airbus-EYD.


Detecting and Reporting Suspected Unapproved parts. Advisory, Civil Aviation Safety Authority Australia, 2002.


"How products are made." Answers. www.answers.com/library/how%20products%20are%20made.


Schmidt-Schieferstein, Hermann, interview by Sara Kheiravar. (7 2007).


**Appendix A: Qualitative Study**

Cresswell (1994) offers the following advices to undertake a qualitative study:

First select a qualitative study because of the nature of the research question. In a qualitative study, the research question often starts with a *how* or a *what* so that initial forays into the topic describe what is going on. This is in contrast to quantitative questions that ask *why* and look for a comparison of groups (e.g., Is Group 1 better at something than Group 2) or a relationship between variables, with the intent of establishing an association, relationship, or cause and effect (e.g., Did Variable explain what happened in Variable Y).

Second choose a qualitative study because the topic needs to be explored. 'By this, I mean that variables cannot be easily identified, theories are not available to explain behavior of participants or their population of study, and theories need to be developed.

Third use a qualitative study because of the need to present a detailed view of the topic. The side angle lens of the distant panoramic shot will not suffice to present answers to the problem, or the close-up view does not exist.

Fourth, choose a qualitative approach in order to study individuals in their natural setting. This involves going out to the setting or field of study, gaining access, and gathering material. If participants are removed from their setting, it leads to contrived findings that are out of context.

Fifth, select a qualitative approach because of interest in writing in a literary style; the writer brings himself or herself into the study, the personal pronoun "I" is used, or perhaps the writer engages a storytelling form of narration.

Sixth, employ a qualitative study because of sufficient time and resources to spend on extensive data collection in the field and detailed data analysis of "text" information.

Seventh, select a qualitative approach because audiences are receptive to qualitative research. This audience might be a graduate adviser or committee, a discipline inclusive of multiple research methodologies, or publication outlets with editors receptive to qualitative approaches.

Eighth, and finally, employ a qualitative approach to emphasize the researcher's role as an active learner who can tell the story from the
participants' view rather than as an "expert" who passes judgment on participants.
Appendix B: Standard Organizations

Standards Organizations for AutoId (Harmon 2007)
Appendix C: EPC Network Architecture-inside the Enterprise

EPC Network Architecture-inside the Enterprise

- Local copy of frequently used ONS data
- Registration for static and dynamic ONS
- Collaboration on asset tracking

- Track and trace serial items
- Referencing business transactions
- Object type data (e.g., pallet/case/item, ...) 
- Instance level EPC data (e.g., expiry date, ...)
- Fine-grained access control policy implementation

- Report data
- Manage readers
- Higher-level filters

- Capture events data (tag and sensors)
- Simple filters

- Transmit ePC data using radio frequency
- Transmit sensor data

ONS

Event data

Business Transactions

Enterprise Application(s)

EPC Information Service (EPC Database)

Savant

Reader

Tag

Sensor

Internal Databases (ERP)

filtered event data

IoT

temperature,

queries, updates

points to
provides data to