Security and Reliability of RFID Technology in Supply Chain Management

Vladimír Modrák
Technical University of Košice, Slovakia

Peter Knuth
Technical University of Košice, Slovakia

INTRODUCTION

RFID (radio frequency identification) technology can be expressed in the most universal manner as wireless identification technology, which does not need the line-of-sight to be read or written. It offers enhancement of identification technologies like barcode technology. Optical barcode technology was developed in 1948 by Silver and Woodland at Drexel Institute of Technology and first commercially used in 1966 (Adams, 2002). Barcode technology stores data in the widths and spacings of printed parallel lines, or in patterns of dots, concentric circles, and hidden within images. The most extended is UPC code which was invented in 1973 and since then became everyday part of our life. Other commonly used types of barcodes are Code 128, Code 93 (Groover, 1980) and DataMatrix 2D barcode. At this time, mostly the barcodes are keeping inventory and shipments moving. RFID and barcode technology complement each other because both of them are beneficial in different situations and can be used together in many applications.

RFID technology has several advantages for managing and collecting object's data or tracking it as it moves through the supply chain (SC). Two of them are related to the increased abilities of security and reliability of the identification systems. These two properties of identification technologies are equally important for their use in supply chain management (SCM).

The purpose of this chapter is to highlight selected areas of this technology that may be critical specific aspects of further RFID development and applications. We have also discussed about differences between RFID and barcode technologies especially in terms of their use in SCM and concluded this article with expectations of further development of this still progressive technology.

BACKGROUND

Security and reliability issues have their roots in history of RFID technology (RFID Journal, 2005). Principles of RFID technology are based on the fundamentals of electromagnetic energy, radio broadcast technology and radar technology. The first active identification friend or foe (IFF) system was developed by the British during World War II. It was radio frequency identification technology for identification of friendly aircrafts. Each plane was equipped with a transmitter, which began to broadcast signal back after receiving signals from radar stations on the ground (Landt, 2001). System was very simple and was not very secure. This is the point where not only reliability, but also security becomes significant issue. The reasons why security and reliability of RFID technology became important are at most actual and are implicitly involved in numerous polemics about security and reliability of RFID technology (Karygiannis, Eydt, Barber, et al., 2007; Rieback, Crispo, & Tannenbaum, 2006a; Thorton et al., 2006; Wyld, 2005; Rieback, Crispo, Tanenbaum, 2006b; Macaulay, Abeysinghe, 2004; Bono, 2005). Explicitly we can see the reasons in existing precedence about potential serious impacts that are mentioned later in this chapter. Another important milestone can be considered the patent on RFID that was granted to Mario Cardullo in 1973. In the same year Charles Walton invented access control system based on RFID (Rieback et al., 2006a). The first widespread RFID tag was 1-bit tag (the bit is either on or off) as a part of electronic article surveillance (EAS). EAS could only detect the presence or absence of the tag. In other words if someone does not pay, the tag remains on and the readers at the door detects the tag and the alarm sounds to alert un authorized removal. The U.S. government was also supporting research and development of RFID systems. Los Alamos National Laboratory in New Mexico soon became a leading center for R&D of this technology (Shepard, 2005). This laboratory developed automated toll payment systems and passive RFID tag to track cows. Both are still used all around the world. Further development lead to use higher frequencies

that allowed greater and faster data transfer rates. In 1999 Uniform Code Councile, EAN International, Procter and Gamble, and Gillette founded an Auto-ID Center project at Massachusetts Institute of Technology for development of RFID standards. The main result of this project was electronic product code (EPC). Other results are air interface protocols (Class 1 and Class 0) and network architecture scheme, which links objects to the Internet through the tag. After that Uniform Code Council and EAN International created joint venture EPCglobal Inc. to commercialize EPC technology due to high importance of EPC technology, since it could dramatically improve efficiencies within supply chain. Previous research responsibilities of Auto-ID center were delegate to EPC global. Recently, more attention is given to security of RFID technology. To corroborate it by facts the following events can be mentioned. In January, 2005, students at Johns Hopkins University broke encryption of SpeedPass electronic payment and RFID point of sale (POS) system. In February, 2006, Adi Shamir reported that he could monitor power levels in an RFID tag which can be used to compromise the secure hashing algorithm 1 (SHA-1) used in some RFID tags (Thorton et al., 2006). However, it is not the reason for a resignation, as a level of risks depends in generally, but also in the specific area, on preventive actions. The example supporting this statement offers the situation in privacy protection. In contrast to barcode technology, RFID technology has greater implications on individuals' privacy, because RFID tags used in personal identification cards can be read from an abundant distance without that person's knowledge or consent. This led to creation of groups like FoeBud or CASPIAN that are against this technology, because they fear, that they could be tracked by tags. In the meantime, blockers for passport RFID tags in a form of passport jackets containing physical barrier and other countermeasures as unique identifier numbers, encryption, and mutual authentification were developed to ensure greater security. On the other hand, the more sophisticated protections bring more opportunities for potential failures.

COMPARISON OF SECURITY AND RELIABILITY BETWEEN THE RFID AND BARCODE TECHNOLOGY

The main difference between barcode technology and RFID technology is that barcode technology is optical technology and RFID technology is radio technology. All other advantages, disadvantages and differences result from this fact. In the supply chain, the biggest advantage that RFID has over barcode is the ability to automatically read large groups of tags eliminating the labor needed to manually scan the large volumes involved in the supply chain. Improving visibility in the supply chain systems gives "management programs better visibility into the supply chain, which enables identification of bottlenecks, targeted recalls, and new forms of market research" (Karygiannis et al., 2007). "Both active and passive RFID tags have significant potential to provide low-cost, short-range, identification for many consumer goods and can help to identify objects" (Finkenzeller, 2003). Potential benefits of RFID implementation in the supply chain management are counterfeit and fraud reduction, improved efficiency, labor cost reduction, stock shrinkage reduction, stocking management improvements and return goods facilitation (improved customer satisfaction). RFID technology can be used in several levels in supply chain management (see Table 1).

When talking about reliability of automatic identification technology, an attention might be focused on the ability of readers to identify codes from tags at the first time. The potential interferences of barcodes make optical barriers such as objects placed between barcode and reader or dirt. Also, they are unreadable under extreme atmospheric conditions such as steam or when vertical damage occurs. Barcode readers are sensitive to dirt, dust, or other foreign object obstructing the lens. But 2D barcodes can be read even if part of the tag is destroyed. Passive RFID tags can interference with environments or fields and various materials such as liquids and metals that affect transmission of radio frequency. Active tags are less susceptible to interference. Despite this, they can be read under extremer weather conditions than barcodes. It is not clear whether tags, that could not be read, can be entered manually as barcodes. Reliability seems to be solved these days by knowing RFID physics (Schlosser, 2004). But there is no universal solution for implementation of RFID at all. It is always necessary to fit RFID system to meet company needs (if company really needs RFID) as far as 100 percent reliability. And because there are numerous types of RFID tags the selection of proper RFID tag system is essential. It is better to start with smaller project and obviously in detail defined problem rather than to fail (Sweeney, 2005).

Security of RFID technology in supply chain management can be seen from many aspects: health (radiation of devices), personnel or vehicle access control and tracking, inventory location, privacy issues, third-person attacks, software and hardware protection, encryption and tracking origin of goods

Table 1. Levels of RFID in supply chain application (Source: D'Hont, 2003, p. 13)

Level	Use	Application
Item	Consumer units	Products and individual items
Case or Carton	Traded units	Boxes (packaging) product carriers
Pallet	Distribution units	Pallets / Trucks