Chapter 12
Radio Frequency Identification in the Smart Supply Chain

Albert Lozano-Nieto
The Pennsylvania State University, USA

ABSTRACT

Radio Frequency Identification (RFID) is a relatively new technology that has emerged from the works of automated identification. RFID is based on the exchange of information between a device called a tag and a device called a reader after the reader queries the tag. The tags can be attached to specific items, boxes of these items, pallets of these boxes, or a combination of the previous, thus enabling the transmission of their contents. Once this information is detected and processed, it can be used as needed by the specific application. Among the different uses of RFID in the supply chain, this chapter focuses on those related to inventory control and the detection of counterfeited products.

INTRODUCTION

It is undeniable that the introduction of barcodes and their acceptance by all industry several years ago resulted in a revolution in the supply chain. We are now facing a similar transformation with the introduction of Radio Frequency Identification (RFID). The use of RFID allows the introduction of an additional level of intelligence in the management of products as they move through the different steps in the supply chain. Of particular interest are the possibilities to track inventory on real time as well as to introduce techniques to detect and prevent counterfeited products. These two characteristics in turn, result in a decrease of losses and a reduction in processing time and labor.

The goal of this chapter is to provide the reader with an introduction to the basic principles of RFID as well as to illustrate how this technology is being currently used to increase the efficiency in the supply chain as well as to fight the counterfeit of products that are critical to our society.

DOI: 10.4018/978-1-4666-0246-5.ch012

The counterfeiting of goods is an increasingly widespread problem through the industrialized and developing world. Recent estimates put the effect of counterfeiting between 5% to 7% of total world trade (Kim and Kim, 2005). The US defines counterfeiting as an item that is a copy or a substitute of a legal item without the right to do so, or whose materials, performance or characteristics are knowingly misrepresented by the manufacturer, supplier or vendor (US Department of Energy, 2004). While counterfeiting evokes the image of products imitating luxury watches, designer purses and other high-end items, the real impact of counterfeited items is more serious and may have extreme consequences. This is especially important as counterfeited products are increasingly appearing in critical systems such as the electronic components used for defense systems, pharmaceutical products and parts used for repair and maintenance of aircraft.

Counterfeiting of Electronic Products

The counterfeit of electronic components happens in different ways such as the remarking of electronic components to make them appear different from what they originally are, selling defective parts staged for disposal by the original manufacturer or parts that result from reselling components taken from electronic boards that were scheduled for destruction or simply knowingly selling components that are not operational (Livingston, 2007). While in this last case components may have been at one time real components, they have been obtained without any quality control procedures and at the very least, they have aged considerably.

The effects of counterfeited electronic components is more worrisome when they are used in critical systems such as avionics, flight controls or defense systems. To make the problem worse, it can be extremely difficult to link the crash of a military aircraft, for example, to counterfeited electronic parts and especially to identify the part that failed as complex systems tend to fail in complex ways. We need to keep in mind that counterfeited electronic products may work correctly for some time, or as long as they do not exceed some operational parameters unknown to the user. A different concern comes from counterfeited electronics products, having a backdoor that can be used to disrupt a service. The use of counterfeited computer processors in systems that control critical missions of critical assemblies, for example the power grid or the control of electrical stations can enable a third party to have access to otherwise secure systems without being known by their legitimate users.

If counterfeited electronic products are difficult to detect after a failure, it is extremely difficult, almost impossible to detect them at the time of use or when assembling the subsystems. It is possible to find several reasons to explain the increase in the counterfeit of electronic products, specifically electronic components. Our society is used to, and demands, lower costs in electronic products. To most users, the only difference between a legally manufactured and a counterfeited cell phone battery is only their cost, especially before there are widespread news of failures and their consequences. The reason for the spread of counterfeited integrated circuits in avionics and military products is double. First, in an effort to save costs, the Department of Defense started an initiative several years ago focused on purchasing electronic components off the shelf instead of having electronic components specifically designed and manufactured by approved manufacturers. In addition, the electronic components tend to remain in service in military ships or airplanes for 10 or 20 years after being discontinued by the manufacturer. This forces military purchasers to use small brokerage firms who buy and sell integrated circuits without knowing who is making them. In turn, this opens the door to counterfeited or defective components to be used in our nation's defense systems. As a response to recent