

# RFID's Finest Hour

Radio frequency identification could play a tremendous role in securing the safety of global trade and supply chains.

Apr. 17, 2006—The Dubai Ports World controversy has highlighted the fragility of our global supply chains and some of their weakest links. Despite all the media attention, the real issue is not about the ports or who manages them, but rather the end-to-end journey of goods and the people, processes and technology that conduct, manage and protect global trade. As we explore these strategic issues, the extent of RFID's ability to help secure this supply chain and fuel growth and innovation for its participants is only now beginning to be realized.

In recent decades, the perfect storm of globalization has opened up the free flow of trade, capital, people and knowledge across developed and emerging markets. Businesses have access to global markets from which to source their goods and services, and to export their finished products in order to grow revenues, reduce costs and improve performance. The world stage provides the opportunity to gain economies of scale, competitive advantage and the differentiation needed to produce the steady incremental growth required by capital markets.

However, the price of admission to this world market is for businesses to tackle increasingly such complex issues as compliance, collaboration, communications and competition. In terms of compliance, businesses must abide by an expanding number of regulations and mandates from a governance, industry and privacy perspective. A typical supplier, importing from overseas, may have to deal with Sarbanes-Oxley (SOX), the Customs-Trade Partnership Against Terrorism (C-TPAT) and possibly both the U.S. Department of Defense and various retailer RFID mandates.

Section 404 of SOX requires companies to have controls in place to protect against adverse, preventable events—including those within their supply chains—that could impact their value. C-TPAT requires companies to take responsibility for the security of their own supply chains. While C-TPAT is voluntary, the consensus is that it may well become mandatory in the near future.

In light of this increasingly complex supply chain and regulatory environment, businesses today are even more pressed to ensure they balance the agility needed for competitive advantage and operational efficiency with the assurance needed for the safety and security of their shipments. Globalization, decentralization, outsourcing and the Internet have, in effect, created a divide between agility and assurance. Businesses are operating with increased agility, yet their security mechanisms are outdated. Too often, security has been an afterthought layered on top of new and existing applications and processes.

The nature and magnitude of threats to the supply chain have also changed. Today's supply chains face ever-increasing disruptive threats such as theft, diversion and counterfeiting, along with the unpredictable acts of governments, port operators and other entities in their supply chains, plus extreme acts of nature (such as Hurricane Katrina) or, worse still, terrorism. As an example to highlight the magnitude of these threats, the World Health Organization (WHO) estimates that 5 to 10 percent of the world's pharmaceuticals are counterfeit. The economic impact of this counterfeiting is estimated at \$1 billion to \$12 billion. The bigger

picture across all global trade is that product counterfeiting now accounts for 5 to 10 percent, or roughly \$350 billion. In addition to counterfeiting, theft and diversions alone affect 1 to 3 percent of all goods in the supply chain.

Throughout history, the military has had to respond and adapt to new threats and continually transform itself to deal with new, asymmetric threats as it has moved from fighting a well-known opponent to being ready for an attack that can occur almost randomly, at any time and any place, and against any target. Today's businesses must also redefine their security posture to mitigate these risks and ensure business continuity for their global supply chains.

To ignore these risks and imperatives would be too costly for both the United States and individual corporations. A recent war-game scenario estimated that closing the nation's ports for as few as 12 days would lead to a 60-day container backlog and a cost to the economy of approximately \$58 billion. What's more, the impact on an individual company can be equally devastating. A senior executive of a Fortune 50 company has stated, "If an act of terrorism were committed using one of our containers, we believe it would be a company-ending event."

As an enabling technology, RFID offers tremendous potential to help address these challenges. While much attention in the past several years has focused on RFID's application for supply chain efficiency and support for DOD and retailer mandates, it can actually play an equally important role in helping raise the security posture of nations, governments and businesses. RFID can help provide the end-to-end visibility we need for goods and assets moving through the supply chain, as well as the identification—and, hence, authorization—we need to keep the good guys in and the bad guys out. An investment in RFID can, thus, serve two purposes: as a business accelerator in terms of supply chain efficiency, and as an enabler for improved security.

Some examples can help to illustrate RFID's potential, and businesses can learn from some of the long-standing and recent programs within the U.S. government.

Within the realm of supply chain visibility, perhaps the best example to date is the U.S. Department of Defense's In-Transit Visibility network. Established in 1994, this has since become the world's largest RFID network. Today, the network tracks ordnance, medical supplies and food across more than 50 countries and more than 750 nodes in the supply chain, including airports, seaports and rail terminals. It secures 350,000 conveyances and 25,000 containers daily.

On the personal identification side, RFID can play a key role in helping support the convergence of physical and logical security across our supply chains. As an identification credential for employees, it can secure and speed access to physical sites, such as ports, ships and warehouses, and also secure access to supply chain management systems that provide information about shipment contents and destinations. The U.S. government is already moving down this path via Homeland Security Presidential Directive 12 (HSPD-12). Issued in 2005 with the aim of establishing a government-wide, standardized credential for personal identity verification, or PIV, for both government employees and contractors, this mandate applies to both physical and logical (computer) access.

RFID has the potential to help secure every aspect of the supply chain—from personal identification and credentialing to goods and assets and on to access control for IT systems. As an enabling technology, it can help businesses close the current gap between agility and assurance, as well as redefine their security posture. Of course, along with this enabling technology, businesses should focus on processes and greater collaboration—whether between public and private entities, supply chain participants or departments within a single corporation. With greater information sharing and collaboration between authorized parties, participants can work together to protect our nation's borders and the security of our supply chains. The

well-known Operation Safe Commerce pilots and the recent Advance Trade Data Initiative (ATDI), which requires importers to share extensive shipment details with U.S. Customs, are strong examples of this public and private collaboration.

Radio frequency identification got its start in World War II for friend-or-foe identification. The signs now are that it is coming full circle. With so much resting on the safety and security of global trade and the supply chains that enable them, this could well be RFID's finest hour.

*Nicholas D. Evans is vice president and general manager of worldwide enterprise security initiatives within Unisys' Strategic Program Office. He is the author of Business Innovation and Disruptive Technology (Financial Times, Prentice Hall) and chairs the RFID Standards Task Group for the Information Technology Association of America (ITAA).*

Copyright ©2005 RFID Journal, Inc. All Rights Reserved