Mitigating Container Security Risk Using Real-Time Monitoring with Active Radio Frequency Identification and Sensors

by

Adam Ian Schlesinger

Bachelor of Commerce
McGill University

Submitted to the Engineering Systems Division in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Logistics

at the

Massachusetts Institute of Technology

June 2005

Signature of Author .....
Engineering Systems Division
May 2005

Certified by .....
David L. Brock
Principal Research Scientist, MIT Auto-ID Lab
Thesis Supervisor

Accepted by .....
Yossi Sheffi
Professor of Civil and Environmental Engineering
Professor of Engineering Systems
Director, MIT Center for Transportation and Logistics

Mitigating Container Security Risk Using Real-Time Monitoring with Active Radio Frequency Identification and Sensors

by

Adam Ian Schlesinger

Submitted to the Engineering Systems Division
on May 6, 2005 in Partial Fulfillment of the
Requirements for the Degree of Master of Engineering in
Logistics

Abstract

The global village in which we live enables increased trade and commerce across regions but also brings a complicated new set of challenges such as terrorist activity, human and drug smuggling and theft in foreign or domestic locations.

Containers travel the globe, across all seven continents. In the wake of intensified security concerns since the September 11, 2001 attacks, tracking containers and their contents presents an increasing concern for those institutions and personnel charged with ensuring their security.

This thesis analyzes the risks associated with global container transport. The concept of an *e-container* is set forth as a risk mitigation technology that uses real-time monitoring of a container's physical status acquired from an array of embedded RFID-enabled sensors. A framework is suggested that relates sensor-identified signatures and phenomena to behaviors representing breaches in container security. A theoretical model suggests which sensors are required to identify the individual breaches in order to mitigate container security risk.

Thesis Supervisor: David L. Brock
Title: Principal Research Scientist, MIT Auto-ID Lab

Acknowledgements

Dr. David Brock – Your brilliance and creativity astounds me. Thank you for your guidance, insight and motivation throughout this journey

Abbott Weiss – Thanks for steering me in the right direction - you set the foundation

Stephen Miles and Ed Schuster – Thanks for helping me take my ideas to the next step

Kevin Emery – Thanks for helping me explore sensors and data layers

Chris Caplice – Thank you for your insight and direction, and instilling the fear that made me finish on-time

The students of the MLOG program – It was intense and very well worth it - you created an incredible atmosphere

Dedication

This paper is dedicated to my family – you believed in me even before I was born

Mom, Dad, Julie - I appreciate you more than you could ever imagine

Gramps and Bubba, this is for you

Biographical Note

Adam is currently a candidate for a Master of Engineering in Logistics at MIT. Prior to MIT, he worked as a six sigma certified business analyst and project manager for Bombardier Aerospace in Montreal, Canada, developing global information system architectures and implementing ERP bolt-on systems. He has experience in procurement, operations, engineering and finance, and has managed teams in five countries. Previous to Bombardier, Adam worked as a technical systems analyst for the NSB Group (STS Systems), developing point-of-sale software. He completed his bachelor of commerce at McGill University in Montreal, specializing in management information systems and strategic management. While in school, he ran a small consulting firm that built distributed networks and IT infrastructure for small businesses. He has consulted on numerous IT outsourcing agreements. Upon graduation, Adam will assume the role of Business Productivity Specialist at Microsoft Corporation in Seattle, Washington.

Table of Figures

Table of Contents

DISCLAIMER

Page has been ommitted due to a pagination error by the author.

(Page 1 & 2)

Section 1 Introduction

This thesis studies the risk involved in global container shipping and how this risk can be mitigated through real-time monitoring of a container's physical status acquired from an array of RFID-enabled sensors. The e-container is introduced as an integrated solution.

The U.S. Department of Homeland Security (DHS) has created the Container Security Initiative (CSI). This consists of four central components:

1. Establishing security criteria to identify high-risk containers
2. Pre-screening containers before they arrive at U.S. ports
3. Using technology to pre-screen high-risk containers
4. Developing and using smart and secure containers

(CBP4, 2002)

The main goal of the CSI is to secure the U.S. and global economy from a container security perspective. The research in this paper is in line with the CSI four components.

1.1 Research Problems and Motivation

Merchandise, supplies, commodities, cargo, and freight, collectively referred to as goods, are at the core of global trade. Most of these goods, estimated to be about 90% of worldwide cargo, are transported by containers. In fact, more than 16 million containers annually arrive in the United States (U.S.). More than half of these containers arrive via ocean cargo ships. Consider that a majority of these containers are large enough to hold multiple nuclear warheads, many tons of Anthrax, and other mass-destruction devices. (CBP1, n.d.) "Clearly, a terrorist attack on a major U.S. port could bring this trade to a grinding halt" (CBP1, n.d.). Just the threat of weapons of mass destruction or other chemical and/or biological weapons making their way to the U.S. poses phenomenal challenges for global supply chains.

The global village in which we live enables increased trade and commerce across regions but also brings a complicated new set of challenges such as terrorist activity, human and drug smuggling, and theft in foreign or domestic locations.

Containers travel the globe, across all seven continents. In the wake intensified security concerns since the September 11, 2001 attacks, tracking these containers and their contents presents a major problem for those institutions and personnel charged with ensuring their security. U.S. Customs and Border Protection (CBP) Commissioner Robert C. Bonner said: "Because of the nature of potential concealment [of weapons] in a container, they are the potential Trojan horse of the 21st century" (Keane, 2004).

The U.S. Department of Homeland Security (DHS) is handing out multi-million dollar grants to security and technology related companies to develop tracking technology; however, for the average size supplier, most of the commercially viable technology is exorbitantly expensive. The adoption of the technology depends greatly on the ability to afford the technology, and if the implementation makes economic sense. In addition, new rules and regulations are increasing inspection times, waiting time, border hold-ups, and are presenting many new interruptions in the supply chain and flow of goods between countries. New partnership agreements such as the Customs Trade Partnership Against Terrorism (C-TPAT) will allow certified shippers to pass though inspections quickly and reduce their waiting times. See Appendix 3 for a more through explanation.

The U.S. government, in its attempt to stop terrorism at the source, is placing customs officials in foreign ports to check and seal containers before they head toward North America. This could mean changes to international treaties such as the NAFTA[1].

To address the aforementioned challenges and security concerns, this research paper will recommend a Real-Time Container Tracking System that secures every container transiting ports of entry as well as domestically (The risks are identified in Section 2). This system is designed to mitigate the major risks associated with container shipping. The system uses RFID-enabled active tags and sensors to monitor and

[1] **North American Free-Trade Agreement (NAFTA):** a comprehensive trade agreement linking Canada, the United States, and Mexico in a free trade area. It called for the gradual elimination of duties and trade tariffs between the member countries.

communicate container status. The scope of the paper is to identify the risks associated with container transport, and demonstrate which sensors would be useful for mitigating each risk.

1.2 Methodology

This paper is comprised of four parts. Firstly, it will examine the risks involved in the transportation of containers. Second, it will describe a variety of sensors and describe how active RFID works. It will then describe the signatures and phenomena the threats introduce and will conclude with the introduction of a system that provides real-time tracking of shipping container vital signs (temperature, humidity, ambient light, etc.) using active RFID and discuss how this system will increase container security and visibility throughout the supply chain.

By surveying current literature the field of container security, RFID and sensors, and interviewing industry experts, I extrapolated a list of the major risks in container shipping security and identified which sensors might help mitigate each risk.

1.3 Literature Review

This section will discuss trends, government activity with regard to corporate partnerships, RFID and counterterrorism as well as outlining the major stakeholders in a global supply chain.

1.3.1 Early Adopters

The recent major North American investment in RFID technology was spearheaded by Wal-Mart's mandate which "...instructed its 100 largest suppliers that they are required to attach RFID tags on pallets and cases of goods delivered to the world's largest retailer's warehouses serving its Dallas stores. An additional 26 suppliers have asked to participate in the program" (Delaney, 2004).

Directives from the United States (U.S.) Department of Defense (DoD) and Federal Drug Administration to implement RFID in select areas of their supply chains came shortly after.

"The U.S. DoD is in the midst of implementing RFID and working to replace its 13 core logistics systems, which include several thousand applications, with a version of SAP AG's software[2] tailored for defense operations" (Songini, 2004).

1.3.2 Partnerships

Boeing and Airbus, which together own the market for large commercial jets, are working together to promote the adoption of industry standard solutions for RFID on commercial airplane parts. "By the end of the year, the Federal Aviation Administration (FAA) is expected to certify the use of these passive RFID tags for parts that will be used on planes" (Roberti, n.d.).

RFID implementation has created some interesting partnerships among major world business players. It is the inability to agree on industry standards that is creating major delays on RFID implementation.

1.3.3 Trends

Growth of Cities

The number of cities in the world is on the rise. The greater the number of cities, the more transportation is required for trade and supply of food, etc. The United States for example has been seeing almost exponential growth in this area over the past 50 years. As the number of cities grows, so does the need to transport goods to these cities. This places stress on logistics systems and increases the need for greater container security. Figure 1 depicts this growth.

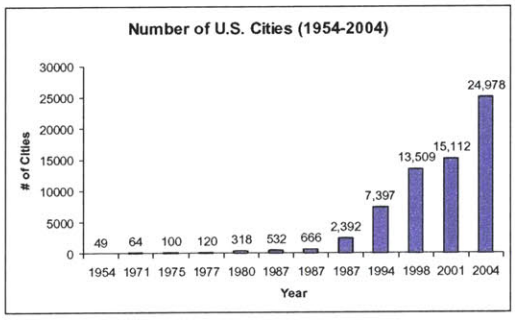


Figure 1. The increase in the number of cities results in a commensurate demand in transportation and logistics investment. Source of original data: (Goentzel, 2004)

[2] SAP is an Enterprise Resource Planning (ERP) software. ERP software can aid in the control of many business activities, like sales, delivery, billing, production, inventory management, and human resources management (Wikipedia.org). Integration with this type of software is discussed further in Section 5.

Spending

Logistics spending is on the rise. U.S. logistics costs increased by $26 Billion from 2003 to 2004. (Beadle, 2004) In fact, China's total logistics spending was estimated at about $500 billion in 2003, with a compound annual growth rate of 8%. This year's estimate exceeds $600 billion. (The Edge Singapore, 2005) Mick Barr, associate director of global physical distribution at Procter and Gamble, says his company spends more than $3 billion a year on logistics services. Almost all of this money is spent on outside logistics service providers, ranging from large integrators to traditional warehouse and transportation firms, as well as 3PLs with niches or geographic specialties. (Bank, 2004)

Speed

Shippers, retailers and customers are demanding shorter lead times and quick delivery of goods. Next-day delivery is a very common offering.

"In 1994, Global Trade and Transportation Magazine stated that regardless of mode, 40% of shippers in the U.S. expedited cargo market said on-time performance was most important. The marketplace will be more information-intensive in order to meet shippers' core requirements" (Chandler, 1994).

Standards

Harmonization is the name given to the effort by industry to replace the variety of product standards and other regulatory policies adopted by nations in favor of uniform global standards. (Public Citizen, n.d.) There are many standards for RFID readers, and tags, globally. The challenge of standardization also conflicts with government spectrum regulation. Developing a unit that can transmit on legal spectrum in all countries may be difficult. "EPCglobal is leading the development of industry-driven standards for the Electronic Product Code to support the use of Radio Frequency Identification."[3]

Exporting Customs Officials and the WCO

On December 9, 2004, the World Customs Organization (WCO) for the first time ever endorsed a Framework of Standards to secure and facilitate global trade that is based

[3] Source: http://www.epcglobalinc.org/

upon principles designed and implemented by the U.S. CBP. The most essential parts of this endorsement involve:

- The 24 hour rule – CBP must obtain advanced electronic information on all cargo shipped to the United Stated 24 hours before it is loaded onto a container.
- Advanced targeting system – used to identify high risk containers
- Container Security Initiative – CBP officers are stationed abroad to screen high-risk containers before they are loaded onboard vessels destined for the United States.
- C-TPAT – as discussed in Appendix 3

(CBP3, 2004)

The CSI will also place CBP officials in foreign ports for pre-screening and inspections prior to shipment to the United States. This will allow more high-risk containers to be identified and examined than U.S. ports can currently handle.

1.3.4 Stakeholders

The stakeholders in the supply chain play a vital role in information sharing, security guarantees, and most importantly, the allocation of investment funds.

The following is a list of stakeholders in a fairly typical supply chain for a company that imports cargo from China to the United States. It is the model that will be used throughout this paper in order to maintain consistency. As supply chain security becomes more comprehensive, this list will undoubtedly grow.

1. Manufacturer
2. Issuers of Letters of Credit
3. Insurance Underwriters
4. Shenzhen Customs
5. Hong Kong Customs
6. Hong Kong Harbor
7. 3PLs
8. Value Added Manufacturers
9. Harbormaster HK
10. Port Facility Manager HK
11. Shipping Company
12. Pirates
13. Terrorists
14. Smugglers
15. US Coast Guard
16. Homeland Security
17. US Customs
18. C-TPAT officers
19. HazMat Officers
20. Immigration
21. Long Beach Harbor
22. Harbormaster US
23. Port Facility Manager US
24. 3PLs US
25. Value Added Manufacturers US
26. TL & LTL Carriers
27. Rail Carriers
28. Distribution Centers
29. Wholesaler
30. Retailer

(Locher, 2005)

All stakeholders have some common concerns:

- Security of the contents
  - Have the contents been tampered with, damaged, stolen?
- Payment schedule
- On-time delivery

1.3.5 Related Background information on Government and Regulations

Governments play a significant role in a global economy. The implications of their regulations, policies, and laws have a strategic value which can significantly impact business and trade operating on a global basis.

Trade Agreements and Organizations

Security is taking center stage in the majority of trade agreements since the aftermath of the September 11, 2001 terrorist bombings. Furthermore, trade agreements increase globalization and increase foreign relations and trade.

North American Free-Trade Agreement (NAFTA)

"The North American Free-Trade Agreement (NAFTA) may take on new members. Bennett Marsh, deputy executive director for trade policy, Caribbean Latin American Action, predicts significant NAFTA growth within 3 years. He expects CARICOM or the Association of Caribbean States to be among new NAFTA members" (Selwitz, 1994).

World Trade Organization (WTO)

The World Trade Organization (WTO)[4], in its attempt to create a safe and "rules-based" trade agreement between the 148 member countries (as of October 2004) has some fragmented mentions of security; mostly with regard to food and perishability.

"Measures with minimal impact on trade can be used freely — they are in a "green box". They include government services such as research, disease control, infrastructure and food security" (Understanding the WTO, n.d.).

---

[4] **The World Trade Organization (WTO):** the only global international organization dealing with the rules of trade between nations. At its heart are the WTO agreements, negotiated and signed by the bulk of the world's trading nations and ratified in their parliaments. The goal is to help producers of goods and services, exporters, and importers conduct their business. (WTO.org, n.d.)

Other Important Agreements with the United States

- Permanent Normal Trading Relations with China (PNTR)
- The U.S.-Chile Free Trade Agreement (FTA) was signed on June 6, 2003
- The U.S.-Singapore Free Trade Agreement (FTA) was signed by President Bush on May 6, 2003 and currently awaits Congressional approval.

1.3.6 Technology

Customs organizations presently employ multiple technologies for scanning and determining the contents of containers:

X-Ray Machines:

The Canadian Border Services Agency utilizes a Pallet Vehicle and Cargo Inspection System known as VACIS. The government has purchased three machines thus far for $2 Million CDN each. The VACIS "is a self-contained stationary gamma-ray scanning system that captures images of pallets and large pieces of freight in customs commercial examination facilities" (Canadian Border Services Agency, 2005). The system is used to aid border officials in examining densely packed freight without having to open containers. It can detect contraband, weapons, and other potentially dangerous goods.

A low-level radiation source penetrates cargo and allows operators to view radiographic images of goods and find hidden areas where unidentified goods may be stored illegally. If the cargo is different than that which was declared in the manifest, inspectors will take action.

Global Position System:

A global position system (GPS) can be used to track the physical location of a container and transmit this information in real-time to a central system. Use of the GPS for tracking of vehicles, aircraft, and containers is common.

E-Seal:

The present technology for securely monitoring containers is a vast improvement over a simple seal and x-ray machine, however it is still insufficient. Firstly, the present systems (called e-seals) do not offer a wide-enough variety of sensors, nor do they communicate vital information in real-time to a data processing subsystem.

The tag collects real-time information, and stores it to memory. When an operator is ready to collect the information, a handheld device is pointed at the e-seal and the data collected by the seal is downloaded to the device. The seals come in the form of a sensor bolt, or "smart seal" that is attached to the outer door of a container.

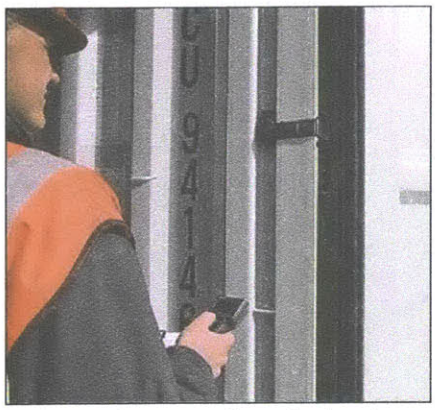


Figure 2. A GE worker reads an e-seal attached to the outer door of a container. Source: http://www.rfidjournal.com/article/articleview/1317/1/1/

The latter also monitors if tampering has occurred with the lock. When the container arrives at a port, the information from the e-seal is downloaded to a central system and the sensor metrics can be traced back to individual time stamps.

"To date the error rates have been so high that it is just not a useful device," said Christopher Koch, president of the World Shipping Council and newly appointed liner carrier representative on the Coast Guard's National Maritime Security Advisory Committee and CBP's Advisory Committee on Commercial Operations. (Kulisch, 2005)

The two largest e-seal manufacturers are GE and SAVI Technology. SAVI uses an active RFID tag in the seal while GE's system is based on a proprietary radio protocol and does not follow the RFID standards. This means that presently, the e-seal cannot keep an inventory count of RFID tagged items within the container. (Kulisch, 2005)

The e-seal option has undergone scrutiny since it is very conspicuous. Thieves are aware that if the e-seal used, the cargo is valuable enough to warrant the expense of the seal. This makes the container more of a target. In addition, the actual container door

can be removed by its hinges without being detected, and the e-seal will not detect a breach from the sides, roof, or floor of the container.

The U.S. CBP is presently promoting a "Smart Box" technology that will give containers "green lane" clearance under the C-TPAT program. The C-TPAT awards: no inspection upon arrival to the United States (except for random inspections), and immediate release to low-risk shippers. The technology that is presently being promoted detects and records whether tampering has occurred to the container seal after it has been affixed at the point of origin.

The problems with this technology are exhibited in the following examples:

1. A terrorist with connections at a port in the Middle East, smuggles a weapon into a container before it has been sealed. The container is sealed, and sent to the United States. Upon arrival in the port of Long Beach, the information about the tag is downloaded. The seal has not been altered or tampered with, and therefore it is cleared through customs and the container is put onto a truck and allowed to pass freely into the United States.
2. A container is sealed in China and put onto a ship destined for America. While at sea, the ship is boarded, and a weapon or drugs is inserted into a container. The "Smart Box" collects information on the date and time the container security was breached. Upon arrival at the port of Los Angeles, the container is transported onto the dock and the tag information is downloaded. The customs official notices that the security of the container was breached, and proceeds to inspect the container – unsure for what exactly he was looking. When the nuclear weapon was inserted into the container, so was a GPS. During the few hours it takes for customs officials to finally inspect the container, the terrorist knew that the container had reached its destination and remotely exploded the bomb.

The preceding two examples call for sensors that can detect nuclear radiation, and transmit the readings in real-time to customs. If the container had this sort of system, the weapon would have never reached North America, and the container could potentially have been removed by helicopter or simply thrown overboard for later diffusion at sea.[5]

The proposed system is discussed in Section 5

[5] Corrective action is out of scope for this thesis but is discussed further in Section 6

Section 2 Containers and their Risks

In the 1930's, Malcolm McLean conceived the idea of using large steel containers as a common method to transport goods by truck and maritime vessel. He thought of the idea while waiting for cargo that he had transported to the port of New Jersey by truck to be unloaded and then re-loaded onto a ship for maritime transport. (CBP4, 2002)

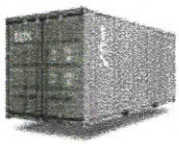
2.1 Containers

This section will provide a background on the different types of containers and their uses. It will then cover how containers are loaded and unloaded. This information is essential to understanding how sensors may affect the physical container and how containers move around a port, dock or yard.

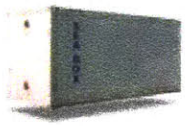
2.1.1 Container Types

The primary function of a container is to hold and protect its contents for transportation purposes. Containers are transported either by rail, truck or ship; however, commonly containers are transported using a combination of all three modes (intermodal).

There are 4 basic styles of closed containers[6] that are used for transportation purposes (containers for other purposes will be discussed later in this section).



The dry freight container is used primarily for any type of good that is not affected by most weather conditions. This type of container will be used for transporting goods ranging from clothing, to other packages, automobiles, etc.



Insulated containers are used for transporting goods that are more weather sensitive such as electronics, and foods that do not require refrigeration.

Refrigerated containers are used for transporting goods that must remain as specific temperature and humidity levels. Examples are frozen goods, perishable foods, and medicine.

[6] Source of container and chassis pictures: http://www.isocontainers.com

Open top containers are used in situations where the goods require very little protection from the elements. The best example is hauling dirt, tree branches, or even garbage.

There is a great surplus of containers in North America due to the fact that the U.S. has a merchandise trade deficit and has been outsourcing a great deal to foreign countries – most specifically China. (WTO.org, n.d.)

Some companies have been finding novel ways to use containers. For example, Disney stacked a wall of containers to use for the world premiere screening of the movie "Pocahontas."[7] They are also used as shelters, storage facilities and workshops.

2.1.2 Container Design

This paper will focus specifically on containers that can are sealable and can be transported using the three major modes – rail, truck, ship. Intermodal containers are designed in such a way that they can accommodate many different types of lifts and jacks. Figure 3 depicts the typical design of an intermodal container.

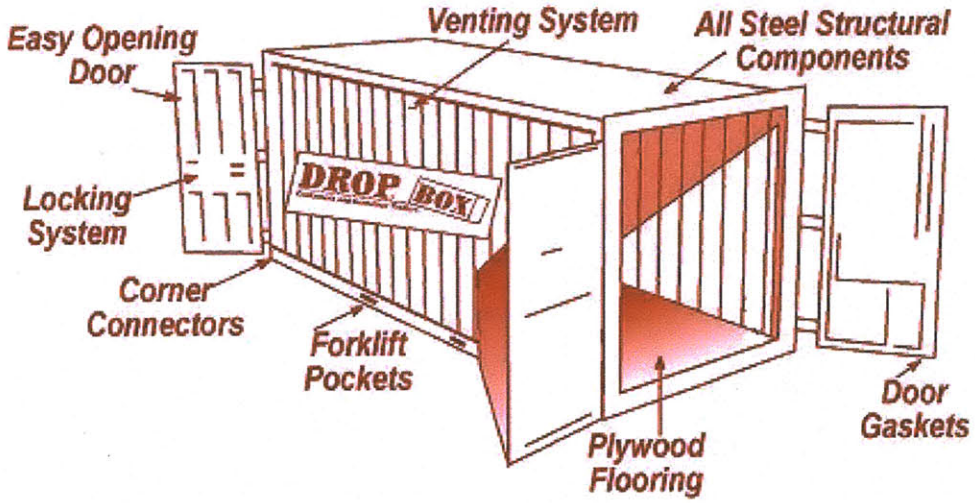


Figure 3. The design of a container is important when considering hardware integration. Diagram Source: http://www.dropboxinc.com/containers/index.htm

[7] Source: http://www.seabox.com/id-51

2.1.3 Transporting Containers

Containers are transported either by rail, truck or ship. A common occurrence is a combination of all three.

When transported by truck, the containers are loaded onto trailer chassis. The chassis are pulled by trucks.

When transported by rail, the containers are loaded onto an empty rail car. If overhead bridges in the area can accommodate it, containers can be stacked two high (double stacked).[8]

Containers travel on ships stacked many stories high.[9]

It is important to note that containers are loaded and unloaded onto rail cars, ships or trucks individually[10]

[8] Picture taken at Intransit Rail Yards, December 2004
[9] Photo Source: http://www.containerinfo.net/le%20container.htm
[10] Picture taken at Intransit Rail Yards, December 2004, Picture taken at Port of Barcelona, January 2005

2.2 Container Security

2.2.1 Security on the Container

Currently, the U.S. Government-approved security tags are small seals that are attached by hand to the container. If a container seal is compromised, the container is inspected upon arrival to a U.S. port. Containers are generally treated fairly roughly by large machinery, and seals are often damaged accidentally. This causes unnecessary inspection.

[11] Container seals are very small rubber and/or metal locks and/or bolts that are attached to the clasp of containers. Recently, stronger mechanical locks and bolts have been introduced to the market.

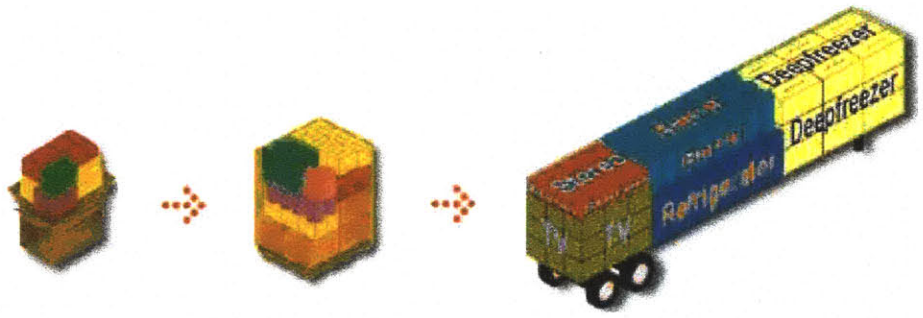
It should be noted that containers seals are removed at different border crossings and resealed. The seal found on a container at its final destination is unlikely to be the initial seal used when the container was loaded if it passed through customs in more that 1 country.

[11] Picture taken at Intransit Rail Yards, December 2004

2.2.2 Inspecting a container

Containers that arrive in ports are usually scanned for hazardous items by x-rays or gamma rays that penetrate the steel containers. Depending on the results, a container will either be loaded on to a ship or proceed to a more invasive examination which involves opening the container and searching through the goods. In 2002, the Australian government planned to "spend $190 million installing massive high technology x-ray machines which can detect anything from bombs to guns to drugs and can scan up to 100 shipping containers a day" (Epstein, 2002).

Containers are commonly loaded by hand or machine and items are stacked to fill as much volume as possible. Utilizing the maximum volume in a container is referred to as "cubing out."



Shipcases... to Mixed Pallets... to Trucks

Figure 4. Cases, pallets and containers are loaded according to software algorithms to maximize volume and weight. The configuration of containers must be considered when inspecting a container.
Diagram Source: http://www.topseng.com/MaxLoadFeatures.html

Containers can be loaded with multiple types of goods, and be partially refrigerated. There are many vendors that sell software specifically for load planning optimization. Figure 4 depicts an "optimally loaded" box, pallet and container.

This is important to note when attempting to conceptualize the effort and time it takes to completely search a container. It is also an area for potential system integration with customs organizations in order to facilitate inspection.

2.3 Risks Associated with Containers and Container Shipping

> The world's heavy reliance on shipping containers, coupled with their vulnerability, means that a terrorist attack using containers is not only possible but would also have high economic costs. The obvious problem is that it's hard to know what is inside the millions of sealed containers. They could be used to transport weapons or other destructive material. They could also be used as weapons on their own.
>
> (OSCE.org, n.d.)

The U.S. Customs and Border Patrol can "rule out 94% of the cargo as potential threats prior to arrival" in a U.S. port of entry (CBP5, 2004). This also means that only 6% of the cargo entering the country is actually inspected. Those containers that have been ruled out may have been safe at the time they left the area where they were sealed, but on their journey to America, there are numerous events that may have occurred. Some of the major risks associated with shipping a container, whether it is by truck, rail or ship are as follows:

- Stowaways & Human Smuggling
- Weapons Smuggling
- Nuclear Materials Smuggling
- Drug Smuggling
- Injection of Chemical and Biological Agents into the container
- Theft of Containers and their Contents (Piracy)
- Explosion or Leakage of Dangerous Materials
- Risk of Damage to Goods During Inspection
- Size of Maritime Vessels

2.3.1 Stowaways & Human Smuggling

In 2001, the U.S. border patrol apprehended 1.2 million people that tried to enter the country illegally. Since 1994, the Border Patrol has made 11.4 million apprehensions nation-wide.[12] Figure 5 demonstrates the living conditions within a container used to transport people from China to the United States.

Figure 5. Human smuggling often involves people living in a sealed container for many days and often weeks with no source of water or food, or pluming. Photo Source: http://msnbc.com/news/354340.asp?cp1=1

"According to the Congressional Research Service (CRS) and the U.S. State Department, 700,000 to 2 million people, the majority of them women and children, are trafficked each year across international borders. Thirty-five percent are under the age of 18 ... According to CRS, trafficking in people represents the third-largest source of profits for organized crime after drugs and guns, generating billions of dollars each year" (Orhant, 2002).

"In June 2000, in Dover, Great Britain, customs officials found 58 Chinese migrants dead. The 54 men and 4 women were asphyxiated in the airtight refrigerated trailer of a truck passing into England" (Interpol, 2005).

2.3.2 Weapons Smuggling

Weapons smuggling is a very profitable, global business that is of increasing concern as the threats of terrorism have increased over the last decade. In 1991, James Guerin, was indicted for laundering $700 million in weapons and cash over an 11-year period. According to testimony, Mr. Guerin and his team smuggled more than "$30

[12] http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/

million of military-related equipment to South Africa in violation of U.S. laws and a United Nations embargo. The material included missile parts, components for night vision goggles, and optical equipment...Some of the items involved ultimately were shipped to Iraq, which used them in artillery shells fired at U.S. troops during the Persian Gulf war." (Pasztor, 1991)

2.3.3 Injection of Chemical and Biological Agents into the container

Chemical warfare agents are among the easiest weapons of mass destruction to produce. "The toxicity of chemical agents falls generally between that of the more deadly biological agents and that of conventional weapons" (CIA, 1996).

- Choke Agents
- Blood Agents
- Blister Agents
- G-Series Nerve Agents
- V-Series Nerve Agents

All of these materials can be easily injected into a container while it is sitting at a truck-stop or on a train that has stopped for refueling, or on a ship that has been boarded in the middle of the night.

Biological warfare agents are just as easily injected into a container, their most effective use would be in a container carrying food.

- Bacteria
- Rickettsiae
- Viruses
- Fungi
- Toxins

All of these materials can be injected or piped through small holes into a container carrying food and the agents can eventually spread to farmland, livestock, grocery stores, pet food stores, etc.

2.3.4 Nuclear Materials

In August 1994, approximately 130 barrels of enriched uranium waste from a storage facility in South Africa was stolen. The location of the contents is still unknown. (CIA, 1996) A standard container can carry many of these barrels at a time. A container is large enough to easily accommodate multiple nuclear warheads.

The greatest threat in these cases is with the following scenario: a manufacturer that is classified as "low threat" for the U.S. CBP ships a container to the United States. The container is intercepted at sea during the night or on land while at a truck stop and the contents are switch from clothing to a barrel of enriched uranium, or a nuclear warhead. The container is then resealed and sent on its way without anyone knowing. If the container is not inspected, the contents will most likely make it through to their original destination.

2.3.5 Drug Smuggling

Drug smuggling generates approximately $20 billion yearly in revenues (mostly from cocaine and heroin) to its collaborators. The supply chain essentially has 3 major locations: source country, transshipment country(s), and destination country. The bulk of the drugs are produced in third world countries where governments have weaker security infrastructure and tend to be more corrupt. It is then transshipped to slightly richer nations where it is sorted and shipped to wealthier countries as a final destination. Premiums are paid at each step in the chain since the risk increases closer to the destination. Approximately 40% of all cocaine shipped is seized along the way. (Reuter, 2002)

What is important to note here is that the drug supply chain has several price markups that are domestic to a country. Once imported, drugs will pass through a chain of dealers and distributors who each take a percentage of the profits.

The United Nations International Drug Control Program estimates the international drug trade at $500 billion in 1997. Some of the expenditures are captured in Figure 6 below:

Estimated Illicit-Drug Expenditures by Nation

Nation	Dependent Users '000s	Per Capita Income (ca. 1994)	Drug Expenditures in $Billion	$ per Dependent User
Italy	170-420	$18,160	7-13	33,898
Sweden	17	$17,900	0.4	23,529
USA	2,700	$24,680	48.7	18,037
Australia	100-300	$18,530	2.0-4.4	16,000
Thailand	1,300	$6,350	1.1-1.9	1,154
Pakistan	3,000	$2,160	1.5	500

Figure 6. It is important to notice that illicit drug use is rampant throughout the supply chain, and monitoring is important from source to final destination. Source Data : (United Nations, 1997a)

A small number of nations account for the vast bulk of production of coca and opium. According to official estimates (e.g. U.S. Department of State, 1999), Myanmar and Afghanistan account for 90 percent of global opium production (3,100 tons out of 3,462 tons); Bolivia, Colombia and Peru account for all of coca production. (Reuter, 2002)

Heroin is usually found concealed in an array of different payloads; frozen fruit pulp containers, wooden furniture and sometimes even suspended in liquids.

2.3.6 Theft of Containers and their Contents (Piracy)

Container theft is a very serious and growing problem worldwide. As international trade and shipping proliferates and grows, so does the risk and instance of container theft. The risk further increases if the goods have a black market value. These goods include computers, entertainment equipment, name brand clothing and footwear, perfume, jewelry, cigarettes and prescription drugs. (Atkinson, 2001) "Worldwide, the direct cost of cargo theft [in 1991] is estimated at about $30 billion USD per year, with indirect costs many times higher" (Mayhew, 2001). The indirect costs stemming from

investigation and insurance payments can cost upwards of two to fivefold the direct losses – in the realm of $20-$60 billion USD. (U.S. General Accounting Office, 1980)

Cost Breakdown by Percentage

Transportation Method	% of Total	$30 Billion *Estimate*
Road Transport (Truck)	87%	$26.1 Billion
Maritime Cargo (Container Ship)	8%	$2.4 Billion
Rail Cargo	4%	$1.2 Billion
Air Cargo	1%	$300 Million

Figure 7. The majority of logistics costs are in the road transportation segment. Source data: (DeGeneste & Sullivan, 1994)

Trucks are inconspicuous, easily identifiable and often left unattended at truck stops, loading docks, and motels.

Maritime theft often occurs in ports (very often through organized crime), at sea when large container ships are boarded by pirates, and on offshore platforms. The goods are thrown overboard into smaller vessels.

2.3.7 Explosion or Leakage of Dangerous Materials

Refrigeration on ships provides the shipping industry with the ability to transport items over long distances that would normally expire through perishability.

Refrigerated containers (reefers) are more commonly cooled using the readily available ammonia. Freon was the standard until its negative environmental effects were discovered. The greatest benefit of a reefer is that the contents (usually food products) do not require unloading into a refrigerated cargo hold. This aids in the prevention of pilfering, loss and spoilage. The major issue with refrigeration is that it can create a combustible atmosphere, and in the event of fire, it will create higher concentrations of carbon monoxide.

Nitrogen is generated on refrigerated ships in order to cool a refrigerated cargo hold. Permeate, is the product of the generation process of Nitrogen and is a strong oxidizing agent and accelerates chemical reactions such as corrosion. It is also combustible. (Guldner, n.d.)

The issues in this section essentially create a situation where a container containing dangerous chemicals or a machine that can generate sparks is the equivalent of a bomb.

2.3.8 Risk of Damage, Loss or Theft During Inspection

When containers are inspected, the risk of damage to goods purely from handling or mishandling increases. When the contents of containers are removed and spread over the floor of a warehouse for inspection, the risk of loss or theft also increases. It is in the interest of customs, the manufacturer, the retailer, and insurance companies to reduce the number of unnecessary container inspections.

2.3.9 Size of Maritime Vessels

The final and most evident risk with regard to container shipping is at sea. Container ports and canals are being expanded in order to accommodate the ever-increasing size of new ships. If one container explodes, all other containers and the ship can sink and/or explode out at sea, or in a port. The larger the ship, the more fuel it can, and usually does carry on board.

China Ocean Shipping (Group) Company ordered four 10,000 Twenty-Foot-Equivalent (TEU)[13] container vessels. The next generation of vessels are expected to have capacities upwards of 18,000 TEU; enough to hold 22 to 24 containers across a 60-meter-wide deck and drafts of 15 to 21 meters. (Fry, 2005)

[13] **Twenty-Foot Equivalent (TEU):** a unit that expresses the relative number of containers based on the equivalent length of a 20' container. For example, 100 containers of 20' is 100 TEUs, while 100 containers of 40' is 200 TEUs. Source: http://www.export911.com/e911/ship/conShip.htm

Section 3 Sensors and RFID Telemetry

In 2002, the U.S. government enacted the United States Container Security Initiative (CSI). The goal of this initiative is to use information technology (IT) to identify, track, and target high-risk shipments for inspection. The existing port infrastructure cannot meet CSI requirements and hence there is a need for new and innovative ways of leveraging cutting-edge technology to cost-effectively meet the requirements. Government and industry are partnering to introduce "smart" containers that employ RFID tags to monitor containers. This collaboration is an extension of the Customs-Trade Partnership Against Terrorism (C-TPAT). It is referred to as the C-TPAT Plus. In fact, 32 ports in the North America are CSI compliant and are experimenting with RFID-enabled containers and about 20 countries have also adopted CSI (CBP1, 2004).

3.1 RFID – Active and Passive

Radio Frequency Identification (RFID) "is essentially the contemporary barcode" (Howe, 2004). It is a technology that allows businesses to automate the collection of supply chain information, thereby creating error-free fulfillment, delivery and visibility. Some of the advantages of RFID over barcodes are:

- No line of sight requirement
- A sealed tag can function in multiple weather conditions
- Long readability range
- Multiple tags can be read/written simultaneously
- Tracking is in real-time
- Tags can hold small amounts of data
- Weather resistant
- Most importantly, RFID tags provide a UNIQUE identification of an item

All RFID systems (Active and Passive) involve 3 main components:

1. Transponder: The RFID tag is affixed to and stores information about a specific object.
2. Transceiver: The RFID reader must be located within a certain distance from the tag and can read and write information to and from the tag.
3. Data Processing Subsystem: The systems that use the data collected from the RFID tag.

A chart defining the RFID class structure can be found in Appendix 2.

3.1.1 RFID Passive Tags

Passive tags do not have any self-contained power sources. They are powered remotely by the reader. The tags are comprised of a single chip and an antenna. Power is emitted from readers in proximity to the tag and the tag responds by command. Each tag contains an unalterable unique identification number which makes passive tags useful in item tracking and security. Passive RFID is frequently used with security badges in high security areas such as airports. These systems track the location, entrance, and exit of personnel through restricted and sensitive areas.

The Chinese government is evaluating the insertion of passive RFID tags into passports. The American government is experimenting with placing RFID tags in the passports of visitors to the USA. (Chabrow, 2005)

3.1.2 RFID Active Tags

Active tags have a power source (usually a battery) that powers a transmitter on the tag. They work more efficiently than passive tags in electro magnetically noisy environments. Comparing to the passive tag, the active tag has longer read ranges, larger data storage capacity, and greater programmability. When Active RFID is combined with sensors, active tags can send information to a reader automatically.

Advantages of Active over Passive RFID:

- Longer read range
  - Passive tags range is usually a few feet while active tags have ranges up to 85 meters
- Larger data storage capacity
  - Passive tags can hold very limited amount of information while active tags can store and save larger quantities
- Data can be sent at pre-programmed times
  - Passive tags are only activated when in the read range of a reader while active tags can activate themselves at pre-defined intervals and send information

The first practical application of active RFID systems was developed and used during World War II. There was a need to remotely identify allied planes to prevent friendly fire. This lead to the development of the Identification Friend or Foe (IFF) system. "This embodied all the basic features of RFID: an interrogatory radio signal was

picked up by the object to be identified, which then automatically replied by transmitting an identifying code" (Goodwins, 2005).

Another of the RFID success stories is EasyPass which allows vehicles to pass through toll booths without stopping. The tag is read and a system automatically debits a customer's account.[14]

When Active RFID is combined with sensors, active tags can send sensor information to a reader automatically. An example would be identifying unscheduled movements of inventory.

3.2 Sensors and What They can Presently Detect

Telemetry sensory can be connected to active RFID tags and used to monitor and detect different metrics that are useful to the supply chain stakeholders (Section 1.3.4) in order to mitigate risk. The sensors are actually used to measure changes in their respective metric such as temperature increase or humidity decrease. The currently available sensors can measure numerous parameters within the containers and will be discussed below:

1. **Ambient Temperature**
2. **Light**
3. **Humidity**
4. **Pressure**
5. **Vibration**
6. **Sound**
7. **Acceleration**
8. **Existence**
9. **Current Draw**
10. **Motion**
11. **Air Exchange**
12. **Explosives**
13. **Location**
14. **Radioactivity**
15. **Weapons Existence**
16. **Chemical**

[14] http://www.eazypass.ie/?sec=faq

A Note Regarding Sensors

Sensor telemetry provides information in analog format. In order for a computer to provide an analysis on the data, it must be converted into a digital format using an Analog-to-Digital Converter (ADC). "However, the way in which we capture environmental data digitally entails practical issues related conversion, resolution, error, delay, and power consumption" (Emery, 2005).[15] The bits are then sampled at predefined intervals to detect changes and patterns since the general idea is to transmit only deviations from a pre-existing state.

1. Ambient Temperature

The ambient temperature in a container will be measured in Fahrenheit, Celsius or Kelvin.

Figure 8. Temperature sensors can give fast and accurate readings with water resistance and physical robustness. Source: http://www.thermometrics.com/htmldocs/jdrel.htm

2. Light

Light sensors exist that are sensitive enough to detect existence and intensity as well as a broad wavelength light sources

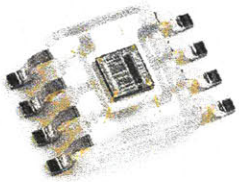


Figure 9. Light sensors can detect existence and intensity of light. Source: http://www.globalspec.com/FeaturedProducts/Detail?ExhibitID=8690&deframe=1

3. Humidity

Humidity sensors detect moisture levels in the atmosphere

Figure 10. This sensor can detect 10,922 humidity and 10,922 temperature measurements simultaneously in real-time. Source: http://www.omega.com/ppt/pptsc_right.asp?ref=OM-CP-MICRORHTEMP&Nav=temhu02&subsection=Hu02&book=Temperature&des=pptsc

[15] For information on practical issues related to conversion, please refer to (Emery, 2005)

4. Air Pressure
Air pressure sensors can detect present and changes in air pressure (measured in Pascals) to help control ventilation.

5. Vibration
Vibration sensors can detect small-scale linear velocity, spatial displacement and acceleration. This detects movement of the object being monitored.

6. Sound
Sensors can measure sound in frequency and decibels. They can detect changes in sound levels that range from sonic to ultrasonic

7. Acceleration
Sensors are able to detect movement of the container in any direction as well as the acceleration.

8. RFID tag Existence
A small RFID reader can be used to take an inventory of the RFID Passive tagged objects within the container.

Figure 11. This RFID reader is small enough to plug into any standard CF slot or PCMCIA slot with an adapter. Source: http://www.rfidjournal.com/article/articleview/393/1/1/

9. Current Draw: on the Tag
The Active RFID tag in the container will require monitoring. A current sensor can be placed on the tag to monitor current draw.

10. Motion
A motion sensor can be used to record movement inside the container.

Figure 12. This Motion Sensor can monitor human movements to measure body segment orientations (3D angles) and kinematic data (such as 3D accelerations) wirelessly with low-weight/low-power requirements. Source: http://www.xsens.com/index.php?mainmenu=applications&submenu=human_motion&subsubmenu=biomechanics

11. Air Exchange
Air exchange sensors can be used to determine air quality - carbon monoxide, carbon dioxide, formaldehyde, volatile organic compounds, etc.

12. Explosives
An explosives sensor can be used to detect any form of explosives the may enter the container.

13. Global Position
A Global Positioning System (GPS) can be used to monitor the container's physical location at all times.

14. Radioactivity
A radioactivity sensor can be used to determine existence and levels or radioactive materials inside the container.

15. Weapons Existence
Ultrasound sensors in early stages of development can scan an object or human and create an ultrasound image of the concealed object.

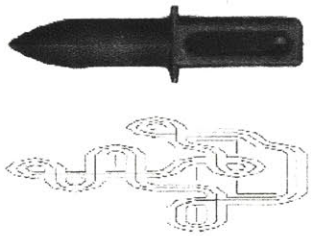


Figure 13. Ultrasound machines in development can create an ultrasound image of a concealed weapon. Source: http://www.jaycor.com/jaycor_main/web-content/eme_sens_ultra.html

16. Chemicals
"Researchers at the Georgia Institute of Technology have developed a chip-based machine that can detect illegal drugs similar to how a police dog does. The Dog on a Chip can recognize as little as one-trillionth of a gram of cocaine from as far away as a drug-sniffing dog could detect it. The research team is enhancing its device to detect additional drugs, chemical agents, bombs, and other harmful substances such as anthrax" (Paulsen, 2004).

Figure 14. Chips can detect cocaine vapor and potentially other illicit drugs and Anthrax. Source: http://www.computer.org/computer/homepage/0504/briefs

Section 4 Threats and Phenomena

Signatures observed by sensors can be interpreted as representing certain threats. Threats will be observed from different perspectives depending on the sensor. For example, human cargo will picked-up in a motion sensor as a moving object. In a humidity sensor, a human presence will be represented by an increase in humidity due to breathing and in a CO_2 sensor by a steady increase in CO_2 levels in the atmosphere.

> More than 90 per cent of global freight nowadays is shipped in containers. According to the World Shipping Council, there were almost 11 million maritime containers in circulation in mid-2003, most of which were not properly secured. Containers can be easily tampered with throughout the stages of their journey and used for terrorist or other criminal activities. (OSCE.org, n.d.)

In section 3, the available sensors were discussed. This section demonstrates how phenomena exhibited by sensors may be interpreted as behavior within the container. Figure 15 maps sensor data to behaviors.

A key assumption used in the creation of the following models is that the sensors will be functioning in a sealed, air-tight container, and will perform their function flawlessly. The sensors can function similarly in a non-air-tight container; however the results must be interpreted differently. Also, it assumes that sensing begins when the container is originally sealed. For instance, weapons smuggling can be exhibited in sensors as a container breach if inserted after the first sealing. This model assumes that the weapons were inserted at the start. If inserted later, the e-container will show signs of a container breach, and show the existence of weapons as well once inserted.

The second model in Figure 16, demonstrates the correlations made between phenomena and sensor identified risks.

The core findings of the modeling done in this thesis are illustrated when the sensor identified phenomena is interpreted as a manifestation of the risks identified in Section 2.3. Figure 17 demonstrates the correlations between sensor activities and the risks of container transport.

Phenomena vs. Sensor Model

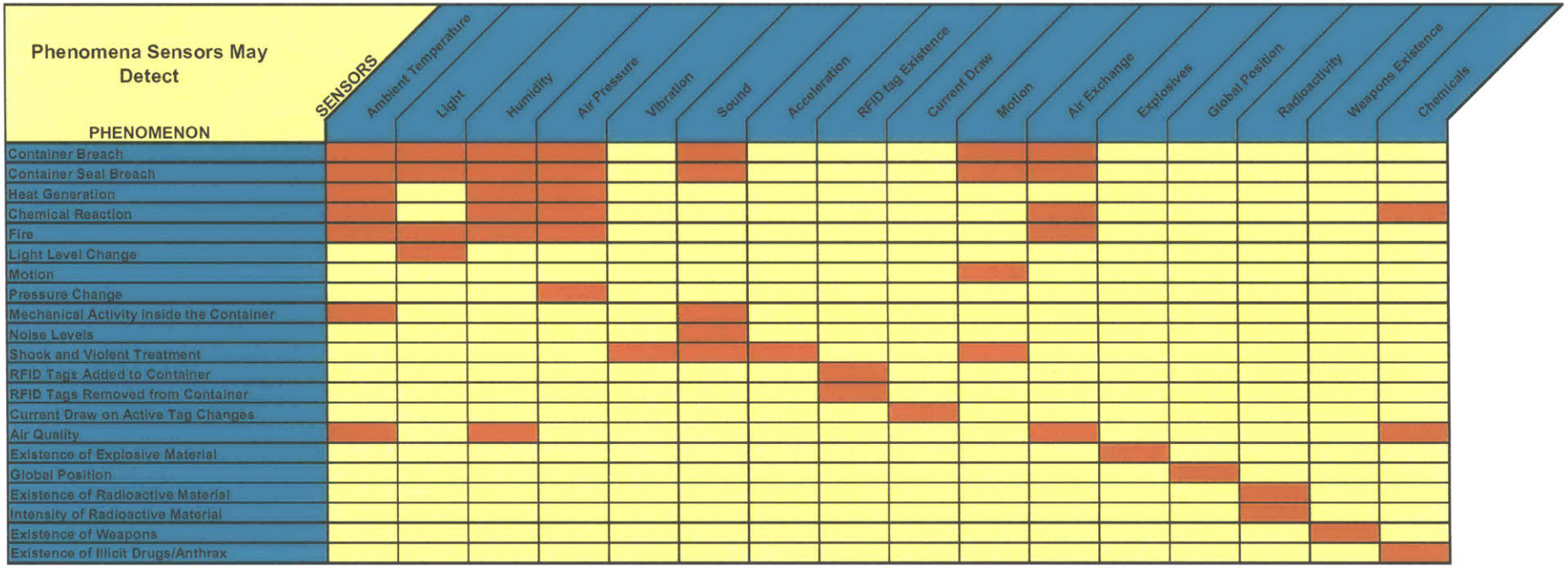


Figure 15. The phenomena sensors may detect is matched with each sensor or set of sensors

Phenomena Correlated to Identified Risks

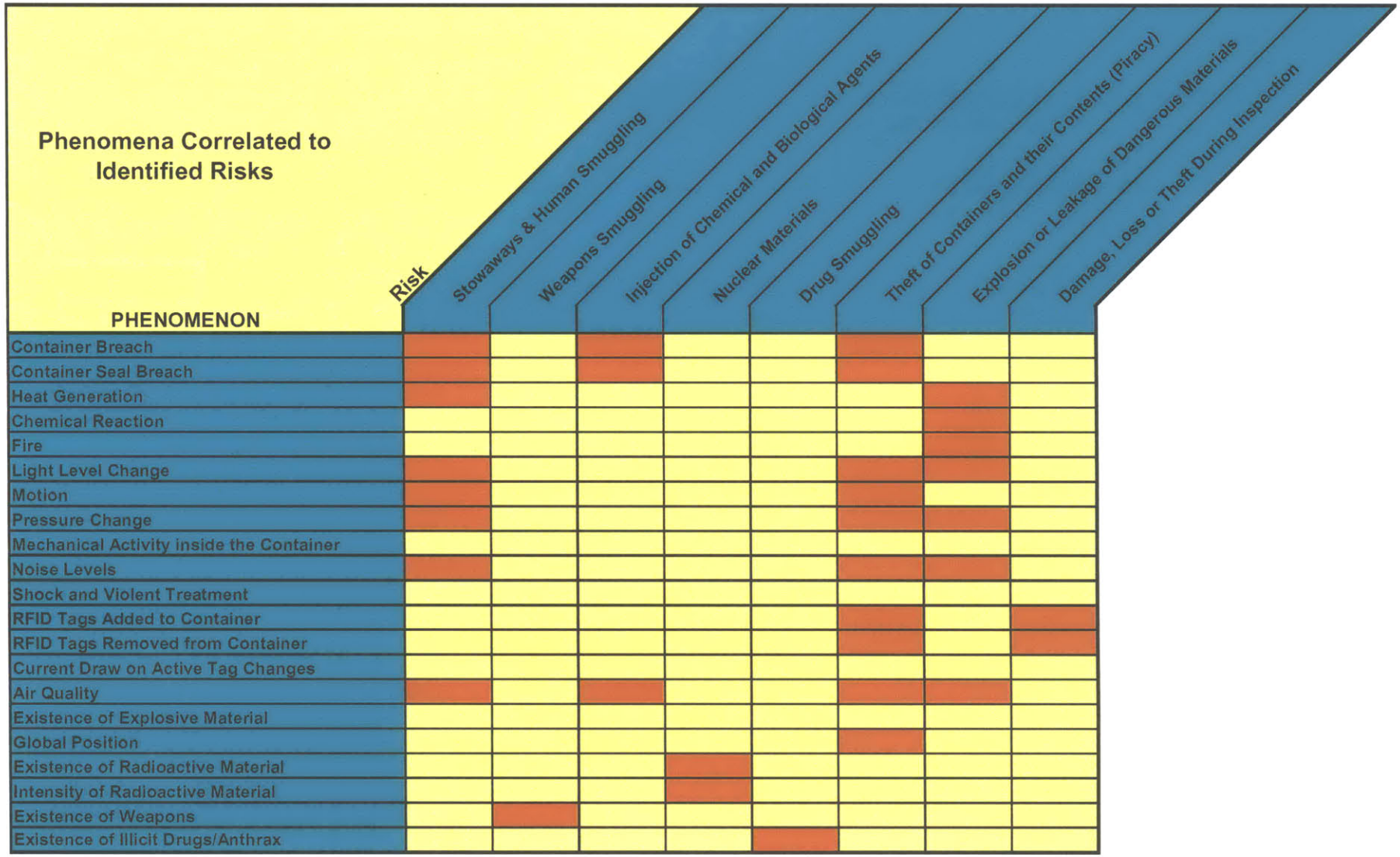


Figure 16. The phenomena sensors can detect is correlated to the Identified Risks from Section 2. It should be noted that in most cases, redundancy using combinations of sensors will obtain the desired result.

Sensors vs. Identified Risks

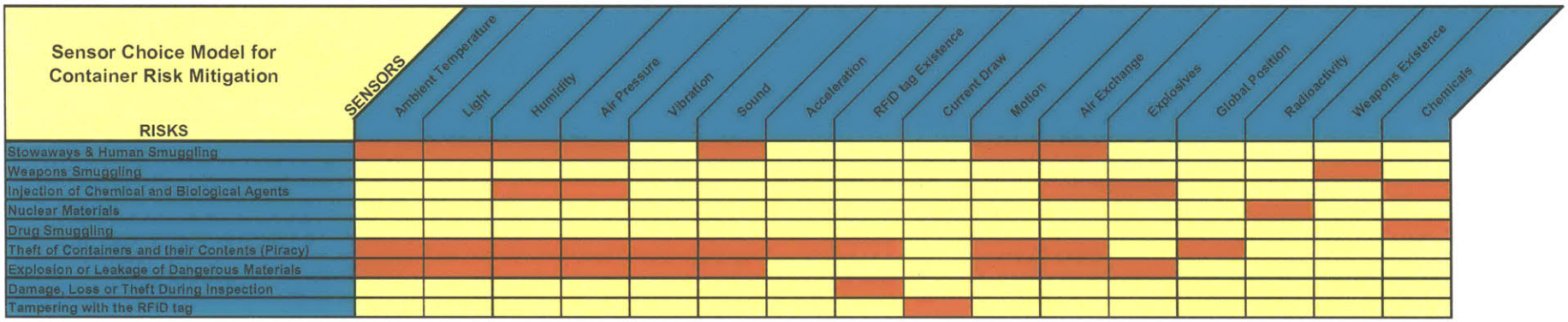


Figure 17. Model of Sensors vs. Identified Risks

4.1 Analysis of Findings

Figure 15 demonstrates the combinations of sensors that are required in order to identify the phenomena exhibited by sensors. There is sensor overlap. When some risks are mitigated using a set of sensors, others will be covered as well. Ports, shippers, governments and the CBP must decide which risks are more likely to occur, and must determine areas of investment.

It is obvious from the findings that the e-container is most effective at discovering an incident of tampering with a sealed container. It is more difficult to determine the safety of container contents. This means that it is relatively easier to detect if someone has broken into a container to insert something than it is to monitor the original items that were put into a container before it was sealed. The reason for this is that it is fairly simple to detect a container breach.

Explosions, Stowaways and Human Smuggling, and Container Theft are three risks that are easier to monitor since they can be observed using a multitude of different sensors. There are many behaviors and phenomena that can be used to interpret a container break-in, theft, or movement in the container. If items are tagged with RFID passive tags, maintaining an inventory of the items inside the container will inform shippers of items that have been removed and not replaced (during a customs inspection, items should be removed and replaced exactly how they were found).

Weapons smuggling is difficult to monitor. There are sensors in development that can scan for weapons, however there are no perfect scanning methods as of yet. It appears from the model that if we consider the situation where a container is sealed and later opened (breached) for weapon insertion, the e-container can treat weapons smuggling as a container breach, and once a breach has occurred, the container will be inspected.

There are some risks that can be discovered only using sensor designed specifically for identifying a specific phenomena. For example, nuclear materials can be discovered only using sensors designed to detect radioactivity and drug smuggling, can be detected only with chemical sensors calibrated for that purpose.

Monitoring the theft of items from a container equipped with an RFID reader will become increasingly easier as more objects are tagged with passive RFID chips.

Monitoring the goods manifest of a container while it is being inspected will save time, loss, and pilferage from the inspection process. In addition, monitoring the theft of an entire container is best done using a GPS and noting movement where it is unexpected.

Ambient Temperature, Humidity, Light, Air Pressure, Sound and Motion are the types of sensors that cover the greatest number of instances of sensor identified phenomena while Humidity, Air Pressure, and Air Exchange are the three most versatile sensors, as they span 4 different risk areas. Acceleration, Current Draw, GPS, Radioactivity and Weapons Existence on the other hand, are only useful for observing a single characteristic per sensor.

Finally, the most effective combination of sensors to use in order to mitigate all the identified risks is: RFID Existence, Air Exchange, Radioactivity, Chemicals, and Weapons Existence. Current draw can be used to detect tampering with the tag.

4.2 When a container must be inspected further

The U.S. CBP has invested in large x-ray machines to scan containers. These machines can x-ray a container and find 5 metal barrels for example, but they cannot determine the barrel's contents. Presently, if the CBP is interested in investigating these barrels further, they are required to open the container. Potentially, with further investment in the x-ray machines, or RFID sensors on containers, the CBP will be able to identify the contents of the barrels.

In section 2.3.9, a risk that was identified is that of the growing size of maritime vessels. If all containers were RFID enabled with the proposed system, a risk mitigation measure could be that the system monitoring all the containers would be able to identify containers that should be placed or stored separately from other containers. An example of this situation would be a container filled with magnets should be stored far from a container full of computer hard drives. Similarly, a container containing cow hides should be stored far from a container loaded with vegetables.

4.3 Customs issues with the technology

Customs often performs random container inspections. However, in order to keep the shippers from determining a pattern, and as part of their practice, they do not want the shippers to know when they perform inspections. It is important for customs to be able to reset the RFID tags and be certain that nobody will be able to know they searched a container.

There is another reason they need to be able to perform this action. I learned from interviewing a Canada Customs agent (who wishes to remain nameless), that if a container is inspected and drugs or contraband items are found, they will put everything back into the container and act as if nothing was found. The container will be monitored closely by camera and microphone in order to catch the criminals in the act and this footage is used as evidence in court.

Section 5 The e-Container – Mitigating the Risk

When the data from sensors is combined with active RFID, the ability to track the security and vital sign of a container emerges.

What this thesis proposes is a system that combines active RFID with a set of sensors (sensor choice model discussed in Section 4) located inside the container with the RFID antenna being the only part of the system on the exterior of the container. On the exterior, the antenna would be protected, and have its own specific sensor that would detect tampering.

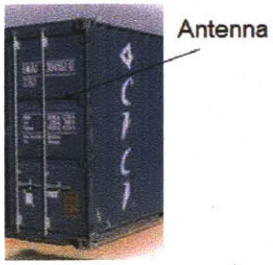


Figure 18. There are many areas on a container where an antenna could easily be inserted and protected.

The reader and tag would communicate more frequently than the present e-seal. However, the advantage of the e-container is that it does not only communicate the tag's unique identification number through RFID, it also communicates the sensor data in real-time.

5.1 Overall System Architecture

The system (Figure 19) gives an end-to-end visibility of the container shipment in real-time. A container can be tracked by satellite when sailing on the sea, by Wi-Fi / Wi-Max network when in the port proximity, or by cellular network when traveling on land. The container has a seamless transition from various readers with no interruption of service.

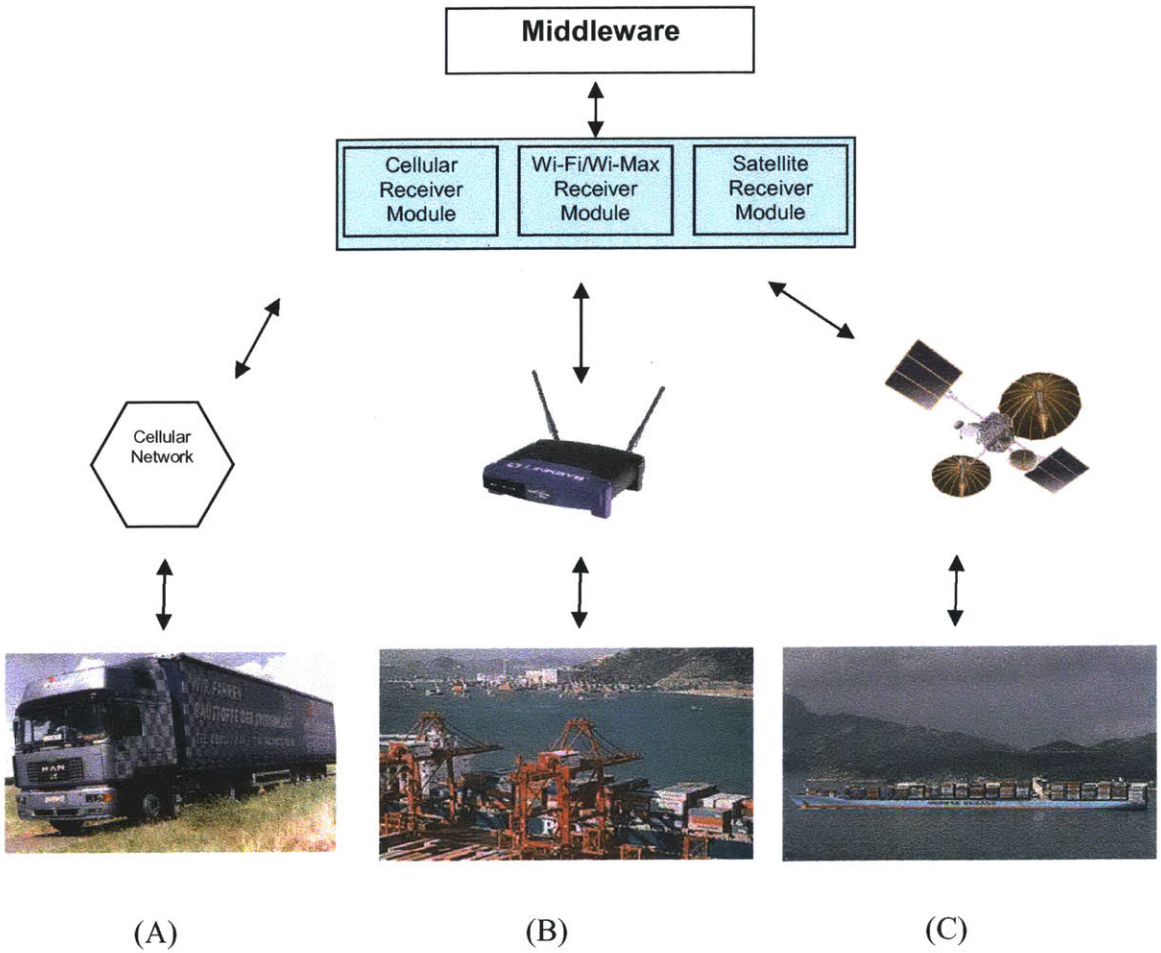


Figure 19. Proposed Overall System Architecture

5.2 The Components

The proposed system consists of the active tag, a reader and a centralized data center. Each component is described below at a high level:

5.2.1 The Active RFID Tag

The active tag is packaged into a rigid mechanical enclosure to ensure its operation in all environmental conditions.

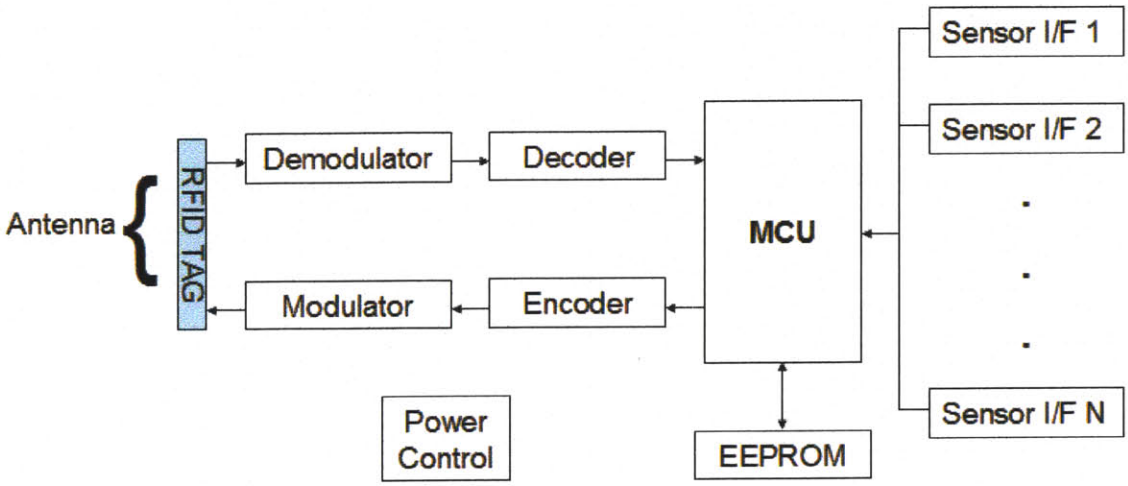


Figure 20. The Active RFID Tag - Explained below

The proposed active tags have the same components as conventional passive tags. However, to interface with the sensor interfaces (I/F) and to provide limited intelligence on the active tag, a miniature micro-controller is installed as part of the active tag. The Multi Controller Unit (MCU) collects sensor information from its various sensor interfaces and proceeds to either transmit directly to the reader through an antenna or store data temporarily on the EEPROM memory. Active tags are powered by batteries; the present e-seal battery guarantees are 10 years on average. These batteries would have a similar lifespan. The active tags are designed to be installed inside the containers while antennas are designed to be installed outside the container. The reason why antennas are installed outside the container is to overcome signal attenuation due to the metallic walls of the container. Presently, the e-seals are installed on the exterior of the container and as mentioned above, are prone to tampering.

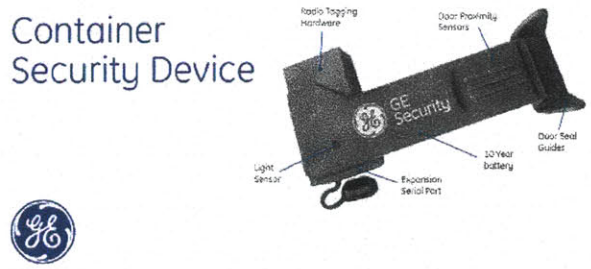


Figure 21. The e-Seal is affixed to the exterior of a container is and prone to tampering. Photo Source: http://www.geindustrial.com/ge-interlogix/docs/2004-2838_Sell.pdf

5.2.2 Active Tag Reader

The Active tag reader will be installed in different transportation modes such as container ships and trucks. Depending on the transportation mode, readers will be equipped with different communication mechanisms:

A) Cellular Functionality

Figure 22. Trucks would be fitted with RFID readers and The signals would be transmitted to the central data center via Cellular technology. Photo Source: http://www.the-truckers-page.com/behrendt.jpg

Each container truck has an active tag reader, which continuously collects the sensor data. The active tag reader communicates to the centralized data center through cellular network, such as GSM, GPRS, EDGE or CDMA network.

B) Wi-Fi/Wi-Max Functionality

Figure 23. RFID readers would be scattered throughout a port and on cranes in order to have a constant flow of information with total coverage. The signals would be transmitted to the central data center via Wi-Fi/Wi-Max technology. Photo Source: http://128.121.48.70/images/guides/hongkong/travel/customs1.jpg

The active tag reader will be deployed on top of the container crane within the container port as well. It communicates with the centralized data center through either Wi-Fi or Wi-Max.

C) Satellite Functionality

The container ship would share several common active tag readers and have an on-board Wi-Fi or Wi-Max network similar to that of the port. The will readers constantly read the responses from the active tags and in turn communicate with the on-ship communication system that will use global satellite services such as Inmarsat or GlobalStar to communicate with the centralized data center.

Figure 24. Satellite Communication is available at open sea. Photo Source: http://www.nas aexplores.com/show_912 _teacher_st.php?id=030509132457

Figure 25. RFID readers would be scattered throughout the ships in order to have a constant flow of information with total coverage. The signals would be transmitted to the central data center via satellite technology. Photo Source: http://www.cont ainerinfo.net/le%20container.htm

5.2.3 Centralized Data Center

The next logical question with regard to data collection is "what do you do with the data once it is collected by a reader?" and "How does the system work?"

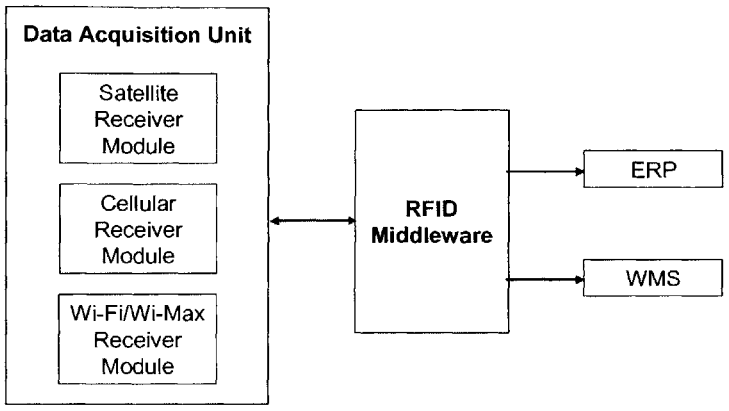


Figure 26. The Centralized Data Center interprets the collected outputs from the Active RFID tags and communicates with various applications and other systems

Centralized data center has a data acquisition unit, which collects outputs from all readers collecting data from active tags that are transmitting real-time information from sensors. RFID middleware will filter and aggregate the relevant information and feed the relevant information to various applications such as ERP, WMS or proprietary government security agency systems. It is important to note the bi-directional arrow between the middleware and the Data Acquisition Unit. With bi-directional communication between the Middleware and the sensors, system operators (the stakeholders) can request more detailed sensor information at will.

5.3 Data Transmissions

There are four types of data transmissions the container would use:

1. **Heart Beat**: Scheduled, used for synchronization - the container's active tag sends a small 1 or 2 bit message to the central system to confirm that all systems are functioning correctly and there has been no tempering[16].
2. **Threshold Break**: Unscheduled, event driven - if any of the sensors detect readings outside of the acceptable range, or if the container's sensors "think" that someone is tampering with the tag or any sensor, a tampering message would be sent to the central system. The message would include a date and time stamp, GPS location and unique identification number of container along with the affected sensor. (See Section 5.3.1)
3. **Scheduled Scan**: Scheduled to a regular programmed interval, the active tag in the container will send a full diagnostic with all collected sensor data to a reader. This information will then be sent to the central system for analysis.
4. **Manual Scan**: At any point, the active tag can be read on-demand by a designated reader.

5.3.1 Sensor thresholds

Sensors would have thresholds or ranges by which they would be monitoring and judging the container's contents. An example is humidity. The owner of the container may suggest that a humidity level of 25% with a standard deviation of 2% is normal. If the humidity in the container exceeds this range, there is a problem. An example problem could be that someone is breathing inside the container.

[16] Should be based on ISO standards

5.4 Other uses for the e-Container

The secondary consequence of this comprehensive security system for containers will be a real-time perishability manifest for customers. An example is a grocery chain importing fish, meat or other perishable goods. If one assumes a five day trip, and the container's monitoring system notices that oranges froze on day two, the company would know in advance and could order another shipment. This would allow the grocery chain to potentially lower safety stock levels since some variability could potentially be removed from the system.

Section 6 Conclusion and Future Research

6.1 Conclusion

This thesis analyzed the risks associated with global container transportation. The phenomena exhibited by each of the identified risks involved in global container shipping can be detected, identified, and monitored using an *e-container*. The e-container concept was set forth as a risk mitigation technology that uses real-time monitoring of a container's physical status acquired from an array of embedded RFID-enabled sensors. This integrated solution is used to capture metrics, and communicate this information to a centralized data center.

By modeling the correlations between sensor-identified phenomena and the risks, this thesis established the optimal selection of sensors to use in order to detect and monitor each risk. As long as one can identify risk occurrence, one can act upon it.

U.S. Customs and Border Protection Commissioner Robert C. Bonner called containers "the potential Trojan horse of the 21st century" (Keane, 2004). With the correct systems and sensors in place to identify and detect phenomena associated with risk, the 6 steel walls of a container become slightly more transparent.

6.2 Future Research

The next logical step in this research is to investigate how the Active Radio Frequency Identification tags, combined with a hybrid of mobile technologies which increase security and visibility throughout the supply chain will subsequently increase the velocity of cross-border shipments, and increase awareness of perishability level breaches – translating this information into cost savings.

It is my hypothesis (for future research) that if a container is tracked and its contents are monitored using the correct metrics, given the security levels of the system, the overall cost of international transportation will decrease; despite the cost of the system. The eventual cost savings will occur as a consequence of the following reasons:

- Reduced risk of inspection
- Shorter waiting times at the border
- Reduced border hold-ups
- Perishability Notices

Important questions that need to be answered:

1. Who determines sensor thresholds?
    a. Will it be the World Customs Organization?
    b. Will it be local governments?
    c. Will there be a world standard set?
2. If a threat is detected, what actions are to be taken?
    a. In a port
    b. On a ship
3. What are the repercussions and associated costs of a false alarm for each risk and who pays the bill?
4. What are the associated costs and ROI's?
5. How can you determine if a container is empty?
6. How will custody (of container) transfer points work?
7. What is the container lifecycle?
    a. How will the system be integrated into the container?
    b. When in the manufacturing cycle?
8. How will the RFID system be integrated into existing legacy, ERP and CRM systems.
9. How can this system help with:
    a. Yard dock visibility
    b. Scheduling
    c. Logistics management
    d. Visibility
        i. Customs
        ii. Suppliers

iii. Manufacturers

e. Reverse logistics

10. How will the e-container system be regulated?
11. What will be the role of the:
    a. DOD
    b. DHS
    c. CBP
12. What will be the effects on:
    a. CSI – Track all containers
    b. C-TPAT – Green Lane
    c. C-TPAT Plus – Green Lane

Section 7 Appendix

7.1 Appendix 1 - Interesting Border Patrol Facts for 2004

Source: http://www.dhs.gov/dhspublic/display?content=4257

U.S. Department of Homeland Security
2004 Year End Review

The following is a snapshot of 2004 accomplishments and statistics for the U.S. Department of Homeland Security:

Customs and Border Protection (CBP):

- 428 million passengers and pedestrians, including 262 million aliens, were processed at land, air, and sea ports of entry. Of that number over 643,000 aliens were deemed inadmissible under U.S. law.
- 1,158,800 illegal aliens were arrested by Border Patrol agents between our official ports of entry.
- The Container Security Initiative (CSI) was expanded to include 21 countries. CSI is now operational in 33 foreign ports in Europe, Asia, and Africa. The port of Dubai recently became the first Middle Eastern port to participate in CSI.
- Three months ahead of schedule, the Integrated Automated Fingerprint System (IAFIS) is now operational at all Border Patrol stations. From September through November, over 23,000 individuals with criminal records have been identified and arrested. 84 of those detained were murder suspects and 151 were wanted for sexual assault.
- The Customs-Trade Partnership Against Terror (C-TPAT) has become the largest government/private partnership to arise from September 11th. Just over 8,000 private sector members have applied to participate in C-TPAT.
- CBP officers and agents made 56,321 seizures of illegal drugs, with a total weight of 2,199,619 pounds. Of this number, CBP officers at official ports of entry made 47,744 seizures nationwide, weighing 844,222 pounds and worth an estimated $1 billion. CBP Border Patrol agents made 8,577 seizures, totaling 1,355,397 pounds of illegal drugs worth an estimated $1.62 billion between the official ports of entry.
- Together with Immigration and Customs Enforcement (ICE), CBP seized more than $138 million worth of counterfeit goods in FY 2004, up from $94 million worth of counterfeit goods in FY 2003.

Federal Emergency Management Agency (FEMA):

- FEMA provided $2.25 billion in aid for individuals and families affected by disasters. The outlay included $1.29 billion in housing assistance, $918 million for other needs assistance, such as medical expenses and personal property losses, and $30.98 million in unemployment benefits.
- More than 1.1 million hurricane victims have registered for assistance since mid-August, the highest ever. $1.43 billion has been spent for individual assistance needs and $1.15 billion in public assistance for the state and local governments.
- 15,560 federal workers were engaged in response and recovery operations for the declared disasters of 2004, including more than 11,000 FEMA personnel and 1,900 disaster medical specialists. As part of the massive response effort in Florida and other

hard hit states this past fall, 163 million pounds of ice, 10.8 million gallons of water, 14 million meals-ready-to-eat and 151,000 rolls of plastic roofing material were delivered to help meet immediate emergency needs.

Federal Law Enforcement Training Center (FLETC):

- Provided basic and advance law enforcement training to more than 44,750 students, representing 81 federal agencies, as well as state, local and international law enforcement organizations.
- Aggressively pursued new initiatives in support of homeland security; developing counter-terrorism training programs and facilities; enhancing intelligence awareness and analysis training offerings; and incorporating sophisticated technologies, such as computer generated or controlled simulations, into training.

Immigration & Customs Enforcement (ICE):

ICE was the second-largest federal contributor to the nation's Joint Terrorism Task Forces (JTTFs) with more than 300 ICE agents assigned to JTTFs nationwide.

- More than 2,500 criminal investigations were conducted involving the illegal export of U.S. arms and strategic technology, including Weapons of Mass Destruction.
- ICE made 1,368 arrests and brought 895 indictments for money laundering and other financial crimes, exceeding arrests and indictments of the prior fiscal year. ICE seized more than $202 million worth of currency, bank accounts, properties and vehicles as a result of financial investigations.
- More than 4,600 child sex predators were apprehended nationwide and over 2,100 child sex predators were deported. The first child sex tourism arrests were made under the Protect Act.
- A 112 percent increase over the prior year for fugitive apprehensions resulted in more than 7,200 arrests. More than 150,000 aliens were removed in FY 2004, 53 percent of who were criminals. This is an all-time record.
- Federal Protective Officers were responsible for 4,426 arrests - a 58 percent increase over the previous fiscal year. They responded to 430 bomb threats and 877 calls about suspicious packages and other items at federal facilities.

Transportation Security Administration (TSA):

Passenger screening has been effective in 2004 by keeping 6,501,193 prohibited items from coming on board aircrafts. The following is a partial list of prohibited items found during screening in 2004:

** 1,895,915 Knives
** 3,285,994 Other Cutting Instruments
** 294,694 Clubs
** 20,509 Box Cutters
** 598 Firearms
** 693,548 Incendiaries

- Over 3,000 arrests were made at security checkpoints.
- Approximately 650 million passengers traveled by air in 2004. 1.8 million Passengers traveled per day and experienced an average screening peak wait time under 12 minutes and an average wait time of 3 minutes in 2004.
- Approximately 600 million checked bags were screened using advanced explosive technologies in 2004.

United States Citizenship & Immigration Services (USCIS):

- 500,000 new United States citizens were naturalized.
- 9,000 active duty military personnel were naturalized through expedited processing. 35 million background checks of persons petitioning for immigration benefits were conducted.
- More than 20,000 children from around the world were adopted by U.S. families due to petitions processed by USCIS.
- Almost 50 million visitors sought information about immigration benefits and procedures from the USCIS web-site.

United States Coast Guard (USCG):

- 255,233 pounds of cocaine were seized breaking the record set in 1997.
- 10,348 migrants were interdicted.
- 5,498 lives were saved and 30,895 search-and-rescue cases were conducted. The Maritime Transportation Security Act (MTSA) was implemented. It is the largest maritime regulatory project in our nation's history, which entailed the establishment of 43 Area Maritime Security Committees as well as the creation of 43 Area Maritime Security Plans, almost 9,200 Vessel Security Plans, and over 3,100 Facility Security Plans.

United States Secret Service (USSS):

- 30 individuals involved in global cyber organized crime, domestically and internationally, were arrested through Operation Firewall. Industry experts estimate that $1 billion in total fraud loss was prevented.
- Completed 13,395 criminal investigations and arrested 5,566 individuals. Of these, 1,956 individuals were arrested for manufacturing or possessing counterfeit U.S. currency, which resulted in the seizure of 499 counterfeit production plants and $46.5 million in counterfeit currency.
- The Secret Service Electronic Crimes Task Force Initiative was expanded to include 15 task forces that work with federal, state and local law enforcement agencies across the country, prosecutors and experts from the private sector and academia.

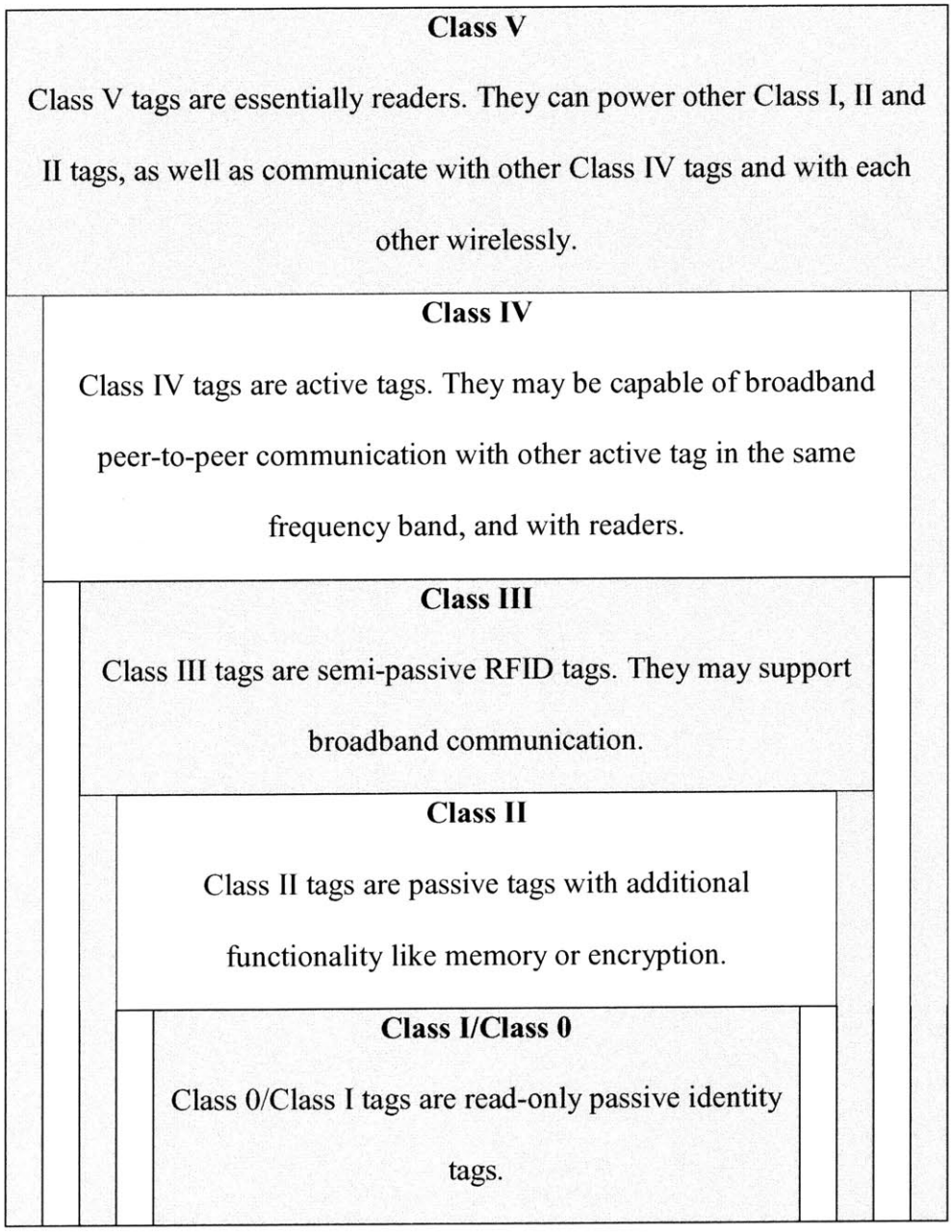
US-VISIT:

In January 2004, US-VISIT (was successfully implemented at all 115 U.S. international airports and 14 seaports. Since that time, more than 370 people with records of criminal or immigration violations have been prevents from entering the U.S. by Customs and Border Protection (CBP) Officers.

On September 30, Visa Waiver Program (VWP) travelers were included in US-VISIT and the program has now processed more than 14 million travelers while not increasing wait times and earning praise for its privacy efforts.

US-VISIT is now operational at the nation's 50 busiest land border crossings where significant time savings are already occurring.

7.2 Appendix 2 - RFID Class Structure



Source: http://www.autoidlabs.org/researcharchive

7.3 Appendix 3 - C-TPAT

In order to increase safety and security along the U.S. – Canadian border, the two governments have created the Free and Secure Trade (FAST) program - "...a common approach to risk management, partnering with those in the trade community who have a history of compliance and are committed to the integrity of their supply chain management processes, using compatible and advanced technology..." (DHS, 2002)

Since the September 11 attacks, the Customs and Border Patrol's (CBP) number one priority is to combat the threat of terrorism. As a sub-section of the FAST program, the CBP created the Customs-Trade Partnership Against Terrorism (C-TPAT) as a means for the trade community to collaborate with the CBP to ameliorate the security of international supply chains that flow through the United States. The C-TPAT is a certification that is awarded to companies which enables customs clearance more quickly and at a lower total cost. These are benefits that only the CBP can provide. The C-TPAT is a major federal initiative designed to make international shipping efficient and secure.

The following are the benefits the CBP provides though C-TPAT certification:

- A reduced number of inspections and reduced border wait times.
- A C-TPAT supply chain specialist to serve as the CBP liaison for validations, security issues, procedural updates, communication and training.
- Access to the C-TPAT members through the Status Verification Inter face.
- Self-policing and self-monitoring of security activities.
- In the Automated Commercial System (ACS), C-TPAT certified importers receive reduced selection rate for Compliance Measurement Examinations (-3X in FY 2003) and exclusion from certain trade-related local and national criteria.
- C-TPAT certified importers receive targeting benefits (-7X in FY 2003) by receiving a "credit" via the CBP targeting system.
- Certified C-TPAT importers are eligible for access to the FAST lanes on the Canadian and Mexican borders.
- Certified C-TPAT importers are eligible for the Office of Strategic Trade's (OST) Importer Self-Assessment Program (ISA) and have been given priority access to participate in the Automated Commercial Environment (ACE).
- C-TPAT certified highway carriers, on the Canadian and Mexican borders, benefit from their access to the expedited cargo processing at designated FAST lanes. These carriers are eligible to receive more favorable mitigation relief from monetary penalties.
- C-TPAT certified Mexican manufacturers benefit from their access to the expedited cargo processing at the designated FAST lanes.

- All certified C-TPAT companies are eligible to attend CBP sponsored C-TPAT supply chain security training seminars. (CBP1, 2004)

The C-TPAT certifications are industry specific. For example, there are different certifications for Importers, Air Carriers, Foreign Manufacturers and Air Freight Consolidators (CBP2, n.d.). Interestingly, the C-TPAT is not required, and application is entirely voluntary. Initially, the program will give companies a competitive edge by granting quicker, hassle-free movement of goods across the border as well as formal security training and other advantages. However, as a greater number of companies are awarded the certification, the C-TPAT will in all probability become an industry standard, and companies that do not apply, or are denied a C-TPAT, will be at a competitive disadvantage.

One of the greatest benefits of the C-TPAT is that with a faster and more reliable flow of goods through the border, companies can better forecast inventory needs and lower safety stock levels. If the program functions properly, one of the potential benefits of the C-TPAT is that companies will have a higher percentage of on-time deliveries. This will allow them to lower safety stock, and should help companies get closer to just-in-time levels of inventory. This having been discussed, the CBP has been slow to react to criticism about the program not meeting expectations.

A major problem companies are facing regarding C-TPAT certification is the cost. The largest costs are not in terms of filling forms or paying for inspections, they are the internal costs and investments in security and consulting. Firms often have to change legacy Information Technology (IT) systems so they can be capable of collecting additional information (NAFTA Certificate of Origin, HS Codes, copies of shipping documents, etc.), change processes, train employees on new processes, and hire consultants to actually define and design the processes.

As the C-TPAT rules evolve, many of the initial all-voluntary guidelines have become regulation. This demonstrates a shift in strategy. Obviously, as the C-TPAT voluntary rules increasingly become regulation, the C-TPAT essentially becomes mandatory. Either way, voluntary or not, companies will have to subscribe to the C-

TPAT rules in order to be competitive or follow regulation – thus, it is in a company's best interest to become C-TPAT compliant and apply for certification as quickly as possible. There have been arguments amongst the National Industrial Transportation League (NIT) and the CPB regarding the present certification rules due to the fact that businesses are not experiencing the promised benefits from their multi-million dollar investments in the program. NIT League Executive Vice President Peter Gatti wrote: "It would also lead many existing participants to re-evaluate whether to continue with the C-TPAT program based on the costs and liability risks associated with the proposal as compared to the benefits derived from C-TPAT" (Keane, 2004).

Some of the major complaints industry has put forth are that shipments are not moving any quicker through the border, nor are they receiving the variety of training that was promised. The information regarding shipment information has also been incomplete or missing.

The C-TPAT program, once the CBP pulls out of this early stage of development, in essence, should be a win-win for the import industry players and the CBP. However, notwithstanding the fact that the program is in its early stages of implementation, the CBP must still work out some of the aforementioned issues if it is to win the support it requires for the program to be considered successful.

Section 8 Bibliography

Atkinson, W. (2001). "How to protect your goods from theft", Logistics Management and Distribution Report, no. 3, March. Retrieved March 12 2005 from http://www.manufacturing.net/lm/index.asp?layout=articleWebzine&stt=001&articleid=CA68557&pubdate=03/01/01

Kulisch, E. (April 2005). 'Smart box' not ready for prime time. *American Shipper*, pp 14-22.

Bank, R. (2004, August). Too Important to Ignore. *Journal of Commerce*, P.1.

Beadle, A. (2004, June). Logistics Costs, Quantified. *Journal of Commerce*. pp. 1.

Canadian Border Services Agency. (2005, January). *Pallet Vehicle and Cargo Inspection System*. Retrieved March 30, 2005 from http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2005/0125pvacis-e.html

CBP1 : U.S. Customs and Border Protection. (2004, November). *Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan.* Retrieved January 19, 2005, from the U.S. Customs Web site: http://www.customs.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf

CBP2 : U.S. Customs and Border Protection. (n.d.). *Commercial Enforcement.* Retrieved January 19, 2005, from http://www.customs.gov/xp/cgov/import/commercial_enforcement/ctpat/

CBP3 : U.S. Customs and Border Protection. (2004, December). JORDAN: World Customs Organization endorses plan to secure and improve the flow of global trade. *Cargo Security International.* Retrieved February 28, 2005 from http://www.cargosecurityinternational.com/channeldetail.asp?cid=11&caid=3904

CBP4 : U.S. Customs and Border Protection. (2002, March). *Container security initiative to safeguard U.S., global economy.* Retrieved February 28, 2005 from http://www.cbp.gov/xp/CustomsToday/2002/March/custoday_csi.xml

CBP5 : U.S. Customs and Border Protection. (2004, October). Fact Sheet: Cargo Container Security - U.S. Customs and Border Protection Reality. Retrieved March 24, 2005 fromhttp://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/5percent_myth.ctt/5percent_myth.doc

Chandler, P. (1994, December). Rockin' and rollin' to a new air cargo beat. *Global Trade & Transportation.* 114 (12), 37.

Chabrow, E. (2005, January). Homeland Security to Test RFID at Borders. *Information Week*. 1024, 26.

CIA (1996, March). *The Continuing Threat from Weapons of Mass Destruction Appendix B: Chemical Agents*. Retrieved February 10, 2005 from http://www.cia.gov/cia/public_affairs/speeches/1996/go_appendixb_032796.html#methods

DeGeneste, H. & Sullivan, J. (1994). *Policing Transportation Facilities*. Illinois: Charles C. Thomas.

DHS : Department of Homeland Security. (September 9, 2002). *United States - Canada Free and Secure Trade Program the FAST Program*. Retrieved January 19, 2005, from http://www.dhs.gov/dhspublic/display?theme=43&content=349&print=true

Delaney, K. (2004, January). Inventory Tool to Launch in Germany; Wireless System Is Seen As Successor to Bar Codes; Metro AG Leads Wal-Mart. *Wall Street Journal (Eastern edition)*. B.5.

Emery, K. (2005, June). Unpublished Masters Thesis. *Eventing Architecture Considerations: RFID and Sensors in the Supply Chain*. Massachusetts Institute of Technology.

Epstein, R. (2002, November 26). *The World Today*. Retrieved April 11, 2005 from http://www.abc.net.au/worldtoday/stories/s735211.htm

Goentzel, J. (2004, November). Vehicle Routing Problems. *MIT Course Notes - ESD.260*.

Goodwins, R. (2005, February). IT Special Report. *ZDNet UK*. Retrieved February 21, 2005, from http://insight.zdnet.co.uk/specials/rfid/0,39026568,39153971,00.htm

Gordon F. & Thompson, M. (2005). Containing the Containers: Assessing Marine Risk Accumulation. *Exposure: Property & Engineering*. (14) 1-2 Quarter. Retrieved March 13, 2005 from http://www.geinsurancesolutions.com/erccorporate/theinstitute/pc/inst_pub_exposure_issue14_art6.htm

Guldner, T. (n.d.) *The Marine Firefighting Institute. Hazards of Refrigeration In Ocean Shipping*. Retrieved March 13, 2005, from http://www.marinefirefighting.com/Pages/Newsletters/Newsletter5.htm

Howe, A. (2004). The Implications and Benefits of RFID. *Retail World*, 57 (20), 34.

Huska, K. (1998). Truck hijackings and cargo theft in Mexico. Issues in Global Crime, United States Department of State, Bureau of Diplomatic Security, Washington DC, pp. 70–75.

Interpol. (2004). *People Smuggling: Challenge and Response*. Retrieved March 24, 2005 from http://www.interpol.com/Public/ICPO/FactSheets/FS15.asp

Keane, A. G. (2004, July). Stopping "Trojan Horses". *Traffic World*, P.1.

Keane, A. G. (2004, December) Shippers Unhappy With C-TPAT Changes. *Traffic World*, P.1.

Locher, M. (2005, January). Unpublished White Paper: *Supply Chain Stakeholders*.

Office of National Drug Control Policy. (1997b) *What America's Users Spend on Illicit Drugs, 1988-1995*. Washington, DC: U.S. Government Printing Office.

Orhant, M. (2002, January). Human Trafficking Exposed. *Population Today*. 2 (1), 3-4.

OSCE.org. (n.d.). *Containing Terrorism*. Retrieved March 13, 2005, from http://www.osce.org/features/show_feature.php?id=260

Pasztor, A & Pound E.T. (1991, November 1). South Africa's Arms Concern, Others Indicted in Weapons-Smuggling Scheme. *Wall Street Journal (Eastern edition)*, pg. 1.

Paulson, L. D. (2004, May). Dog on a Chip. *Computer*. Retrieved April 28, 2005, from http://www.computer.org/computer/homepage/0504/briefs/

Public Citizen. (n.d.). *Harmonization*. Retrieved February 22, 2005, from http://www.citizen.org/trade/harmonization

Reuter, P. (2002, October) Transnational Crime: Drug Smuggling Paper prepared for conference on Transnational Crime, University of Cambridge, January 7, 2000.

Roberti, M. (n.d.). Boeing, Airbus Team on Standards. Retrieved December 9, 2004, from http://www.rfidjournal.com/article/articleview/934/1/1/

Selwitz, R. (1994). NAFTA expansion possibilities. *Global Trade & Transportation*, 114 (10), 17.

Songini, M. (2004, July). Supply Chain System Failures Hampered Army Units in Iraq *Computerworld*. 38 (30), 1-2.

The Edge Singapore (2005, January). Case Stories: The third-party niche. *LexisNexis*. Retrieved February 24, 2005, from http://www.manufacturing.net/lm/index.asp?layout =articleXml&xmlId=255603656

Understanding the WTO. (n.d.). *Chapter 2: The Agreements*. Retrieved February 22, 2005, http://www.wto.org/english/thewto_e/whatis_e/tif_e/utw_chap2_e.pdf

United Nations. (1997a). International Drug Control Program *World Drug Report* Oxford: Oxford University Press.

U.S. General Accounting Office. (1980). *Report by the Comptroller General of the United States: Promotion of Cargo Security Receives Limited Support.* U.S. General Accounting Office. Washington DC.

WTO.org. (n.d.). *International Trade Statistics: 2003*. Retrieved March 1, 2005, from http://www.wto.org/english/res_e/statis_e/its2003_e/its03_overview_e.pdf