# The Intelligent Container Concept: Issues, Initiatives, and Implementation

by

Peter Christopher Bryn

B.S. Naval Architecture and Marine Engineering (2006)
Webb Institute

SUBMITTED TO THE DEPARTMENT OF CIVIL AND ENVIRONMENTAL ENGINEERING
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF

MASTER OF SCIENCE IN TRANSPORTATION
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2007



Signature of Author: _____
Department of Civil and Environmental Engineering
May 25, 2007

Certified by: _____
Professor Henry S. Marcus
Professor of Marine Systems of Mechanical Engineering
Thesis Supervisor

Certified by: _____
James B. Rice
Director of Integrated Supply Chain Management Program of
the MIT Center for Transportation and Logistics
Thesis Reader

Certified by: _____
Professor Nigel H.M. Wilson
Director of Master of Science in Transportation Program of
Civil and Environmental Engineering
Thesis Reader

Accepted by: _____
Daniele Veneziano
Chairman, Departmental Committee for Graduate Students

# The Intelligent Container Concept: Issues, Initiatives, and Implementation

by

Peter Christopher Bryn

Submitted to the Department of Civil and Environmental Engineering
on May 25, 2007 in Partial Fulfillment of the
Requirements for the Degree of Master of Science in
Transportation

**ABSTRACT**

Shipping containers have been under increased scrutiny in recent years for two primary reasons. Within the private sector, they are one component of a continuing process by organizations to use effective supply chain management to their competitive advantage. Within the public sector, they are the central focus of a growing concern over cargo security. Indeed, these issues involve many parties, including regulators, carriers, shippers, container solution providers, research, and academia. Many of the proposed solutions involve new strategies, systems, and technologies applied to containers that fall into what this paper calls the "intelligent container concept." As a relatively nascent field, information is currently very fragmented, standards are still being researched, and few universal goals exist. This study is focused on compiling, understanding, and organizing the universe of options available, the concerns of the parties involved, the relevant and significant initiatives underway or completed, and the issues surrounding implementation. While cost and technology are critical components of the debate, this study focuses more on the benefits that the proposed solutions might add and how they can be incorporated into the supply chain. This study is intended to familiarize the reader with the status and extent of the intelligent container field, though does not delve into the cost or technology issues since they vary greatly and are supply chain specific.

Thesis Supervisor: Henry S. Marcus
Title: Professor of Marine Systems of Mechanical Engineering

Thesis Reader: James B. Rice
Title: Director, Integrated Supply Chain Management Program of the MIT Center for Transportation and Logistics

Thesis Reader: Nigel H.M. Wilson
Title: Director of Master of Science in Transportation Program of Civil and Environmental Engineering

# ACKNOWLEDGEMENTS

I would first like to acknowledge Professor Henry Marcus, my academic and thesis advisor, for his help, guidance, and support here at MIT. Without him, neither this thesis nor my graduate studies would likely have been possible.

Secondly, though no less importantly, I would like to thank Mr. James Rice at the MIT Center for Transportation and Logistics as well for his guidance and support during all stages of this work.

Additionally, a thank you is in place for everyone who provided help along the way, including the librarians at the MIT Libraries and those in industry who were willing to offer a practitioner's point of view to complement the academic background provided in the literature.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# BACKGROUND NOMENCLATURE

## RELEVANT BODIES AND REGULATIONS

| | |
|---|---|
| AMR | Advanced Manifest Rule (24-hour rule): a CBP initiative (part of the ATDI) requiring advanced submittal of cargo manifest data |
| AMS | Automated Manifest System: systems to electronically submit manifest declarations to DHS |
| APEC | Asia-Pacific Economic Community: an economic forum group of countries bordered along the Pacific Ocean |
| ATDI | Advanced Trade Data Initiative: a CBP request that cargo manifests be sent in advance of arrival to the US The 24-hour rule is part of this initiative. |
| ATS | Automated Targeting System: a system implemented by DHS to assess the risk of incoming containers |
| CBP | Customs and Border Protection: a national agency that maintains control over the importation and exportation of goods into a country; unless otherwise specified, refers to US in this report; US CBP is part of US DHS |
| CSD | Container Security Device: although used as a general term typically to describe an ICC that is somewhat more complex and an e-seal, "CSD", or "Advanced CSD" (ACSD), actually refers to a DHS initiative intended to make a container more secure |
| CSI | Container Security Initiative: a DHS-initiated program that places US inspectors in foreign ports and works cooperatively to scan US-bound containers before they leave port |
| C-TPAT | Customs Trade Partnership Against Terrorism: a DHS-initiated program to "validate" players in supply chains as having developed an approved security plan; in return, CBP intends to provide expedited handling and reduced inspection |
| DHS | Department of Homeland Security: a US executive federal department that is responsible for security within the borders, both physical and virtual, of the United States |
| ILWU | International Longshore and Warehouse Union: a labor union that represents longshore and warehouse workers in the US and Canada |
| IMO | International Maritime Organization: a division of the United Nations that oversees the safety and security international maritime affairs |
| ISPS | International Ship and Port Security Code: an IMO regulation, which is part of Safety of Life at Sea (SOLAS), that provides general requirements for security relating to ships and ports, to be implemented and interpreted by each signing nation |

| | |
|---|---|
| MATTS | Marine Asset Tag Tracking System: a DHS initiative to develop a "Future Smart Container" |
| TSA | Transportation Security Administration: a division of DHS responsible for securing transportation systems, including highways, railroads, buses, mass transit, sea and airports |
| TWIC | Transportation Worker Identification Credential: a TSA-initiated program to develop and implement background checks for all unescorted workers in seaports |
| USCG | US Coast Guard: a division of DHS responsible for the safety and security of maritime activities |
| WCO | World Customs Organization: an independent non-profit organization comprised of member nations throughout the world |
| WSC | World Shipping Council: A consortium of ocean carriers that provides a single voice for the industry. |

## RELEVANT SUPPLY CHAIN MANAGEMENT CONCEPTS

| | |
|---|---|
| JIT | Just-In-Time: an SCM philosophy that maintains very low inventories as parts are delivered "just in time" for use |
| SCM | Supply Chain Management: the process of planning, implementing, and controlling the flow of goods with the purpose of satisfying customer requirements as efficiently as possible |
| SKU | Stock Keeping Unit: a number describing one item maintained in stock (could refer to both an individual part in a retail store or box full of parts in a warehouse, depending on the stocking situation) |

## RELEVANT TECHNOLOGY

| | |
|---|---|
| EDI | Electronic Data Interchange: a standard electronic format with which to exchange cargo data and business information |
| EPC | Electronic Product Code: an RFID-based collection of coding schemes created as an eventual successor to product bar codes |
| GPS | Global Positioning System: a satellite based system that provides realtime global location tracking |
| RFID | Radio Frequency IDentification: a radio-frequency based communication method that provides remote identification of a tag within the reader's region |
| SKU | Stock Keeping Unit: an index used by merchants to identify individual goods or services |

# 1. INTRODUCTION

## 1.1 PURPOSE AND MOTIVATION

The purpose of this study is to identify, organize, and assess the universe of intelligent container concepts (ICCs) available today by taking an approach focused on value-added to the supply chain. ICCs are defined in this report to include any process, system, or modification to a conventional shipping container that can be used to either provide additional information about or control some characteristic of a the container or its cargo.

This study is deemed valuable since a significant literature review has not produced any similar study as comprehensive. Instead, most efforts to date focus either on the technological complications of ICCs or look at one particular application of a technology, commonly RFID and security. Therefore, a need was seen to capture and classify the current universe of ICC drivers, issues, and initiatives. This approach should aid a supply chain professional to better understand and make general decisions about ICC implementation before attempting a more specific analysis for his/her specific supply chain.

An important opening disclaimer is the recognition that ICCs are not viewed in this study as a panacea or turnkey solution. It is clearly recognized and respected that an ICC must support the supply chain's ultimate goal as established by the corporate strategies of all parties involved. Further, implementation of an ICC is unlikely to be effective unless (1) it is well understood and accepted by the various parties in the supply chain and (2) all necessary changes needed to fully realize the benefits that the ICC may provide are made. Therefore, while ICCs may be the catalyst for a system-wide upgrade, they are not likely to be the entire solution. This point is raised throughout the study and also discussed in greater detail in *5.1 ICCS AS A SUPPLY CHAIN COMPONENT*.

## 1.2 SCOPE

This study is intended to document and categorize the ICC industry with a particular focus on how ICCs may add value to the supply chain. Since the study covers no specific ICC or supply chain, discussion is necessarily qualitative with limited effort made to address cost or technological concerns. Although these issues are critical to analyze any actual implementation, they vary greatly depending on each initiative, and are therefore reserved for application-specific studies.

Key follow up questions for a supply chain professional reading this study might be, "what is the monetary value of these benefits to my supply chain, what is the state of the technology, how do the regulations discussed affect my supply chain, and what costs exist?"

## 1.3 OBJECTIVES

The specific objectives of this study are to:

1. Establish an appropriate definition for ICCs.
2. Consider general supply chain issues and existing methods, then infer how ICCs might affect them.
3. Understand the universe of intelligent container concepts and develop a taxonomy for it. Include such items as affected parties, regulatory drivers, technical capabilities, initiatives underway, industry opinion, and implementation issues.

### 1.3.1 Tasks to fulfill objectives

To fulfill the stated objectives, the following tasks are to be completed:

1. Conduct a literature review on concepts relating to intelligent containers, security and regulatory issues, supply chain management issues, conveyance tracking, technology and cost issues, etc.
2. Organize the research data to understand the state of the field and major issues confronting it.
3. Develop a taxonomy for the different issues and establish commonality when appropriate.

# 2. INTELLIGENT CONTAINER CONCEPT (ICC) PRIMER

## 2.1 DEFINITION

The "intelligent container concept," or ICC, in this report refers to any method, technology, or system used to monitor or control some characteristic of a shipping container or its cargo in order to provide additional information to parties in the supply chain.

## 2.2 TAXONOMY

Since this is a nascent and developing subject area, this study first attempts to classify the ICC universe by using different common key qualifiers. Note that there are varying degrees of overlap in these categories.

### 2.2.1 By proposed benefit

ICCs are of interest because of the potential benefits they may provide. These benefits are broadly broken into two main categories: Supply Chain Management and Security and Safety.

- Supply chain management
    - Custodial transfer declaration and customs manifesting: automatically declare the arrival of a container for both the port at which the transfer occurs and customs clearance
    - Container and cargo tracking: track containers either on a realtime/near realtime basis, or when intermodal transfers occur
        - Improve supply chain information prevalence and quality: automated processes tend to increase the amount and improve the quality of data available
        - Cargo-centric approach: consider the container as the key item in supply chain, rather than focusing on each mode; this may help improve communication among parties ("join the silos")
        - Supply chain resilience: rapidly respond to supply chain disruptions (equipment failure, terrorism, labor strike, etc.) or locate container while in transit if re-routing or intentional delay is desired
        - Supply chain streamlining: improved information on tracking allows shipping managers more flexibility to make better decisions; long term planning methods increasingly rely on supply chain visibility; carriers may also be able to improve container utilization
    - High-density container area management for custodian: inventory, manage, and quickly find containers in high-density container areas such as a seaport, railyard, onboard a ship, or on a

train; additionally, if containers can bounce signals off of each other (multi-hop), then a connection with one container might be adequate to fully scan a ship or port's inventory

- Dray-specific applications: applications of ICCs that satisfy needs unique to the road carrier industry
  - Pay tolls: automatically pay tolls, or at least provide verification of toll costs to shipper
  - Pay interstate trucking taxes: monitor distance travelled by a truck for paying state trucking taxes
  - Asset tracking (chassis, tractor, trailers): track the location of assets to manage fleets and improve utilization
  - Certification: certifications of container weight (for road limits) and CBP inspection can be indicated on the ICC for quick scanning during the remainder of the voyage
- Quality control: monitor container conditions relevant to cargo needs, for example temperature, humidity, accelerometer (impact, tilt, vibration), and air quality
  - Rapid response: with constant monitoring, if container contents are found to be lost or ruined, a replacement order may be placed quickly
  - Liability: if a problem is detected that is attributable to the custodian, the ICC may establish to whose custody that liability belongs

- Security and safety
  - Container integrity
    - Seals (container doors)
      - Manual seal: either a soft seal that breaks when the door is opened (to indicate break in) or a hard seal intended to lock the container door
      - Electronic seal: an "electronic seal" that can provide the same capability as a manual seal though can perform additional tasks: log door opening, permit legitimate entrances (i.e. customs inspection), immediately alert appropriate parties on event
      - Remote lock/unlock: remotely lock or unlock the container door
    - Detection sensors (container sides and interior)
      - Detect unauthorized container breach: sensors intended to detect a container breach from any of the six sides (i.e. light, humidity, infrared sensors)
      - Verify container contents: sense dangerous materials (i.e. radiological, chemical, biological,

etc.) in self and/or around container; also if x-ray scanned container at the port of departure, carry a copy of the scan image on the ICC so that an X-ray in the receiving port can verify that contents have not been changed
        - Tamper sensor: detect tampering with sensor system
    - Container and cargo tagging and tracking: benefits for tagging and tracking that have security benefits (as opposed to those listed in the Supply Chain Management section above)
        - Quickly locate container: find specific container in the supply chain if it needs to be inspected
        - Geo-fencing/route adherence: establish geographic bands within which the container is expected to travel; send alert if container leaves those bands
        - Proximity to custodian/handlers: ensure that container remains in proximity to custodian
    - Safety
        - Local warnings to handlers: list warnings about unsafe contents and their Material Safety Data Sheets both physically and electronically
        - Container incompatibility: container cargoes, particularly in tank containers, may be dangerous if mixed with contents of other containers, making them "incompatible"; ensure that these containers do not come in close contact
        - Container conditions: ensure that a toxic cargo is not leaking out of its inner containment into the shipping container, prevent overheating of flammable material, etc.
        - Emergency response: if emergency exists, quickly respond (problem known, location known, etc.); include emergency call buttons for trucks
        - Environmental risk reduction: sense leaks to alert custodian and authorities

### 2.2.2 By communication protocol

There are several common methods by which ICCs communicate, though they are not mutually exclusive.

- Passive: a powerless ICC that is only read when a reader checks it
- Active: a powered ICC that can send out a signal
    - Continuous: an ICC that updates the reader regularly at some set time interval

    - Alert: an ICC that only sends a signal when some measured quality (i.e. temperature) falls outside of a pre-determined range
    - Ping-only: an ICC that communicates only when pinged by a reader
- Data carriage: the ability to carry data about the container
- Multi-hop: the ability of ICCs to recognize one another, "hopping" the signal
    - Single point-of-contact: a stack of containers, which can be very difficult and time consuming to survey, can quickly be pinged to find a specific container
    - Proximity recognition: ICCs that recognize one another may be able to provide aggregate data (total weight of a stack of containers), warn against incompatibility issues (unsafe neighboring chemical storage), etc.
- Readable/writable: some ICCs can only be written to once (readable), while others can be re-written indefinitely (writable)

### 2.2.3 By technology

Some common technologies for ICCs are:

- Inherently local (terrestrial)
    - Radio Frequency Identification (RFID)
        - Passive
        - Active
    - SmartCards
    - Wireless sensor networks
- Inherently global (satellite)
    - Global Positioning System (GPS)
    - Global System for Mobile Communications (GSM)

Note that "inherently local" technologies may be made global by adding a local communication port with satellite access.

### 2.2.4 By stakeholders and beneficiaries

There are certain stakeholder groups within a supply chain that would either benefit from or at least have interest in ICCs. Some of the most common are:

- Cargo custodians
    - Ocean carrier
    - Air carrier
    - Rail carrier
    - Truck carrier
    - Seaport
    - Airport
    - Railyard

    - Transload facility
    - Warehouse/distribution center
- Shipper type
    - Retail
    - Grocer
    - Pharmaceutical
    - Manufacturing
    - HazMat/chemicals
    - Military
- Regulatory
    - Customs
    - Homeland security/border patrol
- Industry bodies/consortiums
- Technology providers
    - Legacy providers with existing industry penetration
    - Smaller start-ups with high technology
    - Conglomerates already providing other services to the industry and looking for a new market

### 2.2.5 By level of implementation

Although this study focuses primarily on containers, depending on their goals, many parties are interested in other levels of implementation:

- Conveyance: the custodian's equipment for moving the container (i.e. a chassis, trailer, rail car, etc.)
- Container: the shipping container
- Pallet: a collection of multi-packs or parts bundled on a pallet, typically about 4'x4' and of wood construction
- Multi-pack: a carton (typically cardboard box) containing multiple parts
- Part/SKU: the individual item of interest being shipped

# 3. ICC STAKEHOLDER BACKGROUNDS AND INITIATIVES

Stakeholders in the ICC debate include parties concerned with (1) supply chain management, (2) the container industry, and (3) the development of ICCs. This chapter outlines these stakeholders to prepare for discussions of why ICCs may be of interest to each. The stakeholders discussed are:

- Regulatory bodies
- Carriers and logistics providers
- Shippers
- ICC technology and service providers
- Consortium study groups
- Academia and research

Each section is divided into two main parts: Background, which discusses the stakeholder group and its primary issues; and Initiatives, which discusses some primary ICC initiatives by that stakeholder group.

Note that while the level of tracking of greatest interest for this study was the container, five main levels are considered in the industry: conveyance, container, pallet, multi-pack, and part. Generally, conveyance tracking is included in this study, while pallet level and lower are not. This is because conveyance tracking may indirectly track containers (tracking a ship could effectively track the containers aboard as well), while lower tracking levels are not likely to support container tracking, and in fact may require support from the container to operate anyhow.

A summary of the discussed initiatives is provided in Figure 1 and Figure 2.

*This summary is based on best information available, though not all categories apply to all initiatives, and most initiatives change over time, making this a rough description of the field; an X typically means that specific reference to that ability was found, or it is a primary focus; though lack of an X DOES NOT exclude the initiative from that category (this is particularly true in the technology category); note that not all categories from the study are listed here, only the more prominent ones*

| | SCM | | | | | Security and Safety | | | | | | | | | | Technology | | | | | | | | | | | | Tag Level | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Custodial x-fer | Tracking | High-density container mgt | Dray-specific | Quality ctrl | Seals | | | Detection sensors | | | Tracking | | | | RFID | | | WSN | SmartCards | Satellite | | Data Conveyance Type | | | | Update regularity | | Conveyance | Container | Pallet | Multipack | Part |
| | | | | | | Manual Seal | E-Seal | Remote (un)lock | Non-door breach | Verify contents | Tamper sensor | Geo-fencing | Temp/Humid/etc. | Em'cy call button | Reduce enviro. Risk | Active RFID | Passive RFID | EPC Network | | | GPS | GSM/GPRS | Passive ID | Alert | Data Carriage | Multi-Hop | Realtime | Intermodal x-fer | | | | | |
| ***Regulatory*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ACSD/CSD/SmartBox | X | X | X | | | X | X | | X | | | | | | | | | | X | | | | X | | | | X | | X | X | | | |
| Cargo*Mate | | X | | X | | X | | | | | | | | | | | | | | | X | | | | | | X | | X | | | | |
| Freight Info. Real-Time Sys. for Transp. (FIRST) | | | | X | | | | | | | | | | | | | | | | | | | | | | | | | X | | | | |
| Hazardous Materials Safety and Security | X | X | | X | X | X | | X | | | | X | X | X | | | X | | | | | | | | | | | | X | X | | | |
| Marine Asset Tag Tracking System (MATTS) | X | X | X | | | | | | | | | | | | | | | | X | | | | | | | X | | X | | X | | | |
| Operation Safe Commerce | X | X | | | | | X | | | X | | | | | | | X | | | | X | | | | | | | | | X | | | |
| Pacific Northwest Field Tests | | X | | X | | X | | | | | | | | | | | X | | | | | | | | | | | | X | X | | | |
| PierPASS | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | X | X | | | |
| SAFE Container (SAFECON) Program | | | | | | | | | | X | | | | | | | | | | | | | | | | | | | | X | | | |
| STAR BEST | X | X | | | | X | | | | | | | | | | | X | | | | | | | | | X | | | | X | | | |
| ***Carriers*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Horizon Lines | X | X | | | | | | | | | | | | | | X | | | X | | | | | | | | | | | X | X | | |
| Tamper Resist. Embedded Ctrller. (TREC) | | X | | | X | | | | X | | X | X | X | | | X | | | X | | X | X | X | X | X | | X | X | | X | | | |
| ***Shippers*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Boeing | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | | | X |
| Dow | X | X | | | X | | X | | | X | | X | X | X | X | | X | | | | X | | | | | | | | X | X | | | |
| Safeway (refer to Horizon Lines above) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Starbucks | X | X | | | X | | X | | | | | | | | | | | | | | | | | | | | | | | X | X | | |
| US DOD | X | X | | | | | | | | | | X | | | | X | X | | | | | | | | | | | | X | X | X | | X |

**Figure 1. Summary of initiatives discussed (part 1)**

*This summary is based on best information available, though not all categories apply to all initiatives, and most initiatives change over time, making this a rough description of the field; an X typically means that specific reference to that ability was found, or it is a primary focus; though lack of an X DOES NOT exclude the initiative from that category (this is particularly true in the technology category); note that not all categories from the study are listed here, only the more prominent ones

| | SCM | | | | | Security and Safety | | | | | | | | | | Technology | | | | | | | | | | | | | | | Tag Level | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Custodial x-fer | Tracking | High-density container mgt | Dray-specific | Quality ctrl | Seals | | | Detection sensors | | | Tracking | | | | RFID | | | WSN | SmartCards | Satellite | | Data Conveyance Type | | | | Update regularity | | Conveyance | Container | Pallet | Multipack | Part |
| | | | | | | Manual Seal | E-Seal | Remote (un)lock | Non-door breach | Verify contents | Tamper sensor | Geo-fencing | Temp/Humid/etc. | Em'cy call button | Reduce enviro. Risk | Active RFID | Passive RFID | EPC Network | | | GPS | GSM/GPRS | Passive ID | Alert | Data Carriage | Multi-Hop | Realtime | Intermodal x-fer | | | | | |
| ***ICC Solution Providers*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ARGO Tracker/Brooks | | X | | | X | | X | | | | | | X | | | X | | | | | X | | | X | | | X | | X | | | | |
| CommerceGuard | X | X | | | X | X | X | | | X | | X | X | | | | X | | | | | | | | | | | | X | | | | |
| SAVI Technology | | X | | | X | | | | | | X | | | | | | | | | | | | | | | | | | X | | | | |
| Sensitech (Ryan EZT, TempTale, etc.) | | | | | X | | | | | | | | | | | | | | | | | | | | | | | | X | | | | |
| WhereNet | | | X | | | | | | | | | | | | | | X | | | | | | | | | | | | X | X | | | |
| ***Other initiatives*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Altobridge | | X | | | X | | X | | | | X | | X | | | | | | | | | X | | | | | | | X | X | | | |
| eModal.com | X | | X | X | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | |
| GPS Insight | | X | | X | | | | | | | | | | | | | | | | | X | | | | | | | | X | | | | |
| Intelli-Shield (iShield) | X | | | | X | X | X | | | | | X | | | | | | | | | | | X | | | X | X | | | X | | | | |
| Lloyd's Marine Intelligence Unit | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | |
| Par Logistics Management Systems | X | X | X | | X | | | | | | | | | | | | X | | | | X | X | | | | | | | X | | | | |
| Polestar (Purplefinder.com) | | X | | | | | | | | | | | | | | | | | | | | | | | | X | | | X | | | | |
| Qualcomm | | | | X | | | | | | | | X | | | | | | | | | | | | | | X | | | X | | | | |
| Safefreight Technology | | X | | X | X | X | | | | | | X | X | | | | | | | | X | | | | | | | X | X | | | |
| SeeContainers | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | | | | |
| Silent Commerce | X | X | X | | X | | | | | | | | | | | | X | | | | | | | | | | | | X | | | | |
| Steelroads' NetREDI System | X | X | X | | X | | | | | | | | | | | | X | | | | | | | | | | | | X | | | | |
| WIPRO | X | X | | X | | | | | | | | | | | | | | | X | | | | | | | X | | | X | | | | |
| ***Consortium Study Groups*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| EPCGlobal's Information Services | X | X | | | | | | | | | | | | | | | | X | | | | | X | | | | | | | X | X | X | X | |
| Secure Commerce Roadmap (n/a) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Smart and Secure Trade Lanes | X | X | | X | | X | | | X | X | X | X | | | | X | X | | | | X | X | X | X | X | | X | X | | X | | | | |
| ***Academia and Research*** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Intelligent Container initiative | X | | | | X | | | | | | | | | | | | X | | X | | | | | | | | | | | X | | | | |
| NASA Automated-Tracking Transponders | | X | | | X | | | | | | | | | | | | | | | | X | | | | | | | | | X | | | | |
| Smart Tech for Environmental Safety | | X | | | X | | | | | | | | | | X | X | | | | | | | | | | | | | | X | | | | |

Figure 2. Summary of initiatives discussed (part 2)

# 3.1 REGULATORY BODIES

## 3.1.1 Background

Regulatory bodies exist at local, regional, national, and international levels. Different regulators have different concerns, though in the context of cargo movements, most are focused on the safety and security of people and property within its jurisdiction.

### 3.1.1.1 US Department of Homeland Security (US DHS)/US Customs and Border Protection (US CBP)

The US Department of Homeland Security (DHS), as well as some of its subsidiary departments, most notably US Customs and Border Protection (CBP), has worked heavily in the area of cargo security. The efforts of these organizations was summed into a list of significant initiatives by (Meyer and Meyer 2005), (Trade 2006), and (Secure 2005):

- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Container Security Initiative (CSI)
- Advanced Trade Data Initiative (24-hour rule)
- Advanced Targeting System (ATS)
- Transportation Worker Identification Credential (TWIC)
- Non-intrusive inspections (NII)
- Free And Secure Trade (FAST)
- Advanced Container Security Device (ACSD, "SmartBox")

#### *3.1.1.1.1 Customs-Trade Partnership Against Terrorism (C-TPAT)*

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a partnership between the US CBP and the private sector to ensure that all parties in a C-TPAT compliant supply chain meet certain security standards set forth by CBP. In return for compliance, cargo from these facilities is considered less risky, which is supposed to reduce inspections to both expedite shipping and relieve the burden on CBP inspectors.

US CBP describes C-TPAT as "a voluntary government-business initiative to build cooperative relationships ... through close cooperation with the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. [C-TPAT asks] businesses to ensure the integrity of their security practices and communicate and verify the security guidelines of their business partners within the supply chain." (CTPAT 2006)

US CBP also describes the benefits and success of the program: "Participants receive expedited processing of C-TPAT shipments to C-TPAT partners. (Trade 2006)." Expedited shipping is a result of: fewer inspections for inbound cargo, "green lanes" to move C-TPAT cargo through a port ahead of non-C-TPAT cargo, "restart priority" in the event of port closure, and paperless data exchange by

increasing electronic manifesting (Downey 2006). In favor of ICCs, (Kulisch 2006) suggests that sensors are seen as a best-practice for implementing green lanes, which should reduce overall port congestion.

The World Shipping Council (WSC), which represents the world's largest containership companies, states that the ocean carriers support C-TPAT, and added that industry believes that non-intrusive scanning at foreign ports is the most important tool for regular checks. (In-Transit 2003)

Some large shippers have also expressed their support for C-TPAT. (Downey 2006) states that "Procter & Gamble (P&G), Boeing, Starbucks, and Kmart emphasized that [signing up for C-TPAT] makes good business sense. In addition to the 'moral obligation' to secure cargo ... there [is a] need to 'protect the brand.'" Tim Armstrong, senior director of domestic transportation and logistics services for Anheuser-Busch (A-B), also showed shipper support for C-TPAT. Armstrong stated that A-B regards C-TPAT participation as "both good citizenship and good business. As we add imported beers ... to our distribution system, it's important that we avoid shipment delays and deliver fresh beer to our customers." (Melcer and Tsadik 2006)

Container Security Inc. claimed that C-TPAT could bring savings of $300 per container for faster cargo movement, plus avoidance of inspection which adds $1000 in savings

Still, the rate of implementation is tough to determine. Although CBP claims that 10,000 have participated, (Downey 2006) puts that number into perspective by stating that, as of February 2006, only about 4,000 of the roughly 50,000 importers had adopted C-TPAT. Further, at that time, of all of the claimed C-TPAT benefits, only reduced inspections had been observed and recorded. Costs are also inevitable, and must ultimately be weighed against benefits. C-TPAT is claimed to have already cost Canadian carriers about $400 million in upgrades (Downey 2006).

#### *3.1.1.1.2 Container Security Initiative (CSI)*

The Container Security Initiative (CSI) authorizes the US CBP to station inspectors at foreign ports that send cargo to the US. These inspectors can assess cargo risk (Beisecker 2006) and prevent the smuggling of terrorists and weapons. This initiative is intended to address the realization that scanning a container once it reaches a US port may be too late to prevent a disaster. Presently there are 41 participating ports, which (Stana 2006) claims accounts for about 73% of US-bound containers.

CBP claims that the CSI's intent is to identify and inspect all containers that pose a potential terrorist risk at foreign ports before they are placed on vessels. Teams of US officers from both CBP and Immigration and Customs Enforcement (ICE) work with foreign counterparts to target and prescreen containers, as well as develop leads regarding a terrorist threat to cargo. (CSI 2006)

CBP claims that CSI's four elements are to (CSI 2006):

- Identify high-risk containers using automated targeting tools based on advance information and strategic intelligence
- Prescreen and evaluate containers as early in the supply chain as possible, always before being shipped, generally at the port of departure
- Use technology to prescreen high-risk containers which ensures rapid physical screening; technology includes large-scale X-ray and gamma ray machines and radiation detection devices
- Use smarter, more secure containers to allow US-based CBP officers to identify containers that have been tampered with during transit

The World Shipping Council supports CSI (In-Transit 2003).

#### *3.1.1.1.3 Advanced Trade Data Initiative (ATDI)/Automated Targeting System (ATS)/24-hr Advanced Manifest Rule (24-hour rule)*

The Advanced Trade Data Initiative (ATDI), Automated Targeting System (ATS), and 24-hr Advanced Manifest Rule (AMR) all refer to parts of a system in place that assesses risk to containers based upon various data.

The ATDI is an umbrella initiative that ultimately developed the more-commonly known 24-hour rule. This rule requires all importing carriers to submit a cargo declaration to US CBP 24-hours before cargo is loaded onto a vessel with a port of call in the US. This information allows CBP to designate a "load/do not load" status to each container before it has been placed aboard the ship (Maersk 2006). The policy affects all containers, including those from CSI ports (Panagopoulos 2007). Since it is a national effort, a container on a ship visiting several US ports before its final destination may be scanned in an earlier port, for example a container moving on a ship through Boston could be scanned there before finally arriving in NYC or Savannah (Vikesland 2006).

Risk is assessed by the Automatic Targeting System (ATS) at the National Targeting Center (NTC) in Virginia (Trade 2006). Fundamentally, ATS provides a system with which to significantly reduce the amount of physical cargo screening that is needed. This is seen to be absolutely critical to ensure that ports are not brought to a halt trying to screen all cargo. Several studies have focused heavily on why 100% cargo screening is said to be infeasible, and (Cirincione and Cosmas 2006) offers five main reasons why:

- Ambiguity of 100% cargo scanning policies
- Technology limitations
- Cost
- Logistical difficulties
- Stakeholder support

Therefore, the ATS assessment issues containers a score that reduces the number of containers physically inspected by limiting scanning to those that are

high-risk. The information used to develop that score includes (Automated Targeting 2006):

- Sea/Rail/Air Manifests (Automated Manifest System/AMS-Air)
- Truck Manifest, Automated Commercial Environment (ACE)
- Cargo Selectivity Entries (Automated Broker Interface)
- Express Consignment Services (bills of lading)
- CCRA Manifest (bills of ladings), Canada Customs and Revenue (CCRA)
- CAFÉ, QP Manifest Inbound (bills of ladings), AMS
- Inbound Data (bills of ladings), AMS
- Food and Drug Administration (FDA) Entries/Prior Notice (PN), Automated Commercial System (ACS)
- Census Import Data, Department of Commerce

The World Shipping Council openly "understands and accepts the strategy of cargo risk assessment and targeting (Comments 2006)," and therefore supports the 24-hour rule (In-Transit 2003). (Lake and Robinson 2005), a report written for the US Congress, also supports the notion. It states, "the key to success [of facilitating trade while interdicting malicious cargo] is the ability to accurately and efficiently identify high-risk passengers and cargo, target them for inspection, and prevent entry."

Some sources are critical of ATS in its current state. A GAO audit (Stana 2006) mentioned various shortcomings:

- CBP had not yet put adequate controls in place to ensure the effectiveness of the ATS [ (van de Voort and O'Brien 2003) supports this idea by suggesting that random checks should be used as a benchmark to determine the effectiveness of ATS]
- The system is not refined enough to analyze information learned from routine inspections and implement it in future inspections, but instead only reads data from different, unconnected databases

(Cirincione and Cosmas 2006) also comments on the ATS:

- CBP has no means to guarantee manifest authenticity
- Ship manifests are often an inaccurate record of cargo contents, even when authentic
- "According to GAO, ATS not been proven to be any better than selecting containers at random"

Finally, (Flynn 2004) notes that DHS does not gather information itself, rather only analyzes it, and therefore cannot control what it obtains.

#### *3.1.1.1.4 Other initiatives*

- Transportation Worker Identification Credential (TWIC): a program initiated jointly by the Transportation Security Administration (TSA) and the USCG that requires workers that are unescorted in maritime facilities

to have a TWIC card (TSA: Transportation 2007). Acquiring a TWIC card requires a full background check on personal data, fingerprints, and, if applicable, job and employer (Transportation Worker 2006).

- Non-intrusive inspections (NII): a container scan that uses non-intrusive technologies; these include radiation portal monitors, personal radiation detectors, radiation isotope identifiers, and large-scale X-ray and gamma-ray imaging systems
- Free And Secure Trade (FAST): expedites US/Canada and US/Mexico cargo moving between partnering C-TPAT compatible importers
- SmartBox: a public/private partnership that is discussed in *3.1.2.1 Advanced Container Security Device (ACSD/CSD)/SmartBox*

#### 3.1.1.2 US Coast Guard (USCG)

The US Coast Guard focuses on maritime matters, mainly safety and security, for the US government. USCG has five primary "missions":

- Maritime Safety
- Maritime Security
- Maritime Mobility
- National Defense
- Protection of Natural Resources (Coast 2006)

The USCG, which is a peer to the US CBP under the US DHS, supports CBP activities that deal with ships and maritime security.

#### 3.1.1.3 World Customs Organization (WCO)

The World Customs Organization (WCO) is an international organization that represents 171 member countries' customs administrations accounting for 97% of all global trade (Trade 2006). The WCO, in close collaboration with the US and other customs agencies, created the *Framework of Standards to Secure and Facilitate Global Trade* (*Framework*).

The *Framework* was developed concurrently with US regulations, and therefore is quite similar in several regards. The "international equivalent" of some of the key US regulations listed above is evident in the four principles behind the *Framework* (Beisecker 2006):

**Table 1. US CBP and WCO Framework parallel regulations**

| US CBP Regulation | WCO Framework equivalent |
|---|---|
| The Customs and Trade Partnership Against Terrorism (C-TPAT) | providing benefits to businesses (designated as "Authorized Economic Operators") that agree to minimal standards for supply chain security. These benefits include faster processing of goods at borders and reduced examination rates |
| The Container Security Initiative (CSI) | requiring exporting countries to agree to perform inspections, preferably through non-intrusive detection equipment (i.e. x-rays, gamma ray detectors) at the reasonable request of importing countries |
| The 24 Hour Advance Manifest Rule | harmonizing advance electronic manifests and reducing complex reporting procedures |
| The Automated Targeting System (ATS) | using risk management approaches to target suspect shipments |

The World Shipping Council supports WCO's *Framework* (In-Transit 2003).

#### 3.1.1.4 European Union (EU)

The European Union amended its Customs Security Program with the Community Customs Code in 2005. The amendments added were (Supply Chain Security EU 2006):

- require traders to provide customs authorities with information on goods prior to import to or export from the European Union
- provide reliable traders with trade facilitation measures [Authorized Economic Operator (AEO)]
- introduce a mechanism for setting uniform Community risk-selection criteria for controls, supported by computerized systems.

These amendments intentionally closely mirror those of the WCO's *Framework* (EUROPA 2006).

As part of their increasing security standards, ports must also now be able to account for all cargo, an application for which Michael Lux, head of the European Commission's customs legislation unit, suggested that electronic tracking could be helpful. (Possible 2004)

#### 3.1.1.5 International Maritime Organization (IMO)

The IMO, which has historically focused mostly on maritime safety, has implemented the International Ship and Port Security (ISPS) code that establishes minimum-security standards for ports and ocean vessels (Secure 2005). The code requires certain plans and procedures to be developed for ships and ports intended to enhance security of both, including their crews and cargos. The code is intentionally written at a high-level to allow member governments to clarify how the guidelines are to be met, which is understandable since they are also responsible for enforcing the regulations. (International Ship 2002) Therefore, any regulation coming from US CBP or USCG will probably be at least as stringent as IMO regulations.

### 3.1.2 Initiatives

#### 3.1.2.1 Advanced Container Security Device (ACSD/CSD)/SmartBox

| | |
|---|---|
| Project Lead: | US DHS |
| Partners: | Savi Technology (Savi Networks, Lockheed Martin Corporation), GE, and several others responded by developing technology |
| Tagging Level: | Container |

*Both CSD and ACSD are used as general terms, though they refer to a specific initiative put forth by DHS's Advanced Research Projects Agency (HSARPA). The CSD initiative is intended to develop methods to make containers secure. The ACSD research awards from HSARPA ranged in technology from removable intrusion detection devices to composite material containers with electronic monitoring inherent in the material* (HSARPA 2006).

The CSD project lays out several requirements for the device, such as sensing capabilities, alert methods, data storage, communication procedures, physical interface requirements, and operational considerations (Request 2006). The effort began in January 2004, when CBP partnered with four C-TPAT importers to incorporate a CSD into the container sealing process. When in company with specified sealing standards and techniques, the CSDs are said to create a "Smart Box" that enhances container security (Jacksta 2005).

##### *3.1.2.1.1 Issues*

Some have remarked that while the CSD initiative has a general definition, it is overall quite vague (Kulisch 2006). This perception is perhaps because the term is used by so many in industry, including officials at CBP, while standards have not been widely publicized.

It is said by the World Shipping Council, for instance, that "there is currently no official definition of a CSD or its purpose," which, says the WSC, leaves the industry unsure as to what a CSD would actually have do: "should it record opening of one door, both doors, all-door entry?" They claim that, "there appears to be little

interest in or benefit to commercial shippers or carriers from an RFID CSD (Comments 2006)."

Further, the US CBP often refers to a container with a CSD as a "SmartBox," though it is still hard for many to discern between the terms. Perhaps offering some explanation is Robert Bonner, CBP Commissioner, who stated that, "A Smart Box will communicate evidence of tampering and the container security device will register every legitimate, as well as unauthorized, opening of the container (How do you? 2003)."

Still, stakeholders complain of an inconsistent government vision. One stated, "I have budget this year to execute Smart Box trials... [but] I do not want to invest and install infrastructure in 2005 that is not compliant to the 2006 vision. Therefore, I'm forced to wait (Secure 2005)."

#### 3.1.2.2 Cargo*Mate

| | |
|---|---|
| Project Lead: | US DOT (funded) |
| Partners: | Port of Charleston, PANYNJ; US DOD through Norfolk |
| Tagging Level: | Conveyance (truck chassis), Container |

*Cargo*Mate is a DOT initiative intended to track chassis and, when loaded, the containers that they carry as well. This system was supported by a sister project, the Freight Information Highway (FIH) and Chassis Tracking system, which attempted to develop standards for intermodal computer based communication.* (The Freight 2005)

The program tracked and integrated e-seals with chassis in Charleston, New York/New Jersey, and in US Department of Defense (DOD) military operations through Norfolk. The program was funded by the DOT Field Operations Test (FOT) program, 2002-2003. A savings of $210.35 per container chassis was claimed by the DOT FOT's due to increased utilization. (The Freight 2005)

#### 3.1.2.3 Freight Information Real-Time System for Transport (FIRST)

| | |
|---|---|
| Project Lead: | US DOT |
| Partners: | PANYNJ; FHWA (funding); I-95 Corridor Coalition (funding) |
| Tagging Level: | Conveyance (truck chassis) |

*FIRST aimed to reduce terminal congestion. The approach was an IT system that provided realtime information on traffic delays in and around the port. The system included electronic tracking of chassis and containers in the area* (The Freight 2005).

FIRST tests were conducted at the Ports of New York and New Jersey, then went into full use there. Unfortunately, though, it has ultimately failed to raise interest and use from the shipping community. It suffered technical problems and security concerns on startup that discouraged users from participating. Additionally,

it was fraught with a limited funding timeline that expired before the project's completion, and no revenues to support it. (Petrakakos 2005)

#### 3.1.2.4 Hazardous Materials Safety and Security

| | |
|---|---|
| Project Lead: | US DOT (funded) |
| Partners: | US Federal Motor Carrier Safety Administration |
| Tagging Level: | Container |

*This project intended to test a suite of technologies including asset tracking to monitor four types of hazmat shipments: Bulk Fuel, Less-than-Truckload High Hazard, Bulk Chemicals, and Truckload Explosives. Technologies were evaluated on improvements to safety and security. The test included freight movements for both the US Department of Energy and US Department of Defense.* (The Freight 2005)

While the focus of this program was more technology-performance based than assessing value to the supply chain, some interesting conclusions were provided (Hazardous 2004):

- E-seals were determined to require more technical development, for example they often had trouble communicating with the driver's in-cab system; though over the duration of the test they had improved
- Utilization by participants of the Electronic Supply Chain Manifest was disappointing and statistically irrelevant for the test
- Geofencing was tested twice; the participant who used it viewed it as effective for both security and oversight for management to prevent trucks from going where they did not want them to be
- The Remote Door Look system testing, while inconclusive due to only 16 data points, showed promise
- Positioning update frequency ranged from 17 to 70 minutes depending on operational conditions of each participant: desired reporting frequency for the shipper, commodity type, length of route, etc.
- Technology alone is estimated to be able to address at most one-third of Hazmat vulnerabilities

(Hazardous 2004) also estimated the vulnerability reduction that they believed various technology combinations provided, which is shown in Figure 3.

| Technology Scenario | Bulk Fuel | LTL-High Hazard | Bulk Chemicals | Truckload Explosives |
|---|---|---|---|---|
| Wireless Communications + GPS Position (base) | 17% | 16% | 16% | 12% |
| Driver ID + (WC + GPS Position) | 25% | 25% | 23% | 18% |
| Panic Alert + (WC + GPS Position) | 27% | 25% | 25% | 21% |
| Panic Alert + Remote Vehicle Disabling + (WC + GPS) | 32% | 32% | 31% | 25% |

**Figure 3. Hazardous Material FOT estimated vulnerability reduction**
*(Hazardous 2004)*

If a dollar value is placed on a potential attack for each possible case, the value of these security benefits can be calculated. An example for the Bulk Fuel scenario is provided in Figure 4.

| Technology | Percent Vulnerability Reduction | "Worst-Case" Attack Consequences | Estimated Security Benefits | Estimated Benefit Cost Ratios |
|---|---|---|---|---|
| Wireless Communication with GPS (base) | 17% | $3.7 Billion | $622 Million | 1.5:1 |
| Base + Driver Identification | 25% | | $933 Million | 2.1:1 |
| Base + Panic Button | 27% | | $995 Million | 2.3:1 |
| Base + Panic Button + Remote Vehicle Disabling | 32% | | $1.207 Billion | 2.6:1 |

**Figure 4. Hazardous Material FOT security benefit for Bulk Fuel scenario**
*(Hazardous 2004)*

### 3.1.2.5 Marine Asset Tag Tracking System (MATTS)

Project Lead: US DHS, Small Business Administration
Partners: iControl
Tagging Level: Container

*"DHS established the three-phase MATTS program in 2003 under the direction of the Homeland Security Advanced Research Program Agency (HSARPA). MATTS requirements include worldwide, bi-directional, secure communications and tracking of containers from the point-of-stuffing to the point-of-devanning. The MATTS system must also be remotely reconfigurable, low-cost, and last the life of the container without maintenance."* (iControl 2006)

MATTS consisted of "container tags, gateways, and web-based data distribution and network operation servers (iControl 2006)." iControl handled the technology for this project. Phase I consisted of proof-of-concept and prototype development using existing commercial products. Phase II included a functional demonstration in commercial pilot programs. Phase III is intended to deploy the MATTS system in both international and domestic routes. (iControl 2006)

iControl goes beyond port-centric container monitoring to include road, rail, and marine. Diane Quick, iControl's MATTS Program manager, recognizes that "managing the supply chain is not the same as securing the supply chain... Terrorists do not fill out manifests ... Securing populations, property, and economies requires continuous container tracking and monitoring." (MATTS 2006)

In addition, the initiative aims to allow communication between containers since they are typically stacked tightly together (Downey 2006).

#### 3.1.2.6 Operation Safe Commerce

| | |
|---|---|
| Project Lead: | US TSA (funded) |
| Partners: | US CBP/US DOT (manage) |
| Tagging Level: | Container |

*Operation Safe Commerce (OSC) is a collaborative federal grant program involving, among others, US DHS, the Office for Domestic Preparedness (ODP), the three largest US container port complexes, cargo and supply chain security solution providers, shippers, carriers, terminal operators, etc. The goal of the program is to "develop, test, and share best practices in order to improve the security of containerized cargo movements."* (Operation 2005)

OSC is DHS's primary port and cargo security initiative, and it has developed over time into three phases. Phase I of the project involved tracking a container movement of light bulbs from Slovakia; through Germany, through Canada, to eventually arrive at Hillsborough, NH. (Peckenpaugh 2002) Work on this project was carried out by the US DOT's Volpe Center, and is illustrated in Figure 5. The project documented security practices and technologies in the supply chain and identified vulnerabilities that existed. (Volpe 2003)

Phase II of the project examined eighteen different supply chains moving through the three major US port complexes: Seattle/Tacoma, Los Angeles/Long Beach, and New York/New Jersey. The project addressed container security vulnerabilities and examined "the testing and deployment of selected technologies and business practices to improve" supply chain security. (Operation 2005)

This phase focused on three areas (Operation 2005):

1. Reasonable Care and Due Diligence: Ensure that all parties exert reasonable care and diligence in packing, securing and manifesting container contents.
2. Secured Data Transmission: Review various methods used to transmit data and ensure that shipment information was complete, accurate, and secure.
3. Container Security Procedures: Take measures to test the multi-layered security approach in technologies, business practices, and data collection.


**Figure 5. Operation Safe Commerce Phase I schematic**
*(Volpe 2003)*

Phase III of the project is still underway, though funding was available for projects that demonstrated at least one of the following (Operation 2005):

1. Verify empty container integrity prior to stuffing.
2. Verify integrity of cargos stuffed into containers.
3. Verify and maintain integrity of the containers and cargos throughout the supply chain.
4. Verify and maintain integrity of supply chain management information and information systems.
5. Demonstrate and record information exchange for OSC container documents with appropriate US CBP program requirements.
6. Test whether commercially available technologies address any of the supply chain primary and secondary nodal goals (in the reference's Appendix B).

The port complex of Los Angeles and Long Beach ultimately was awarded the Phase III contract, and their stated goals are to (Ports Receive 2005):

- Maintain and communicate accurate data on cargoes
- Verify that empty containers have not been tampered with before being loaded with goods
- Verify that cargoes loaded into containers do not contain threat items
- Verify that container integrity is not breached in transit

Many in industry are optimistic about OSC, as it shows the government's desire to find and demonstrate technology that not only improves security, but can also be cost effective. Michael Zachary of the Port of Tacoma remarked, "our goal is

to make sure that whatever comes out of OSC is economically and commercially viable. That means minimal financial and operational impact to the trade. That may be a pipe dream; we don't know." (Sowinski 2004)

The WSC generally supports the OSC as well, though was sure to raise several issues early on that it saw of concern. WSC warned against the OSC becoming a "forum for technology vendors." Instead, WSC supports OSC as a way to compare all different alternatives to meet the specific security objectives. Additionally, WSC argues that tests should not "presuppose that technology will provide superior security" to other solutions.

#### 3.1.2.7 Pacific Northwest Field Tests

| | |
|---|---|
| Project Lead: | US DOT |
| Partners: | Ports of Seattle and Tacoma |
| Tagging Level: | Conveyance (truck chassis), containers |

*The Pacific Northwest Field Tests was an initiative intended to track containers between the US northwest ports of Seattle and Tacoma and the Canadian border using truck transponders and web-based tracking. It was tested on the I-5 corridor, and the containers were fitted with e-seals* (The Freight 2005).

The project consists of (US-Canada 2002):

1. A northbound automated border crossing development project
2. A test of e-seals and information exchanges with port terminals
3. A southbound automated border crossing development project

The goals included improved efficiency for truckers, shippers, and enforcement officials, plus improved compliance with Customs requirements at the international border. (The Freight 2005)

#### 3.1.2.8 PierPASS

| | |
|---|---|
| Project Lead: | Ports of Los Angeles/Long Beach |
| Partners: | eModal, WhereNet |
| Tagging Level: | Container |

*PierPASS is a program intended to relieve port congestion at the Ports of Los Angeles and Long Beach. The program implements quicker check-in using RFID tags (WhereNet) on trucks, which are registered with eModal. The program also focuses on moving more traffic to off-peak hours.* (Truck 2006)

Since the program's inception, over 12,000 tags have been sent to road carriers. The visibility that the system allows yard managers, "might mean that a can doesn't miss a train." (RFID on track 2006)

#### 3.1.2.9 SAFE Container (SAFECON) Program

| | |
|---|---|
| Project Lead: | US CBP |
| Partners: | n/a (still out to bid) |
| Tagging Level: | Container |

*SAFECON is an effort to demonstrate complete high risk/high payoff systems or subsystems. The goal was to succeed in a 2-5 year timeframe to create "revolutionary rather than incremental improvements to homeland security," including both emerging threats and operational challenges. As of February 2007 this project was at bid, and initial demonstrations are desired within six months after contract award.* (SAFE 2007)

Interest lies primarily in the following areas (SAFE 2007):

- Chemical party detectors
- Biological party detectors
- Explosives detection
- Advanced lightweight composites
- Detection of living persons
- Other contraband detectors

#### 3.1.2.10 STAR BEST (Secure Trade in the APEC Region: Bangkok Efficient and Secure Trade)

| | |
|---|---|
| Project Lead: | US Trade Development Agency |
| Partners: | Port in Malaysia, Thailand; the Ports of Seattle and Tacoma |
| Tagging Level: | Container |

*STAR BEST involved "two tests that estimated the benefits to shippers of technologies and processes designed to improve security via intermodal cargo visibility* (The Freight 2005)*." Shipments were moved from Thailand and Malaysia through the Ports of Seattle and Tacoma.*

Results of the program suggested savings of about $400/container to shippers, mostly in inventory reduction from better asset tracking (The Freight 2005).

## 3.2 CARRIERS AND LOGISTICS PROVIDERS

### 3.2.1 Background

To attract shippers, carriers of all modes compete on many metrics, including competitive pricing, reliable service, flexibility, supply chain visibility, and total logistics solutions (for instance door-to-door service). This can be an incredibly complex task as the number of shippers, origin and destination locations, and other carrier links needed in the complete supply chain all increase.

Competition exists both intra- and inter-modally, which creates even stronger competition. Intra-modal competition varies, with some modes highly fragmented and therefore highly competitive, while others have become centralized. Inter-modal competition exists when multiple mode choices can service the same route. For instance, the China to east-coast US trade can be serviced by four primary options: (1) an all-water route through the Panama Canal, (2) a China to US water route and rail transportation east, (3) a China to US water route and truck transportation east, and (4) an all-air route. For some cargoes, mode choice may be an apparent decision, though when it is not, service providers must compete.

Carriers ultimately must balance customer service, which they often tout as their differentiating factor over competitors, with efficient asset utilization. This balance is felt by any party in the supply chain that provides equipment or infrastructure. To this end, supply chain visibility is a crucial component for carriers for three primary reasons: to provide visibility to their customers, to provide visibility for law enforcement, and for efficient fleet utilization. Technologies have been applied to varying degrees to support all of these needs.

#### 3.2.1.1 Air carriers and airports

Air cargo transport is a much higher-speed, expensive alternative to sea, rail, or truck transport. It therefore is primarily reserved for cargo that commands a premium for speed. Although air carriers transport the same types of cargo as other modes, for reasons of space and weight, they do not typically use conventional sea containers, but instead smaller, lighter, "Unit Load Devices." (Belobaba 2004)

Air cargo is generally divided into three categories (Belobaba 2004):

- Express/time definite: small packages (less than 50 kg.)
- Heavyweight freight shipments (greater than 50 kg.)
- Mail transport

Air carriers are also grouped into two primary categories (Belobaba 2004):

- All-Cargo Airlines
    - Integrated Express Carriers (express/small packages; door to door service; examples: UPS, FedEx, USPS)
    - Non-integrated Freight Carriers (heavyweight freight shipments; work with freight forwarders, etc.)
- Passenger (Combination) Airlines
    - Can carry air freight, express packages and mail in passenger aircraft belly or on "combi" aircraft
    - Also can have dedicated freight aircraft

The air cargo industry is small in terms of absolute numbers of cargo carried, but is growing rapidly, as illustrated in Figure 6 and Figure 7.

| MARKET SHARE (%), BY MODE | | | |
|---|---|---|---|
| | 1980 | 1990 | 1999 |
| Air Courier | 0.2 | 0.3 | 0.4 |
| Trucking | 18.6 | 23.0 | 28.7 |
| Rail | 30.7 | 32.4 | 37.6 |
| Other | 50.5 | 44.4 | 33.4 |

**Figure 6. Relative domestic US market share of air cargo to other modes**
*(Belobaba 2004)*

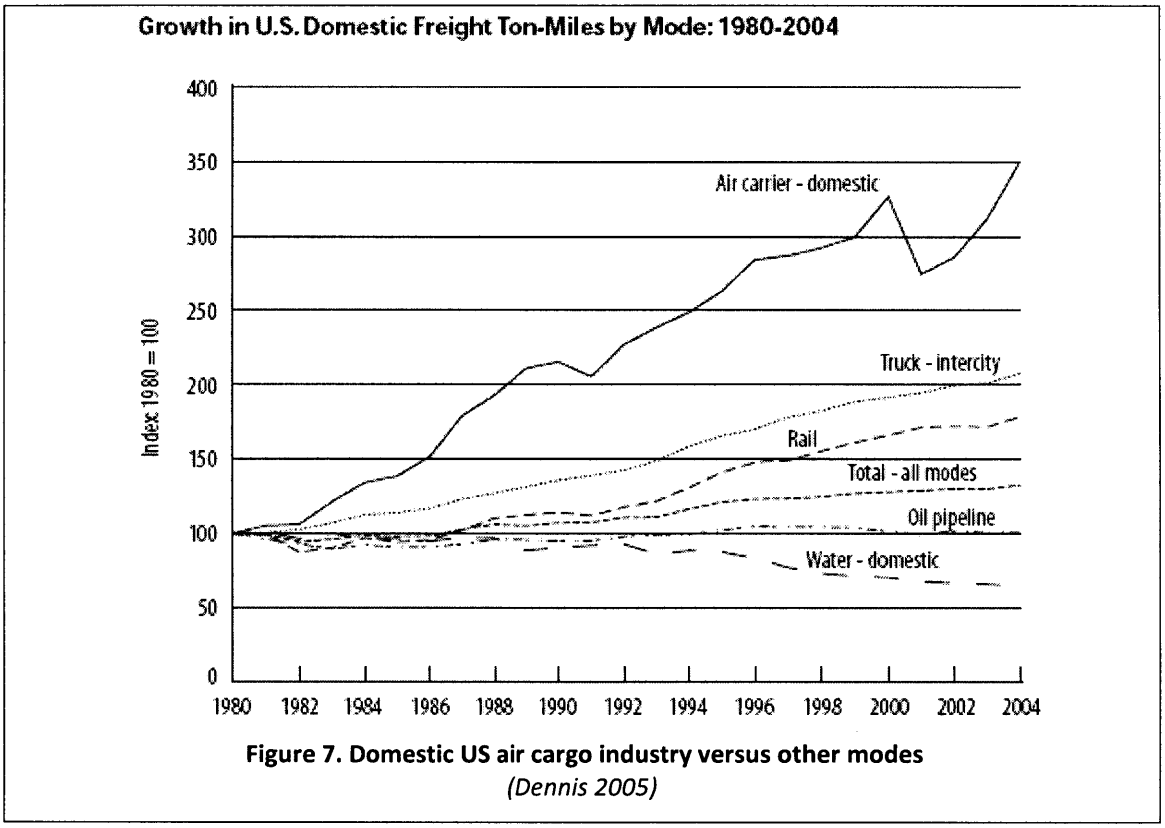



**Figure 7. Domestic US air cargo industry versus other modes**
*(Dennis 2005)*

Equipment size is also growing, as Boeing claims that, "worldwide air cargo traffic will more than triple over the next 20 years, driving the number of airplanes in the freighter fleet to nearly double. Wide-body freighters will come to represent a greater share of the fleet, growing from roughly half of the fleet today to more than 60% of the fleet by 2025 (World Air 2007)." As the air cargo business expands, operators are also integrating other modes to offer door-to-door service, as has been done by many ocean carriers. (Belobaba 2004)

While it is clear that growth is strong, unlike the passenger air market there is still little traffic and pricing data publically available. Instead, cargo carriers often operate flexibly on daily or weekly demand, which complicates scheduling. (Belobaba 2004) Scheduling is even tougher for combination carriers since they must interact with the passenger side of the business. Historically, passenger operations have dominated routes and revenues, although as the cargo business grows there have been signs that this is changing. Different carriers have treated their cargo

operations very differently, with some creating independent subsidiary companies and others highly integrating the business into passenger operations. A looming issue for combination carriers is the security threat that cargo poses. Just one serious incident involving cargo, even if no passenger is affected, could generate significant public and political scrutiny that could severely limit the ability of combination carriers to operate. (Conway 2006)

Indeed, cargo security is already a big concern for air carriers given the political pressure to act on security matters. There is a bill in US Congress that proposes 100% screening of airplane cargo. Reactions are varied to this legislation. "Auditors for [Congress] looked at what [the] proposed law ... would cost, they came up with a final tab of $3.6 billion over 10 years." It is claimed that some companies would not be able to cope with the cost, forcing them out of business. Still, not all in the industry oppose 100% scanning. Olivier Bijaoui of World Flight Services says, "the first few days would be a problem, but we would manage it. In the U.K., we currently screen over 50 percent of American Airlines' freight because a large portion of their freight is unknown; if required to step up to 100 percent, we could do it." (Moorman 2007)

#### 3.2.1.2 Ocean carriers and seaports

There are roughly 400 ocean carriers in the container business, of which about twenty exist in the "top-tier," meaning that they command at least 2-3% of the world's container traffic. Most top-tier carriers must offer door-to-door service to remain competitive. They do this by maintaining large ship fleets with reliable, typically weekly service. Many have moved their logistics service group into a subsidiary division that treats the ship-operating division merely as a component of the supply chain. The high fragmentation of this industry has also led to "alliances" among many of the top-tier players that allow each one to offer a wider array of services by sharing cargo with their fellow alliance members.

Needless to say, customer service has been a dominating driver of the changes that have occurred within the industry. By offering integrated logistics, cargo visibility and quality assurance have the potential to improve as shippers should ideally need only one portal through which to monitor their cargo status. This is one area in which ICCs could provide much more detailed information to clients while cargo is en route.

Seaports are typically owned and managed locally, particularly in the US, where ports are much less regulated than in many other countries (Petrakakos 2005). Ports are either "operator" or "landlord" ports, which refers to who actually operates the terminal. In operator ports, the owner of the port manages operations, while in a landlord ports, operations are handled by a lessee, often an ocean carrier's subsidiary.

Most US ports are fraught with tight budgets, capacity overutilization, tough labor relations, and ageing infrastructure. While there is a need to expand, many

hurdles exist, including high real estate and capital construction costs, environmental regulation, local public resistance, and local intermodal (truck and rail) capacity limits.

With so many difficulties facing ports, ICCs may be seen as nothing more than added cost by port operators and a threat to job security by labor. Still, some ports have invested in ICCs to manage inventory while in the port itself. Additionally, if ICCs improve asset utilization, it may effectively add capacity to the port, an attractive solution to adding costly infrastructure.

#### 3.2.1.3 Rail carriers and railyards

The North American rail industry, which is perhaps the largest and most integrated in the world, is highly deregulated, with the vast majority of rail infrastructure and equipment owned both by the private rail carriers and shippers. Although there are about seven major rail carriers in the US and Canada, they are also regional, meaning that each carrier is the dominant service provider in most of its respective operating area. (Sussman 2000)

The rail industry maintains a fleet of rail cars specifically designed to carry containers. Containers are loaded on the trains and then linked together in railyards, ideally in an order that will allow for cars to be easily taken off in groups at their destinations. Different types of container rail cars exist, the most common of which are "double-stacked," which doubles the carrying capacity of a train over single stack cars. Additionally, gondola (open-top) cars, tank cars, refrigerated cars, auto-rack cars, and others are available depending on the freight type. (Sussman 2000)

For many years, bulk freight has dominated both the volume and revenue stream for the railroad industry, namely coal, grain, and ore. Coal, for instance, accounted for 43% of all rail in 2003. However, 2003 was also the first year that intermodal traffic (namely container) overtook coal as the highest revenue generator for the industry. (Rodrigue, Comtois and Slack 2006) As container traffic continues to grow, it gains the attention of rail operators and encourages investment in level of service increases.

ICCs for tracking have so far been implemented by several services, including NetREDI (see *3.4.2.6.12 Steelroads' NetREDI System*) and Silent Commerce (see *3.4.2.6.11 Silent Commerce*).

#### 3.2.1.4 Road carriers

Road carriers in the US range from individual truck operators to large companies with extensive fleets. Despite the few large players, this is an extremely fragmented industry; in 2005, there were over 600,000 registered truck operating companies (Number of U.S. 2006).

As for technology, over the past few decades the road carrier industry has focused on tracking tractor fleets by using GPS. Knyanesh Paktar of Schneider International's RFID group stated that "our role is increasing visibility." (Johnson

2005) Historically, cargo quality has also been monitored for many cargoes with special needs, like refrigerated containers, though typically not with realtime reporting.

A recent security issue affecting the road carrier industry is the TWIC program being instituted by TSA (see *3.1.1.1.4 Other initiatives*). This program requires that all who enter a seaport unescorted have a TWIC card, thereby including many road carriers since they operate to ports regularly. This has the potential to affect these carriers both administratively and financially, as the TSA expects the required background checks and card to cost roughly $139 per worker (Transportation Worker 2006). For ICCs, TWIC presents the possibility of improving custodial accountability by better associating custodians to the containers that they transport.

#### 3.2.1.5 Transload facilities and distribution centers

Facilities exist throughout many supply chains to handle and store inventory as it passes through to its final destination. These facilities are utilized differently based upon the corporate strategy of the shipper. Transload facilities and distribution centers apply mostly to container traffic in a retail distribution system, and are often owned or at least operated by the shipper.

Transload facilities are docking facilities typically located near a seaport or railyard and used to strip marine containers of their contents, store them if necessary, then reload them onto over-the-road trailers for delivery to a distribution center. "Cross docking" occurs when inventory skips the storage phase and moves directly from marine container to OTR trailer. This is preferable to reduce idle inventory.

Distribution centers receive shipments from the transload facilities (or container ports directly) and redistribute them to regional end-users, typically retail stores, as needed.

ICCs have been proposed both to help manage incoming containers to these facilities, or even more boldly to allow supply chains to bypass them altogether.

#### 3.2.1.6 Container ownership and operation

The container industry is tied most closely to the ocean vessels that carry them, since containers were first developed to speed up and reduce cost of the in-port stevedoring process. What was once a manual effort to unload the bulk cargo shipments delivered to ports and load them onto a ship was replaced in the mid-1950's by containers that could quickly be loaded as a complete unit onto the ship using a crane.

It is often suggested that an ocean carrier needs roughly three times the number of containers than the capacity of its ship fleet since one third will be on one shore, one third on the other, and one third on the ship itself. The carrier companies own a bit over half of the world's estimated 13-million (Fourth 2001) strong

container fleet, while the remainder is mostly owned by container lessors (Institute 2006).

Containers are offered in a variety of sizes and services. The most common container today is a 40' dry container, though 20', 35', and 45' containers also exist. Containers offer many services depending on their type, such as refrigerated (reefer) containers, tanks, open top, flat racks, etc. (Institute 2006)

Probably the most common ICCs in use already are temperature sensors for reefers.

#### *3.2.1.6.1 Over the road trailers*

In addition to maritime containers, there are over-the road (OTR) trailers, which usually measure 53' long in the US. These trailers are mostly towed over the road by tractors, but can be driven onto roll-on roll-off (RO/RO) ships for sea transport or flatbed railcars for rail transport. Though these trailers have considerably more volume than maritime containers (2,560ft$^3$ for a 40' dry container versus 3,961ft$^3$ for a 53' trailer), they are limited in operation since they have attached wheels and therefore cannot be stacked. While management of trailer fleets can be complex, these fleets generally do not operate in nearly as large a geographic region as sea containers since truck transport is usually used as a local-distribution solution. Typically, once transport distances exceed about 400 miles, where available, it is more economical to place cargo on a train.

## 3.2.2 Initiatives

### 3.2.2.1 Horizon Lines

| | |
|---|---|
| Project Lead: | Horizon Lines |
| Partners: | Identec Solutions, Safeway Supermarket |
| Tagging Level: | Container |

*Horizon Lines' subsidiary, Horizon Services Group, implemented an RFID, event-based tracking system provided by Identec Solutions that can offer container visibility from origin to destination. Safeway, the first customer to utilize the system, is tracking containers as they leave DCs in Washington State, travel over sea to Alaska DC's, and end up in to the chain's Alaska stores. The RFID system went live in late September with 5,100 of Horizon's 7,000 cargo containers tagged.* (Swedberg 2007) *Horizon claims that this effort is, "the ocean carrier industry's first fully functional end-to-end intermodal active RFID tracking solution* (Forsyth 2007)."

In addition to their Alaskan efforts, Horizon has been pilot-testing RFID tracking of pharmaceuticals entering the US from Puerto Rico. This has accompanied the FDA's continued push for all pharmaceuticals to be tagged by 2007. (Johnson 2005)

#### 3.2.2.2 Tamper Resistant Embedded Controller (TREC)

Project Lead: IBM/Maersk Logistics
Partners:
Tagging Level: Container

*TREC is a unit mounted at a container door that is comprised of sensors, processors, data storage, and wireless radio. The sensors can detect door openings, light, temperature, humidity, acceleration, position (through GPS), and more.* (Schaefer 2006)

TREC transmits data realtime, and a pilot project was planned to occur in fall of 2006. Chris Sciacca of IBM suggests that TREC will allow firms to immediately act in response to unexpected circumstances. (Melcer and Tsadik 2006) Henrik Ramskov of Maersk Logistics claims the TREC network can "eliminate the time lag of the physical container status to provide real-time visibility [which allows for] truly adaptive planning while also maintaining data quality." (IBM and Maersk 2005)

(Schaefer 2006) claims that TREC will provide three primary benefits:

1. Container Tracking Service (CTS): Real/neartime tracking and monitoring of container shipments.
2. Container Information Service (CIS): Securely exchange container data between parties, such as container content/manifest, location history, door openings, environmental data, etc. Databases can also be pinged that maintain information on the shipment.
3. Supply Chain Process Services (SCPS): Business process integration and choreography between parties. The aim is to provide an integration platform that parties can subscribe to and rely on, for secure mediation between all parties.

## 3.3 SHIPPERS

### 3.3.1 Background

Supply chains can be incredibly complex, and many companies no longer view logistics as a secondary component. Instead, supply chain management can become inherent to many companies' core operating strategy and be used competitively. Since supply chains involve many companies as well as many parties within the shipper's own company, coordination is key. Failure to coordinate can lead to provincialism, or "sub-optimizing" each part of the supply chain without regard to the rest of the system. This may ultimately lead to supply chain *inefficiency* and detract from the bottom line. The cargo-centric approach that ICCs might provide is a potential tool to mitigate this problem

However, the way in which a supply chain is operated and the complexities that it endures must be understood before implementation of an ICC should be considered. (Sheffi, Resilient Enterprise 2005) discusses some common issues:

- Sourcing
  - International sourcing and manufacturing: a single garment may begin from a set of textiles procured from several companies, then be shipped somewhere to have zipper added, shipped again to be assembled, then finally moved to its retail location
  - Dual supplier sourcing: to increase resilience, a shipper can source both locally as well from as a distant, more cost-effective location; normally source the majority of product from the distant location, though maintain a small stream from the local source to maintain production and ramp up in times of need
  - Just-in-time (JIT) manufacturing: a supply chain methodology where inventories and lead times are made as slim as possible to reduce inventory depreciation and holding costs; this philosophy must be embraced at all levels of an organization to work effectively
- Inventory can be considered in one of two phases:
  - Work In Progress (WIP): inventory is having value added to it
  - Down time: the time in between processes
  - Example: DuPont estimated that yarn takes 168 days from raw material to consumer, though only 8 hrs of that is WIP time
- Bullwhip effect: the tendency of mild variations in ordering at the retailer/consumer end to compound to larger variations for the supplier, with effects continuously magnifying upstream
  - Underscores the importance of continuous communication in the supply chain (suppliers need to know *why* retailer is ordering extra; does it indicate an upward trend such that the supplier should stock more inventory, or does it merely represent a promotion or replacement of lost/stolen goods?)
  - Tighter supply chains expose quality problems more effectively
  - Vendor Managed Inventory (VMI) allows suppliers direct access to the inventory on a company's shelves, and the supplier is responsible to keep them full
- Aggregate forecasting: forecasting an aggregate of a product (for instance, all the hats that will sell this year) is usually more accurate than forecasting a more specific item (all red hats) since it spreads risk in the way that managing a balanced investment portfolio does
  - Postponement: by postponing a product's customization, inventory can supply an aggregate demand, with last-minute personalization saved until the product is near delivery
  - Increase the number of personalized "built-to-order" products

    - Option packages can provide choice while minimizing risk since it aggregates together desired options
- Centralized inventory management: can better balance needs at different locations

Ultimately, the many needs and goals of a supply chain rely on increasingly improved, realtime data exchange among supply chain parties. Some supply chains, for instance one utilizing JIT, may find ICCs a very useful tool. Several sample supply chains are discussed below to introduce different issues facing shipper groups today, and how ICCs may help them.

#### 3.3.1.1 Retail

| | |
|---|---|
| Major concerns: | Inventory transparency, inventory reduction, product obsolescence, theft prevention |
| Existing initiatives: | Most on pallet level (notably Wal-Mart, Target) |

The retail industry is one of the largest worldwide. In the United States, it is the second largest in both number of establishments and employees, with $3.8 trillion in annual sales and 11.7% of US employment. The number of stock keeping units (SKUs) continues to grow dramatically, which has accompanied a similar growth in sales. (Wamba and Lefebvre 2006)

Growth in SKUs has led to the need to capture sales information that has almost exclusively gone electronic. Manual inventories are error prone, increase transaction costs, and can cause inventory inaccuracies. Procter & Gamble is a key example of this, who was shown to spend between $35 and $75 to process each customer invoice by involving numerous human interactions. (Wamba and Lefebvre 2006)

Key issues for the retail industry include product obsolescence, minimizing inventory, international sourcing and markets, long term sales forecasting, aggressive competition, increased cost pressure, and rise of customized demand, among others (Wamba and Lefebvre 2006).

##### *3.3.1.1.1 State of the art*

Retail has gone to extensive lengths to incorporate tracking technology to streamline supply chain processes and control costs. Most of this tagging has been at the part, multi-pack, and pallet level, with little focus on containers.

To support "intra- and inter organizational business processes, decision making, workflow management and automatic information exchange with their supply chain partners," retailers have implemented different information technologies, including (Wamba and Lefebvre 2006):

- Enterprise Resource Planning (ERP)
- Warehouse Management System (WMS)
- Transportation Management System (TMS)

- Automatic Identification and Data Collection (AIDC)

To improve performance, retailers have also supported new customer-focused concepts:

- Vendor-Managed Inventory (VMI)
- Point of Sale (POS)
- Collaborative Planning, Forecasting and Replenishment (CPFR)

Retailers still focus on emerging technologies to achieve further improvements, though many issues remain. While (Wamba and Lefebvre 2006) claims that RFID and EPC Networks are promising, implementation hurdles such as cost exist. For instance, (Theo 2006) claims that Wireless Sensor Networks are often cost-effective enough to implement at the pallet level, though still too expensive at the part level.

With regard to RFID specifically, (Rutner and Waller 2004) considers three benefits to retailers:

1. RFID may increase the power of retailers in the supply chain relative to suppliers.
2. RFID may reduce retailers' reliance upon suppliers for category management.
3. RFID may increase the economic power of larger retailers in supply chains as compared to smaller retailers.

#### 3.3.1.2 Food and grocery

| | |
|---|---|
| Major concerns: | Product spoilage, increasing item variety, inventory transparency, inventory reduction, tampering |
| Existing initiatives: | Many for supply chain management designed to streamline inventory (some discussed below); for tracking, Safeway and Horizon Lines are tracking containers in Pacific Northwest |

The grocery retail industry faces many significant challenges: varying spoilage and storage requirements for different goods, increasing item variety, tough price competition from big-box retailers, and prevalence of new supply chain management strategies.

The fruit trade exemplifies many of the spoilage issues that complicate grocery logistics (Jedermann and Behrens 2006):

- 57.1 million tonnes of maritime reefer cargo in 2005, 56% of which were fruit transports
- Fruit matures during transport, making it very fragile
- Products must be chilled between 0-15°C
- Variation in maturity: bananas have 3 weeks, strawberries have 3 days

- Autonomous sensors cannot detect most characteristics such as firmness, starch or sugar content, taste, color; instead these typically require unpacking or even destructive methods
- Local freezing of freight in the container can cause significant losses
- American regulations require four temperature sensors in the container, a "wireless sensor network [can] monitor the gradient of different environmental parameters"

As mentioned, inventory variety has also grown, from nearly 6,000 SKUs in the 1960s to almost 40,000 today (Wamba and Lefebvre 2006). These difficulties are exacerbated by the fact that grocery supply chains have been found to be very inefficient. A study in the early 1990s showed that, on average, "it took 104 days for dry grocery products from supplier to consumer." A primary reason for this inefficiency was provincialism of the supply chain approach: stock was pulled through by replenishment orders for stores, while warehouse inventory was pushed by trade promotions and forward buying practices, which emphasizes the large-volume discounts offered by manufacturers. This difference caused substantial inventory growth. (Prater and Frazier 2005)

Much of this issue is tied to the marketing strategy of supermarkets. Spending on trade promotions from 1981 to 1991 were shown to increase from 34-50% while advertising fell from 43-25%. It was argued that, if removed, this inefficiency could save about $10bln, or 10.8% of sales turnover. Several strategies, many of which are variations on Automatic Replenishment Programs, are being embraced to try to ameliorate this situation. One study of nine grocery chains that implemented an ARP-type program, Efficient Consumer Response (ECR), found that while inventory turns decreased and levels increased, net profit margins increased by 22%. A reason cited for the improved margin were larger volume purchases. (Prater and Frazier 2005) Figure 8 illustrates both current and future conditions in addition to the expected tools and techniques needed to get there.

| Current conditions | Future conditions | Tools and techniques that will get us there |
|---|---|---|
| *Personnel* | | |
| A few highly knowledgeable people: most workers are minimally trained and educated<br>Limited resources of employees due to cutbacks and downsizing<br>"Command and control" management style | Formation of production teams<br>Highly trained personnel and cross-training within organization<br>Management by integration and self-control | Team concept and management<br>Theory Y use of management techniques<br>Behavioral systems engineering<br>Ergonomics and occupational biomechanics<br>Cognitive engineering design<br>Total quality management |
| *Communications* | | |
| Overuse of printed media leading to large waste of paper<br>Delays in ordering stock items due to lack of personnel and lack of feedback to warehouse and manufacturer<br>Delays in price comparison and updates due to long lead times between change and final resolution | Incorporated use of information systems and computers networks to establish rapid communication between retailer, warehouse and supplier to expedite supply requirements, pricing information changes and production problem resolution | Flow process analysis<br>Manufacturing system optimization<br>Operations research<br>Systems management<br>Manufacturing information systems<br>Neural networks<br>Critical path methods/program evaluation and review techniques |
| *Inventory reduction* | | |
| Large inventory levels on shelves and in storage at retail level and in warehouse<br>Production difficulty at manufacturer due to excessive or insufficient manufacturing rates | Minimum inventory levels on shelf at retail level<br>Limited or non-existent inventory levels at retailer and warehouse<br>Production scheduling more closely linked to actual requirement of marketplace<br>Manufacturer's restructured packaging methods for smaller unit quantity per case to help minimize back-stock levels at warehouse and retailer. Improved methods to streamline process and allow for increased unit volume sales | Just-in-time inventory<br>Integrated logistics planning<br>Cost management<br>Engineering economy<br>Regression and analysis of variance<br>Linear and non-linear optimization<br>Production and inventory control<br>Stochastic processes<br>Simulation modeling<br>Dynamic programming<br>Probability applications<br>Production engineering<br>Work measurement<br>Queuing theory<br>Markov chains |

**Figure 8. Current and possible future trends in grocery retail**
*(Prater and Frazier 2005)*

Additionally, grocery supply chains face a liability due to the nature of the business: selling food for the general public. Several instances have occurred with contaminated food being sold to the market place and needing to be tracked down: for example an E. coli breakout in Odwalla apple juice in 1996, and the more recent E. coli breakout in spinach in 2007. In the latter example, the bar code on the bag was used to trace the spinach back to California's Salinas Valley, though a significant search effort for the grower then followed. Meanwhile, any spinach that could possibly have been affected was pulled from supermarket shelves, costing the industry up to an estimated $74 million. It has been said that RFID tracking of these bags and the containers within which they travelled would have led investigators much more quickly to the source, which implies that most of the spinach removed from shelves may not have to had been. An potentially more significant scenario is if a common food ingredient such as a stabilizer or flavor additive is found to be toxic, where many food products could possibly be affected. These possibilities introduce another case for tracking at both the container and item levels. (Weier 2007)

Beyond the commercial and safety complications faced by grocers, cargo security standards for identification and screening under the 24-hour Rule has been said to be "far too restrictive on the produce industry… Based on climate, based on the perishable nature of products, there should be some way that [grocers should] get some latitude here (What Regulations 2003)."

The fragility of grocery goods, ever-increasing number of SKUs, new supply chain approaches being implemented, food recalls, and security standards are all factors that have been said to make "grocery ... a prime candidate for RFID implementation." Tracking is likely to become ever more important as grocery supply chains approach a JIT strategy. (Prater and Frazier 2005) In addition, cargo quality may be an area in which to expand ICCs. While sensors have shown to be limited in this application, they have only been used to monitor cargo conditions rather than actively control them (outside of temperature). A cargo-quality control system that, for example, responds to container conditions by introducing $CO_2$ to ripen bananas while underway rather than having to unload them upon arrival into a ripening facility, tie them up for several days, then reload and transport them to the stores as is currently done, might lower inventory and handling costs. Admittedly, such a move would probably introduce risk and require a very tight supply chain, though may nevertheless be a worthwhile ICC implementation. Finally, electronic manifesting through ICC tagging may have the potential to expedite the manifesting requirements that add pressure to the supply chain.

#### 3.3.1.3 Pharmaceuticals

Major concerns: Product security from tampering, cargo source transparency, counterfeit imitations

Existing initiatives:

The pharmaceutical supply chain faces some of the typical issues that other shippers face with regard to inventory management, although the importance of these products adds extra, even more critical elements: ensuring product integrity, reducing tampering, and preventing counterfeiting.

An example of the vulnerability of the pharmaceutical supply chain occurred recently when a toxic syrup, diethylene glycol, was found in 260,000 bottles of cold medicine to be sold in Panama. The syrup is used as a sweet-tasting, cheaper alternative to safer syrups in various medicines, and has led to at least eight mass poisonings over the last two decades. This batch of counterfeit glycerin was tracked back through "three trading companies on three continents, yet not one of them tested the syrup to confirm what was on the label. Along the way, a certificate falsely attesting to the purity of the shipment was repeatedly altered, eliminating the name of the manufacturer and previous owner." (Bogdanich and Hooker 2007)

In the United States, counterfeit products account for less than 1% of the total. However, in parts of southeast Asia and Africa this number is nearly 50%. Technologies that can track drugs from the manufacturer to the pharmacy might provide both a proactive approach that helps ensure integrity and prevents counterfeiting, while also improving and simplifying a common reactive approach: the product recall. (Tiemey 2004) This opinion is supported by (Ashton 2006), who states that "tagged packages of drugs... can now come with digital security" to determine that a package is genuine.

(Tiemey 2004) raises the importance of industry participation in the development of technologies and regulation to ensure that the peculiarities of the industry are represented. For instance, scanning technologies must be tested to ensure that they do not affect the quality and safety of pharmaceuticals.

Venture Development Corporation's Mike Liard sums up the outlook for the pharmaceutical industry's possible future with RFID: "[Pharmaceuticals have] a lot more to gain in security and safety with RFID. They can choose the high-risk, high-value products, like Viagra, for anti-counterfeiting and safety. You can save lives with RFID on prescription drugs. That factor added to the value proposition makes it a [much] easier sell... We're struggling with visibility now. Next comes security, and then quality, using RFID and sensing technology. Pharmaceuticals [are] already ahead in these scenarios." (Navas 2004)

#### 3.3.1.4 Hazardous Materials (HazMat) and chemicals

Major concerns: Transport safety and accountability, theft
Existing initiatives: Dow Chemical Company

One of the key elements for hazardous material supply chains is ensuring safety and security for customer safety, regulatory compliance, risk mitigation, and public image.

Several regulatory bodies are involved in the transport of hazardous materials, not the least of which is TSA. TSA has focused on potential terrorist threats to hazardous cargoes, "especially when they sit idle and are near major population centers." It is requiring that rail workers and shippers constantly monitor such loads, and is also planning to require higher levels of shipment tracking and data reporting in the near future. In addition, new handoff rules for hazardous material receivers in 46 high-threat urban areas are planned. (Feds 2007) TSA published a best practices guide with suggestions to meet the new standards. Among those relating to ICCs include (Hazardous 2006):

- Use tamper-resistant or tamper-evident seals and locks on cargo compartment openings.
- Consider using advanced technology to track or protect shipments en route to their destinations. For example, you may wish to install tractor and trailer anti-theft devices or use satellite tracking or surveillance systems. As an alternative, consider frequent checks with drivers by cell phone to ensure everything is in order.
- Install tamper-proof seals on all valves and package or container openings.
- Implement a system for a customer to alert the shipper if a hazardous materials shipment is not received when expected.

For these reasons and more, "the chemical industry is a natural place where you will see supply chains implementing a mix of RFID and GPS," remarks Dan Mullen, president at AIM Global. He goes on to say that companies are looking for

security and traceability. (Sullivan 2006) Indeed, hazardous material transporters are in fact looking to ICCs solutions, among others, to improve supply chain security and efficiency. A prominent example of these is Dow Chemical. More discussion of hazardous material trade and Dow's approach to that is discussed in *3.3.2.2 Dow Chemical Company*.

#### 3.3.1.5 Military

| | |
|---|---|
| Major concerns: | Immense item inventory and sourcing, highly volatile demand, transport security, inventory transparency |
| Existing initiatives: | US DOD Defense Logistics Agency's Automatic Identification Technology; Cargo*Mate |

The issues facing military logistics are addressed in greater detail in section *3.3.2.5 US DOD: US Defense Logistics Agency*, which discusses the US's primary military logistics effort.

### 3.3.2 Initiatives

Shippers are typically concerned more about their cargo than the containers within which they travel. Therefore, their initiatives have mostly focused on tracking levels below containers, namely pallet, multipack, and part level. Further, (White 2004) states that "smart containers" may be a misguided focus when cargo transparency is the real goal, which would instead call for "smart cargo."

Some of the most prominent shipper initiatives are presented in Table 2.

**Table 2. Prominent initiatives involving shippers**

| Shipper | Container level | Pallet or below |
|---|---|---|
| Boeing | X | X |
| Dow | X | |
| Exel | | X |
| Intel | | X |
| Kmart | | X |
| Marks and Spencer | | X |
| Metro Group | | X |
| Safeway Supermarkets | X | |
| Scottish Courage | | X |
| Starbucks | X | |
| Tesco | | X |
| US Department of Defense | X | X |
| Wal-Mart | | |
| Woolworths | | X |

Significant initiatives involving containers are discussed below (for Safeway, see *3.2.2 Initiatives*).

#### 3.3.2.1 Boeing Corporation

Project Lead: Boeing
Partners:
Tagging Level: Container, part

*Boeing has become involved in container tracking on two fronts: as a shipper and as a technology provider.*

As a shipper, Boeing has been an active participant at conferences and in the OSC initiative. Boeing presented at the "eyefortransport" North American Cargo Security 2005 Forum, and argued that complying with C-TPAT makes good business sense, is a "moral obligation," and is necessary for companies to protect their respective brands. Boeing has also conducted e-seal tests at the request of CBP, using both a device designed by Boeing itself as well as the CommerceGuard (Downey 2006). This led to using smart seals, with serial numbers and manifest data that employees check upon arrival at the warehouse, on all of its containers (Melcer and Tsadik 2006). In addition to container tracking, Boeing and Airbus have jointly required suppliers to use tracking tags on all aircraft parts (at the part level). (The Freight 2005)

As a technology provider, Boeing has also participated in OSC and other programs. Boeing is searching for commercial, off-the-shelf technology that requires minimal customization. "What we're doing with OSC is taking a family of

components, applying an architecture, and integrating them into and end-to-end solution," said Mike O'Neil, Program Manager, Maritime Cargo Security Systems for Boeing. (Sowinski 2004)

Despite Boeing's size and purported involvement, however, not much more information than this has been found available in the public domain.

#### 3.3.2.2 Dow Chemical Company

| | |
|---|---|
| Project Lead: | Dow Chemical |
| Partners: | |
| Tagging Level: | Conveyance (rail cars), Container |

*Dow Chemical, an international chemical producer and transporter, moves more than 2 million products annually, of which 20% involves crossing an international border. Movements are made via road, rail, ocean and other transportation modes* (Sullivan 2006). *In 1995, Dow undertook a 10-year program to improve its supply chain safety and security on a number of metrics. In 2005, it renewed the program for another ten years, the results of which are seen in their current efforts* (Reese 2007). *This renewed program is intended to increase supply chain visibility and improve emergency preparedness and response. It should "rely on sensor networks, global positioning systems and auto-identification technologies to improve efficiencies and supply chain processes," claims a company executive.* (Sullivan 2006)

Dow's next supply chain strategy consists of four parts, of which the second directly addresses an ICC solution (Reese 2007):

- Supply Chain Redesign: Reduce the number of shipments and container-miles for highly hazardous materials
- Supply Chain Visibility: Improve visibility of shipments through implementation of RFID and GPS technologies
- Shipping Container Design: Improve container design to prevent tampering and to reduce the potential for chemical releases due to accidents or security incidents
- Enhanced Collaboration: Enhance collaboration with carriers and local communications to improve emergency preparedness and response should a chemical release occur

Dow's program intends to combine RFID with GPS first for its rail fleet, followed by a pilot program for intermodal containers. David Kepler, Dow's Chief Information Officer, said that "[Dow's] experience to date has proven that enabling technologies such as RFID will play a very important role in our supply chain sustainability strategy by helping to provide enhanced shipment visibility and information sharing with our supply chain partners." (Katz 2007) This is no small task, as Dow is North America's largest bulk chemical shipper by truck and by rail, and it owns the second-largest fleet railcars in the world, at 26,000. (Reese 2007) Understandably, Dow is making a long-term investment, as they acknowledge that

the pilot projects will probably take 10 years to reach their full payback potential. (Katz 2007)

Another goal of the program is to improve emergency response through cooperation with industry bodies. For instance, Dow is working with the Chemical Transportation Emergency Center (CHEMTREC), which is an emergency call center that helps to manage immediate emergency response information for parties involved in accidental chemical releases and clean ups. A demonstration project is intended to improve information sharing between the two organizations. (Reese 2007)

#### 3.3.2.3 Safeway Supermarket

| | |
|---|---|
| Project Lead: | Horizon Lines |
| Partners: | Safeway Supermarkets |
| Tagging Level: | Container |

Safeway has jointly undertaken an initiative to track containers with Horizon Lines. See *3.2.2.1 Horizon Lines* for more information.

#### 3.3.2.4 Starbucks Coffee Company

| | |
|---|---|
| Project Lead: | Starbucks Coffee Company |
| Partners: | CommerceGuard |
| Tagging Level: | Container |

*Starbucks installed CommerceGuards on some containers full of coffee beans travelling from Guatemala to the US and Europe. The CommerceGuard monitors movements and door-openings, and regularly updates users throughout the entire shipping process.* (Thomas 2006)

Starbucks and others have suggested that complying with C-TPAT makes good business sense. In addition to being a "moral obligation," the company must protect its brand reputation (Downey 2006). Dorothy Kim, executive vice president of Starbucks' supply chain operations, stated that "Starbucks recognizes that enhancing international supply chain security while reducing the risk of suspending container traffic, contributing to real-time management and quality assurance are necessary in order to ensure that worldwide commerce can operate in a wide range of security conditions. We are taking a proactive approach in securing our supply chain to ensure the safety of our customers, partners (employees), communities and countries of origins. CommerceGuard is an enabler in helping us move towards that goal." (Thomas 2006)

##### *3.3.2.4.1 Result*

Motivations for Starbucks included increased security, increased visibility, and better coordination for on-time deliveries to reduce inventory (Kulisch 2006). On the security side, during a three-month test period, the units accurately recorded all door openings. (Thomas 2006). Additionally, humidity sensors were used with the intention to detect and thwart stowaways.

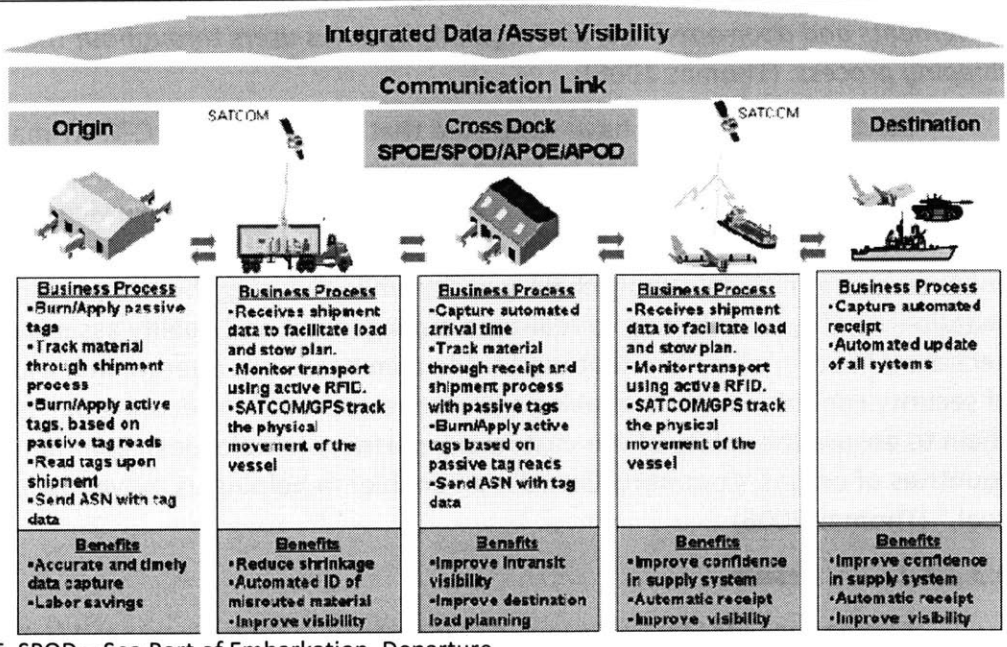
What resulted, however, was a revelation that prolonged periods of high-humidity existed for some containers. The cause of these humidity variations were not stowaways, but in fact a supply chain bottleneck for some containers that would wait extended periods of time in hot conditions for a ship headed to Seattle. This quickly became a quality-assurance concern since high-humidity is not desired for coffee beans, and a new strategy in the supply chain resulted. (Zachary 2007)

### 3.3.2.5 US DOD: US Defense Logistics Agency:

Project Lead: US Defense Logistics Agency
Partners:
Tagging Level: Container, Pallet, Part

*The US Department of Defense's primary logistics provider, the Defense Logistics Agency (DLA), has received much attention for its focus on tracking technologies, most notably RFID. The DLA supplies the military with virtually every item and logistical need that arises, from personal care products to bulk fuels, and from domestic bases to theatres of war. The DLA was created in 1961, has a presence in 48 US states and 28 foreign countries, handles 5.2 million item types, and in 2005 provided nearly $32 billion in goods and services worldwide.* (DLA at a Glance 2006) *To address the growing needs of cargo visibility and security, an office called "Automatic Identification Technology" (AIT) was created within DLA to investigate and manage its tracking technology portfolio.*

The AIT office describes DOD's supply chain as shown in Figure 9.




SPOE, SPOD = Sea Port of Embarkation, Departure
APOE, APOD = Aerial Port of Embarkation, Departure

**Figure 9. DLA's AIT information network**
*(DOD Logistics 2007)*

The GAO has considered DOD's ability to track and identify inventory a high-risk area since at least 1990, as inventory management systems and procedures were deemed ineffective (Better Strategic 2005). Operations Desert Storm and Desert Shield were the US DOD's first widespread use of containers, and logistics problems were suffered on many fronts, one significant contributor of which was poor documentation and "no visibility," even though active RFID tracking was being trialed at the time. Some of the results of this execution include (Burke 2006):

1. At one point, nearly 17,600 containers were unaccounted for in Saudi Arabia.
2. Accurate assessments of orders (or reorders) were nearly impossible, which led to duplicates, hording, and inaccurate reporting to commanders.
3. The disaggregate collection of development-stage systems could not communicate with each other.
4. A $1.2 billion discrepancy between the value of supplies shipped to the theater and the amount acknowledged as having been received. Army generals attributed this to poor communications, to which container tracking can be considered a significant contributor.

Many efforts are underway at DLA to address these problems, including better aligning supply and demand, leveraging industry capabilities, designing a best-value IT environment, training and retaining more experienced personnel, etc. (Defense Logistics 2007) To address visibility and accountability, however, much focus has also been placed on improving ICCs. In the early 1990s, active RFID was intended to provide nearly real-time, in-transit visibility of shipments for Operations Desert Shield and Desert Storm, though, as discussed, this was not entirely successful. In 1997 the AIT office was formed specifically to focus on technology to improve supply chain visibility (DOD Logistics 2007). A primary change still underway has been the inclusion of passive RFIDs to accompany existing active RFIDs. This change is envisioned to make inventory management more accountable, accurate, efficient, and hands-free. Some of the specific expected visibility benefits are (Better Strategic 2005):

1. Near real-time, in-transit visibility for all classes of supplies and materiel
2. "In the box" content-level detail for all classes of supplies and materiel
3. Quality, nonintrusive (hands-off) identification and data collection that enables enhanced inventory management
4. Better item-level visibility. RFID tagging of DOD materiel is applicable to all items except bulk commodities such as bulk liquids, sand, and gravel.

However, Paul Donato, a Defense Department consultant, reaffirms that technology alone is not the solution. He states: "RFID is a data capture mechanism... the value of RFID will not come from physics. The real value will depend on how you create intelligence from all the data you capture." (Johnson 2005) Similarly, a GAO

audit has called for much stronger management to accompany any new RFID technology. Additionally, they feel that some key metrics are lacking, namely (Better Strategic 2005):

1. General and long-term goals and objectives
2. A description of specific actions to support goals and objectives
3. Performance measures to evaluate specific actions
4. Schedules and milestones for meeting deadlines
5. Identification of total resources needed and annual cost estimates for passive RFID implementation into the supply chain
6. Evaluation of the overall program with specific processes to allow for adjustments and changes.

GAO also claims that, while the situation has improved, some problems have existed in Operation Iraqi Freedom that did during the previous Iraq wars. (Better Strategic 2005) Still, progress is evident in some of the statistics. Donato claims that all DOD shipments from the continental US are active tagged, while passive tagging occurs at the pallet level. He also claims that "RFID has helped with a 36% increase in operational efficiency, while reducing wrongly routed shipments 3%." (Johnson 2005)

In addition to visibility, cargo quality and security are important issues for DOD. A DOD "best practices" brochure discusses container seals, GPS tracking, RFID tags, and container condition sensors (temperature, light, humidity, etc.) (Melcer and Tsadik 2006). DOD has also taken part in several pilot programs, including the DOT's Hazardous Material program (see *3.1.2.4 Hazardous Materials Safety and Security*).

## 3.4 ICC SOLUTION PROVIDERS

### 3.4.1 Background

ICC technology and service providers encompass a wide range of companies, from container-specific veteran players to smaller start-ups to giant conglomerates. Most have been actively engaged in marketing, industry standardization, research, and development of their products. Most have found some shipper or niche industry in which to test their products, however few industry-wide standards exist, and therefore no provider, either officially or unofficially, currently dominates the landscape.

## 3.4.2 Initiatives

### 3.4.2.1 ARGO Tracker/EJ Brooks

Project Lead: ARGO Tracker/EJ Brooks
Partners:
Tagging Level: Container, Pallet, Multi-pack, Part

*ARGO Tracker sells its ARGO Tracker Unit that is designed to remain inside a container and transmit both location and any container data stream via cellular and GSM networks. Common data streams offered include temperature, humidity, and impact sensors, as well as video capture. EJ Brooks is a veteran manufacturer of seal products for containers, truck trailers, tanker valves, and other industrial applications.*

ARGO and Brooks have developed a joint solution that combines a Brooks E-seal and an ARGO Tracker Unit. The E-seal regularly communicates its status to the ARGO Tracker, and effectively becomes one of the data streams received by the unit that is transmitted via satellite to the home office. This combined service solution can then provide tracking, cargo monitoring, and container integrity information all in one. (Electronic 2006) (ARGO Tracker 2007)

### 3.4.2.2 CommerceGuard (and related projects)

#### *3.4.2.2.1 Technical description (CommerceGuard)*

Project Lead: GE Security, Mitsubishi Corporation, Samsung Corporation, Siemens Building Technologies
Partners:
Tagging Level: Container

*CommerceGuard is a removable device primarily developed in response to CBP's CSD initiative. Although it is primarily an e-seal, it has a port through which additional sensors can be connected and data transferred.* (CommerceGuard 2006)

#### *3.4.2.2.2 Industry support program (International Container Security Organization [ICSO])*

Project Lead: GE, GreenLine Systems, J.P. Morgan Chase, Mitsubishi Corporation, Siemens AG, Unisys Corporation
Partners:
Tagging Level: Container

*The ICSO is an industry organization developed to create industry standards for container security devices. "ICSO intends to assist in furthering and implementing the work of the World Customs Organization (WCO)... ICSO will focus on defining standards for systems and devices that detect and report in-transit container intrusions and other irregularities* (International Container 2006)*."*

#### *3.4.2.2.3 Pilot program (Tamper Evident Secure Container [TESC])*

Project Lead: China International Marine Containers Group (CIMC), Unisys

Partners:

Tagging Level: Container

*The TESC is a proof-of-concept demonstration for containers travelling from China to the US utilizing CommerceGuard technology. Unisys tracked 18 GE containers from Guangdong, China, which were transported to Hong Kong by truck, loaded aboard a ship to transport them to Los Angeles/Long Beach, then trucked again to their final destination.* (GE 2005)

Unisys attempted more than 15 different security breaches in mainland China, Hong Kong, and the United States. Twelve of the containers were not tampered with, but Unisys conducted five scripted break-ins on the others, and one container was opened by customs officials. (GE 2005)

#### *3.4.2.2.4 Issues*

CommerceGuard has several issues associated with it. First, CommerceGuard does not comply with agreed-upon ISO standards for frequency that are being used by most other technology developers, but instead has developed its own. This is in discord with the US Port Security Bill since it calls for standards consistent with ISO, IMO, and WCO. (Kulisch 2006)

Second, the CommerceGuard system is proprietary versus open; therefore, all user data passes through the central CommerceGuard system, rather than working through an open network. Therefore, the CommerceGuard system operator would exclusively create, own, and control the global database of container readings (Comments 2006).

Last, it has been implied that the ICSO is an extraneous standards organization. The WSC states that the ICSO was "an unnecessary and counterproductive initiative... inconsistent with the extensive efforts of international ocean carriers, terminal operators and technology developers at the ISO." WSC suggests that the ISO includes all, while the ICSO is proprietary. Further, WSC claims that GE did not participate with ISO standards development, and therefore ICSO is simply redundant. (Comments 2006)

#### *3.4.2.2.5 Limitations, problems, and costs*

CommerceGuard is said to be insufficient since the US Port Security Bill calls for detection of any intrusion, not just door openings. Additionally, CBP has not found false-positives to fall below 1% yet, which was the maximum requested. (Kulisch 2006)

GE estimates the amortized cost of CommerceGuard to add $25/trip, which is greater than initial estimates of less than $10/trip and $60/device. The cost of a

fixed reader is said to be $1,500, and a handheld $1,000. Work is being done to lower these costs (Kulisch 2006).

#### 3.4.2.3 SAVI Technology

| | |
|---|---|
| Project Lead: | SAVI Technology [a joint venture between Savi Technology (a subsidiary of Lockheed Martin), Lockheed Martin, and Hutchison port holdings] |
| Partners: | |
| Tagging Level: | Containers |

*Savi Technology has installed RFID tags on containers and readers in a worldwide network. Information is available to clients through the SaviTrak system* (SaviTrak 2006). *The system is not proprietary, as it complies with ISO standards for e-seals, and can therefore work with other systems like WhereNet* (Kulisch 2006).

SAVI has used the term "SmartBox" quite frequently to describe containers implementing its system, consistent with CBP. SAVI aims for its technology to be a standard in the US by meeting CBP and ISO standards, and by associating its technology with C-TPAT compliance.

##### *3.4.2.3.1 Results*

SAVI claims that their product reduces inventory, stock-outs, lead-time variance, administrative fees, theft, and lost containers; and increases manufacturing uptime. (Petrakakos 2005) SAVI has estimated these benefits could number $1,200 in savings per container. (Haveman and Shatz 2006)

#### 3.4.2.4 Sensitech (Ryan EZT, TempTale, etc.)

| | |
|---|---|
| Project Lead: | Sensitech |
| Partners: | |
| Tagging Level: | Container |

*Sensitech sells a variety of condition monitoring and recording sensors for containers (and a few other applications). Their products typically record temperature data onto a paper chart that is sealed into the unit, which is broken upon arrival by the receiver, checked, and may be filed. Ryan EZT has been in existence for more than 80 years, and the technology is a standard in reefer shipping.* (Sensitech 2006)

#### 3.4.2.5 WhereNet

| | |
|---|---|
| Project Lead: | WhereNet |
| Partners: | |
| Tagging Level: | Conveyance (truck chassis while in port), Containers |

*WhereNet provides RFID tag systems used primarily to manage containers and conveyance equipment (tractors, chassis, etc.) in seaports or other high-density container areas.* (RFID on track 2006) *WhereNet tags are also used at some distribution centers and warehouses.*

WhereNet is already running in ten of the thirteen terminals at the Ports of Los Angeles and Long Beach. Further, their RFID tags have been placed on most of the independent trucks operating in southern California, and railroads may be their next step. It is suggested that its port terminal tags alone will "allow railroads to accommodate annual intermodal growth of 6 to 7 percent. (RFID on track 2006)"

#### 3.4.2.6 Other initiatives

In addition to the solutions above that are more directly related to containers and either well underway or mature, there are other initiatives that are considered because they fall into one or both of the following categories:

- Emerging technologies about which little information has been found
- Complementary (or potentially competitive) technologies

##### *3.4.2.6.1 Altobridge*

Project Lead: Altobridge
Partners:
Tagging Level: Conveyance (ship), Container

*Altobridge provides satellite communication services to ships, and also allows transmissions from containers through that system. This ultimately allows for tracking, condition tracking, and any other relevant data.* (Altobridge 2006)

##### *3.4.2.6.2 eModal.com*

Project Lead: eModal.com
Partners:
Tagging Level: Conveyance, container

*eModal is a single, web-based system that brings together ship and container tracking data for the "intermodal community" (mostly truck and rail) at various container ports around the country. The system offers detailed container, vessel, and terminal information for the dray industry* (E-Modal 2006).

##### *3.4.2.6.3 GPS Insight*

Project Lead: GPS Insight
Partners:
Tagging Level: Conveyance (truck chassis)

*GPS Insight tracks tractors (and in essence trailers) using GPS units. The tracking information provides realtime visibility to the supply chain, and also helps with certain tasks like calculating highway mileage taxes.* (GPSInsight.com 2006)

Costs total about $550 per unit plus $35 per month for the service per unit (GPSInsight.com 2006).

#### *3.4.2.6.4 Intelli-Shield (iShield)*

Project Lead: Intelli-Que
Partners:
Tagging Level: Container

*Intelli-Shield units are reusable e-seals with a wireless communications network for inter-container communication (multi-hop or "Daisy Chain"). The units also can provide quality control information and geofencing. The units can be set to update automatically or reply when pinged.* (Intelli-que 2006)

#### *3.4.2.6.5 Lloyd's Marine Intelligence Unit*

Project Lead: Lloyd's Marine Intelligence Unit
Partners:
Tagging Level: Conveyance (ship fleets)

*Lloyd's Marine Intelligence Unit (MIU) is an internet portal that allows users to track almost any vessel in the world. Information is gathered via an international network consisting of both employed parties and "AIS readers," which are units that read the Automatic Identification System (AIS) data put out by most ships as required by USCG. Updates on vessel location, status, next port of destination, etc. is updated nearly realtime, though with varying regularity.* (Lloyd's 2006)

#### *3.4.2.6.6 Par Logistics Management Systems*

Project Lead: PAR LMS
Partners:
Tagging Level: Conveyance (trailers), containers

*PAR LMS was created in 1998 as a result of the US DOT Cargo*Mate initiative. PAR LMS now markets its Cargo*Mate product to track chassis for intermodal and port efficiency management, with thousands of units having been deployed in various ports. Additionally, its newest product, Cargo*Watch, uses "GPS, RFID, satellite, cellular, and internet technologies to provide relevant and accurate information on cargo, container status and security." PAR LMS regards critical that "actionable information on asset status and location must be available, reliable, and most importantly, affordable."* (PAR LMS 2007)

#### *3.4.2.6.7 Polestar (Purplefinder.com)*

Project Lead: Polestar
Partners:
Tagging Level: Conveyance (ship fleets)

*"Pole Star's Marine Asset Tracker system (MAT) is comprised of reliable satellite tracking hardware linked to a powerful web-based service. It provides an effective way of automatically tracking powered and unpowered marine assets (ships and harbor craft) in real time.* (Polestar 2007)"

#### *3.4.2.6.8 Qualcomm*

Project Lead: Qualcomm
Partners:
Tagging Level: Conveyance (tractors and trailers)

*Qualcomm is a large conglomerate that provides tracking services to many industries, including road carriers. Its truck tracking solution, TrailerTRACS, is used for both tractor and trailer management. Many services are available, including location tracking, geofencing, tethered/untethered status updates, etc. Despite its involvement in the global tracking market, however, Qualcomm does not yet appear to be directly involved, at least commercially, in container tracking.* (Qualcomm 2007)

#### *3.4.2.6.9 SeeContainers*

Project Lead: Hi-Tech Solutions
Partners:
Tagging Level: Container

*Hi-Tech's SeeContainers product is an optical-recognition product intended to read already-existing ISO and IMO labels on containers at intermodal transfer points. The product is an alternative to one proposed ICC benefit: the declaration of an intermodal transfer.* (SeeContainer 2006)

#### *3.4.2.6.10 Safefreight Technology*

Project Lead: Safefreight Technology
Partners:
Tagging Level: Conveyance (truck chassis)

*Safefreight Technology provides fleet management solutions for road carriers. Services include GPS tracking, geographic information systems (GIS), and onboard sensors* (Safefreight 2006).

#### *3.4.2.6.11 Silent Commerce*

Project Lead: Accenture
Partners:
Tagging Level: Conveyance (rail cars)

*Accenture is adding RFID tags to rail cars for more effective management and linking of trains in railyards. The active RFID tag solution allows for realtime tracking of rail cars both on the track and with relation to one another in a given train. The cargo sequencing and tracking functions then become automated.* (Accenture 2006)

The Accenture tags capture certain data: wagon contents, shipping route information, storage requirements, temperatures and other environmental conditions.

#### *3.4.2.6.12 Steelroads' NetREDI System*

| | |
|---|---|
| Project Lead: | Steelroads (NetREDI) |
| Partners: | North American railroads (BNSF, CN, CPR, CSX, KCS, NS, UP, etc.) |
| Tagging Level: | Conveyance (rail cars) |

*A system in use by the US rail industry to track and manage rail cars as they are en route. Updates are typically accurate to within a few hours, as signals are sent locally (not via satellite) from the train.* (Steelroads 2006)

The rail industry has invested heavily in Automatic Equipment Identification (AEI) technology to capture arrivals, departures, and passing points. The system allows shippers to access position data from over 300 railroad companies in North America (Intermodal Freight 2005) (Steelroads 2006).

#### *3.4.2.6.13 WIPRO Wireless sensor networks*

| | |
|---|---|
| Project Lead: | Wipro |
| Partners: | |
| Tagging Level: | Conveyance (railroad cars, truck chassis), Container |

*Wipro provides a wide array of wireless sensor network (WSN) solutions. WSNs are made of many nodes and one or more gateways which centralize the data gathered by sensor nodes.* (Theo 2006) *One example of Wipro's work was the installation of nodes in conveyance equipment owned by an intermodal equipment provider (mostly container chassis). The equipment provider desired scanning for web-based tracking of its equipment at intermodal facilities.* (WIPRO 2006)

## 3.5 CONSORTIUM STUDY GROUPS

### 3.5.1 EPCGlobal's Information Services

| | |
|---|---|
| Project Lead: | EPCGlobal |
| Partners: | DHL, Maersk, NYK, Oracle, Savi Technology, Schenker, Schneider National, etc. |
| Tagging Level: | Container, Pallet (or smaller) |

*EPCglobal, the Electronic Product Code standards organization, ratified an initiative to develop RFID technology standards for containers. The first phase of tests of this technology is to track containers and "cartons" realtime between Hong Kong and Japan using RFID. "The test matched tagged products with purchase orders for a footwear manufacturer."* (ElAmin 2007)

This first phase is intended to display interoperability among supply chain partners, test and develop requirements for active RFID, and identify standards opportunities for logistics, among others. (EPCglobal 2006) A second phase is to begin in February, 2008, that is intended to track goods from Shanghai to Long Beach and test information exchange between users for automated customs clearance. (ElAmin 2007)

### 3.5.2 Secure Commerce Roadmap

Project Lead: Unisys
Partners:
Tagging Level: Conveyance (railroad cars, truck chassis), Container

*The Secure Commerce RoadMap is an effort by a large industry consortium, including shippers, ports, carriers and regulators, to develop a summary and analysis of key supply chain security issues. The report focused on various technologies and initiatives currently being discussed about supply chain security. Specific recommendations were developed by and for various stakeholders in the supply chain.* (Secure 2005)

The study had many key findings regarding security, though perhaps its most telling conclusion is evident in a graphic provided that compares the options they evaluated and how each ranks by value to improve security and ease of implementation. Among these options are several ICC solutions. The graphic is provided in Figure 10.

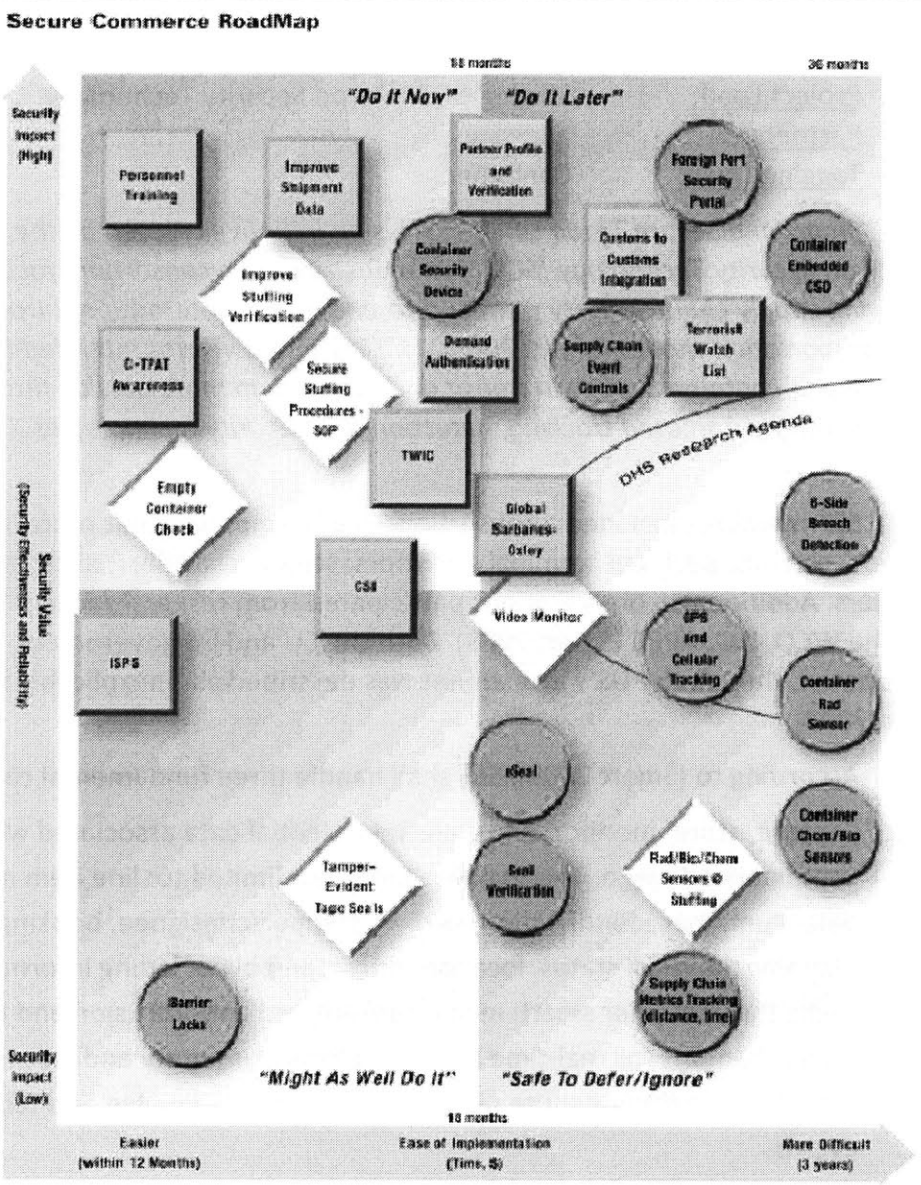



**Figure 10. Secure Commerce Roadmap evaluation of security options**
*(Secure 2005)*

### 3.5.3 Smart and Secure Trade Lanes

Project Lead: Strategic Council on Security Technology
Partners:
Tagging Level: Container

*Smart and Secure Trade Lanes (SST) is an initiative created by the Strategic Council on Security Technology (SCST), an industry-driven consortium focused on improving supply chain security from end-to-end, across international trade lanes and transportation modes* (Smart 2003). *The SST initiative was intended to detect tampering of containers while in transit and move them more quickly through customs using automated tracking, detection and security technologies.* (Hudson 2006)

SST members included a consortium of 65 companies that represented shippers, carriers, port and terminal operators, service providers, and technology providers. Additionally, organizations participated from research/academia along with the WCO, ISO, APEC (Smart 2003). Both the EU and US government participated, though the US's investment was described as "inexplicably modest" by (Flynn 2004).

According to (Smart 2003), SST shall handle three fundamental capabilities:

1. Capture, store, monitor, and transmit essential data associated with containerized cargo. This includes but is not limited to: line item manifest data, container identification, sealing, shipper/consignee, booking, route planning, physical status, location, origin, and bill of lading information.
2. Make the container smart: include automated anti-intrusion and tracking sensor systems for real-time location, physical integrity and status of the containers, including route planning, deviations from plan and tampering events.
3. An automated end-to-end supply chain security audit trail that may be used by the participants in the supply chain as well as international regulatory government agencies.

## 3.6 ACADEMIA AND RESEARCH

### 3.6.1 Intelligent Container initiative

Project Lead: University of Bremen
Partners:
Tagging Level: Container

*The Intelligent Container initiative is a project led by the University of Bremen's Microsystems Center to develop a monitoring system for containerized perishable and sensitive goods. Sensor data includes temperature, humidity and*

*gaseous metabolism products like carbon dioxide and ethylene. Information is sent to local units, then run through a quality prediction model to determine possible quality risks. If any exist, the system sends a warning to the transport operator* (Lassek 2006) (Jedermann and Behrens 2006). *To date, this has been entirely a research effort.*

The system adapts automatically to the supervision requirements of loaded freight. It uses RFID and wireless sensor networks, with nodes automatically identified and added to the network in an ad hoc manner.

### 3.6.2 NASA Automated-Tracking Transponders

Project Lead: NASA
Partners:
Tagging Level: Container

*The NASA transponder, to date purely a research effort, would be used to monitor cargo quality and location. A transponder would store data on the cargo in the container and respond to both local and remote inquiries. This is an end-to-end supply chain approach, as communication is not dependent on local repeaters.* (Automated Cargo 2006)

### 3.6.3 Smart Technology for Environmental Safety and Knowledge Enhancement

Project Lead: Italian Association of Regional Sciences (AISRe)
Partners:
Tagging Level: Container

*This study analyzes the supply chain rather abstractly, but focuses on how various parties communicate with the container, and how best to coordinate them using an ICC to mitigate environmental risk when transporting environmentally-hazardous cargos.* (Barletta 2006) *To date, this has been entirely a research effort.*

# 4. PROPOSED ICC BENEFITS

In this section, ICCs are classified primarily by benefit, though there is some overlap (tracking, for instance, may support both Supply Chain Management goals as well as Security goals). The classification used is the same as that presented in *2.2.1 By proposed benefit*).

## 4.1 SUPPLY CHAIN MANAGEMENT

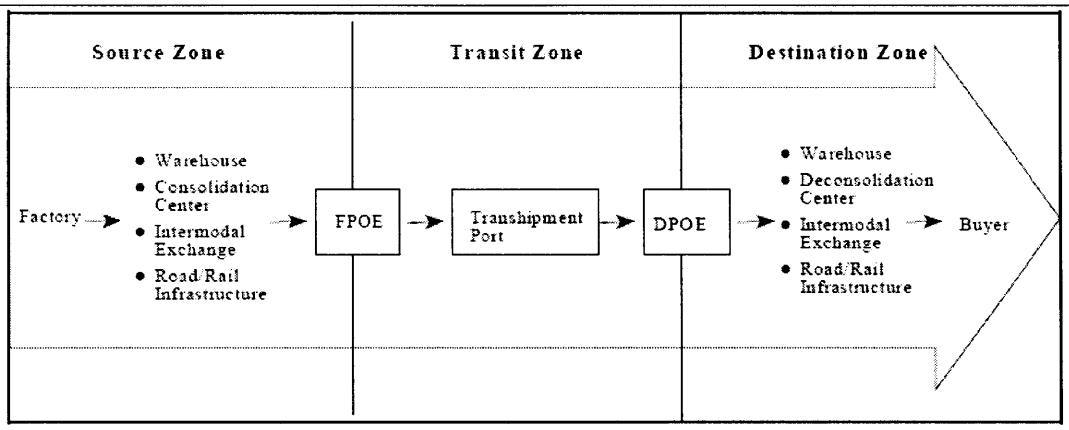
This section discusses ICCs that have the potential to help manage supply chains of containers and their cargo. Technically, this refers mostly to ICCs that electronically store and provide container information, such as the container's ten-digit IMO identification tag number, origin, destination, manifest data, etc., and the systems that support them.

The complexity of managing a containers is immediately evident in the statistics involved (provided by (Secure 2005) and (Flynn 2004)):

- Average container move involves:
  - 20+ "handoffs" (between custodians)
  - 25-40 separate documents
  - 200+ data elements
- The average container ship generates as many as 40,000 paper documents per trip (Global 2006)
- Legal issues
  - International jurisdiction
  - Public/private sector integration

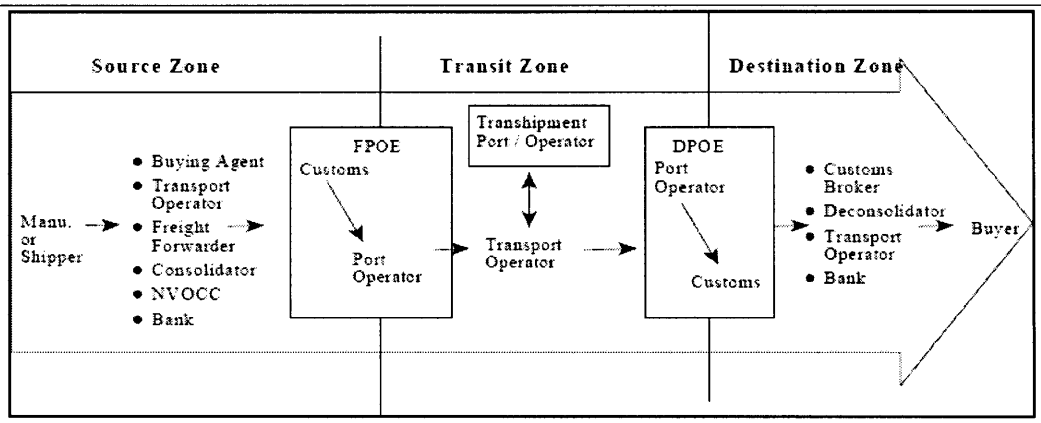
Many sources attempt to document the complexity of an average container movement from one country to another involving an ocean transit. Three of these are presented in the figures below:

- (Lake and Robinson 2005) compares the flow of goods to the flow of custody
  - Figure 11. Transfer of goods from place to place
  - Figure 12. Transfer of custody from person to person
- (Intermodal Process 2006) illustrates flow of goods and information for export and import
  - Figure 13. Intermodal export custody and information flows
  - Figure 14. Intermodal import custody and information flows
- (Petrakakos 2005) compares complexities of cargo flows in the US versus rest of the world (Singapore as an example)
  - Figure 15. Stakeholder interaction of export process in the US
  - Figure 16. Stakeholder interaction of export process in Singapore




**Source:** CRS analysis of OECD figures in *Security in Maritime Transport.*
**Note**: FPOE = foreign port of exit, and DPOE = domestic port of entry.

**Figure 11. Transfer of goods from place to place**
*(Lake and Robinson 2005)*




**Source:** CRS analysis of OECD figures in *Security in Maritime Transport.*
**Note**: FPOE = foreign port of exit, and DPOE = domestic port of entry. NVOCC = non-vessel operating common carrier.

**Figure 12. Transfer of custody from person to person**
*(Lake and Robinson 2005)*

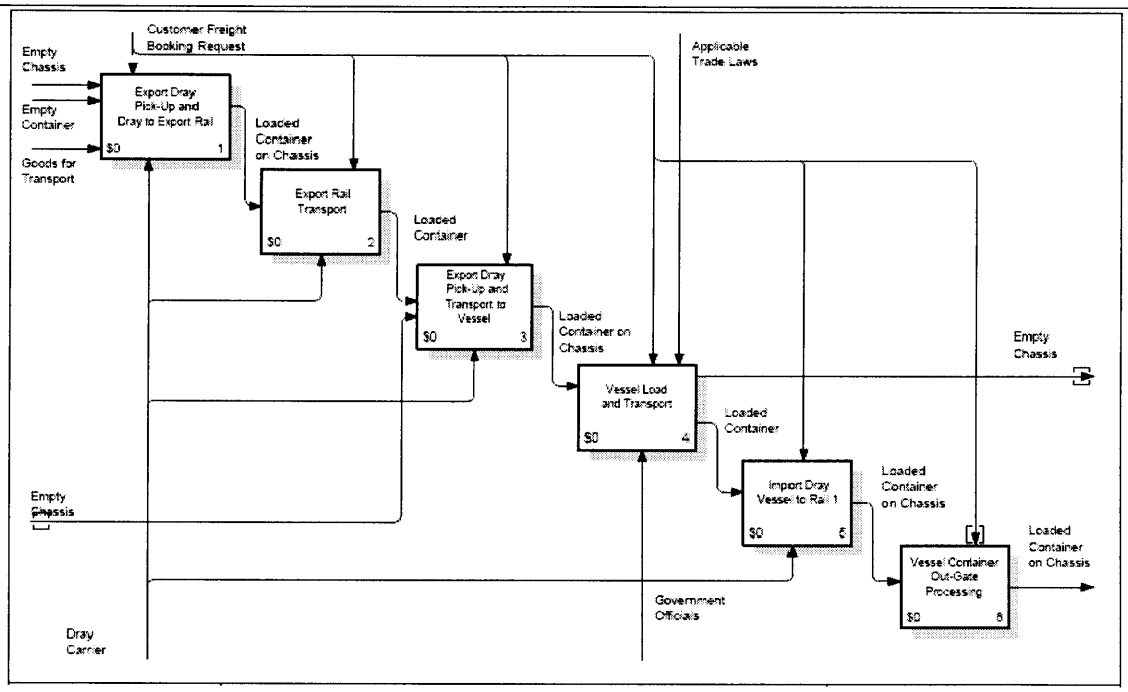



**Figure 13. Intermodal export custody and information flows**
*(Intermodal Process 2006)*

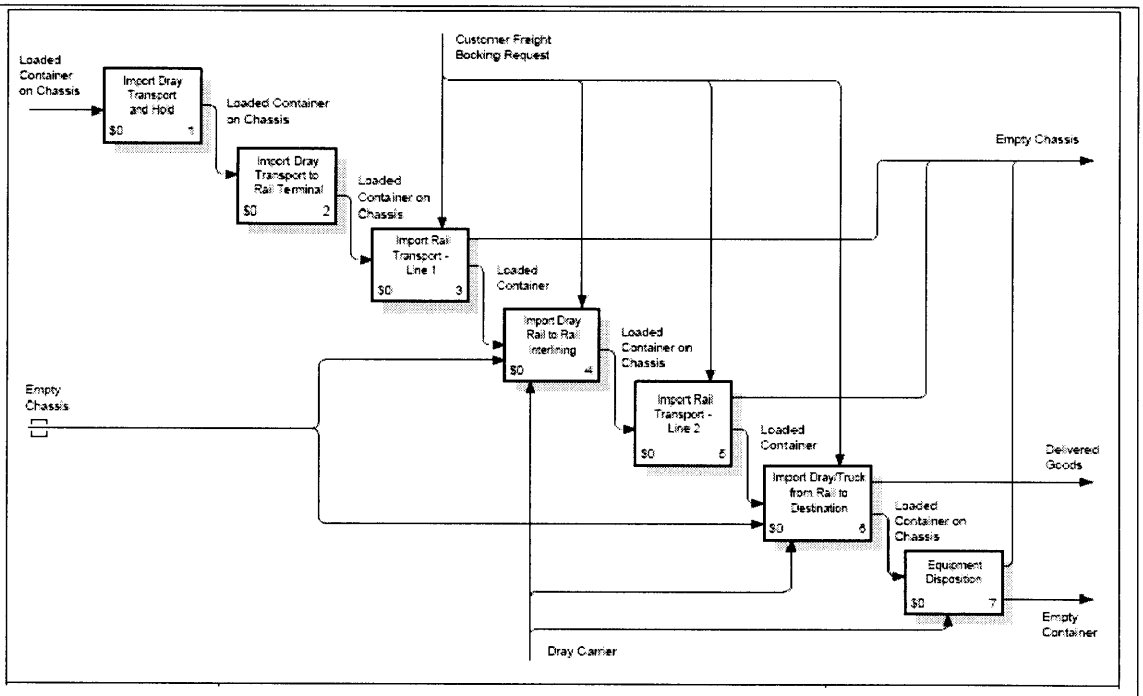



**Figure 14. Intermodal import custody and information flows**
*(Intermodal Process 2006)*

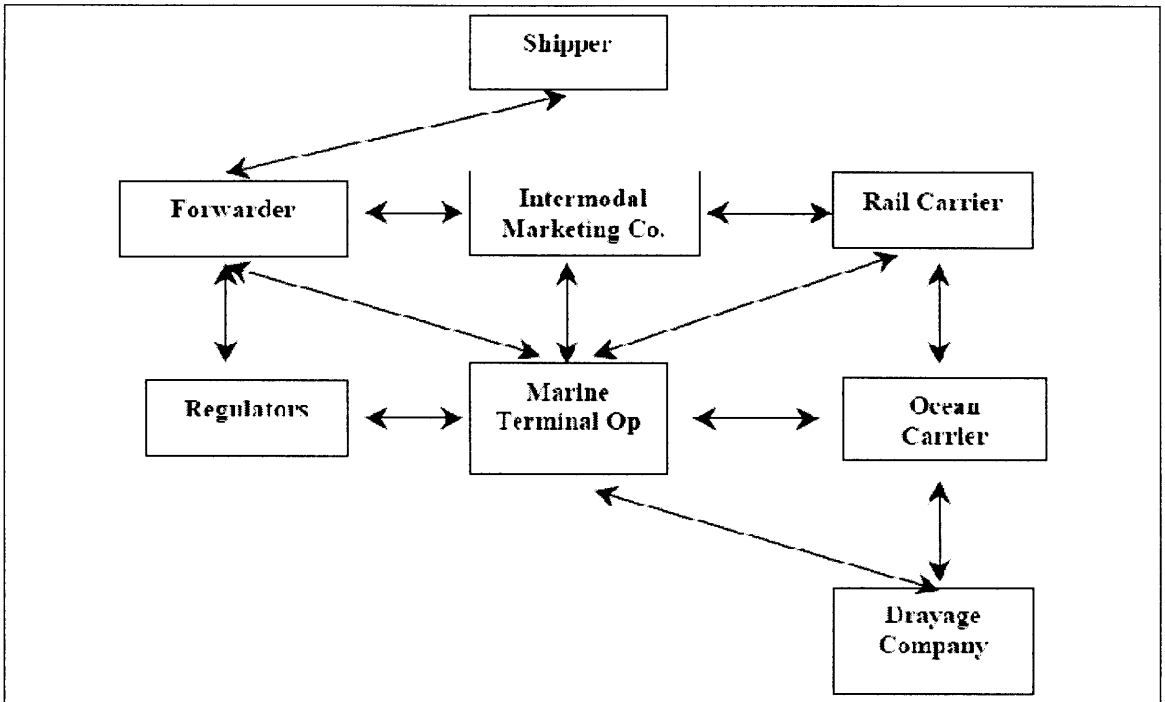



**Figure 15. Stakeholder interaction of export process in the US**
*(Petrakakos 2005)*

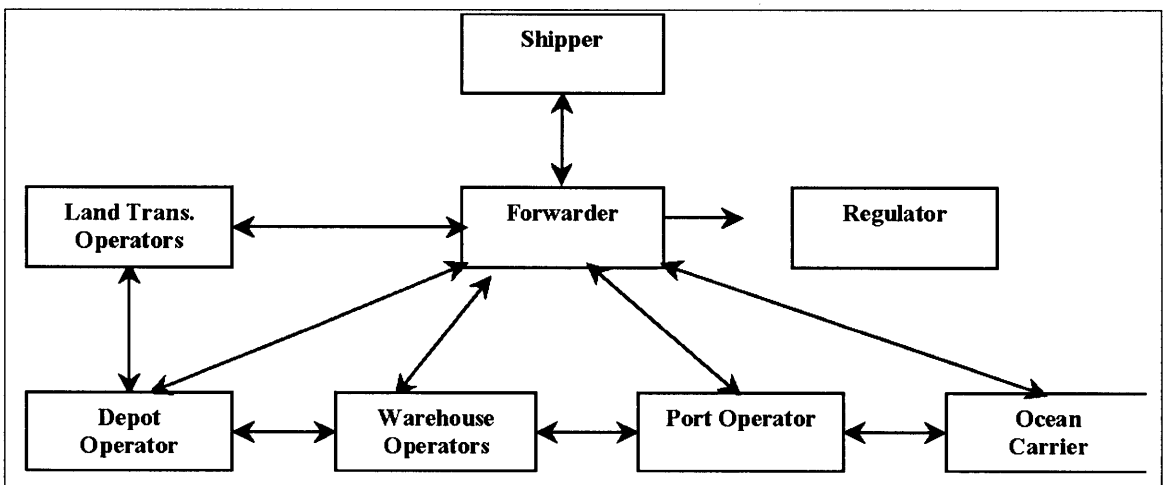



**Figure 16. Stakeholder interaction of export process in Singapore**
*(Petrakakos 2005)*

### 4.1.1 Custodial transfer declaration and customs manifesting

A declaration of transfer is, or at least should, be made every time a container changes custody. This often occurs at intermodal checkpoints like a railyard, warehouse, or seaport. At the very least, a declaration should be known by the sending carrier, the receiving carrier, and, if applicable, the port in which it is occurring. The carriers then have the ability to provide supply chain visibility by

updating the shipper and other key parties when the transfer has occurred, including relevant government agencies at border crossings.

ICCs can act as electronic "license plates" for containers to computerize these declaration processes that have remained manual and labor intensive in many places. (Wamba and Lefebvre 2006) explains that RFID replaces human-to-human with process-to-process or machine-to-machine interactions. This could reduce cargo dwell time, labor costs, and both deliberate and accidental human mis-recording of container movements. This may create resistance from labor, however, as discussed in *5.6 LABOR*.

Once the containers themselves are more automated, (Panagopoulos 2007) suggests that RFID tags can create an Electronic Manifest, which could conceivably be used by US CBP to help verify the import or export of every container. (Ashton 2006) builds on the concept more aggressively by claiming that RFID provides "irrevocable proof that a transaction has taken place. Imagine using RFID to prove beyond any doubt that something was shipped or received." Although "irrevocable proof" assumes that tampering is prevented, weight is given to this argument by the Smart and Secure Tradelanes (SST) program (see *3.5.3 Smart and Secure Trade Lanes*). In one instance, the SST system registered a container arrival automatically that the manifest submittal (submitted by Electric Data Interchange, or EDI) to customs indicated would not arrive for another two days (Smart 2003). In this case, the ICC provided oversight that identified a discrepancy.

Additionally, ICCs might record and maintain different clearances that the container receives throughout transport, for instance from a CBP party or weigh station. The ICC can then verify this clearance during the remainder of the voyage and potentially reduce further container inspections.

Some discord exists within the industry as to what technology should be used and what capabilities they should provide. (Panagopoulos 2007) suggests using Active (versus Passive) RFID tags, since only they "have adequate data storage and include searchable data capabilities, which are essential to record an electronic manifest, such as customs inspection." However, many sources concerned with security argue that container tags should strictly be readable (rather than writeable) to prevent tampering. Further, for security and simplicity purposes, containers and their tags should keep the absolute minimum of information onboard with them. (In-Transit 2003) emphasizes that cargo contents should not be maintained with the container since:

1. Information on the tag is only as good as the party filling it out
2. Theft could increase if contents are known
3. The carrier and US CBP already have the shipper's cargo description anyway.

### 4.1.2 Container and cargo tracking

The status of container tracking varies depending on whom one asks. (In-Transit 2003) supports the claim that a container's location can be found through the custodian: if the container is on the vessel, the carrier can provide the vessel's position, as well as the container location on the vessel. Similar information can be made available by the port, train, and truck carriers with GPS. (Sheffi, SCM Under 2001) suggests a very different view, that some logistics managers describe their logistics system as "black hole," in that shipments disappear to the carrier until they are delivered.

Both statements are probably true for certain supply chains, or even different parts of a given supply chain. Tracking, where currently available, typically utilizes information obtained at the custodial transfer locations discussed above. Large integrated ocean carriers or 3PLs with massive logistics systems may be able to offer this information through their website, conversely a small foreign road carrier may know very little if anything about the container except for his/her portion of the trip.

Clearly, there is currently no universally accepted system or practice to track containers, which may be a missed opportunity. (Wamba and Lefebvre 2006) claims, "product tracking... can lead to a tremendous reduction in inventory levels and better collaboration among supply chain players." (The Electronics 2006) adds that "information transfer ... is an area where improvements in speed, accuracy, and visibility could result in large rewards." At the very least, with little change to the existing supply chain operation, ICCs may be able to improve tracking in one (or both) of two ways:

1. automate the current process by replacing existing manual systems at custodial transfer points to track containers
2. provide realtime or near-realtime tracking information throughout entire container voyage

Tracking can be conducted in a number of ways. GPS appears to be most common, though a network of local sensors is also possible. In addition, an accelerometer and gyroscope combination has been proposed to estimate location in between updates (Quick and Tubb 2006).

#### 4.1.2.1 Adapt to improved tracking

As with any ICC, the supply chain must adapt to fully harness the capabilities that one focused on tracking may provide. The ability to accurately locate cargo through a single portal may cause a paradigm shift in the management of containers and their cargo for both carriers and shippers. Therefore, some pertinent questions should be answered before implementing an ICC that can provide tracking benefits:

1. How are information flows currently incorporated into decision making? (Srinagesh 2005)
2. How does one determine which information is useful? Is it worth gathering? (Srinagesh 2005) To whom is it useful? With what regularity is it needed (realtime, near-realtime, only at custodial transfers)?
3. How much money can be invested in collecting the information? (Srinagesh 2005)
4. How should the supply chain structure and operating policies be changed to make the best use of the information? (Srinagesh 2005)

#### 4.1.2.2 Improve supply chain information prevalence and quality

Perhaps the most likely and basic benefit to implementing ICCs is to improve information prevalence and quality.

Information prevalence is improved since the container itself can actively alert supply chain managers of its position or any other relevant data rather than those managers trying to follow cargo just to learn of its whereabouts. Information quality is also improved since information in current tracking systems can be prone to human error or inconsistency, as discussed in section *4.1.1 Custodial transfer declaration and customs manifesting*.

This notion was supported by managers from both Kroger and Albertsons grocery chain stores. "Once accurate information is available, companies can move from focusing on functional requirements to supply chain solutions, increasing the visibility of the supply chain and allowing for greater control and efficiencies. (Prater and Frazier 2005)"

#### 4.1.2.3 Cargo-centric approach

Even in the best case tracking scenario today, cargo tracking is focused around the carriers and custodial transfer ports in the supply chain, leaving shippers and 3PLs in the position of having to inquire about their cargo through multiple parties. Conversely, ICCs may make the container the center of focus. This could be the basis to an open platform into which various parties in the supply chain may read and write data entries about a given container movement. Ultimately, a paradigm shift could occur from the existing reactive, custodian-centric approach, to a proactive, cargo-centric approach.

The benefit of improving communication between parties, or "joining the silos," should not be understated. Current standards are quite fragmented, and few common processes or means of communication exist among the various parties, "from the ports and airports to the shipping companies to the corporations shipping goods to the customs and immigration bodies and port authorities ... even within China, there isn't one custom clearance standard. We have to do one EDI for Shanghai, and different EDI formats for Qingdao (Global 2006)." ICCs may help to

coordinate these parties, as (Wamba and Lefebvre 2006) found that RFID with Electronic Product Code enhances the information exchanged by different parties in a supply chain, and in turn allows greater integration of all firms involved.

#### 4.1.2.4 Supply chain resilience

Increased visibility and information presents the possibility of improving supply chain resilience (Sheffi, SCM Under 2001) since quality information is available and updated at the desired interval. Note that this is one area in which it must be stressed that while ICCs may prove to be an essential component of an effective supply chain upgrade, they must be accompanied by effective management and supporting tools to make any significant impact.

Supply chain disruptions can arise from a number of sources:

- Internal disruptions
    - Mechanical failure of a custodian's equipment
    - Documentation error
    - Cargo lost to quality failure (see section *4.1.5 Quality control*)
    - Desire to change destination
    - Financial distress (Pickett 2003)
    - Infrastructure error (both IT and non-IT) (Pickett 2003)
- External disruptions
    - Port strike [consider the 2002 US west coast ILWU incident, during which a 10-day lockout cost an estimated $10-20 billion (Rice and Spayd 2005)]
    - Terrorist attack/response to terrorist attack [9/11, for example, caused five US Ford plants to shut down (Rice and Spayd 2005)]
    - Extreme weather (earthquakes, floods, fires, etc.) (Pickett 2003)
    - Supply or demand disruption

(Pickett 2003) investigated many supply chain disruption case studies and developed from them ten recommendations to improve supply chain resilience. Those that it is believed ICCs might support are underlined:

- Build a Resilient Culture!
- Expect to Fail
- <u>De-centralize risk:</u> risk can be mitigated by geographically distributing operations, despite inefficiencies that naturally result; under both normal and especially distressed operations, supply chain visibility is key to managing multiple sourcing locations
- Understand the Risks Inherent to Sole-Sourcing
- <u>Know your Supply Chain:</u> knowledge of typical cargo conditions, flows, and vulnerabilities throughout one's supply chain is important for a number of reasons, not least of which is resilience; ICCs can provide supply chain managers with both data that they are seeking and data that may be of surprise (see the Starbucks example: *3.3.2.4.1 Result*).

- Hedge Disruption Risk with Inventory Buffers
- Develop Backup & Recovery Processes for All Data/IT Infrastructure, and practice!
- Implement Enterprise Standards: this suggestion is geared more toward implementing internally-consistent software solutions for all employees of a firm, although, more generally, this supports the importance of process and technology consistency, which a "cargo-centric" supply chain focused around ICCs may provide
- A Flexible Supply Chain is a More Resilient Supply Chain: "Visibility is facilitated [by employees and] supply chain management tools. In [the Company A versus B case, Company A's] ability to quickly detect the supply disruption allowed them to capture all of [C's] alternate production capacity before [B] could, which put them in a much better competitive position (Pickett 2003)." This example again emphasizes the importance of visibility, a potential ICC benefit.
- Insure Wisely

The flexibility discussed above applies not only to external disturbances, but can also apply to more localized ones such as cargo quality failure. Bananas meant for a supermarket that are delayed, for instance, may be diverted to a baby-food company that uses more ripened fruit. Alternatively, a manufacturer can be alerted if his/her shipment of fragile goods is damaged en route to refill the order and minimize delay to retailers (Melcer and Tsadik 2006).

Limitations to flexibility exist, however. (Srinagesh 2005) studied the effectiveness of information flows in the supply chain by creating and running different models. In its two-stage supplier model with a "newsvendor at each stage," the study found one perhaps obvious but critical restriction. The benefit afforded a supply chain by improved information flows increases with supplier capacity, since additional capacity is used to mitigate disruptions. Regardless of information, overly tight capacity may not provide any flexibility, and therefore can provide little benefit. This conclusion further supports the claim that ICCs cannot alone improve flexibility in the supply chain.

#### 4.1.2.5 Supply chain streamlining and asset management

Probably the most attractive end result of improved visibility to shippers and carriers is improving asset utilization and reducing waste. Greater knowledge of where assets are allows managers to make better decisions to manage those assets most effectively.

For instance, (Downey 2006) suggest that ICCs may reduce the number of touches (amount of handling) in the supply chain. It also cites a survey of the top 100 US importers and exporters that revealed that parties expect to save $1150/container from tracking efficiencies such as reduced inventory and stock outs.

Once functioning *properly*, information-centric supply chains are seen to be so effective that (Srinagesh 2005) proposes a study to question whether distribution centers provide any value in these systems at all. Further, once adequate transparency exists in a supply chain, "a company [may] reduce excess inventory [and] take immediate action if a crucial item is delayed," said Debbie Turnbull, program manager for supply chain security at IBM Corporation (Melcer and Tsadik 2006).

Still, not everyone agrees entirely. A study by (Fourth 2001) showed that 3PLs were hesitant to invest in ICCs as a service to their customers since "most [shippers] want to hear about the exceptions only," i.e. when a problem arises. However, it does go on to say that most carriers will probably build on to their existing information systems under competitive pressure to improve visibility to shippers.

In addition to shippers, ICCs also hold promise to benefit carriers, perhaps even more directly. Currently, on average, containers make only 5 full trips per year. With a tracking system, American President Line's William Hamlin guesses that could increase to six, representing a 20% increase in asset utilization (Flynn 2004). This does not appear to be an isolated opinion. (Fourth 2001) found that, "all in all ... information coming from tracking ... systems is necessary for carriers to perform good asset management and to improve service reliability." Finally, Peter Henry of Cognizant has said, "redeployment of containers is what makes RFID attractive to terminals... carriers [also] want redeployment. They don't know where 50% of their containers are at any time (Johnson 2005)."

### 4.1.3 High-density container area management for custodian

Container management is not a trivial issue for seaports, railyards, ships or trains. Just as focus has been placed on ICCs to manage containers throughout an entire supply chain, ICCs also hold promise to help manage containers in high-density areas. Probably the most significant container management effort is experienced in seaports, however, and therefore it is the main focus of most programs (see *3.4.2.5 WhereNet*).

Managing port container inventories in ports is not only difficult, but also suffers from underutilization of existing information in some places. For instance, as containers are loaded aboard a ship, it is usually known which are to end up on rail and which on truck once they reach the destination port. However, that information is not currently being used effectively, which results in more picks (or touches, the number of times a container is handled) (Fourth 2001). Therefore, making the shift to a more automated process could involve ICCs that would instruct port managers where each container needs to go as it is taken off the vessel.

(Botti 2004) investigated port container management from an IT standpoint, and sees port management broken into many categories, though suggests four primary ones:

- Marine Side Interface: the loading and unloading of containers. Normally two or three gantry cranes are used per ship
- Transfer System: transfer of containers between the apron and the container storage yard. Yard trucks perform transports within the terminal. Transtainers are used to pick up or to put down a container on the storage area of the yard (see Figure 17)
- Container Storage System: allocation and control of containers in the yard (see Figure 18)
- Land Side Interface: interactions with the land transportation modes.

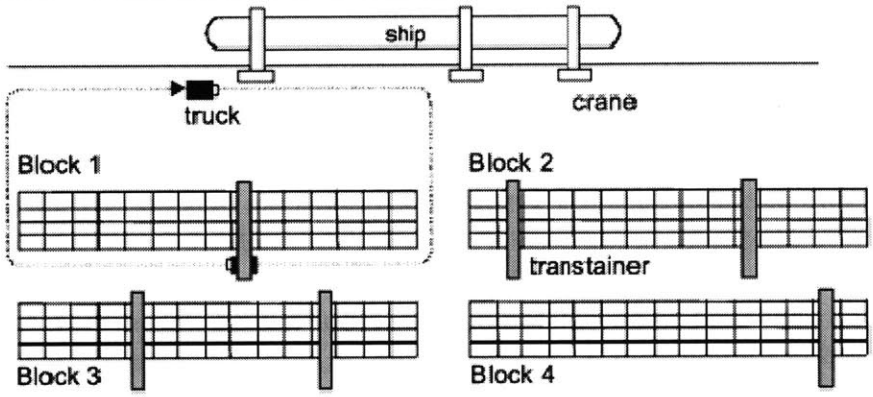



**Figure 17. Simple diagram of typical container port: truck route**
*(Botti 2004)*

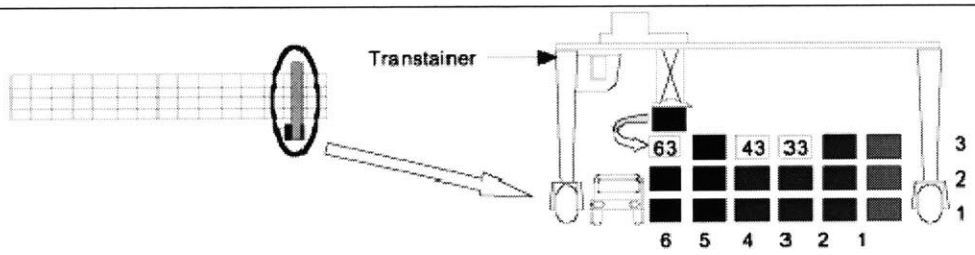



**Figure 18. Simple diagram of typical container port: transtainer**
*(Botti 2004)*

(Botti 2004) also provides some insight as to the different parties involved with the transfer process, which further stresses the need for a container-centric architecture accessible by all parties:

- Ship parties determine the ships' loading/unloading sequence
- Stevedore parties manage the ships' loading/unloading process
- Service parties distribute the containers in the port terminal
- Transtainer parties optimize the use of their machines
- Gate parties interact with the land transport (I/O of containers by land)

To expand their ability in high-density container areas, ICCs also have the potential to include a multi-hop capability, where an alert from one container can

"hop" through other containers to communicate with the custodian. This is important given the technology limitations of most ICC signals to penetrate multiple containers. The custodian, then, can either find a single container or list all containers present in a stack, which might help not only port managers, ship crews, train operators, and railyard managers, but also US CBP to quickly scan a container inventory to find potential problem containers.

Inter-container communication in high-density areas also has the potential for containers to communicate with one another should the proximity of two containers present a danger. This is discussed in *4.2.3 Safety*.

### 4.1.4 Dray-specific applications

The dray (or road carrier) industry consists of a wide array of operators that range in their adoption of technology from extremely automated to relying on approximation and strict voice communications to meet customer's tracking needs (Intermodal Freight 2005). Nevertheless, many truck carriers implemented near realtime truck location tracking in the 1990s with two-way digital communications and found it to be a "huge money-maker (The Freight 2005)." Some existing applications of "intelligent truck" technology, as suggested by (GPSInsight.com 2006), are:

- Cargo location tracking (typically through tracking the tractor)
- Driver performance
    - Location, speed
    - Driving habits, hours, and stopped time
    - Find and verify road congestion
- Conveyance performance (fuel economy, mechanical alerts)
- Asset management (chassis, tractor, trailer, etc.)
- Pay interstate trucking taxes
- Pay tolls

A US CBP report on best practices (Supply Chain Security Best 2006) recommends these systems so that OTR trailers and trucks can be monitored during cross-border shipments by the company headquarters. CBP also suggests a data port through which the driver may transmit messages, which ultimately enhances the company's ability to monitor its inbound shipments.

Since road transportation is also the only major mode that typically carries only one (but up to three) container at a time, some unique opportunities may exist between the tractor and container. Since weight for trucks on the highway is a considerable concern, and can cause significant delay when required to wait for a weigh-in, container weight could be verified and "cleared" on the ICC so that future weigh stations can scan and pass the truck through more quickly, at its discretion. Also, a shipper's ICC might provide verification of road toll and tax charges that they may be assessed by the carrier.

There are several other existing and proposed dray-specific benefits, though most are security related and discussed throughout section *4.2 SECURITY*.

### 4.1.5 Quality control

An often-quoted benefit of ICCs is the ability to better track container conditions that relate to cargo quality. Common applications may include but are not limited to:

- Temperature and humidity (conditions for perishable goods)
- Air quality (spoilage of perishable goods) (Jedermann and Behrens 2006)
- Accelerometer (tilt, shock, vibration for fragile goods)

Statistics of freight losses due to improper handling have been difficult to obtain, likely because the number of quality control issues that could arise are as diverse as the cargo mix itself. Therefore, the need for cargo quality control ICCs will probably be very dependent on the individual supply chain and cargo.

Once implemented, these ICCs hold the potential to detect a cargo quality problem and alert supply chain parties immediately so that early action can be taken, such as replacing that container with a new order. Further, less ambiguity should exist over liability since container custody should be lucid.

Conversely, the current practice for reefers, for example, is to record temperature throughout the voyage on a paper that is collected upon receipt of the shipment. While this may verify that a problem has occurred, it delays reaction and may cloud liability.

## 4.2 SECURITY AND SAFETY

Perhaps more than anything else, security has been a significant motivation for ICC development in recent times. Security is of concern for two primary reasons: cargo theft and smuggling. (van de Voort and O'Brien 2003)

Theft is costly for the entire industry, and varies by mode. Although it is dated, Figure 19 provides statistics regarding cargo theft value by mode, and supports the general notion that most cargo is lost while it is on the road. The numbers in this figure are likely an underestimate since carriers are suspected of absorbing the cost of smaller losses to avoid poor publicity. (Intermodal Cargo 1999)

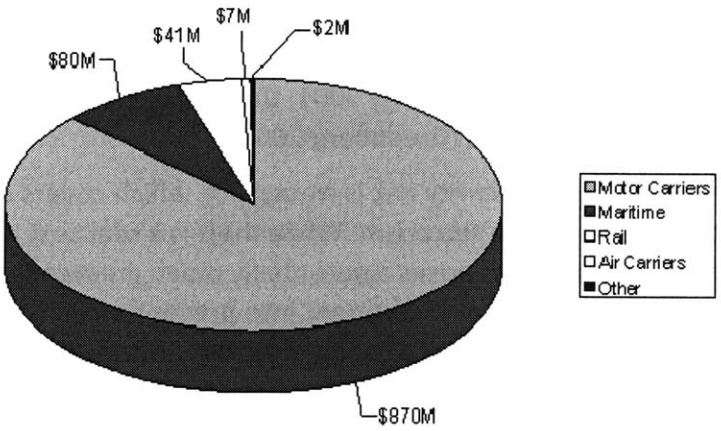
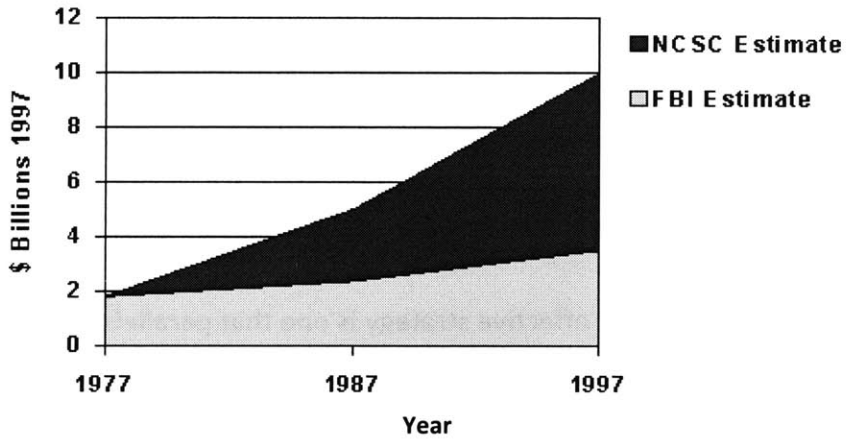



**Figure 19. 1977 data on theft from various sources by value**
*(Intermodal Cargo 1999)*

The total loss value varies by study, depending on what factor is used to estimate unreported claims and some other factors, which results in varying trends of estimated cargo loss, shown in

Figure 20. (Intermodal Cargo 1999)




NCSC: National Cargo Security Council
FBI: US Federal Bureau of Investigation

**Figure 20. Cargo loss estimates between 1977 and 1997 (two sources)**
*(Intermodal Cargo 1999)*

The problem of theft is particularly complicated since it is suspect that container theft is primarily conducted as organized crime. The method by which theft is carried out is found to be rather systematic, and criminals often "act with apparent information about cargo manifests, suggesting that collusion is occurring with transportation employees (Intermodal Cargo 1999)." (Greenberg 2001) supports the claim by suggesting that most thefts are "driver give-ups," where a driver is paid, typically $2-3 thousand to park the vehicle along a road and leave it. Insurance rates have risen to reflect the increased risk. (Greenberg 2001) relays statistics from insurance provider Avalon Risk Management Inc. that showed in the

late 1990's, low target items like shampoo, tires, and books could be insured for $0.15-$0.25 per $100 of cargo value and high-target items like consumer electronics for $0.25-$0.35 per $100 of value. By 2001, these values increased to $0.23-$0.55 and $0.35 to $1, respectively. (Greenberg 2001)

The second main security risk is smuggling, which covers countless items, but of greatest concern today is terrorism. While theft is a real cost borne by supply chain participants, terrorism poses a potentially much greater societal cost, and therefore draws a premium of investment into prevention. While it is usually impossible to put a definitive price tag on a terrorist event, either past or expected, some estimates provide insight: 9/11 was estimated to have cost society between $50 and $100 billion, while a 10-kiloton nuclear weapon detonated in the Port of Long Beach is expected to cost in excess of $1 trillion (Meade and Molander 2006). Therefore, while only some parties in the supply chain bear direct responsibility for securing the cargo, security issues concern all. Among those directly affected is labor, which, through the ILWU, has stated that "the smuggling of weapons of mass destruction in containers through our ports is [our] worst nightmare (What Regulations 2003)." In response, they have put forward a proposal to inspect empty container ("empties") seals since they see empties as the most vulnerable threat (What Regulations 2003). Clearly, the stakes are high for everyone to secure cargo.

Container security can be broken into several general responsibilities: stuffing and sealing, for which the shipper is typically responsible (In-Transit 2003), in-transit security, which the carriers must provide (In-Transit 2003), and oversight, which is provided by regulators and port authorities. (Flynn 2004) supports this list, though in place of oversight, suggests more specifically a "quick and effective scanning system in port."

Probably the most effective strategy is one that parallels a recurring theme in this study, that there is no single "silver bullet" approach to solve the problem. Instead, security must be layered, with many different opportunities to foil a criminal, none of which must be 100% effective (Flynn 2004). This layered approach recognizes that different security measures with different capabilities and varying success rates can collectively provide adequate security. Consider that four levels of security that each provide a 33% chance of finding a weapon collectively provide an 81% chance. However, there *are* real-world limitations to this collective probability theory that alter success rates, notably false positives (Haveman and Shatz 2006) and the reality that failures of each security approach are not necessarily independent, therefore the same failure may exist across all approaches. Nevertheless, layered security is the approach accepted by most, and (Haveman and Shatz 2006) claims that proper implementation calls for new measures in:

- intelligence
- the early provision of more and better information and documentation about container contents

- activating shippers, all the way up and down the chain, to greater procedural uniformity, fastidiousness, and vigilance
- greater control and background screening of those having access to containers and ports
- developing and installing new inspection and tracking technologies

Based on this list, ICCs alone do not appear to be a total solution to security, but certainly could accompany others. In (The Freight 2005), US DOT focuses on five high-level technology categories it sees as essential to enhance security, and ICCs hold the potential to aid some of them:

1. Asset tracking: Various technologies to track trucks, containers, and cargo
2. On-board status monitoring: Monitor both vehicle and cargo conditions, and detect tampering or intrusion.
3. Gateway facilitation: Non-intrusive inspection technologies like scanners and RFID tags to be used at terminals, inspection stations, and border crossings to search for contraband.
4. Freight status information: Web-based technologies to facilitate information exchange on freight shipments and improve data flows.
5. Network status information: Cameras, road-sensors, and display technologies monitor congestion, weather conditions, and incidents.

## 4.2.1 Container integrity

The protection of a container can be both active and passive. Seals, be they manual or electronic, are an active protection to try to prevent unauthorized container breaches, while detection sensors provide a passive solution intended to both deter breaches and alert appropriate parties to respond.

### 4.2.1.1 Seals (container doors)

Container seals are intended to deter thieves and terrorists from breaking into a container, and alert custodians or shippers that a breach has occurred.

#### *4.2.1.1.1 Manual seal*

Manual seals are already used on many containers, and come in a variety of types. Some are merely plastic tags that provide no physical protection but do indicate that the doors have been opened, while others physically slow or deter a break in entirely.

The carriers support seals and enforcement of them. They have suggested that the US government should set a date by which seals should be in place (In-Transit 2003). This notion is supported by (Haveman and Shatz 2006): "tamperproof locks and location trackers [come] first on every list," since they are cheaper than sensors (see *4.2.1.2 Detection sensors (container sides and interior)*), are already proven, and have commercial benefits (see *4.1.2 Container and cargo tracking*). This

combination of seal and tracker should indicate whether the container has been opened and where. (Haveman and Shatz 2006)

There is dissent, however. Some argue that regardless of the seal, the container's integrity simply cannot be assured. This is in part because a seal only ensures that a door opening is known, yet does not protect the other five sides of the container. The goal of a criminal is to enter the container without attracting attention, and try not to break the seal in doing so. There are several ways to do this, and it is believed that an experienced thief can break in under 20 minutes, since the quality of a door seal does not affect the possibility of working around it, merely the time that it takes to do so. Finally, to complicate the problem, containers are not as standardized as they may seem, which contributes to a lack of sealing standards (van de Voort and O'Brien 2003).

#### *4.2.1.1.2 Electronic seal (E-seal)*

E-seals have probably received the most attention among ICCs. While at the minimum they describe a container seal that has some electronic alert capability to notify the custodian or shipper about a door opening, they have also been described more generally, to include tracking capability, container quality sensors, remote locking/unlocking ability, etc. (see *3.1.2.1 Advanced Container Security Device (ACSD/CSD)/SmartBox*).

Some of the attention that e-seals have received has been about standardization, although two standards have resulted. The first standard, which establishes both the technology (RFID) and two frequency bands within which to operate (RFID gets 2006), came from ISO: "ISO 18185-4:2007 specifies requirements for the data protection, device authentication and conformance capabilities of electronic seals for communication to and from a seal and its associated reader (ISO 2007)." A second set of standards is being developed by the International Container Security Organization, although this organization has been questioned by some (see *3.4.2.2.2 Industry support program (International Container Security Organization [ICSO])*).

US CBP is a strong supporter of its "Smart Box" initiative, claiming that it can improve a company's ability to detect whether a container has been compromised (Supply Chain Security Best 2006), though much debate still surrounds the subject. While the World Shipping Council, for instance, supports improved risk assessment through cargo data screening over e-seals or something similar (RFID gets 2006), they claim to remain unconvinced that e-seals will provide any additional security over manual seals. "An RFID device that does not impede entry but only records whether one, or perhaps either, container door has been opened [and is] only read by geographically fixed readers... provides questionable additional security benefits, but would add costs of hundreds of millions... per year (Comments 2006)," commented WSC. However, if e-seals are eventually required, WSC maintains some specific suggestions (In-Transit 2003):

- have unique number to be read electronically and visually
- record date when seal was activated
- record date when seal was opened
- if an RFID, operate within a single radio frequency
- read by a universal reader
- perform reliably in all environments with insignificant number of false readings
- meet the ISO high security seal standards
- there is no need to have the container number attached to seal number since both are in the documents
- commercial availability and low cost of units must be met
- no seal will replace scanning

Despite CBP's open support of SmartBox, Christopher Koch of WSC has said that DHS has been hesitant to mandate e-seals because they "would require deploying technology on a global scale... yield little useful security info, and... have not been shown to have significant supply chain management benefits." (RFID gets 2006)

Some also note that, "until we have confidence about what's in the box ... putting a device on the outside ... may not add much to security (Kulisch 2006)." Every door opening may also require a search, and the most common door openings are customs inspectors. These and other false alarms have the potential to stop many containers, which might "be acceptable if it assured nothing bad made it into the country, though this would not be a likely result (Kulisch 2006)." To help avoid these false positives, some suggest adding a write capability to e-seals (Downey 2006), though it has been mentioned elsewhere that a write capability may increase vulnerability. Finally, (Kulisch 2006) argues that an e-seal may give false sense of security.

#### 4.2.1.2 Detection sensors (container sides and interior)

Neither a manual or e-seal would be able to detect container breeches not through the door. Additionally, verification of container contents is not a trivial issue. To address these potential shortcomings, sensors to detect container integrity and cargo contents have also been proposed.

##### *4.2.1.2.1 Detect unauthorized container breach*

While much effort has been dedicated to securing container doors using a seal, the possibility of breaching the container in another spot, though perhaps more difficult, is possible (Kulisch 2006). This may provide motivation for ICCs that aim to detect any container breach. DHS's Advanced Container Security Device program (see *3.1.2.1 Advanced Container Security Device (ACSD/CSD)/SmartBox*), for instance, calls for detecting "six-wall intrusion" and dangerous materials (Downey 2006).

A number of sensor types have been or may be considered to detect container breaches, including light or infrared to detect movement, humidity to detect a person, and even advanced composite wall materials to directly detect a compromise of the container itself. These systems are currently very costly, and are therefore limited to high-value goods (van de Voort and O'Brien 2003).

#### *4.2.1.2.2 Verify container contents*

One of the most significant "layers" of security is ensuring that the contents of a container are legitimate, which includes being safe, legal, and matching what is stated in the container's manifest. Most agree on the importance of this. Shippers and carriers "[understand and accept that] preventing and detecting ... unlawful nuclear or radiological material is the #1 container security priority... the industry fully supports... piloting and examination of ... radiation and non-intrusive cargo density screening of all containers (Comments 2006)." Further, it is quite reasonable to believe that container manifest data describing cargo contents and source can often be "incomplete, misleading, or outright falsified (Wamba and Lefebvre 2006)."

Despite accord over the importance of this security layer, two primary debates exist over proper execution:

- What should be sensed?
- Where to implement the technology? Should sensors be installed in the container itself (an ICC solution) or as a fixed scanning unit in the port?

Many possibilities exist as to "what" should be sensed that would enhance security. While ensuring that a heat-sensitive cargo is not lost to heat damage may clearly call for a temperature sensor, ensuring that a container does not contain "any dangerous materials" is not quite as straight forward. Common technologies include x-ray pictures; radiation, biological, explosive, and chemical detection; and temperature, humidity, motion, light sensors (Haveman and Shatz 2006). Implementation can be quite creative, too. For instance, an X-ray picture may be taken both at the stuffing location as well as the importing location and then the pictures compared to ensure that the contents have not been altered (Flynn 2004).

The second question of where to implement the technology, either in fixed locations or as an ICC, tends to receive more attention. However, this is not independent of the first question since not all ICC type sensors would work as fixed sensors and vice versa.

(Haveman and Shatz 2006) provides support for in-container sensors, claiming that "they should be obligatory in all containers entering US ports from abroad." They also are included in many container security proposals, including US CBP initiatives.

The WSC, however, has taken an opposing viewpoint. While they support scanning technology "deployed by government inspectors at ports," they do not

believe that sensors should be applied to world's container fleet. Some reasons stated by the group are (In-Transit 2003):

- approximately eleven million containers around the world (versus much smaller number of ports)
- containers pass through numerous parties who can tamper with or disable the detector or sensor
- unclear what is to be sensed, as the list is endless (as mentioned above)
- the operational reliability of sensors is still unknown
- work is already underway on sensors and detectors for nuclear, radiological, drugs and other substances that can be more effectively and efficiently deployed via inspection of the container at the port
- the next step should be years, not decades away
- even if such sensors could be applied to containers, there are types of containers on which they would be completely ineffective, such as open tops and flat racks. Port based sensors and non-intrusive inspection equipment is the only way to effectively address security concerns about these kinds of shipments
- outfitting millions of containers with one or more electronic devices would raise very substantial information system issues

Additionally, an interesting business case can be made for in-port scanners that might not be valid for any in-container counterpart. X-ray scanners have been shown to generate additional taxes from contraband to the point "that they can be regarded as a profitable investment instead of a costly expenditure (van de Voort and O'Brien 2003)."

Nevertheless, not all fixed sensors have proven overwhelming successes. In Hong Kong, radiation sensors created, "a PR boost, but did not even try to address the difficult, real world operational issues that, it is hoped, the next round of pilots will address (RFID gets 2006)."

An interesting compromise has been suggested by (Guo and Fano 2005), that just "a small percentage of 'smart' containers can provide incremental levels of security even for their 'dumb' container counterparts." Essentially, the containers with sensors should sense any dangerous material both inside itself and in its vicinity. Given the frequent close proximity of high numbers of containers typical in logistics processes, it is argued that these few containers could be sufficient to protect the entire system.

### 4.2.2 Container and cargo tagging and tracking

ICCs that provide tagging and location tracking were discussed earlier with regard to the commercial supply chain benefits that they provide. However, there are also potential benefits to security. Several notable security benefits exist for container tagging and tracking:

- Geo-fencing: (preventative) ensure that container adheres to a pre-specified route during trip to detect theft
- Proximity to custodian: (preventative) ensure that the container remains in carrier's custody throughout trip (requires communication with custodian's equipment)
- Locate container: (reactive) find a container of interest quickly while underway (for law enforcement, first responders, etc.)

Currently, tracking containers is "not sufficiently transparent, i.e., the information about what is being transported, by whom, and from where is not easy to check (van de Voort and O'Brien 2003)." Tracking is, therefore, generally considered overly difficult. Information flows accompanying container are also not considered helpful, especially since "the real origin of a container can be hidden ... with the help of corrupt officials at intermediate ports (van de Voort and O'Brien 2003)."

CBP has been a proponent of container tracking improvements. Their best practices suggests that companies track the status of shipments worldwide. In addition to commercial benefits, the system may reveal "unusual delays or anomalies that may point to illegal activity (Supply Chain Security Best 2006)." If satellite tracking is or cannot be used, CBP alternatively recommends using regular checkpoints to update the container's location. (Supply Chain Security Best 2006)

The Smart and Secure Tradelanes program provided a proof-of-concept of the greater capabilities that tracking provides to identify both dwell time, since cargo at rest is at risk; and routing variability, which complicates reporting and planning (Smart 2003). (van de Voort and O'Brien 2003) has claimed that systems combining door-opening notification (such as those provided by an e-seal) with geo fencing have so far shown that theft becomes virtually non-existent, and local authorities are able to quickly respond to any remaining incident.

Still, there is much skepticism. Christopher Koch of the WSC has been critical of companies that "attempt to create a market for RFID... by convincing the US government they are an imperative security tool." Koch argues that technology would provide "marginal, if any, security protection," and does not answer key question: what is in the container? (RFID gets 2006) Additionally, concerns about geofencing exist. (In-Transit 2003) has noted that many false alarms may occur as routes are altered by the carrier, which introduces another question "what constitutes being 'off route?'"

### 4.2.3 Safety

Containers come in a variety of types and can therefore handle a variety of dangerous legitimate substances, from toxic to explosive. Though ICCs have the potential to monitor cargo and alert custodians of potential dangers, there does not appear to be very much literature dedicated to safety applications of ICCs, likely because regulation has focused mostly on the security area in recent years.

Nonetheless, possible ICC applications for enhancing the safety of containers include:

- List unsafe contents and Material Safety Data Sheets (MSDSs) both physically and electronically
- Incompatible cargoes (those that could be dangerous if mixed; tanker ships, for example, do not place incompatible cargoes adjacent to one another without a cofferdam in between)
    - Inter-container communication may warn of adjacent placement of containers with incompatible cargoes
    - Maintain tank cargo history to prevent incompatible cargoes from being used in the same tank sequentially
    - Detect spills that could lead to environmental pollution
- Container conditions
    - Toxicity sensor in containers holding substances that could leak
    - Temperature, humidity, or other environmental condition sensors that alert custodian of potential cargo danger
- Emergency response (The Freight 2005)
    - Emergency responders can be notified immediately with incident location [there is currently no unified system for communication with and among first responders (Canada 2005)]
    - Emergency call button for truck driver (The Freight 2005)

Many of these benefits have the potential to improve container safety to the benefit of all supply chain parties as well as the environment (Barletta 2006).

# 5. ICC IMPLEMENTATION ISSUES

Implementation issues can vary based on many factors, such as the technology selected, application(s) intended, funding source, project lead, relevant regulation in place, etc.

## 5.1 ICCS AS A SUPPLY CHAIN COMPONENT

Supply chain strategies vary greatly depending on the corporate strategies of the parties involved, and the contributions of the ICC should reflect that. It is critical to recognize that no ICC is likely to be a panacea. Instead, the ICC should become an integral part of a broader system in place to address the various needs of the supply chain.

ICCs are not likely to make a container secure, for instance, until the data that they provide can be securely transmitted to the correct party and elicit an appropriate response. ICCs are therefore a supplemental deterrent to a potential terrorist or thief, not a total solution. They should accompany complementary measures to provide a layered approach to security, since ultimately no container is impenetrable, and it is unlikely that any sensor technology will be immune from tampering. Similar arguments can be made for ICC benefits to tracking, safety, quality control, and any other proposed benefit of an ICC.

One illustration of an ICC failing to integrate into the broader supply chain is the shortcomings of RFID tracking in grocery retail. (Prater and Frazier 2005) states, "one of the reasons for ARP (Automatic Replenishment Program, a grocer supply chain strategy to reduce inventory) failures is the desire of grocers to continue with forward buying practices. Research needs to be conducted to see how the use of RFID can be integrated with forward buying if inventories are being managed by the [distribution center]."

## 5.2 ICC MARKETING

Different parties are interested in ICCs for different reasons. Security, for instance, is a concern for regulators who wish to secure borders, carriers that must comply with regulations, and shippers worried about both theft and public image (a terrorist attack carried out by the failure of a "big-box retailer" to secure its containers could severely tarnish its image). Tracking is of interest to these same parties, but for different reasons. Regulators can use tracking to find a container en route that poses a threat, carriers may wish to offer a higher level of service to their clients, shippers might better manage their supply chains, and container owners can manage their equipment fleet.

These examples illustrate that while few people are interested in every service an ICC may offer (except perhaps the provider of that technology), many are interested in at least a few. Further, with shared benefits comes the possibility of

shared responsibility, whereby each beneficiary of a particular ICC can participate in its funding.

IBM's Stefan Reidy, leader of the IBM Intelligent Trade Lane program, realized this when he stated, "at the beginning, we started by focusing on security, because that is what governments wanted. But we realized that private parties will invest and only invest if they have an ROI and the return comes from the visibility of the supply chain. (IBM, Maersk to equip 2005)" Carriers have emphasized the need to clearly state ICC benefits by differentiating between security and supply-chain goals (Downey 2006).

(van de Voort and O'Brien 2003) supports these claims with the example that if theft is not a problem for a particular shipper or forwarder, he/she is not likely to invest in a theft-prevention ICC. (Petrakakos 2005) discusses the efforts of various ports, though mostly the Port of NY/NJ, to implement systems intended to reduce congestion and improve data exchange. The report claimed that most systems failed in part because they did not satisfy user needs to improve supply chain management, but instead focused heavily on security. Further, they failed to provide confidence that proprietary information would be protected. Ultimately, for any technology implementation to be successful, all interested parties must have an incentive to participate.

(The Freight 2005) conducted surveys to get a sense of what benefits are important to different parties in the supply chain in four areas: efficiency, service, compliance, and "others." While the source stresses that the surveys were unscientific, certain trends were noted:

- Shippers gave equal weight to efficiency and service, rating them twice as important as compliance
- Truck carriers weighted the choices relatively equally, with improving service first
- Marine carriers and terminal operators strongly favored efficiency over service and compliance, which was a close third
- Rail industry respondent put safety and compliance far ahead of efficiency and service

As ICCs develop, their providers must both compete with one another as well as defend this generally young industry. As with any product, the benefits of a product are typically the main focus of marketing, and there appear to be three primary models being followed to support these efforts, discussed below.

### 5.2.1 Model A: Specific focus with collateral benefits

A model to illustrate ICC benefits that some follow is to emphasize a key ICC benefit, for instance tracking for the benefit of security, and treat all other aspects as "collateral." This marketing approach may entice those interested in that key benefit, with the versatility provided by collateral benefits as an additional selling point. Two prominent examples of this are SAVI Technology and CommerceGuard.

(Rice and Spayd 2005) took this approach to describe investing in supply chain security. Since security was the key in this study, it was divided into specific investment categories, with each benefit shown to have both direct and collateral benefits, many of which could easily be categorized into commercial or safety benefits. (Rice and Spayd 2005)'s categories were:

- Asset visibility and tracking
- Personnel security
- Physical security
- Standards development
- Supplier selection and investment
- Transportation and conveyance security
- Building organizational infrastructure awareness and capabilities
- Collaboration among supply chain parties
- Proactive technology investments
- Total Quality Management (TQM) investments
- Voluntary security compliance

A prominent example of this approach appears to be the ARGO/Brooks project (see *3.4.2.1 ARGO Tracker/EJ Brooks*).

### 5.2.2 Model B: Broad focus

Another prevailing model among the technology-provider community intent on offering a comprehensive product, but also amongst many researchers and academia, has been a more broad approach to introduce container technologies or concepts that "do it all." These technologies equally stress the many benefits that can be offered, and do not focus on any particular benefit. Two prominent examples of this approach (although both started more as a Model A approach) are SAVI (see *3.4.2.3 SAVI Technology*) and CommerceGuard (see *3.4.2.2 CommerceGuard (and related projects)*).

### 5.2.3 Model C: Specific focus

The last main marketing approach for ICC technologies is to focus on a specific or small collection of benefits and not attempt to be "everything to everyone." Most of these technologies are those that are already in use, for instance Sensitech's RyanEZT (see *3.4.2.4 Sensitech (Ryan EZT, TempTale, etc.)*) which is focused mostly on recording reefer temperature, and WhereNet (see *3.4.2.5 WhereNet*) that is used mostly for port container management.

## 5.3 COST ASSESSMENT

This section first presents some common cost estimates provided in the literature, then discusses issues surrounding the assignment of cost.

### 5.3.1 Estimation of cost

Perhaps the most apparent cost of developing an ICC network is the cost of purchasing ICC units themselves. However, in reality there are many, among others:

- Infrastructure
  - ICC unit purchases and installation
  - Software development and installation
  - Reader infrastructure
  - ICC and infrastructure upkeep and replacement
- Education
  - Study of system cost/benefits
  - Train labor to work with system
  - Cooperation with industry and regulators
- Adjustment (growing pains)
  - System failures
  - Premium paid for new technology
  - Risk of lower level of service
- Management
  - Overhead costs to manage ICC units (especially if removable)

These and other costs are all functions of the many factors, though most considerable is probably technology choice. RFID, for instance, (Kulisch 2006) requires "investing in a network of readers to support a tag system [which would be a] major challenge." Conversely, a satellite-based technology may not require nearly as much infrastructure.

Nevertheless, radio-frequency tags and readers appear to be the most common discussed, and some literature has been dedicated to estimating their costs. (Prater and Frazier 2005) cites that the cost of RFID tags dropped from about US $1 per tag in 2000 to between 15 and 20 cents by 2005. When the cost drops to around 5 cents, experts believe that demand will grow rapidly. (Karkkainen and Holmstrom 2002) provides a similar estimate of "between $0.25 and $1.00, depending on production volumes... The price of a reader is... $1,000." (Prater and Frazier 2005) also suggests that Wal-Mart's RFID program could create the "Wal-Mart effect" by putting "downward pressure on the cost of the technology."

E-seals come in several technological forms, though an often-quoted price for a seal that is "smart" is about $25, which is supposed to last for 10 years without needing a recharge (Haveman and Shatz 2006).

(Haveman and Shatz 2006) provides an aggregated cost, suggesting that while cost estimates vary quite a bit, the most common value, including everything needed for the RFID network (locks, RFID tags, sensors, etc), is $500 per container. The amortized cost of an RFID tracking system over an expected container life of ten years, (Flynn 2004) suggests, is $5 per shipment.

Finally, (Panagopoulos 2007) provided some economic analysis of the STAR BEST project. Figure 22 illustrates the trend of expected inventory cost savings per container as a function of the container's value. Figure 22 illustrates the trend of expected cost savings as a function of the percentage of stock outs that result in missed sales.

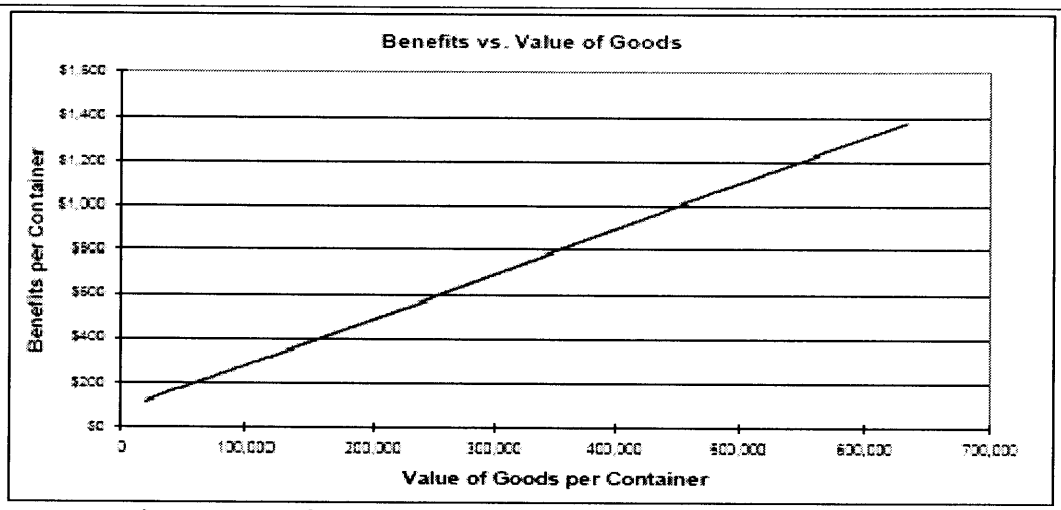



**Figure 21. Benefit per container versus cargo value (STAR BEST project)**
*(Panagopoulos 2007)*

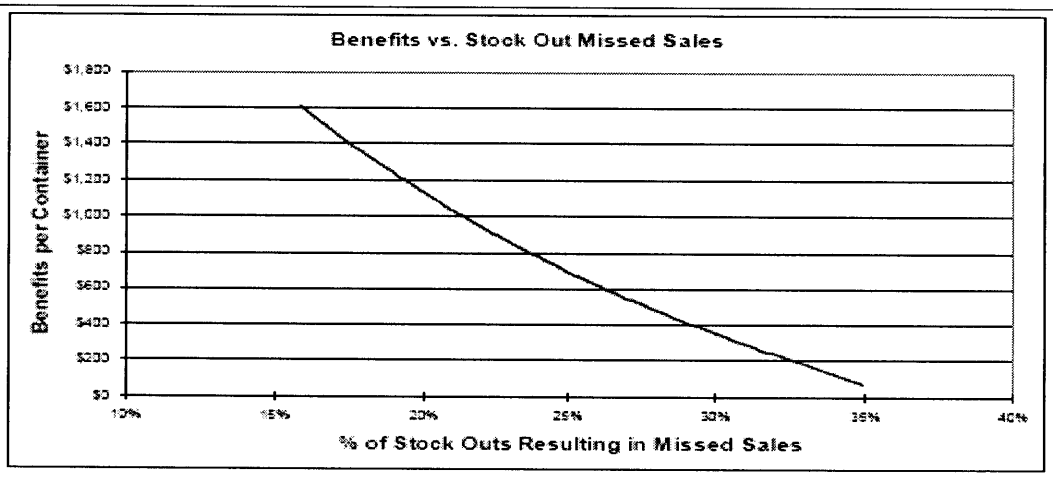



**Figure 22. Sample values for cost and benefit per container (STAR BEST project)**
*(Panagopoulos 2007)*

## 5.3.2 Assignment of cost

Assignment of benefit has been discussed to attempt to determine assignment of cost. These benefits are the most likely places to generate interest enough to spur investment: "[industries] need to examine their organizations' current business practices and identify where enhanced information and visibility from [an ICC] would provide the biggest and fastest returns. Pilot programs would focus on the areas of greatest opportunity (Rutner and Waller 2004)." (Petrakakos

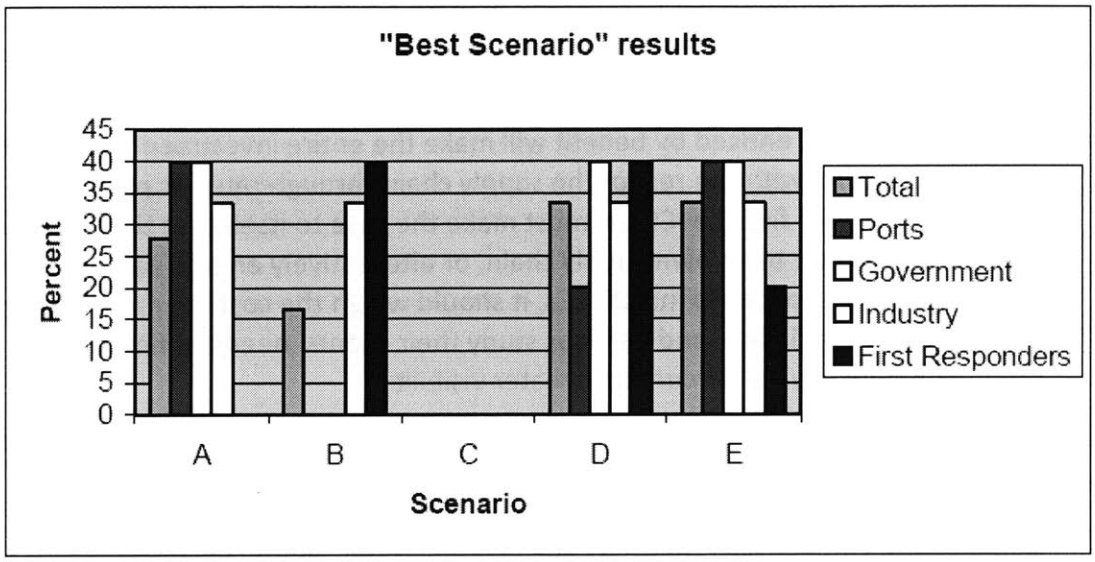
2005) adds the example of eModal, which was much more successful than other similar programs (for instance FIRST) because, "it was more focused on meeting user needs on time and cost benefits rather than satisfying government needs for maritime homeland security."

However, sharing the cost of an ICC installation can be quite complicated since benefits may be tough to quantify, existing equipment ownership may be shared, and costs may arise from different sources as discussed earlier.

The more likely scenario might be that the party either required by regulation or most enticed by benefit will make the entire investment, and then try to share the costs with the rest of the supply chain through rates or premiums. If a shipper chooses to finance ICCs, it must make the case to itself that the benefits will be of enough value to its own supply chain, or alternatively engage partners to share cost. If a carrier chooses to install ICCs, it should weigh the cost over alternatives to meet security regulation, and perhaps study their clients' needs to find which shippers would pay a premium for greater visibility.

Limited funding may be available from the public, most likely in the form of a "security tax" like those assessed to airplane passengers of $20 per person. However, the majority of the measures are likely to place cost primarily on the shippers and carriers (van de Voort and O'Brien 2003). More conservatively, (Canada 2005) concluded that "government is not willing to share costs associated with [ICCs], does not want to be responsible, or create a new agency for monitoring [ICCs]." (Canada 2005) also conducted surveys to understand industry opinion on the implications of ICC funding based on owner, shown in Figure 23. The "First Responders" category is indicative of the report's partial focus on emergency response.

**Scenario A: Container owner owns/operates the intelligent container technology;**
**Scenario B: Government owns/operates the intelligent container technology;**
**Scenario C: Importer owns/operates the intelligent container technology;**
**Scenario D: Third party owns/operates the intelligent container technology;**
**Scenario E: Combination of the above.**




The above table indicates that the majority of surveyed ranked scenarios in the following order:

1. Scenario D and Scenario E "Third party owns/operates the intelligent container technology" and "Combination", i.e. distributed responsibilities between government and industry
2. Scenario A – Container owner owns/operates the intelligent container technology
3. Scenario B – Government owns/operates the intelligent container technology

**Figure 23. Industry surveys comparing ICC ownership preferences**
*(Canada 2005)*

## 5.4STANDARDIZATION

The ICC industry is young and standards are still developing. Standards for ICCs are likely to come in two areas: regulation and technology.

### 5.4.1 Regulation

Most regulatory requirements for the transportation industry are geared toward safety, security, and duties collection. Accordingly, government focus on ICCs has been mostly on container security and to a lesser degree manifest verification. However, most projects are still in the phase of conducting studies on best practices to determine a best way forward.

As a result, despite significant talk and study over security initiatives by government (see *3.1.2 Initiatives*), few ICC (or other) standards have yet been mandated or standardized. "Government has failed to articulate a clear vision ... 'We are willing to invest ... into validating that our partners are secure. However, [the government must] define these requirements. My biggest fear is that we implement

a large project for supplier security in 2005, and the government issues new requirements in 2006.' (Secure 2005)" These concerns over the "standards debate" are voiced by many (Tiemey 2004).

### 5.4.2 Technology

In addition to regulatory standards, industry must develop technology standards for performance, capabilities, and communication. This difficulty is exacerbated by the regulatory standards issues discussed above: without clear definitions and requirements, technology does not have a universal set of goals.

Probably the most work that has been done to standardize technology is the ISO effort to standardize e-seals (see *4.2.1.1.2 Electronic seal (E-seal)*).

In addition, EPCglobal has begun testing its EPCIS system that has the possibility to help integrate container and part tracking to existing EPC systems (see *3.5.1 EPCGlobal's Information Services*).

## 5.5 LIABILITY

Information added to the supply chain presents several new liabilities, perhaps the greatest of which is the protection of proprietary data. While an ICC benefit continuously mentioned is the electronic collection and transmission of data that may introduce vast efficiencies, it also opens the possibility of proprietary data interception. The first aspect of this concern is specific to technology providers that require clients to use their specific network (for instance CommerceGuard), thereby increasing the possibility of a leak. It is instead "better to have [an] open network of competitors amongst which data can flow directly between parties (Kulisch 2006)." The second aspect of this concern is on the physical side, that data stored on the container traveling around the world may be very vulnerable "and hence must be secured (Schaefer 2006)." This refers both to proprietary data leakage as well as tampering to falsify information, which must be prevented and/or detected (Kulisch 2006). These added liabilities were some of the primary concerns that prevented stakeholders from sharing information in one pilot project, FIRST (see *3.1.2.3 Freight Information Real-Time System for Transport (FIRST)*) (Petrakakos 2005).

Another set of liability issues arise from greater data availability: how to respond to alerts. What procedure would be in place should an alert be sent that indicates radiological material is aboard a ship coming to port? Would this require the ship to stop well outside the port to be inspected by US Coast Guard and other officials? Since several legitimate cargoes (like granite) might set off these alarms, can false alerts be verified? Once an intrusion is detected, does the carrier bear responsibility to intercept (In-Transit 2003)? Less grave than terrorism but very important still are cargo quality sensors that may be seen by carriers only as a way for shippers to assess blame, and therefore are quite unattractive. Once these questions are addressed, the threat of false positives could still put a significant operating burden on shippers and carriers.

Needless to say, while ICCs may appear an excellent way to expedite many processes by some, they might also be seen as nothing more than a liability by others.

## 5.6 LABOR

ICCs have the potential to streamline the supply chain by automating many processes that are currently manual. Therefore, it has been seen as a potential threat by labor, which is highly organized in North America through the International Longshore and Warehouse Union (ILWU) and to varying degrees throughout the rest of the world. ILWU officials have said that while they are not opposed to new technology, they would want members retrained and jobs kept on site. Steve Stallone, a union spokesperson, is clear about their position: "The ILWU is a group that takes care of its own. We want to make sure that the jobs that are controlled by and are traditionally the union's, remain union jobs." (Nero 2002) Therefore, any ICC discussions must include labor so as to avoid possible conflicts.

## 5.7 ICC LOGISTICS

If ICCs are to be implemented, a choice must be made whether to make the onboard technology permanent or removable.

If made permanent, the container might demand a premium as would a reefer or any other type of specialized container. Therefore, it should only carry cargo that utilizes the ICC to collect that premium, which may fundamentally change (and limit) the container's logistics. Additionally, ownership of a container is traditionally limited to one party, which may complicate funding if anyone other than the container owner intends to participate in funding the ICC.

If made removable, then flexibility may be gained, but the ICC units will require a separate, "sub" supply chain that needs to be managed separately of both the main cargo supply chain and the existing container supply chain.

## 5.8 PATH TO IMPLEMENTATION

Implementation must address the items already discussed and perhaps more, though some sources have discussed implementation specifically. (The Freight 2005), for instance, presents a detailed list of implementation triggers:

1. Pursuit of competitive advantage: likely to be the main trigger for as market leaders seek to improve their standing and profitability
2. Keeping up with competitors: catalyst for market followers. Success by market leaders progressively erases doubt and skepticism
3. Compliance: either commercial or regulatory. Commercial compliance arises when customers demand innovation. Regulatory compliance is self explanatory.

Additionally, (The Freight 2005) provides several implementation barriers:

- Skepticism about efficacy is the fundamental concern.
- Immature standards can deprive vendors and users of a common and fair template for deployment.
- Concerns about negative operational impacts, such as the need to replace batteries in the field, may mobilize opposition from service providers.
- The credibility of the business case is often the dominant concern, with the strongest skepticism reserved for estimates of benefits.
- Exposure to government actions or inaction adds barriers to some intelligent freight projects that depend on government funding to deploy common infrastructure or affects decisions on which path to take.
- Concerns about the loss of proprietary information may keep some firms from committing to new technologies and networks.

(Jedermann and Behrens 2006) has proposed that ICCs will likely be implemented through three successive generations:

1. Only read measurement at end of transport. This does not comply with JIT.
2. "On the road" access to sensor data.
3. A final generation characterized by:
    a. Autonomous configuration
    b. On-the-road sensor access
    c. Autonomous assessment and decision making

Currently, (Mary and Lee 2005) argues that RFID is mostly in a "replacement" phase, as it is simply replacing barcodes and is "not creating anything new except for that it is easier to use." This is consistent with the first phase above.

Though discussions in this report are all at a fairly high-level, if ICCs arrive, it will be as initiative-by-initiative, which will in turn require many companies to conduct their own assessment comparing various ICC options as well as alternative solutions to meet their specific supply chain needs. If an ICC solution is chosen, it will have to demonstrate that it really can, as Patrick Connaughton of Forrester Research Inc. puts it, "really drive top-line growth." (Katz 2007)

# 6. CONCLUSIONS

The Intelligent Container Concept will inevitably mean different things to different parties. Opinions currently vary widely on proposed benefits, their relevance to the supply chain, and whether they can outweigh costs. As can be expected, technology providers are ambitious about new technologies. Carriers have actively participated as well, and have supported much of the regulation that has been put forward, though they tend to be more conservative (or pragmatic) about new technologies. Shippers have demonstrated different levels of interest in ICCs depending on the size of, nature of, and relevant regulations affecting their respective supply chains. Finally, regulatory bodies have been under scrutiny from everyone, including Congress, the general public, and virtually every affected party in the supply chain to move forward with initiatives, and they have.

A wide variety of benefits have been proposed, though each one has fallen into one of two general categories: Supply Chain Management, a direct commercial benefit; or Security and Safety, typically a required investment that is essentially insurance. These benefits are crucial to determine and evaluate since, despite the hype and elegance of new technology, ICCs will probably only be successful if they provide sufficient value to the supply chain, either directly or as mitigated risk. Since shippers and carriers are likely to bear the brunt of the direct costs, it is especially important to make these benefits clear to them. This is not always done, as Eric Mensing of APL Logistics demonstrates in his assertion that technology vendors are "finding problems for their technologies" rather than the other way around (Moorman 2007).

In fact, there is an incredible diversity of needs among different parties, which should be the primary focus of ICC developers. Truck carriers must manage growing tractor fleets, Starbucks must protect its containers from stowaways, ports must manage ever more containers, grocery retailers must prevent spoilage, Wal-Mart must track and account for ever more SKUs, and Maersk Line must administer over a million containers (Maersk 2007) while providing flexibility to their customers. Many initiatives, particularly those that are already commercially successful, focused on only one or two of these specific needs each. That degree of specialization attests to the fact that, currently, there are no "one size fits all" solutions, and any vendor intending to provide one must make it incredibly adaptable so that the required performance can be achieved without excess "bells and whistles" that would equate to over-engineering.

That all having been said, there certainly is room for innovation that will not only support stated needs, but also create new possibilities never before considered. Without complete supply chain visibility, for instance, most supply chain managers may not have considered inventory pooling with other shippers. Therefore, nor would have the carriers or 3PLs prepared themselves to deal with the excessive re-routings that might result. In another example, some have suggested that ICCs could

allow managers to remove entire portions of the supply chain, namely distribution centers. These changes are fundamental changes to the way in which the system currently operates.

The fragmentation and varying needs within industry make continued and improved collaboration crucial to developing clear baseline goals. Collaboration is needed now in the early phases of research to understand each party's particular issues. It will be needed as trials take place to share best practices. It will eventually be needed to determine ownership of new infrastructure, especially given the ownership arrangements of existing infrastructure, where, for instance, containers, trailers, and other assets are typically owned by either the carriers or an independent party.

Collaboration will also be needed to provide coherent and consistent comment to regulators as standards are developed, which raises the parallel issue of collaboration on the public side. While "the government" may be referred to as a single entity, in reality it is an incredibly diverse set of bodies that support different aspects of the nation's transportation system. For instance, before September 11, "fourteen agencies [had] a role in port security, but not one counted it as its top mission (Peckenpaugh 2002)." This fragmentation has led to many public initiatives that, even when lauded on their own as being effective, have not been put into the context of a clear overall strategy. This lack of strategy has, in turn, been a large hurdle for the private sector to develop its own strategy.

Last, but certainly not least, it is important to reiterate one last time that ICCs should not act in isolation, but instead accompany and support other technologies, methods, and the overall supply chain strategy that it serves. Indeed, many implementation plans described in this study take entire supply chain approaches, often with ICCs contributing to portions of it, but few if any have shown it as a sole solution. Failure to properly integrate ICCs has also already been shown to have prevented past initiatives from succeeding.

Despite all of the hurdles, though, ICCs are in a favorable position. As companies increasingly compete through their supply chains by balancing lean principles with resiliency, a variety of possible solutions, including ICCs, are on the table. Additionally, recent supply chain disruptions of various origins have brought Supply Chain Risk Management (SCRM) to executive-level attention. One report notes that 54% of the 89 executives surveyed said that their companies planned to increase spending on SCRM in the following year. (Reese 2007) Combined with regulation, these commercial factors are likely to spur ever more focus on improved supply chain strategies, of which intelligent container concepts could become a central and critical component.

# WORKS CITED


*Accenture: Freight Tracking datasheet.* 2006. http://www.accenture.com/Global/Services/Accenture_Technology_Labs/R_and_I/FreightTracking.htm (accessed February 19, 2007).

*Altobridge: Global Integrated Maritime Monitoring.* 2006. http://www.altobridge.com/applications%20container%20security.htm (accessed February 25, 2007).

*American Shipper.* "RFID on track to help intermodal." November 2006.

*ARGO Tracker.* 2007. http://www.argotracker.com/ (accessed May 15, 2007).

Ashton, Kevin. "The New Killer App." *RFID Journal*, 2006.

*Automated Cargo-Tracking Transponders.* 2006. http://www.nasatech.com/Briefs/Sept98/NPO19769.html (accessed December 17, 2006).

*Automated Targeting System.* Washington, DC: US Customs and Border Protection, 2006.

Barletta, G L. *Smart Technologies for Enviro Safety (AISRe).* Pisa, Italy: Italian Regional Science Association (AIRSe), 2006.

Beisecker, Randall. "Securing and Facilitating Trade: Conflicting Goals under the World Customs Organization." *Center for Nonproliferation Studies*, 2006.

Belobaba, Peter. *Air Cargo: Industry Overview.* Cambridge, MA: Massachusetts Institute of Technology, 2004.

*Better Strategic Planning Can Help Ensure DOD's Successful Implementation of Passive Radio Frequency Identification.* Washington, DC: GAO Reports, 2005.

Bogdanich, Walt, and Jake Hooker. "From China to Panama, a Trail of Poisoned Medicine." *The New York Times*, May 6, 2007.

Botti, Vincent J. "Multi-Agent System Technology in a Port Container Terminal Automation." *ERCIM News*, January 2004.

Burke, Adrian. "Has Strategic Distribution Made a Difference to the Last Tactical Logistics Mile?" *Logistics Spectrum*, Jul-Sep 2006.

*Canada - United States Cargo Security Project Operation Safe Commerce - Northeast - Intelligent Container Technology Infrastructure and Interoperability "Best Practices".* Portsmouth, NH: NI2 Center for Infrastructure Expertise, 2005.

*Cargo Security International.* "iControl Incorporated Awarded U.S. Department of Homeland Security Contract for Worldwide Tracking and Secure Communications of Cargo Containers." March 6, 2006.

Cirincione, R, and A Cosmas. *Barriers to the Success of 100% Maritime Cargo Container Scanning.* Cambridge, MA: Massachusetts Institute of Technology, 2006.

*Coast Guard Missions.* November 24, 2006. http://www.uscg.mil/top/missions/ (accessed May 5, 2007).

*Comments on the 'International Container Standards Organization' and its Efforts to Propose New Standards for Container Security Technologies.* Washington, DC: World Shipping Council, 2006.

*CommerceGuard datasheet.* 2006. http://www.gesecurity.com/GESecurity/News/CommerceGuard/CG-System-Brochure.pdf (accessed February 15, 2007).

Conway, Peter. "Does cargo count?" *Airline usiness*, November 2006.

*CSI In Brief.* 2006. http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml (accessed May 5, 2007).

*CTPAT Frequently Asked Questions .* 2006. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml (accessed May 5, 2007).

*Customs and Border Protection Today.* "How do you make a box smart?" December 2003.

*Defense Logistics Agency Strategic Plan FY07-13.* Fort Belvoir, VA: Defense Logistics Agency, 2007.

Dennis, Scott M. "Improved Estimates of Ton Mile." *Journal of Transportation Statistics* (US Department of Transportation: Bureau of Transportation Statistics) 8 (2005).

*DLA at a Glance.* Fort Belvoir, VA: Defense Logistics Agency, 2006.

*DOD Logistics AIT Office.* 2007. http://www.dla.mil/j-6/ait/About.aspx (accessed 18 2007, May).

Downey, Leslie. "International Cargo Conundrum." *RFID Journal*, February 6, 2006.

ElAmin, Ahmed. "RFID standard passes shipping test." May 2, 2007.

*Electronic Container Seal (E-Seal) datasheet.* Livingston, NJ: E.J. Brooks Company, 2006.

*E-Modal InternetSite.* 2006. http://www.emodal.com/ (accessed January 18, 2007).

"EPCglobal Inc Initiates RFID Pilot Project to Enable Sea Container Visibility between Hong Kong and Japan." October 30, 2006.

*EUROPA - Taxation and Customs Union - Customs and Security.* 2006. http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/index_en.htm (accessed May 1, 2007).

Flynn, Stephen. *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism.* New York, NY: HarperCollins Books, 2004.

Forsyth, Gordon. "Horizon Lines Chairman Points to Projects Already Underway in Alaska and Puerto Rico Trades." January 19, 2007.

"Fourth Forum on Intermodal Freight Transport Between Europe and the United States (Executive Summary)." Report of Genoa Proceedings, 2001.

"GE tests cargo container security system." March 2005.

*Global Innovation Outlook 2.0.* Armonk, NY: International Business Machines Corporation, 2006.

*GPSInsight.com.* 2006. http://www.GPSInsight.com (accessed January 10, 2007).

Greenberg, David. "Crime on the Waterfront - cargo container theft in the Los Angeles area." *Los Angeles Business Journal*, 2001.

Guo, Chunlong, and Andy Fano. "Cargo Container Security using Ad Hoc Sensor Networks." *The Fourth International Conference on Information Processing in Sensor Networks.* Los Angeles, CA: Accenture Technology Labs, 2005.

Haveman, Jon D, and Howard J Shatz. *Protecting the Nation's Seaports: Balancing Security and Cost.* San Francisco, CA: Public Policy Institute of California, 2006.

*Hazardous Materials Safety and Security Technology Field Operational Test Volume I: Evaluation Final Report Executive Summary.* Washington, DC: US Department of Transportation, 2004.

*Hazardous Materials Transportation: Enhanced Security Requirements.* Washington, DC: US Department of Transportation Research and Special Programs Administration, 2006.

*HSARPA BAA Awards.* 2006. http://www.hsarpabaa.com/main/HSARPAAwards.asp?SortField=Project Title&BAAID=9 (accessed March 15, 2007).

Hudson, Scott. *Smart and Secure Tradelanes (SST).* February 21, 2006. http://scm.ncsu.edu/public/security/sec060221.html (accessed December 16, 2006).

"IBM and Maersk Logistics provide real-time cargo monitoring for global supply chain optimisation." September 20, 2005.

*Institute of International Container Lessors: About the institute.* 2006. http://www.iicl.org/IICLBackground.htm (accessed March 25, 2007).

*Intelli-que: Robust Wireless Container Tracking and Security.* 2006. http://www.intelli-que.com/ishield.html (accessed February 12, 2007).

*Intermodal Cargo Transportation: Industry Best Security Practices.* Cambridge, MA: US Department of Transportation: Volpe Center, 1999.

*Intermodal Freight Technology.* Washington, DC: US Department of Transportation, 2005.

*Intermodal Process Map - Information Exchange Descriptions.* Washington, DC: Intermodal Freight Technology Working Group , 2006.

*International Container Standards Organization Backgrounder: About ICSO.* 2006. https://www.containersecurity.org/tools/inc/get_file.php/Backgrounder-

29Jun06.pdf?file_name=386964b4fadf9fc3875e34e61ad02937&swa_customerID=863d01e3075ffa1fb2db7c8162a09d48&table=swt_news (accessed February 18, 2007).

*International Ship and Port Securit Code and SOLAS Amendments (2003).* London, England: International Maritime Organization, 2002.

*In-Transit Container Security Enhancement.* Various: World Shipping Council; International Mass Retail Association; The National Industrial Transportation League, 2003.

*ISO 18185-4:2007.* April 4, 2007. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=40809&scopelist=PROGRAMME (accessed April 20, 2007).

Jacksta, Robert. *The Testimony of Mr. Robert Jacksta.* Washington, DC: US Customs and Border Protection, 2005.

Jedermann, Reiner, and Christian Behrens. *Applying autonomous sensor systems in logistics - Combining sensor networks, RFIDs and software agents.* Bremen, Germany: University of Bremen, 2006.

Johnson, Eric. "RFID: taking the next step." *American Shipper*, November 2005: 26-32.

Karkkainen, Mikko , and Jan Holmstrom. "Wireless product identification: Enabler for handling efficiency, customisation and information sharing." *Supply Chain Management*, 2002.

Katz, Johnathan. "RFID Gains Credibility." *Industry Week*, January 2007.

Kulisch, Eric. "Not-so-Smart Box." *American Shipper*, November 2006.

Lake, Jennifer E, and William H Robinson. *Border and Transportation Security: The Complexity of the Challenge.* Washington, DC: CRS Report for Congress, 2005.

Lassek, Olaf. *The Intelligent Container.* Bremen, Germany: University of Bremen, 2006.

*Lloyd's MIU.* 2006. http://www.lloydsmiu.com/ (accessed February 12, 2007).

*Maersk Line: About Us.* 2007. http://www.maerskline.com/link/?page=brochure&path=/about_us (accessed May 21, 2007).

*Maersk logistics - 24 hr rule.* 2006. http://www.maersklogistics.com/sw18204.asp (accessed January 7, 2007).

*Marine Log.* "MATTS: securing the supply chain." January 2006.

Mary, Murphy-Hoye, and Hau L Lee. "A Real-World Look at RFID." *Supply Chain Management Review*, July/August 2005.

Meade , Charles, and Roger C Molander. *Considering the Effects of a Catastrophic Terrorist Attack.* Santa Monica, CA: RAND Corporation, 2006.

Melcer, Rachel, and Rebekah Tsadik. "Securing cargo and profits Partnership protects imported goods and supply chains." *St. Louis Post-Dispatch*, September 8, 2006.

Meyer, Andrea, and Dana Meyer. "Symposium Summary." Cambridge, MA: The Resilient and Secure Supply Chain (MIT Center for Transportation and Logistics), 2005.

Moorman, Robert W. "Drawing New Security Lines." *Air Cargo World*, March 2007.

Navas, Deb. "Too Much, Too Soon." *Supply Chain Manufacturing and Logistics*, December 6, 2004.

Nero, Mark. "Labor talks open on the docks." *Long Beach Press Telegram*, May 6, 2002.

*Number of U.S. Trucking Companies.* Washington, DC: American Trucking Association, 2006.

*Operation Safe Commerce Phase III.* Washington, DC: US Department of Homeland Security, 2005.

Panagopoulos, Nikolaos-Stavros V. *Analyzing the Use of Radio Frequency Identification (RFID) on the Container Industry.* Cambridge, MA: Massachusetts Institute of Technology, 2007.

*PAR LMS: About PAR LMS.* 2007. http://www.parlms.com (accessed May 15, 2007).

Peckenpaugh, Jason. "In Transit." *Government Executive*, July 15, 2002.

Petrakakos, Nikolaos H. *Port Security and Information Technology.* Cambridge, MA: Massachusetts Institute of Technology, 2005.

Pickett, Christopher B. *Strategies for Maximizing Supply Chain Resilience: Learning From the Past to Prepare for the Future.* Cambridge, MA: Massachusetts Institute of Technology, 2003.

*Polestar: Marine Asset Tracker datasheet.* February 1, 2007. http://www.polestarglobal.com/brochures/Pole-Star-Marine-Asset-Tracker.pdf (accessed February 25, 2007).

"Ports Receive $6.9 Million Security Grant: Grant Funds Phase III of Operation Safe Commerce at the Ports of Los Angeles and Long Beach." April 12, 2005.

Prater , Edmund, and Gregory V Frazier. *Future impacts of RFID on e-supply chains in grocery retailing.* Arlington, TX: University of Texas at Arlington, 2005.

*Qualcomm: Trailer and Container Management Solutions.* 2007. http://www.qualcomm.com/technology/assetmanagement/platforms/trailersolutions.html (accessed May 18, 2007).

Quick, and Tubb. "Tracking Marine Containers for Homeland Security." *Desktop Engineering Magazine*, June 2006.

Reese, Andrew K. "Disaster-proofing the Supply Chain: Using supply chain solutions to prepare for the next "Big One"." *Supply & Demand Chain Executive*, April/May 2007.

*Request for Information (RFI): Container Security Device.* 2006. http://www.hsarpabaa.com/Solicitations/CSD-RFI-ver-8.pdf (accessed March 15, 2007).

"RFID gets slammed." October 2006.

Rice, James B, and Philip W Spayd. *Investing in Supply Chain Security: Collateral Benefits.* Cambridge, MA: Massachusetts Institute of Technology, 2005.

"Risk Assessment and Prioritization." *Volpe Journal 2003: Transportation and Security*, 2003.

Rodrigue, Jean-Paul, Claude Comtois, and Brian Slack. *The Geography of Transport Systems.* New York, NY: Routledge, 2006.

Rutner, Stephen, and Matthew A Waller. "A Practial Look at RFID." *Supply Chain Management Review*, September 2004: 1.

*SAFE Container (SAFECON) Program.* Washington, DC: US Department of Homeland Security, 2007.

*Safefreight white paper.* 2006. http://www.safefreight.com/images/stories/documents/safefreight-solution.pdf (accessed March 7, 2007).

*SaviTrak datasheet.* 2006. http://www.savinetworks.com/resources/collateral/SaviTrak%20Datasheet%20LP021006F.pdf (accessed February 19, 2007).

Schaefer, Steffen. "Secure Trade Lane A Sensor Network Solution for More Predictable and More Secure Container Shipments." Portland, OR: OOPSLA'06, 2006.

*Secure Commerce RoadMap: The Industry's View for Securing Commerce.* Blue Bell, PA: Unisys Corporation, 2005.

*SeeContainer datasheet.* 2006. http://www.htsol.com/Files/ContainerBrochures.pdf (accessed February 25, 2007).

*Sensitech Ryan EZT datasheet.* 2006. http://www.sensitech.com/PDFs/products/RyanEZT_DS.pdf (accessed March 19, 2007).

Sheffi, Yossi. "Supply Chain Management Under the Threat of International Terrorism." *The International Journal of Logistics Management*, 2001.

—. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage.* Cambridge, MA: Massachusetts Institute of Technology, 2005.

Sichel, Alexander R. *Supply Chain Security along the Columbia River: An Analysis of Maritime Supply Chain Security with Respect to Communication between Security Experts.* Cambridge, MA: Massachusetts Institute of Technology, 2005.

"Smart and Secure Tradelanes white paper." 2003.

Sowinski, Lara L. "Port Security Is A 'Sink Or Swim' Proposition." *World Trade Magazine*, January 2004.

Srinagesh, Gavirneni. *Simulation based evaluation of info-centric supply chains.* Ithaca, NY: Cornell University, 2005.

Stana, Richard M. *Cargo Container Inspections - Preliminary Observations on the Status of Efforts to Improve the Automatic Targeting System.* Washington, DC: Government Accountability Office, 2006.

*Steelroads (Net REDI) InternetSite.* 2006. https://www.steelroads.com/index.jsp (accessed February 19, 2007).

Sullivan, Laurie. "Dow Chemical Focuses On Supply-Chain Tech." *TechWeb*, June 5, 2006.

*Supply Chain Europe.* "Possible EU boost for tagging as logistics pre-notification kicks in." June 2004.

*Supply Chain Security Best Practices Catalog.* Washington, DC: US Customs and Border Protection, 2006.

*Supply Chain Security EU Customs' role in the fight against terrorism (EU Customs Security Programme).* Brussels, Belgium: European Commission, 2006.

Sussman, Joseph. *Introduction to Transportation Systems.* Boston, MA: Artech House, Inc., 2000.

Swedberg, Claire. "Safeway Tracks Shipments to Alaska Stores, DCs." *RFID Journal*, January 24, 2007.

*The Electronics Freight Management Initiative.* Washington, DC: US Department of Transportation, 2006.

*The Freight Technology Story.* Washington, DC: US Department of Transportation, 2005.

Theo, Forbath. *Wireless Sensor Network Market Analysis Executive Summary.* Doddakannelli, India: Wipro PSA Group, 2006.

Thomas, Leslie. "All Aboard." *Security Products*, September 2006.

Tiemey, Stephen. "US Pushes drugs toward RFID." *Supply Chain Europe*, June 2004.

*Trade: Key Initiatives, Organizations and Technologies.* Washington, DC: US Customs and Border Protection, 2006.

*Traffic World.* "Feds set rail security track." January 12, 2007.

*Transportation Worker ID Credential – Proposed Rule.* May 22, 2006. http://www.eei.org/meetings/nonav_2006-05-22-rm/EisenhartHandouts.pdf (accessed May 17, 2007).

*Truck TAG (PierPass): The New PierPASS RFID Program datasheet.* 2006. http://www.pierpass.org/pdf/TruckTAG_Flyer_ENG_020206.pdf (accessed March 15, 2007).

*TSA: Transportation Worker Identification Credential (TWIC) Program.* 2007. http://www.tsa.gov/what_we_do/layers/twic/index.shtm (accessed 2007).

*US-Canada International Mobility and Trade Corridor.* Washington, DC: US Department of Transportation, 2002.

van de Voort, Maarten , and Kevin A O'Brien. *Seacurity - Improving the Security of the Global Sea-Container Shipping System.* Santa Monica, CA: RAND Corporation, 2003.

Vikesland, Lynn. *Massachusetts Port Authority* (November 17, 2006).

Wamba, Samuel Fosso , and Elisabeth Lefebvre. "Enabling Intelligent B-to-B eCommerce Supply Chain Management Using RFID and the EPC Network: A Case Study in the Retail Indutsry." Fredericton, New Brunswick: The Eighth International Conference on Electronic Commerce, 2006.

Weier, Mary Hayes. "RFID Tags Are On The Menu: Tracking technology will improve food safety and lower costs." *Information Week (Tech Portal)*, February 2, 2007: 49.

*What Regulations are Needed to Ensure Port Security?* Washington, DC: Committee on Government Reform, 2003.

White, Henry F. "Cargo-centric." *The Journal of Commerce*, April 19, 2004.

*WIPRO: Web based system for container movement for a large rail road consortium.* 2006. http://www.wipro.org/webpages/itservices/industries/travel&transport/traveltransportcasestudy12.htm (accessed February 12, 2007).

*World Air Cargo Forecast.* Chicago, IL: Boeing Corporation, 2007.

Zachary, Michael. *Port of Tacoma* (January 21, 2007).

*ZDNet.* "IBM, Maersk to equip ship cargo with sensors." September 2005.