**PROJECT PAPER**

# GLOBAL SECURITY SYSTEM

# FOR CONTAINERIZED COMMERCE

**ENSE623 System Validation and Verification Spring 2006**

**Submitted to: Professor Mark Austin**

**Submitted by: Sana Shaikh and Jason Smith**

# INDEX

# 1 Acknowledgments

We would like to thank those that have helped and supported us throughout this project. Most of all we would like to thank our project advisor, Dr. Mark Austin of the Department of Civil and Environmental Engineering and Institute for Systems Research at the University of Maryland. In particular, his excitement for our project and knowledge of LTSA inspired us. In addition, we'd like to thank LCDR Mike Dolan from the United States Coast Guard Headquarters Cargo & Facilities Division and LT Nichole Rodriguez from United States Coast Guard Sector Baltimore Prevention Department Waterways Management Division. We want to thank them both for their containerized commerce security system overview from their respective regulatory and field perspectives, for the contacts they provided us to get other perspectives, and for making the arrangements to see the working process at the Port of Baltimore.

Thanks to you all, your time and information was invaluable and is very much appreciated.

# 2 Project Description

## *2.1 Objectives*

In the wake of the September 11th events, numerous government and private transportation organizations hurried to secure aspects of the industry that appeared vulnerable to future attack. One aspect in particular, containerized commerce or intermodalism (transport of standardized containers throughout different modes of transportation) presented a great risk due mainly to the fact that the standardized container is often unrevealed (type and source), is transported quickly, and is completely global. Because of this increased risk, U.S. and international regulations were implemented to mitigate potential weak points. With increased complexity of today's transportation system and available security tools (electronic seals, RFID seals, etc.) there is a great need to clearly represent both the multiple user domains and multiple states that a container undergoes throughout the process. These domains and states must be considered when developing and implementing regulations and security systems. This project aims at studying the current global security system for containerized commerce from the following three aspects:

1. First, developing a high level model which will be used to recognize vulnerabilities and requirements of a secure system. As identifiable vulnerabilities are discovered, further drilling down may be conducted to better analyze the specifics. Standard UML visual representations will be utilized to accurately define system behavior and structure.

2. Second, from the models developed and governmental regulatory feedback/studies a list of requirements and specifications of a secure system will be created and mapped.
3. Third, tools such as LTSA will be used to model the system and verify whether the specifications of the system satisfy the properties required of its behavior.

## 2.2 Motivation

While all types of transportation have specific vulnerabilities to terrorist attacks, perhaps none are more dangerously exposed than containerized commerce. The potential insertion of weapons or stowaways into standardized containers is a particularly acute risk in this context. A recent CIA analysis concludes that the delivery of Weapons of Mass Destruction (WMD) into the United States via these mechanisms is more likely than any threat to the country from ICBMs[1] (intercontinental ballistic missiles). The reason for this acute risk is due to the following factors:

- Numerous often unknown actors
- Numerous often unknown locations of loading, storage, and transportation
- Differing degrees of government intervention and support for security
- Contents are concealed unless under costly and time consuming inspections
- Industry's need to rush container movement resulting in fewer less quality checks

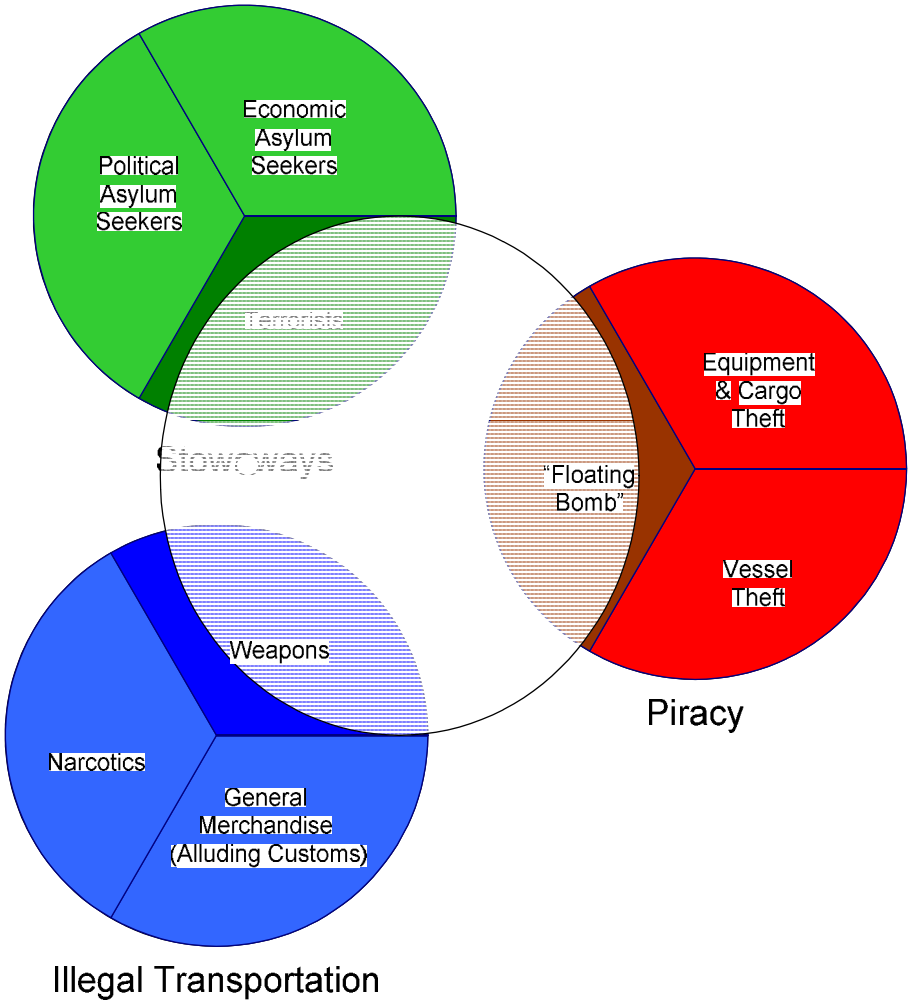
Addressing the security of the containerized commerce supply chain requires a comprehensive global framework throughout all modes of transport. Although similar framework may exist at particular modes of transportation (i.e. models covering maritime transport) or states along the supply chain (i.e. models covering ports, there is little evidence indicating any comprehensive intermodal framework exists.

[1] United States. Central Intelligence Agency. Foreign Missile Developments and the Ballistic Missile Threat Through 2015: Unclassified Summary of a National Intelligence Estimate. 2002. 1 Oct. 2006 <http://www.cia.gov/nic/pubs

## *2.3 Framework, Boundary, and Limitations*

**Framework:** Includes the interaction between actors and use cases as defined in Section 2 below. The system is a cradle (supplier) to grave (customer) high level representation a global container's security measures throughout multiple states. It can be used to include for both empty and loaded containers, in all modes of transportation, and any iteration of carrier to port interface.

**Boundary:** Since it is only a high level representation it does not include specific use case details. In order to allow modularity, the use cases represent commonalities throughout varying types of carriers and national requirements. The scope is limited only to the security aspects of container security without respect to time or costs. For the purposes of this paper, security is defined as precautions taken to guard against crime, attack, sabotage, or, espionage towards a nation. It does not include protection from theft, asylum seekers, or transportation of illegal materials for personal gain.


Economic Asylum Seekers
Political Asylum Seekers
Terrorists
Stowaways
Equipment & Cargo Theft
"Floating Bomb"
Vessel Theft
Piracy
Weapons
Narcotics
General Merchandise (Alluding Customs)
Illegal Transportation

**Limitations:** The following scenarios have been omitted from the analysis due to available information and time constraints.

- Use of container other than "sealable containers". Containers without means to seal (i.e. open top, flat rack, and platform containers) have not been specifically addressed.
- Presence of inter-governmental agreements (i.e. NAFTA, EU, etc.) that precede international and national security regulations (i.e. ISPS & MTSA)
- Variations for changes in security levels. Current governmental transportation security regulations set specific deterrents based on the locally set security level (typical level I, II, or III; similar to the U.S. DHS Advisory System threat levels.). Currently this model does not represent either security procedure or tool changes when and if local security levels increase or decrease.
- Attacker scenario: when an attacker is able to either remove or add cargo to the containerized commerce during its lifecycle or is able to remove or add the entire container into/from the container lifecycle. This scenario is only security critical when the commerce is altered after the container is sealed by the supplier until the point where the container is opened by the customer.

# 3 Terminology

**CBRN:** Chemical, Biological, Radiological or Nuclear Weapon

**bMSC:** Base Message Sequence Chart

**Consolidator:** Cargo containing shipments of two or more shippers or suppliers. Container load shipments may be consolidated for one or more consignees[2].

**Container:** A truck trailer body that can be detached from the chassis for loading into a vessel, a rail car or stacked in a container depot. Containers may be ventilated, insulated, refrigerated, flat rack, vehicle rack, open top, bulk liquid or equipped with interior devices. A container may be 20 feet, 40 feet, 45 feet, 48 feet or 53 feet in length, 8'0" or 8'6" in width, and 8'6" or 9'6" in height[1].

**CSI:** Container Security Initiative. A customs-to-customs partnership driven by the U.S. CBP to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels. Through CSI, CBP officers work with host customs administrations to establish security criteria for identifying high-risk containers. CSI is currently operational at 50 of the largest foreign ports.[3]

[2] "Glossary of Shipping Terms." Maritime Administration. 5 Oct. 2004. Department of Transportation. 1 Oct. 2006 <http://www.marad.dot.gov/Publications/glossary/A.html

[3] "CSI in Brief." Container Security Initiative. United States Customs and Border Protection. 1 Oct. 2006 <http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml

**FSM:** Finite State Machine

**hMSC:** High Level Message Sequence Chart

**ICBM:** Intercontinental Ballistic Missiles

**LTS:** Labelled Transition System

**LTSA:** Labelled Transition System Analyser

**MSC:** Message Sequence Chart

**NII:** Non-Intrusive Inspection technology. Container inspections conducted with specialized equipment such as x-ray, sonar, etc. Enables thorough examinations of container contents without the costly, time consuming process of unloading cargo for manual searches, or intrusive examinations of conveyances by methods such as drilling and dismantling.[4]

**PSA:** Publicly Available Standard - International Organization for Standardization

**Seal:** Products placed on the access point(s) of a container that visually identify if a container has been opened. Security seals vary in complexity from basic plastic seals to high security seals and RFID tags that can track the container, record environmental conditions, and send alerts/notifications. Security seals can be divided into three types[2]

[4] "Supply Chain Security Glossary." Retail Leaders, Leaders Association. 1 Oct. 2006 <http://rila.interactive.biz/scs_glossary.htm

# 4 Use Case Analysis

The use case development from this section is used to recognize vulnerabilities and generate requirements of a secure system. As identifiable vulnerabilities are discovered, further drilling down may be conducted to better analyze the specifics.

## *4.1 Actor Definitions*

All primary actors in the system have been listed and defined below. Primary actors are listed by number with some generalized actors listed by letter. Since the project represents a high level system, not all generalized actors are addressed. These actors including terminal operators, country specific border protection agencies (other than U.S. CPB); and flag state registry officials and classification society's (i.e. U.S. Coast Guard, DNV, etc.), national and local department of transportation officials, etc. should be included in future detailed study of this system. As discussed in section 1.4., limitations, the attacker scenario is not yet incorporated into this system; therefore the attacker actor is also not defined below.

**Supplier:** a business engaged in manufacturing product that is provided for others. For the purposes of this project, supplier can include any manufacturer, distributor, etc. who ships containerized commerce to a customer (end user).

**Freight Forwarder**: A person whose business is to act as an agent on behalf of the shipper. A freight forwarder frequently makes the booking reservation.

**Consolidator**: A person or firm consolidating shipments of two or more suppliers/freight forwarders. Container-load shipments may be consolidated for one or more consignees. The consolidator takes advantage of lower full carload (FCL) rates, and savings are passed on to shippers.

**Port Authority:** A government commission or business that manages facilities of a port where commerce is either stored and/or exchanged between carriers. Port authorities are similar to a landlords that lease lots for a wide variety of activities, including cargo and/or passenger loading and unloading. Port authorities may delegate shore-side operations, to the terminal or carriers.

- **Shipping Port**: Location where ocean carriers load/offload commerce for either storage or exchange to another (typically truck or rail) carrier.
- **Airport:** Location where air carriers load/offload commerce for either storage or exchange to another (typically truck) carrier.
- **Rail Yard:** Location where rail carriers load/offload commerce for either storage or exchange to another (typically truck or rail) carrier.
- **Truck Yard:** Location where truck carriers load/offload commerce for either storage or exchange to another (typically truck) carrier.

**Carrier**: Any person or entity who, in a contract of carriage, undertakes to perform or to procure the performance of carriage by rail, road, sea, air, or by a combination of such modes.

- **Ocean Carrier**: Carrier who transports commerce by sea.

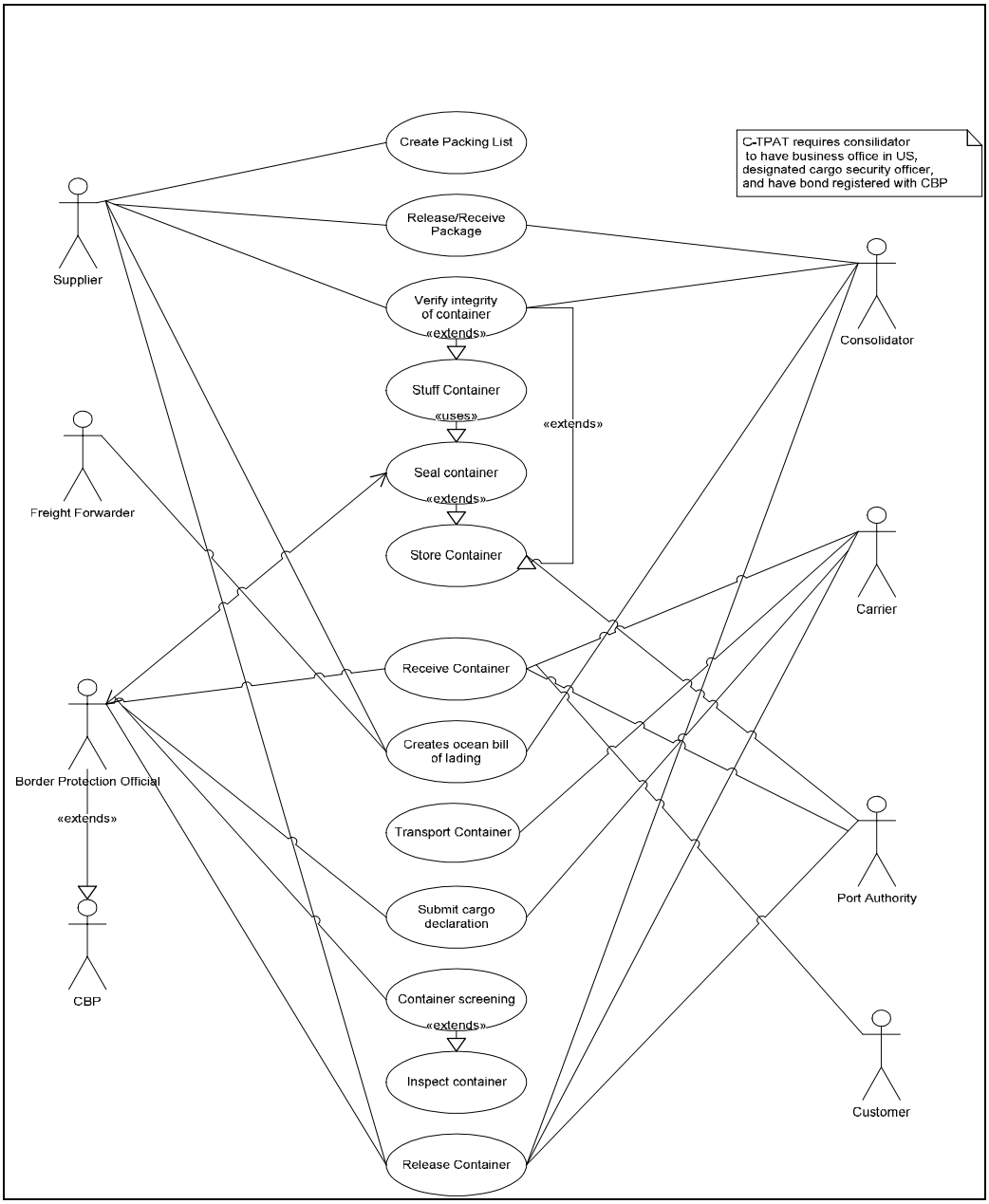
- **Air Carrier**: Carrier who transports commerce by air.
- **Rail Carrier**: Carrier who transports commerce by rail.
- **Truck Carrier**: Carrier who transports commerce by road.

**Border Protection Agency:** Government agency charged with enforcing the rules passed to protect the country's border.

**Customs and Border Protection Agency (CBP):** The United State's designated Border Protection Agency. The CBP falls under the Department of Homeland Security and is tasked to manage the following functions; customs inspection, immigration inspection, and border patrol (www.cbp.gov)

## 4.2 Use Case Diagram

The system use case diagram below represents the interaction between all actors and use cases in UML standard.



## 4.3 Use Cases

The following high level use cases have been developed to model the global security system for containerized commerce within the framework, boundaries, and limitations discussed in section 1.3.

### 4.3.1 Use Case: Create Packing List

**Identifier: UC01**

**Description:** Packing List is an itemized list of the commodities description, quantity, and weight contained in the package but cost values are typically not indicated. The list is used to fill the customer's order and ensure no additional contents are included in the package. The list may only contain the contents of one of many packages within a container if the container is to be consolidated with many packages. If the container has only one shipper and only one customer, the packing would contain all the contents of the container.

**Goal**: To create a packing list for the order received from the customer

**Actors**

1. Supplier

**Preconditions**

1. Order has been received from the customer

**Basic Course**

1. Use case begins when the *Supplier* has received an order
2. *Supplier* creates packing list matching *customer's* order
3. *Supplier* completes origination and destination information:
    - Ship From

- Ship To

4. *Supplier* signs and dates packing list
5. Use case ends when the *Supplier* signs and dates the packing list

**Post conditions**

1. Packing list is complete and order can be filled when necessary

**Notes**

1. Only those details of the packing list which will have an impact on the security of the container being shipped have been considered in this use case.

### 4.3.2 Use Case: Release/Receive Package

**Identifier**: **UC02**

**Description:** The *Consolidator* receives custody of the package and packing list from the *Supplier*.

**Goal:** To Release/Receive a package with proper document verification

**Preconditions**

1. Package is prepared for release by the *Supplier*
2. *Consolidator* is prepared to receive package
3. A legal agreement exists between the supplier and the consolidator

**Assumptions**

1. Consolidator is contracted by the Supplier to conduct the following use cases:

    - Verify Container Integrity (UC03)
    - Stuff Container (UC04)
    - Seal Container (UC05)
    - Store Container (UC06)
    - Release Container (UC13)

    Otherwise this use case is not utilized and the above listed use cases are conducted by the Supplier.

**Precondition**

1. Packing List is complete (UC01)

**Basic Course**

1. Use case begins when the *Supplier* is prepared to release the package.
2. *Consolidator* receiving the package must be positively identified
3. *Supplier* and *Consolidator* verify the package matches the packing list
4. Document on packing list that package has been verified against packing list and has been released to the *Consolidator*.
5. Use case ends when the *Consolidator* remains in custody of the package.

**Alternate Course A:**

**Condition:** Package does not match information on packing list

A4. Package is not released / received until discrepancies are corrected.

A5. Once discrepancies are corrected, use case ends when the Consolidator maintains custody of the package.

**Post conditions**

1. *Consolidator* remains in custody of the package.

### 4.3.3 Use Case: Create Bill of Lading

**Identifier: UC03**

**Description:** Bill of Lading is the official legal document representing ownership of cargo, a negotiable document to receive cargo, and the contract for cargo between the shipper and the carrier. In relation to security it documents the contents of the container or references specific packing lists and ID the seal and container serial numbers.

**Goal:** Create a Bill of Lading

**Actors**

1. Supplier
2. Consolidator

**Preconditions**

1. All container contents have completed and available packing lists.

**Basic Course**

1. Use case begins when the *Supplier, Consolidator, or Freight Forwarder* has determined the full contents (description, weight, etc.) and final destination of the container.
2. Bill of lading is completed to include the following information
    a. Point of origin
    b. Point of destination

c. Contents

3. *Supplier, Consolidator, or Freight Forwarder* signs and dates the Bill of Lading
4. Use case ends when the *Supplier, Consolidator, or Freight Forwarder* signs and dates the Bill of Lading

**Post conditions**

1. Bill of lading is complete and ready to be used to stuff container.

**Actors**

1. Supplier
2. Freight Forwarder
3. Consolidator

**Notes**

1. C-TPAT Foreign Manufacturer Security Criteria Procedural Security, Manifesting Procedures

### 4.3.4 Use Case: Verify Container Integrity

**Identifier**: **UC04**

**Description:** The actor who initially stuffs the container must verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers.

**Goal**: Verify the integrity of container prior to stuffing

**Actors**

1. Supplier
2. Consolidator

**Preconditions**

1. Container is empty
2. Container is located in a facility appropriate to enable container inspection (secure, well lit, etc.)

**Assumptions**

1. Personnel assigned to conduct the inspection are properly trained.

**Basic Course**

1. Use case begins when the actor is ready to stuff the container

2. Verify the container's integrity at the following areas:
    - Front wall
    - Left side
    - Right side
    - Floor
    - Ceiling/Roof
    - Inside/outside doors
    - Outside/Undercarriage
3. Document the condition of the container
4. Any necessary repairs are to be made and properly documented prior to stuffing
5. Use case ends when the supplier has verified and documented the integrity of the container

**Alternate Course A:**

**Condition:** Container damage is beyond repair

A5.Container is removed from service.

**Post conditions**

1. Integrity of the container is verified and documented

**Extended Use Case**

1. Stuff Container (UC04) if container is ready to be stuffed.
2. Store Container (UC06) if container if not ready to be stuffed.

**Notes**

1. Initial use case of secured container. Container security must be maintained until the container is released to the customer. to protect against the introduction of unauthorized material and/or persons.
2. Reference: C-TPAT Foreign Manufacturer Security Criteria; Container Security http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_criteria/security_criteria_foreign_manuf/foreign_mfc_security_criteria.xml#ProceduralSecurity

### 4.3.5 Use Case: Stuff Container

**Identifier**: **UC05**

**Description:** The container is stuffed (loaded) as detailed in the bill of lading.

**Goal:** Successfully stuff the container as per the Bill of Lading

**Actors**

1. Supplier
2. Consolidator

**Preconditions**

1. Container has passed an integrity inspection (UC04) and has been in a secure facility ever since.

**Basic Course**

1. Use case begins when container is ready to be stuffed.
2. Container is stuffed (loaded) as per bill of lading details.
3. Document container identification number on bill of lading
4. Include UC06
5. Use case ends when the supplier affixes a high security seal and documents the details.

**Post conditions**

1. Container is stuffed and sealed with high bolt security seal.
2. Container identification and seal serial numbers are documented on the bill of lading
3. Container is either released (UC11) for transport (UC09) or stored (UC06)

**Included Use Cases**

1. Seal Container (UC06)

**Notes**

1. Reference: Container and Trailer Security Container and Trailer Seals

### 4.3.6 Use Case: Seal Container

**Identifier**: **UC06**

**Description:** The container is sealed to prevent tampering while in transit. The seal is always installed following Stuff Container use case (UC05) and when ever Border Protection Official conducts a visual inspection (UC12). The sealing of containers and continuous seal integrity, are the most crucial elements of a secure supply chain.

**Goal:** Seal the container to ensure a secure supply chain.

**Actors**

1. Supplier
2. Consolidator
3. Border Protection Official

**Preconditions**

1. Container has passed an integrity inspection (UC03) and has been in a secure facility ever since.

**Assumptions**

1. Written procedures stipulating how seals are to be controlled and affixed to loaded containers, to include procedures for recognizing and reporting compromised seals and/or containers to the appropriate authority are in place and being followed.

**Basic Course**

1. Use case begins when container is stuffed and ready to be sealed.
2. Designated employee distributes high bolt security seal meeting PAS ISO 17712 standards.
3. Affix high bolt security seal to container.
4. Document the details of the seal on the bill of lading.
5. Use case ends when the supplier affixes a high security seal and documents the details.

**Post conditions**

1. Container is sealed with high bolt security seal.
2. Seal serial number is documented in the bill of lading
3. Container is either released (UC13) for transport (UC09) or stored (UC06)

**Extended Use Case**

1. Release Container (UC13) – if all pre conditions of UC13 are met;
    a. Container is prepared for release by the releasing actor
    b. Receiving actor is prepared to receive container (ref. UC02)
2. Store Container (UC07) – if all pre conditions of UC13 are not met

**Notes**

1. Reference: Container and Trailer Security Container and Trailer Seals

### 4.3.7 Use Case: Store Container

**Identifier UC07**

**Description:** Containers must be stored in a secure area to prevent unauthorized access and/or manipulation.

**Goal:** Store the container in a secure area

**Actors**

1. Supplier
2. Consolidator
3. Carrier
4. Border Protection Official
5. Port Authority

**Preconditions**

1. Container has been inspected for integrity and passed (UC02)

**Assumptions**

1. Procedures are in place to control access and prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect facility's assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

2. Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.
3. Physical barriers and deterrents that guard against unauthorized access must be installed to maintain facility security and regularly inspected for integrity and damage. At a minimum the following equipment must be present:
    *a.* Perimeter fencing surrounding cargo handling and storage facility.
    *b.* Manned or monitor gates
    *c.* Buildings must be constructed of materials that resist unlawful entry.
    *d.* All external and internal windows, gates and fences that at not manned must be secured with locking devices.
    *e.* Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.
    *f.* Alarm systems and video surveillance cameras should be utilized to monitor premises

**Basic Course**

1. Use case begins when a container needs to be stored
2. Store the container in a secure area to prevent unauthorized access.
3. Document the storage details of container.
4. Use case ends when a container is securely stored.

**Post conditions**

1. Container is stored in a secure area.

**Notes**

1. *Reference; C-TPAT Foreign Manufacturer Security Criteria Container and Trailer Storage*

### 4.3.8 Use Case: Receive container

**Identifier**: **UC08**

**Description:** The receiving actor* receives custody of the container and associated documentation (bill of lading, packing lists) from the releasing actor*. This use case signifies acceptance of custody of the container.

**Goal:** Receive a container with proper document verification

**Actors**

1. Carrier
2. Border Patrol Official
3. Port Authority
4. Customer

**Preconditions**

1. Container is prepared for release by the releasing actor (ref. UC13)
2. Receiving actor is prepared to receive container.

**Assumptions**

1. Procedures are in place to ensure that all information used in receiving the container, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. This information includes; content

description and piece count, labeling, marking, seal number, etc. Documentation control must include safeguarding computer access and information.

2. Procedures are in place to ensure that information received from business partners is reported accurately.
3. Procedures should also be established to track the movement of incoming and outgoing goods.

**Basic Course**

1. Use case begins when the releasing actor is prepared to release the container.
2. Actor releasing the container must be positively identified
3. Verify pick up order matches bill of lading
4. Reconcile container against information on the bill of lading (content description and piece count, labeling, marking, seal number, etc.)
5. Document that container has been verified against pick-up order and is in acceptable condition.
6. Use case ends when the receiving actor remains in custody of the container.

**Alternate Course A**

**Condition:** Container does not match information on purchase order or container is not in acceptable condition.

A5. All shortages, overages, container damage, sign of tampering, or other significant discrepancies or anomalies must be resolved and/or investigated appropriately.

A6. Discrepancies must be documented

A7. Border protection agencies must be notified if illegal or suspicious activities are detected.

A8. Discrepancies must be corrected; otherwise, container is unable to be received.

A9. Use case ends when the receiving actor remains in custody of the container.

**Post conditions**

1. Receiving actor remains in custody of the container.

**Notes**

1. Receiving actor is the actor physically receiving (taking custody of) the container and may include the *Carrier, Border Protection Official, Port Authority,* or *Customer.*
2. Releasing actor is the actor physically releasing the container and may include the *Supplier*, *Consolidator, Border Protection Official, Carrier,* or *Port Authority.*
3. Ref. C-TPAT Foreign Manufacturer Security Criteria; Procedural Security, Shipping and Receiving

### 4.3.9 Use Case: Transport container

**Identifier: UC09**

**Description:** Container is transported to its next destination.

**Goal:** Transport a container securely to its next decision.

**Actors**

1. Carrier

**Preconditions**

1. Container has been stuffed/sealed (UC04) or is empty.
2. Container has been received (UC08) and is in the custody of the carrier

**Assumptions**

1. Procedures are in place to maintain security of the container from unauthorized entry or tampering. When ever possible carrier must maintain control of employees and visitors. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.
2. Procedures must be in place for reporting and neutralizing unauthorized entry into containers.
3. Physical barriers and deterrents that guard against unauthorized access must be installed to maintain security and regularly inspected for integrity and damage. At a minimum the following equipment must be present:

**Basic Course**

1. Use case begins when the container is in the custody of the carrier
2. The container is securely loaded onto the carrier
3. The container is transported to its proper destination as detailed on the container documentation.
4. Use case ends when the container has been transported to the proper destination and is waiting to be received by the receiving actor.

**Post conditions**

1. Container has been transported to the proper destination and is awaiting to be received by the receiving actor

### 4.3.10 Use Case: Submit Cargo Declaration

**Identifier**: **UC10**

**Description:** Cargo declaration is submitted prior to or upon carrier's arrival. The declaration is used by the Border Protection Agency to determine risk severity of container.

**Goal:** Submit a Cargo Declaration to the Border Protection Agency

**Actors**

1. Carrier
2. Border Protection Agency

**Preconditions**

1. Carrier with container has arrived at new country destination or when advance notification is required, is in route to destination.

**Basic Course**

1. Use case begins when the *carrier* is required to submit cargo declaration to *Border Protection Agency*
2. *Carrier* completes cargo declaration form as detailed by the container's destination government.
3. *Carrier* submits cargo declaration form as detailed by the container's destination government*.

4. Use case ends when the *Border Protection Agency* has received the *Carrier's* cargo declaration.

**Post conditions**

1. Cargo declaration has been completed and submitted to the Border Protection Agency

**Notes**

1. United States requires advance cargo manifests by electronic transmission twenty-four hours prior to loading aboard a vessel destined for the U.S. This manifest is known as AMS (Automated Manifest System) and includes 14 data elements used to screen containers and identify those containers that are of a high risk category. It is multi-modular (use for all modes of transportation).

### 4.3.11 Use Case: Screen Container

**Identifier: UC11**

**Description:** Container Screening identifies high-risk containers through a collaborative targeting and analysis process adopted by the destination country. The process utilizes prior data collection and intelligence to rank the container's security risk based off the submitted cargo declaration data elements.

**Goal:** Screen a container to identify high-risk container

**Actors**

1. Border Protection Agency

**Preconditions**

1. Carrier submits cargo manifests as required by the container's destination government.

**Assumptions**

1. Written procedures stipulating how container screening is conducted to determine container security risk level are in place and adhered to by the Border Protection Agency
2. Risk based decision matrixes/processes are updated regularly based on accurate data and current intelligence.

**Basic Course**

1. Use case begins when *Border Protection Agency* receives carrier's cargo manifests
2. *Border Protection Agency* enters data elements from cargo declaration into pre-defined security risk decision matrix.
3. Use case ends when the containers security risk level has been determined.

**Post conditions**

1. Container's risk level has been determined.

**Extended Use Case**

1. Inspect Container (UC12) – if container is determined to be high risk warranting container inspection.

**Notes**

1. The U.S. Customs and Border Protection Agency uses an automated targeting tool known as ATS (Automated Targeting System) to identify containers that pose a potential risk for terrorism. ATS receives 14 data elements submitted by the carrier through the AMS.

### 4.3.12 Use Case: Inspect container

**Identifier: UC12**

**Description:** Containers identified as high risk by the *Border Protection Official* are inspected upon arrival. Depending on the severity and facilities, inspections may be either NII or physical.

**Goal:** Inspect a high risk container

**Actors**

1. Border Protection Official

**Preconditions**

1. Container is has been identified as high risk by the Border Protection Official.

**Basic Course**

1. Use case begins when the Border Protection Official initiates hold on container for inspection
2. *Border Protection Official* alerts *Port Authority* of container inspection details
3. *Port Authority* informs *Border Protection Official* of container time and location of destination.
4. *Border Protection Official* verifies seal matches container bill of lading
5. Border Protection Official breaks seal.
6. *Border Protection Official* conducts internal inspection.

7. *Border Protection Official* documents and corrects any deficiencies.
8. Immediately upon the conclusion of an inspection UC07; Seal container . .
9. *Border Protection Officials* notifies the *Port Authority* when the inspection is completed; results of inspection, any discrepancies, and the serial number of the newly installed high-security bolt seal.
10. Use case ends when the *Border Protection Officials* terminates hold on container.

**Alternate Course A:**

**Condition:** If NII technology is utilized

A5.*Border Protection Official* conducts NII.

A6. *Border Protection Official* documents and corrects any deficiencies.

A7. *Border Protection Officials* notifies the *Port Authority* when the inspection is completed; results of inspection and any discrepancies

A8. Use case ends when the *Border Protection Officials* terminates hold on container.

**Post conditions**

1. *Border Protection Officials* terminates hold on container and container is allowed to return to the supply chain.

**Included Use Cases**

1. Seal container (UC06) – unless alternate course (NII) is conducted.
2. Release Container (UC13)

**Notes**

1. Ref; Containerized Cargo Sealing Policy (01/27/06) http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/port_security/container_sealing.xml
2. The U.S. government inspects 5.5% - 6% of all inbound containers (those that raise a red flag in the government screening process) using either X-ray or gamma ray technology or through physical inspection of the container.
3. High risk containers bound for the US may be inspected prior to loading at the departure port if a CSI arrangement is operational with the host country.

### 4.3.13 Use Case: Release Container

**Identifier: UC13**

**Description:** The releasing actor releases custody of the container and associated documentation to the receiving actor

**Goal:** Release the container with proper verification.

**Actors**

1. Supplier
2. Consolidator
3. Carrier
4. Border Patrol Official
5. Port Authority

**Preconditions**

1. Container is prepared for release by the releasing actor
2. Receiving actor is prepared to receive container (ref. UC02)

**Assumptions**

1. Procedures are in place to ensure that all information used in receiving the container, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. This information includes; content

description and piece count, labeling, marking, seal number, etc. Documentation control must include safeguarding computer access and information.

2. Procedures are in place to ensure that information received from business partners is reported accurately and timely.
3. Procedures should also be established to track the timely movement of incoming and outgoing goods.
4. Security measures are in place to ensure the integrity and security of processes relevant to container handling, transportation, handling, and storage.

**Basic Course**

1. Use case begins when the receiving actor is prepared to receive the container.
2. Actor receiving the container must be positively identified
3. Verify purchase order matches container documentation
4. Reconcile container against information on the cargo manifest (content description and piece count, labeling, marking, seal number, etc.)
5. Document container has been verified against purchase order and is in acceptable condition.
6. Use case ends when the receiving actor remains in custody of the container.

**Alternate Course A:**

**Condition:** Container does not match information on purchase order or is not in acceptable condition.

A5.All shortages, overages, container damage, sign of tampering, or other significant discrepancies or anomalies must be resolved and/or investigated appropriately.

A6.Discrepancies must be documented

A7.Border protection agencies must be notified if illegal or suspicious activities are detected.

A8.Discrepancies must be corrected; otherwise, container is unable to be received.

A9.Use case ends when the receiving actor remains in custody of the container.

**Post conditions**

1. Receiving actor remains in custody of the container.

**Notes**

Ref. C-TPAT Foreign Manufacturer Security Criteria; Procedural Security, Shipping and Receiving

# 5 Scenarios and Activity Diagram

## *5.1 Basic Scenario*

Initial research in the project began with the development of a “basic scenario”. This scenario is a simplistic yet encompassing sample scenario that ensures the interaction between all primary actors (with the exception of freight forwarder) and all use cases. It was developed to test the use case development and for use with LTSA and MSC.

- Supplier prepares package for shipment and releases package to Consolidator

  **Use Cases included**: UC01 and UC02

- Consolidator receives package from Supplier, consolidates packages and then stuff, seals, stores, and finally releases container to Carrier; Truck Carrier. Consolidator also develops necessary container documentation (Bill of Lading).

  **Use Cases included:** UC02, UC03, UC04, UC05, UC06, UC07, UC13.

- Carrier; Truck Carrier receives container from Consolidator, transports container, and releases container to Port Authority; Ocean Port.

**Use Cases included**: UC08, UC09, and UC13

- Port Authority; Ocean Port receives container from Carrier, Truck Carrier, stores container, and releases container to Carrier; Ocean Carrier.

  **Use Cases included**: UC08, UC07, and UC13

- Carrier; Ocean Carrier receives container from Port Authority; Ocean Port and transports container over country border. Carrier; Ocean Carrier submits cargo declaration to the Border Protection Agency.

  **Use Cases included**: UC08, UC09, and UC10.

- Border Protection Agency receives cargo declaration and screens container. Container is determined to be high risk and requires container inspection prior to transfer to Port Authority; Ocean Port.

  **Use Cases included**: UC10 and UC11.

- Carrier; Ocean Carrier releases container to the Border Protection Agency.

**Use Cases included**: UC13.

- Border Protection Agency receives container from Carrier, Ocean Carrier and conducts intrusive inspection (ie. Non intrusive inspection such as x-ray not available or applicable). No threat is found and container is sealed and released back to Carrier; Ocean Carrier.

  **Use Cases included**: UC08, UC12 and UC13.

- Carrier; Ocean Carrier receives container from Border Protection Agency and releases container to the Port Authority; Ocean Port.

  **Use Cases included**: UC08 and UC13.

- Port Authority; Ocean Port receives container from Carrier, Ocean Carrier, stores container, and releases container to Carrier; Rail Carrier.

  **Use Cases included**: UC08, UC07, and UC13

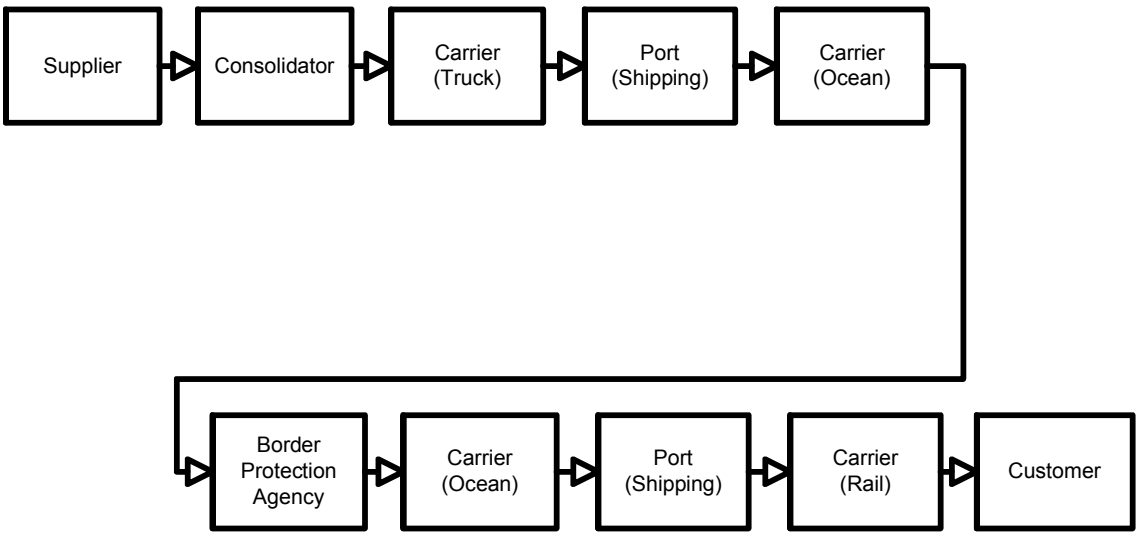
- Carrier; Rail Carrier receives container from Port Authority; Ocean Port, transports container, and releases container to Customer.

**Use Cases included**: UC08, UC09, and UC13

- Customer receives container from Carrier; Rail Carrier

  **Use Cases included**: UC08

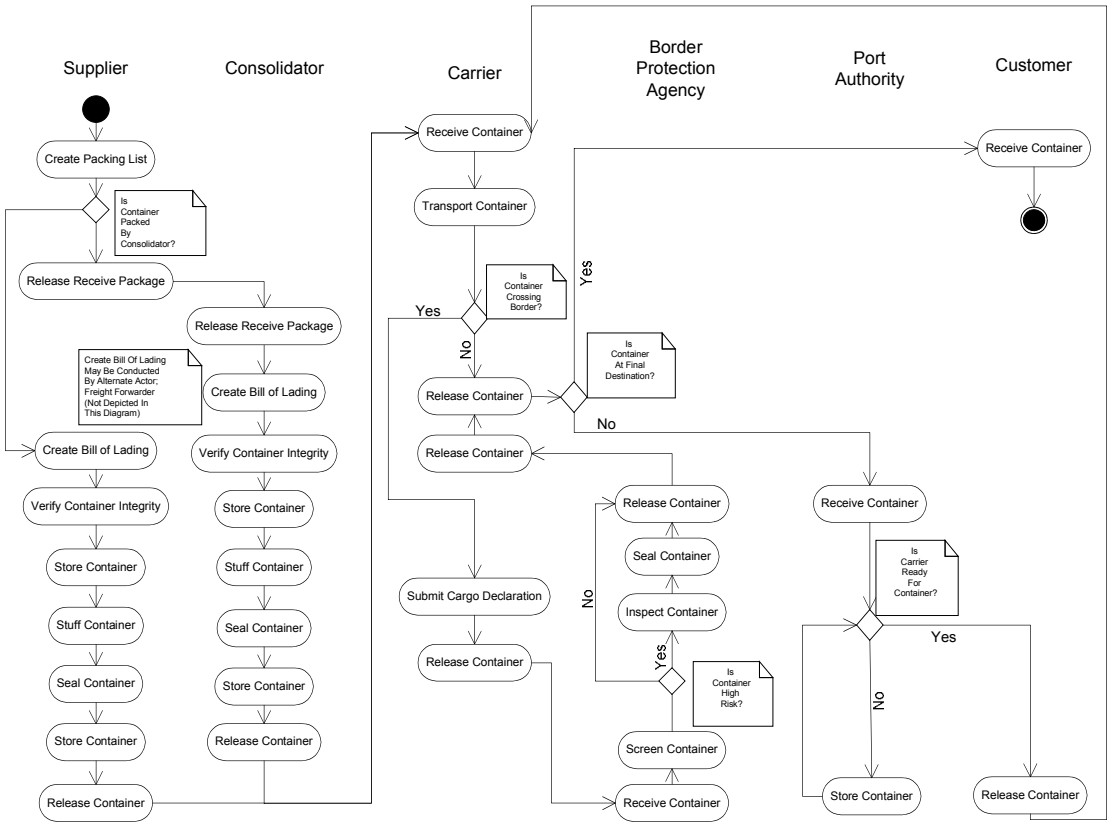
**Basic Scenario Diagram**



## 5.2 High Level Activity Diagram

The following high level activity diagram was created to provide a holistic view of the system. It too represents all primary actors (with the exception of freight forwarder) and all use cases. In addition to the basic scenario, it includes decision nodes that allow for any number of the following iterations;

- Carrier to Port Authority
- Carrier to Border Protection Agency
- Port Authority storage



# 6 System Requirements

## *6.1 High Level Requirements from Use Cases*

The following are high-level system requirements generated from the use case analysis.

1. Every package should contain a packing list
2. If a supplier uses a consolidator, there should be a legal agreement between the supplier and the consolidator
3. The Supplier, Consolidator or Freight Forwarder creates the Bill of Lading (BOL)
4. The container is verified in a facility appropriate to enable container inspections
5. When stuffing the container, security must be maintained
6. All stuffed containers must be sealed
7. Storage and transport facilities for containers must be secure
8. Document the storage details of the container
9. Procedures are in place to ensure that the information is accurate
10. The parties releasing and receiving the container must be positively identified
11. Container documentation must be verified prior to releasing or receiving a container
12. All discrepancies must be addressed prior to releasing or receiving a container

13. The carrier securely transports the container to its destination
14. The carrier must follow all BPA regulations
15. BPA must screen incoming cargo as detailed by the container's destination government and determine its security risk
16. BPA must inspect incoming cargo as detailed by the container's destination government if the container is identified as high risk

## *6.2 Synthesis and Break Down of High Level Requirements*

The following are decomposed high level system requirements from section 3.2 that form the basis of the system's low level requirements/specifications:

| High Level Requirement | Detailed Requirements |
|---|---|
| 1 | 1.1 All contents of the package should be listed on the packing list |
| 1 | 1.2 A packing list must contain a single point of origin and a single point of destination |
| 1 | 1.3 The supplier should sign and date the packing list |
| 2 | 2.1 The agreement must specify means of identifying the consolidator. |
| 2 | 2.2 The agreement must specify steps for verifying the packing list |
| 2 | 2.3 The agreement must specify the procedures to follow when packing list isn't verified successfully |
| 3 | 3.1 The BOL should specify the point of origin, contents and final destination of the container. |
| 3 | 3.2 The Supplier, Consolidator or Freight Forwarder sign and date the BOL |
| 4 | 4.1 The facility is secure and well-lit. |

| High Level Requirement | Detailed Requirements |
|---|---|
| 4 | 4.2 The personnel assigned to conduct the inspection should be properly trained |
| 4 | 4.3 The personnel should document the condition of the container. |
| 4 | 4.4 Damaged containers must be removed from service |
| 5 | 5.1 Prior to stuffing, the container must have come from a secure facility |
| 5 | 5.2 The container should be stuffed as per BOL details |
| 5 | 5.3 The container identification number should be specified on the BOL |
| 6 | 6.1 Procedures should be in place to control and affix security seals |
| 6 | 6.2 Only designated employees distribute seals |
| 6 | 6.3 All seals must meat PAS ISO 17712 standards. |
| 6 | 6.4 Seal identification number must be documented on the BOL |
| 7 | 7.1 Procedures should be in place to control access and prevent unauthorized entry |
| 7 | 7.2 Procedures must be in place for reporting and neutralizing unauthorized entry |
| 7 | 7.3 Physical barriers must be installed to prevent unauthorized entry |
| 8 | -NA- |
| 9 | 9.1 Procedures are in place to ensure that all information used in receiving the container is legible, complete, accurate and protected |
| 9 | 9.2 Procedures are in place to ensure that the information received from business partners is reported accurately |
| 9 | 9.3 Procedures should also be established to track the timely movement of incoming and outgoing goods |
| 10 | -NA- |
| 11 | 11.1 Ensure that the pick-up order matches the BOL |

| High Level Requirement | Detailed Requirements |
|---|---|
| 11 | 11.2 Reconcile container against information on the BOL |
| 11 | 11.3 Document that the container has been verified against pick-up order and is in acceptable condition |
| 12 | 12.1 Discrepancies must be documented |
| 12 | 12.2 Discrepancies must be reported to BPA if illegal or suspicious activities are detected |
| 12 | 12.3 Discrepancies must be corrected |
| 13 | -NA- |
| 14 | 14.1 Carrier completes cargo declaration form as detailed by the container's destination government |
| 14 | 14.2 Carrier submits cargo declaration form as detailed by the container's destination government |
| 15 | -NA- |
| 16 | 16.1 BPA coordinates with the Port Authority to inspect the container |
| 16 | 16.2 BPA verifies whether the seal matches the container BOL |
| 16 | 16.3 BPA must break and properly replace the security seal if non-intrusive inspection (NII) is not available |

# 7 Labelled Transition System Analyser

**Finite state machines:** A finite state machine (FSM) or finite state automaton (plural: automata) is a model of behavior composed of a finite number of states, transitions between those states, and actions. A state stores information about the past, i.e. it reflects the input changes from the system start to the present moment. A transition indicates a state change and is described by a condition that would need to be fulfilled to enable the transition.[5]

A FSM can be represented using a state diagram

**Labelled Transition System Analyser (LTSA)**: LTSA is a verification tool for concurrent systems. It checks that the specification of a concurrent system satisfies the properties required of its behavior.

A system in LTSA is modeled as a set of interacting finite state machines. The properties required of the system are also modeled as state machines. LTSA performs compositional reachability analysis to exhaustively search for violations of the desired properties.

Each component of a specification is described as a Labelled Transition System (LTS), which contains all the states a component may reach and all the transitions it may perform. However, explicit description of an LTS in terms of its states, set of action labels and transition relation is cumbersome for other than small systems. Consequently, LTSA supports a process algebra notation (FSP) for concise description of component

[5] http://en.wikipedia.org/wiki/Finite_state_automata

behavior. The tool allows the LTS corresponding to a FSP specification to be viewed graphically.

# 8 MSC

Message sequence charts (MSCs) are mechanisms for specifying scenarios that describe patterns of interactions between processes or objects. It gives us a good visualization of various scenarios in a system.

A MSC is basically a sequence diagram, which shows interaction between different objects, using messages.

We have used MSCs to depict the intended behavior of our system using different scenarios. We will elaborate on how we did this in the following sections.

# 9 MSC Plug-in

The MSC plug-in is an extension to the LTSA, which allows models to be described by graphically editing sets of scenarios in the form of message sequence charts. The LTSA can be used to detect the presence of *implied scenarios* in the system as part of an iterative design process.

The MSC plug-in provides a very easy user interfaces with just the basic blocks required for creating the sequence charts.

There are two main parts to drawing the sequence chart:

1. hMSC – High level MSC
2. bMSC – Base level MSC

The bMSC consists of various objects passing messages to each other creating a scenario each.

The scenarios, when connected together, model the entire system. The hMSC consists of various bMSCs as nodes, connected together to model the entire system.

The particulars of the model for this system are discussed in Section 8.

# 10 Verification using LTSA and MSC Plug-in

We used the MSC Plug-in to model our system as a combination of scenarios.

Since a lot of security checks and documents happen without an interaction between any defined actors in the system, the model of our system will only show the instances (release/receive) in which there are interactions between the actors.

Different scenarios are defined as bMSCs. The actors are modeled as objects and their interactions are modeled as messages passed between the objects.

The bMSCs are linked together to form the hMSC. The bMSCs form the nodes of the hMSC and are connected by directional links showing the various sequences in which the scenarios could possibly occur. The hMSC essentially models the interaction between actions for the entire system.

Our Global Container Security System has 6 Scenarios and so, 6 bMSCs modeling the following behavior:

1. The interaction between the Supplier and the Carrier
2. The interaction between the Carrier and Customer
3. The interaction between the Carrier and the Border Protection Authority
4. The interaction between the Carrier and the Border Protection Authority
5. The interaction between the Port Authority and the Carrier
6. The interaction between the Border Protection Authority and the Carrier

The bMSCs are shown in Appendix B.

We have realized that keeping the scenarios as simple as possible allows you to model the interactions between the scenarios easily.

The hMSC is created by linking the various scenarios in all the possible ways the Container can be moved among various actors.

The hMSC is shown in Appendix B.

The hMSC is compiled in the MSC Plug-in editor. At this point the MSC plug-in allows for the checking of "implied scenarios".

The Architectural model was compiled in the LTSA. This gave the Labelled Transition Systems (LTS) for the individual actors.

Composing the LTS for the actors gave the LTS for the entire system.

The LTS for the actors and the entire system is shown in Appendix C.

## *10.1 Verification methods using LTSA*

At this point we can go ahead and perform various verification methods to the models we created:

**Implied Scenarios:** An architecture model can be very close in behavior explicitly described in a positive MSC specification. But, it is possible that in some cases this is not possible and that for some MSC specifications all architecture models of the specification exhibit traces that have not been specified in the MSC specification. Moreover, as discussed further on, these traces are particularly interesting as they uncover important

gaps of the partial system description that should [6] be elaborated. These traces are called "implied scenarios". These implied scenarios can be categorized as positive or negative depending on the nature of the trace using the MSC plug-in.

Our system doesn't have any implied scenarios; most probably because of the simplistic model defined. Moreover, the plug-in doesn't allow to explicitly define any "negative" scenarios.

**Deadlocks:** A system is said to be "deadlocked" when two or more processes in the system are waiting for each other to release resources and neither does.

LTSA provides a tool to check for deadlocks. We find that our system doesn't deadlock. The screen print showing this is attached in Appendix XX. This result is as we expect, because we know that given the practicality and the economics involved in our system, it would never deadlock

**Liveness / Progress[7]:** A system is said to exhibit the "Liveness" property if something good eventually happens. LTSA disregards temporal logic to specify Liveness and deals with a restricted class of Liveness properties called "Progress". A progress property asserts that whatever state a system is in, it is always the case that a specified action will eventually be executed.

[6] Incremental Elaboration of Scenario-Based Specifications and Behaviour Models Using Implied Scenarios by Sebastian Uchitel

[7] Magee, Jeff, and Jeff Kramer. Concurrency: State Models & Java Programs. 2nd ed. Vol. 1. West Sussex, England: John Wiley and Son Ltd, 2006. 1-407

LTSA provides a tool to check for Progress. As shown by the screen-print in Appendix C, the system shows progress violation for a sequence of actions. These actions are the unlimited number of loops between the Carrier, the BPA and the Port Authority. Again, given the system and the economics of the system under check, the Progress property will never be violated in a real-life scenario.

# 11 Future Work and Recommendations

1. Create an LTS to verify whether you get the same LTS for the actors as derived from the MSC Plug-in automatically – this wasn't done this semester due to time constraints.
2. Incorporate attacker scenario
3. Incorporate "un-sealable containers"
4. Incorporate variations for changes in security levels
5. Incorporate most recent system tool development
6. Differentiate country specific regulations
7. Drill down to explicit threats

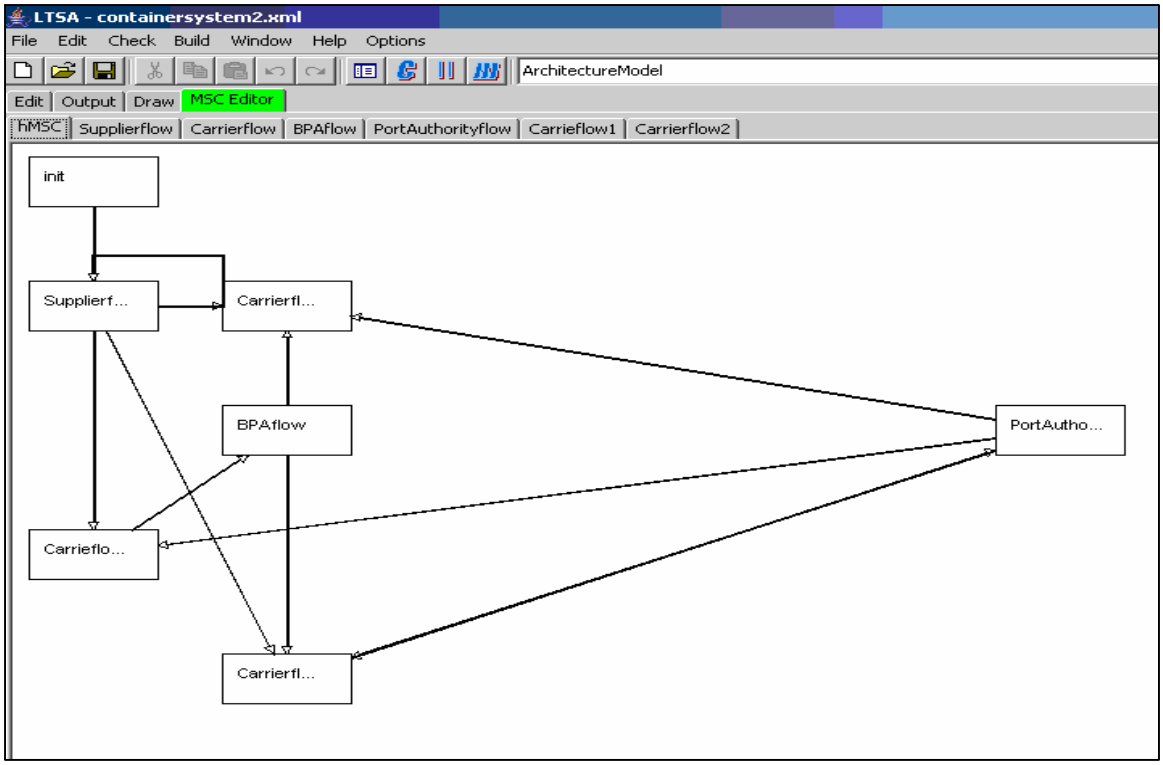
# 8. Appendix A – Traceability Matrix

The following traceability matrix maps both high level and detailed requirements to related use cases.

| Requirement | | Use Case | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | UC01 | UC02 | UC03 | UC04 | UC05 | UC06 | UC07 | UC08 | UC09 | UC10 | UC11 | UC12 | UC13 |
| 1 | | * | | | | | | | | | | | | |
| | 1.1 | * | | | | | | | | | | | | |
| | 1.1.1 | * | | | | | | | | | | | | |
| | 1.2 | * | | | | | | | | | | | | |
| | 1.3 | * | | | | | | | | | | | | |
| 2 | | | * | | | | | | | | | | | |
| | 2.1 | | * | | | | | | | | | | | |
| | 2.2 | | * | | | | | | | | | | | |
| | 2.3 | | * | | | | | | | | | | | |
| 3 | | | | * | | | | | | | | | | |
| | 3.1 | | | * | | | | | | | | | | |
| | 3.2 | | | * | | | | | | | | | | |
| 4 | | | | | * | | | | | | | | | |
| | 4.1 | | | | * | | | | | | | | | |
| | 4.2 | | | | * | | | | | | | | | |
| | 4.3 | | | | * | | | | | | | | | |
| | 4.4 | | | | * | | | | | | | | | |
| 5 | | | | | | * | | | | | | | | |
| | 5.1 | | | | | * | | | | | | | | |
| | 5.2 | | | | | * | | | | | | | | |
| | 5.3 | | | | | * | | | | | | | | |
| 6 | | | | | | | * | | | | | | | |
| | 6.1 | | | | | | * | | | | | | | |
| | 6.2 | | | | | | * | | | | | | | |
| | 6.3 | | | | | | * | | | | | | | |
| | 6.4 | | | | | | * | | | | | | | |
| 7 | | | | | | | | * | | | | | | |
| | 7.1 | | | | | | | * | | | | | | |
| | 7.2 | | | | | | | * | | | | | | |
| | 7.3 | | | | | | | * | | | | | | |
| 8 | | | | | | | | * | | | | | | |
| 9 | | | | | | | | | * | | | | | * |
| | 9.1 | | | | | | | | * | | | | | * |
| | 9.2 | | | | | | | | * | | | | | * |
| | 9.3 | | | | | | | | * | | | | | * |
| 10 | | | | | | | | | * | | | | | * |
| 11 | | | | | | | | | * | | | | | * |
| | 11.1 | | | | | | | | * | | | | | * |
| | 11.2 | | | | | | | | * | | | | | * |
| | 11.3 | | | | | | | | * | | | | | * |
| 12 | | | | | | | | | * | | | | | * |
| | 12.1 | | | | | | | | * | | | | | * |
| | 12.2 | | | | | | | | * | | | | | * |
| | 12.3 | | | | | | | | * | | | | | * |
| 13 | | | | | | | | | | * | | | | |
| 14 | | | | | | | | | | | * | | | |
| | 14.1 | | | | | | | | | | * | | | |
| | 14.2 | | | | | | | | | | * | | | |
| 15 | | | | | | | | | | | | * | | |
| 16 | | | | | | | | | | | | | * | |
| | 16.1 | | | | | | | | | | | | * | |
| | 16.2 | | | | | | | | | | | | * | |
| | 16.3 | | | | | | | | | | | | * | |

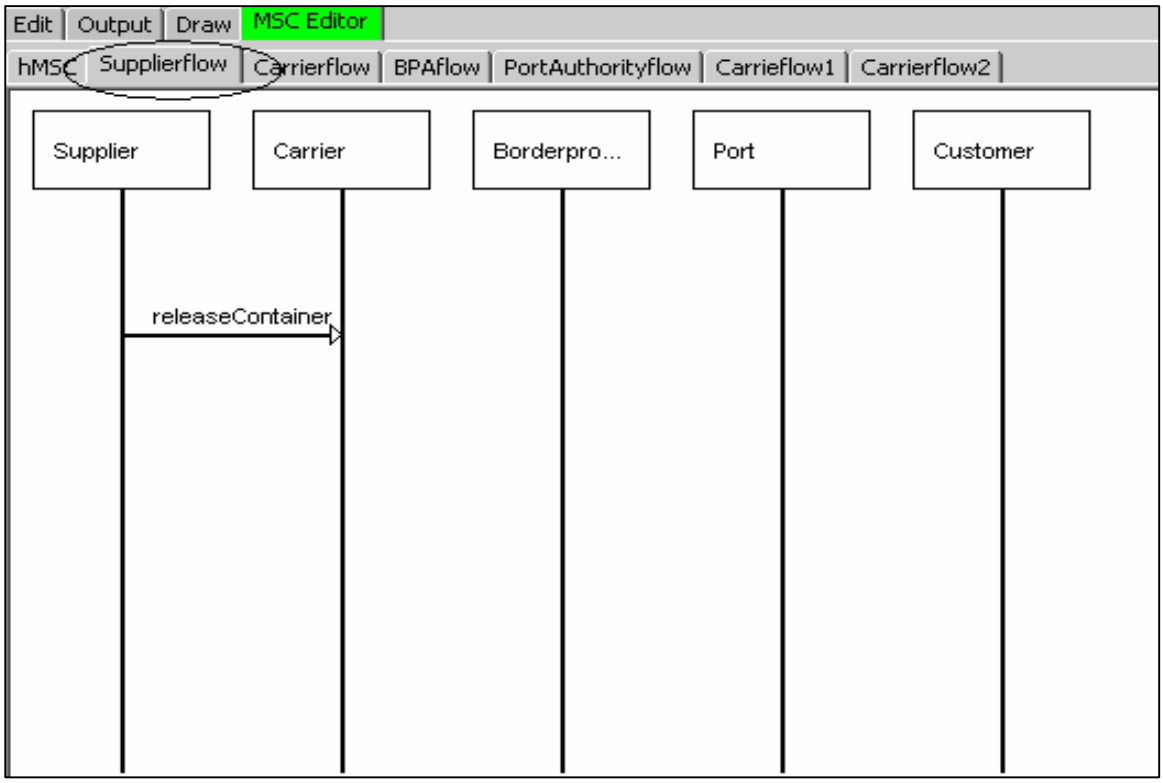
# 9. APPENDIX B: MSC diagrams

## *a. hMSC diagram*

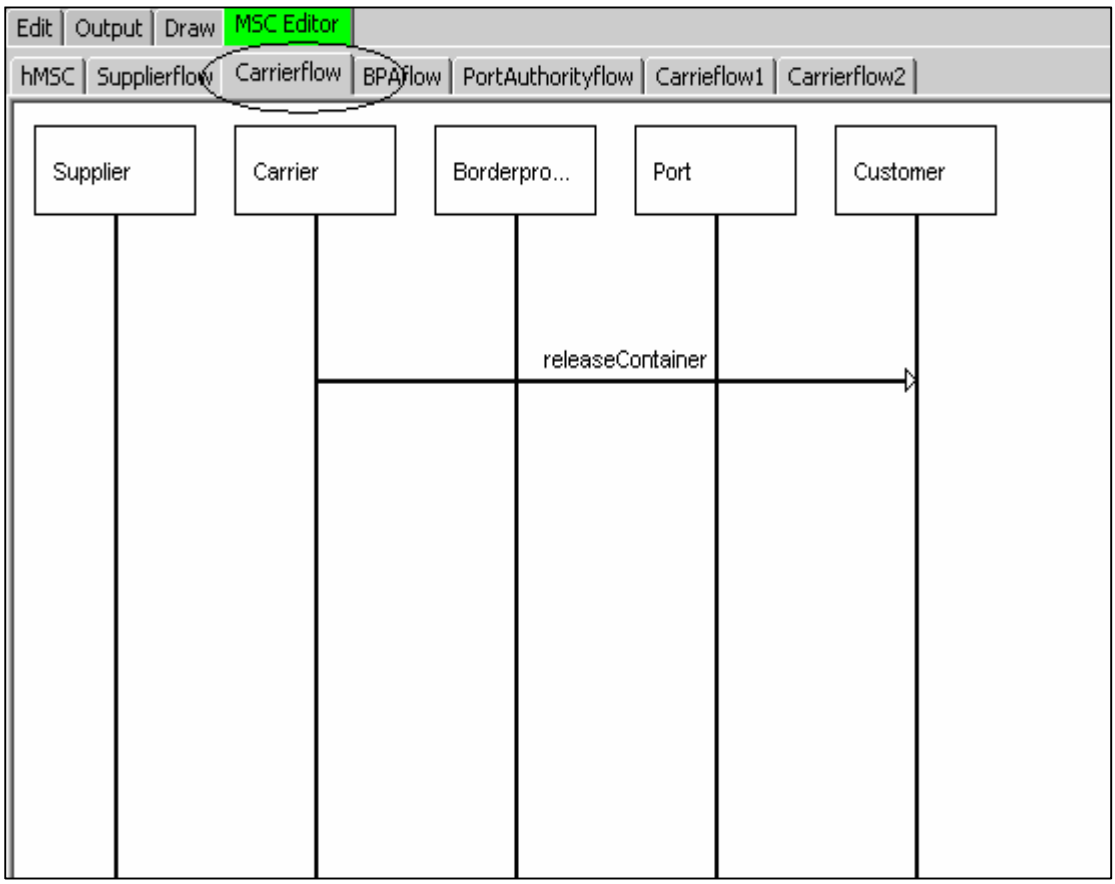


## *b. bMSC diagrams*

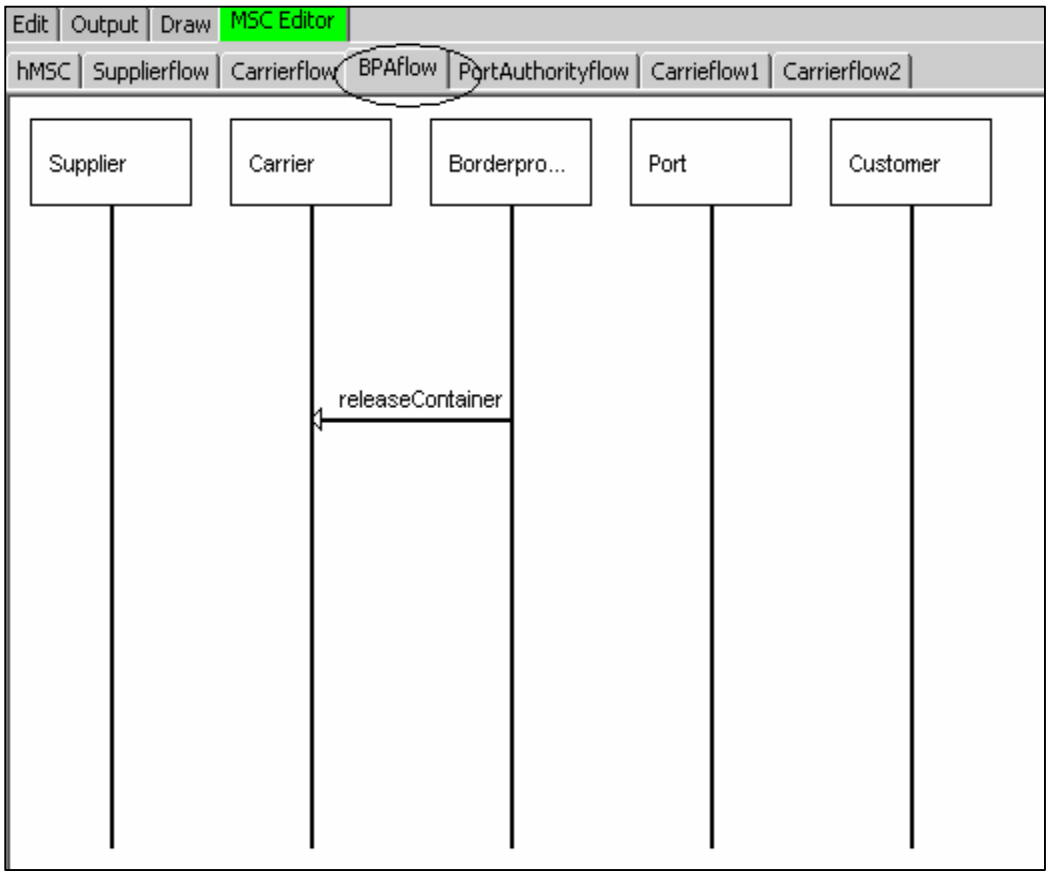
**SUPPLIER TO CARRIER**



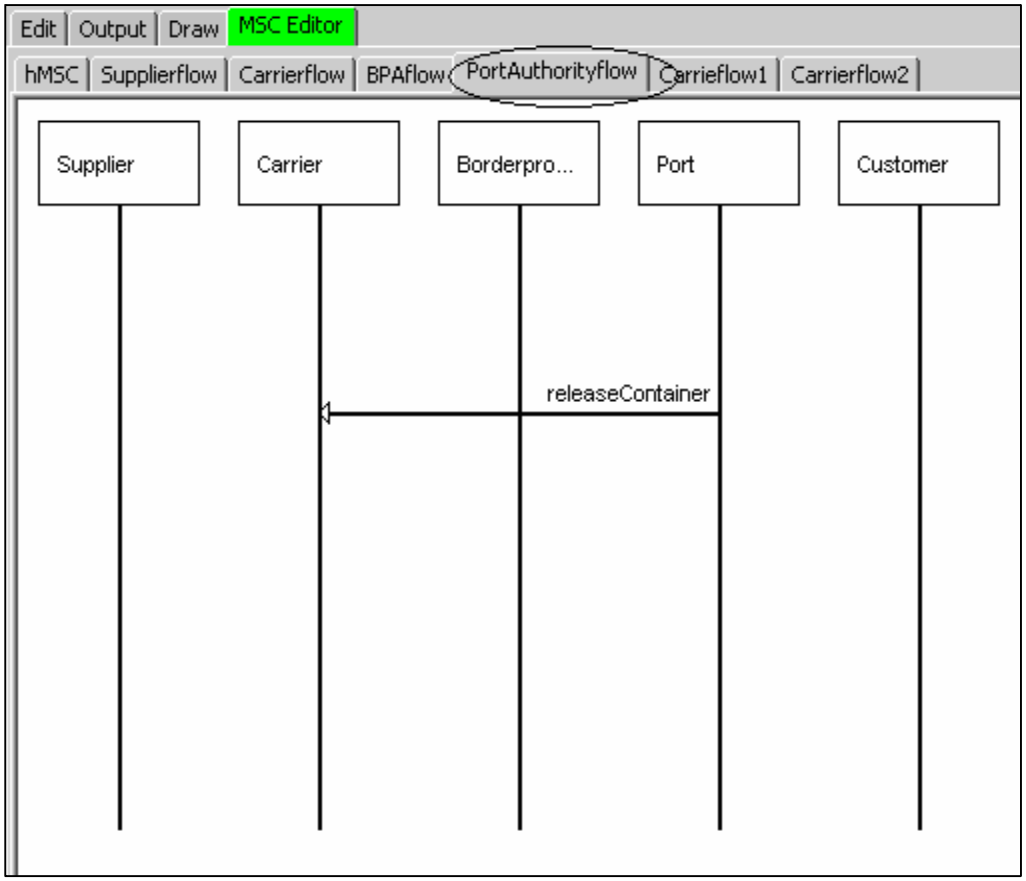
**CARRIER TO CUSTOMER**



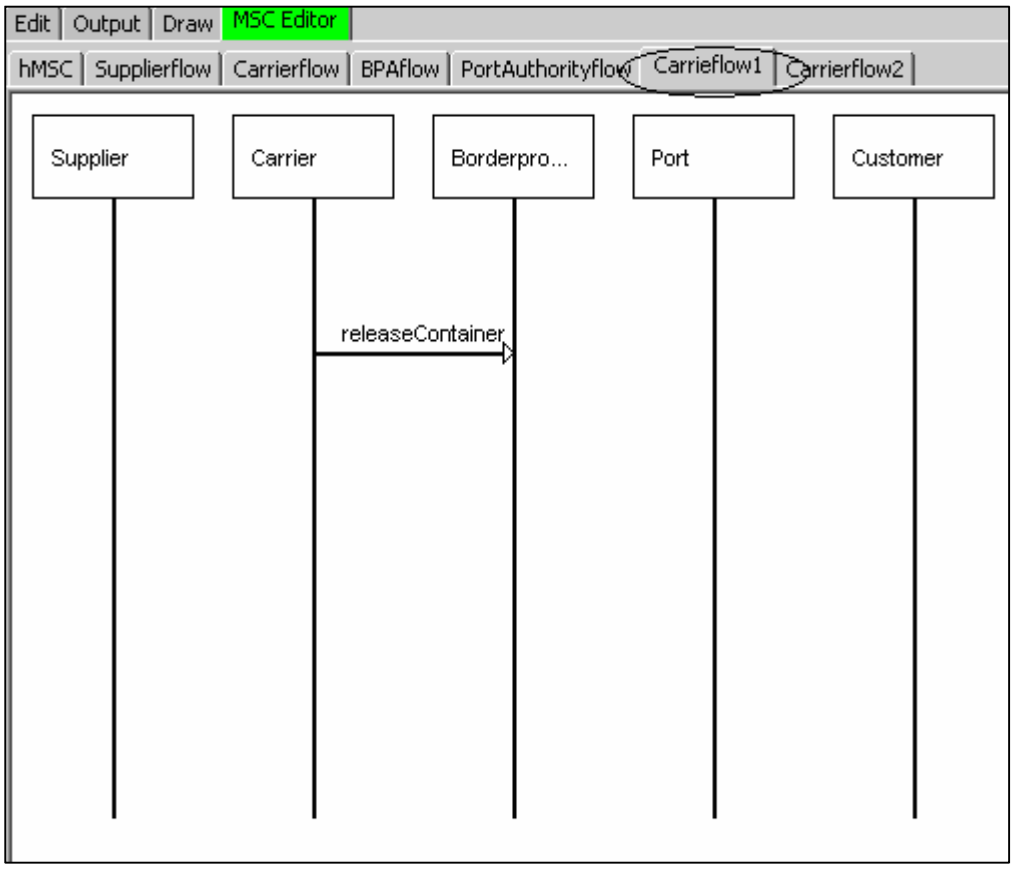
**BORDER PROTECTION AGENCY TO CARRIER**



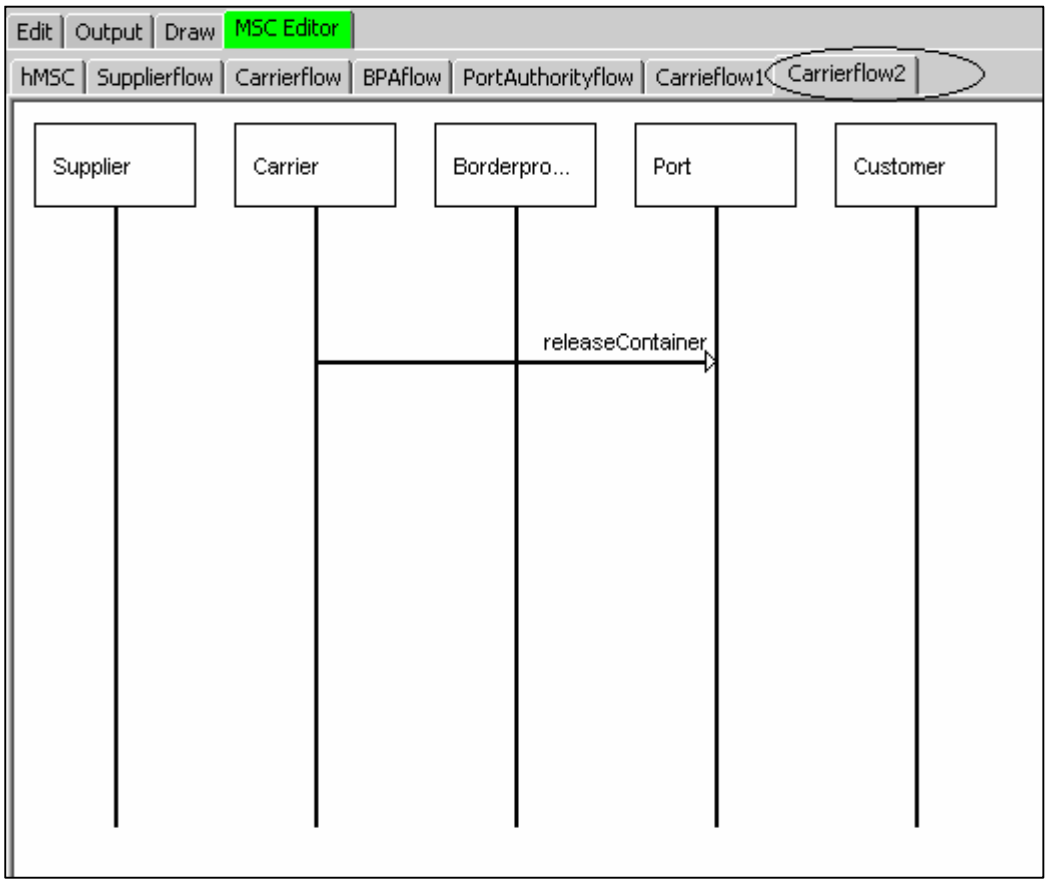
**PORT AUTHORITY TO CARRIER**



**CARRIER TO BORDER PROTECTION AGENCY**

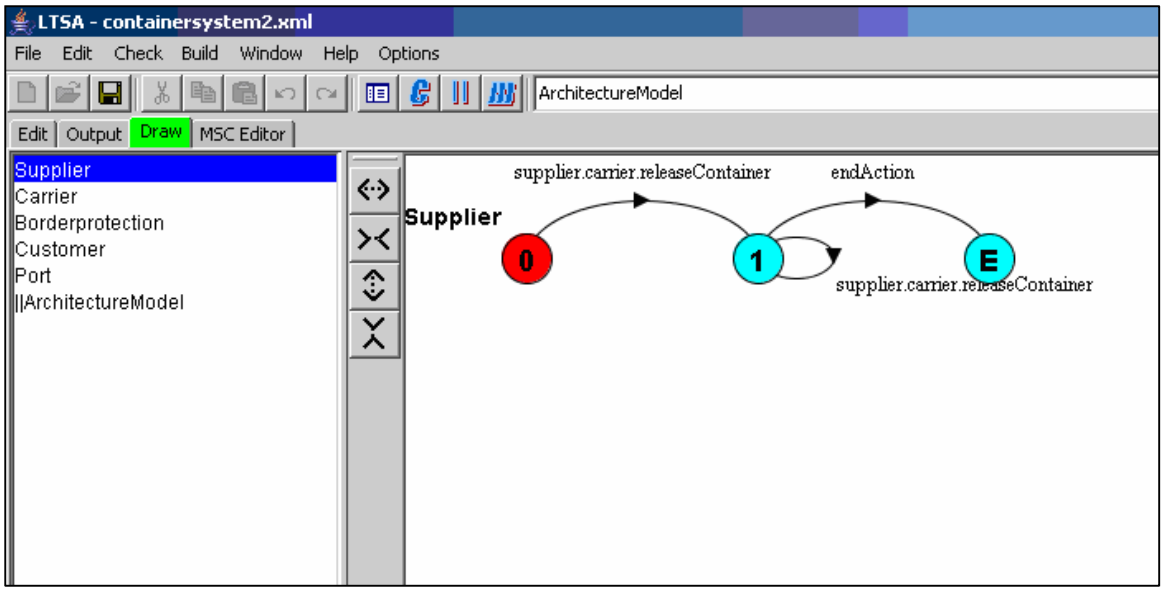


**CARRIER TO PORT**

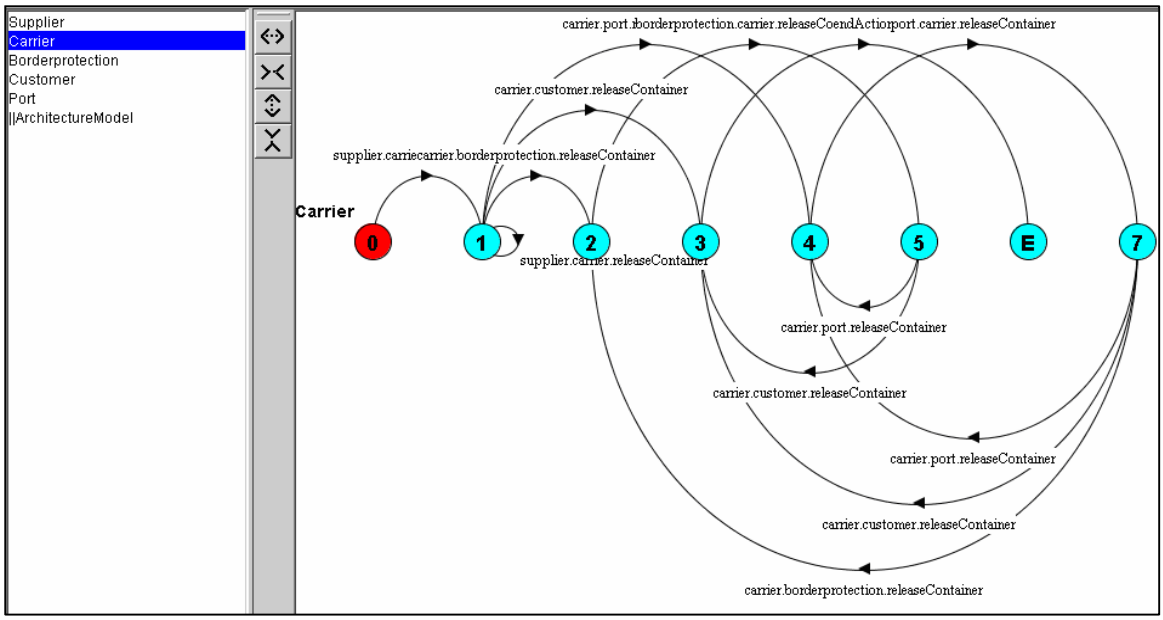


# 10. APPENDIX C LTSA diagrams

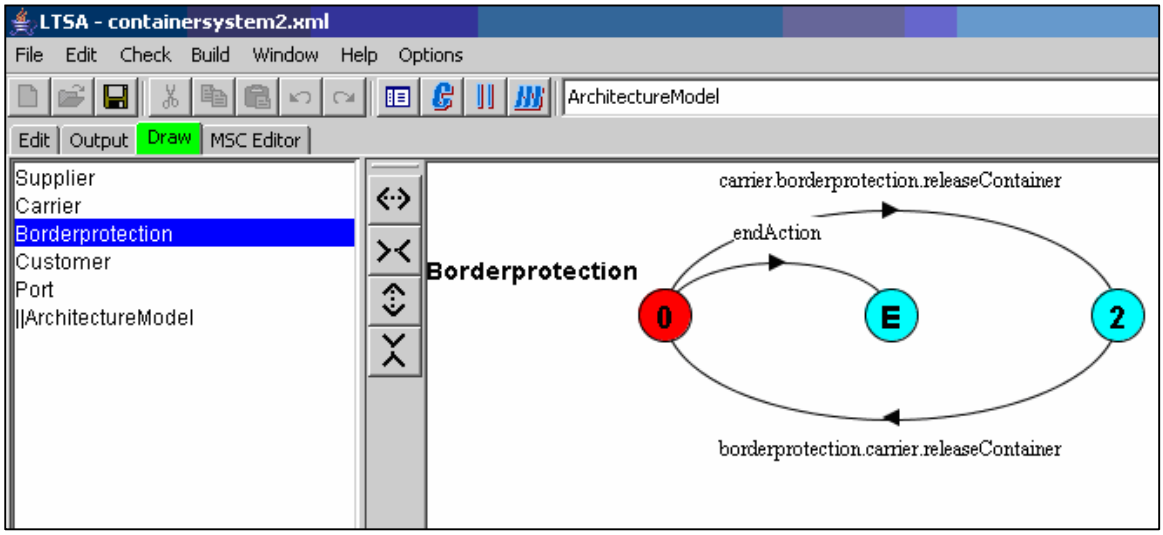
**SUPPLIER LTS**



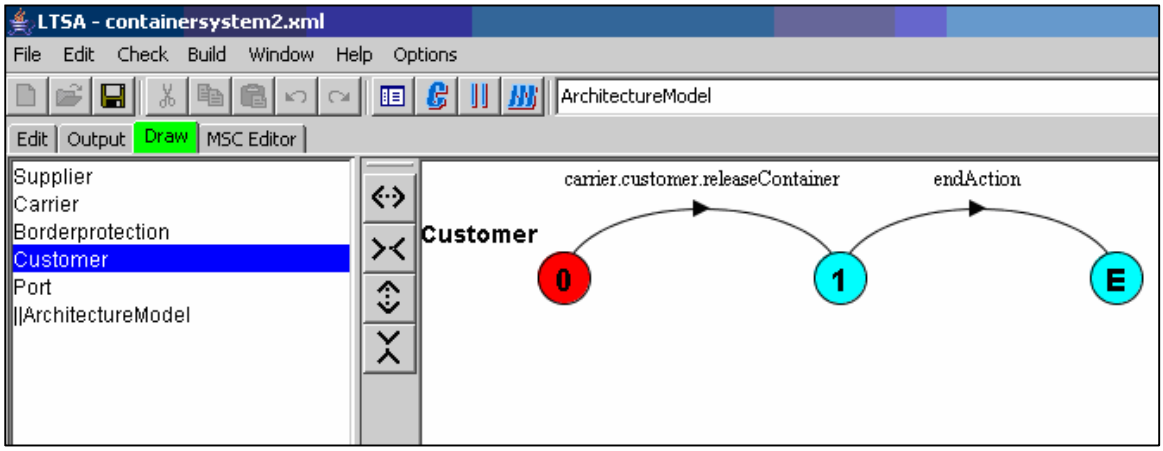
## CARRIER LTS


Supplier
Carrier
Borderprotection
Customer
Port
||ArchitectureModel
carrier.port.iborderprotection.carrier.releaseCoendActionport.carrier.releaseContainer
carrier.customer.releaseContainer
supplier.carriecarrier.borderprotection.releaseContainer
Carrier
0
1
2
3
4
5
E
7
supplier.carrier.releaseContainer
carrier.port.releaseContainer
carrier.customer.releaseContainer
carrier.port.releaseContainer
carrier.customer.releaseContainer
carrier.borderprotection.releaseContainer

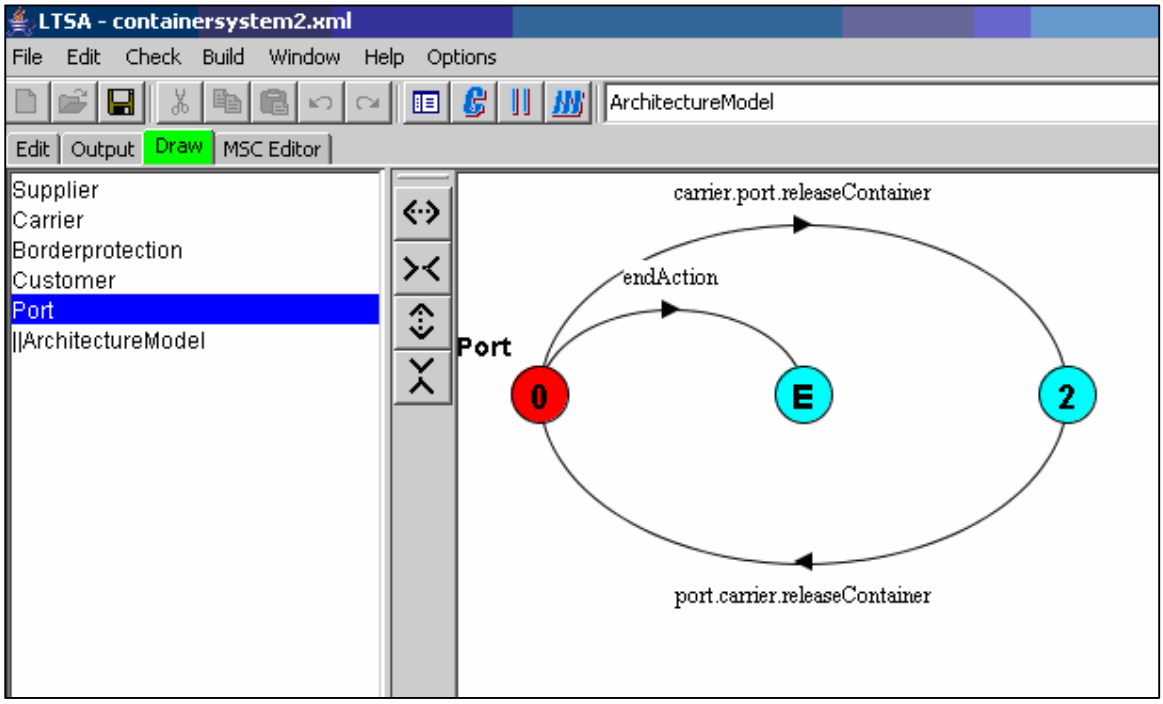
**BORDER PROTECTION AGENCY LTS**



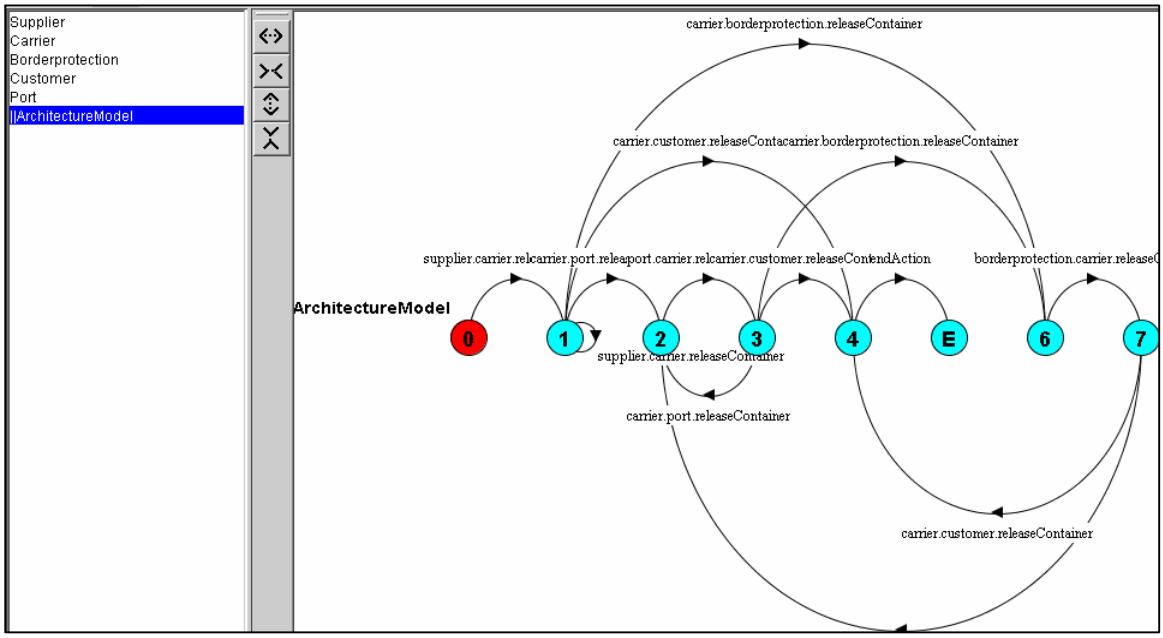
**CUSTOMER LTS**



**PORT LTS**


LTSA - containersystem2.xml
File Edit Check Build Window Help Options
ArchitectureModel
Edit Output Draw MSC Editor
Supplier
Carrier
Borderprotection
Customer
Port
||ArchitectureModel
carrier.port.releaseContainer
endAction
Port
0
E
2
port.carrier.releaseContainer

## ARCHITECTURAL MODEL - LTS



# 12 Appendix D - References


1. "CSI in Brief." Container Security Initiative. United States Customs and Border Protection. 1 Oct. 2006 <http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml>.
2. "Customs-Trade Partnership Against Terrorism (C-TPAT): Partnership to Secure the Supply Chain." C-TPAT. United States Customs and Border Protection. 1 Oct. 2006 <http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml>.
3. "Glossary of Shipping Terms." Maritime Administration. 5 Oct. 2004. Department of Transportation. 1 Oct. 2006 <http://www.marad.dot.gov/Publications/glossary/A.html>.
4. Magee, Jeff, and Jeff Kramer. Concurrency: State Models & Java Programs. 2nd ed. Vol. 1. West Sussex, England: John Wiley and Son Ltd, 2006. 1-407.
5. Report on Container Transport Security Across Modes. Organization for Economic Co-operation and Development. 2004. 1-10. 1 Oct. 2006 <http://www.oecd.org/dataoecd/29/8/31839546.pdf>.
6. "Supply Chain Security Glossary." Retail Leaders, Leaders Association. 1 Oct. 2006 <http://rila.interactive.biz/scs_glossary.htm>.

7. United States. Central Intelligence Agency. Foreign Missile Developments and the Ballistic Missile Threat Through 2015: Unclassified Summary of a National Intelligence Estimate. 2002. 1 Oct. 2006 <http://www.cia.gov/nic/pubs>.