GLOBAL SECURITY SYSTEM FOR CONTAINERIZED COMMERCE

- ENSE623
  System Engineering Design Project
  Fall 2006
  Professor: Dr. Mark Austin

- Sana Shaikh and Jason Smith

- December 5, 2006

History

- The events of September 11th sparked immediate attention to aspects of our society which appeared vulnerable to future attack.
- Containerized commerce or intermodalism presented one of the greatest risks due to the following;
  - most often unrevealed (type and source),
  - is transported quickly,
  - and is completely global
- In order to mitigate the risks international and national regulations and security tools were/are urgently needed.

Project Goals

- With increased complexity of today's transportation system and high tech security tools 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:
  - 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.
  - from the models developed and governmental regulatory feedback/studies a list of requirements and specifications of a secure system will be created and mapped.
  - 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.

Motivation

- 90% of the world's goods are transported by containerized commerce
- If a containerized commerce is tracked and its contents are monitored using the correct metrics, the overall security of international transportation will increase, despite the cost of the system

Source: http://ken.mit.edu/images/posters/8.pdf

Requirement Collection

- **USCG Headquarters**
  LCDR Michael Dolan
  Cargo & Facilities Division
- **Port Of Baltimore**
  Melvin P. Jackson
  Senior Security Specialist

Container Types

- Dry Freight Container - used for goods that are not affected by most weather conditions such as clothing, automobiles, etc.
- Insulated Containers - used for goods that are weather sensitive such as electronics and foods but do not require refrigeration.
- Refrigerated Containers - used for goods that must remain at specific temperature and humidity levels such as frozen foods, perishable foods, and medicine.
- Open Top, Flat Rack, or Platform Containers - used for goods that require very little protection from the elements and may or may not be oversized such as gravel, waste, airplane wing, etc..

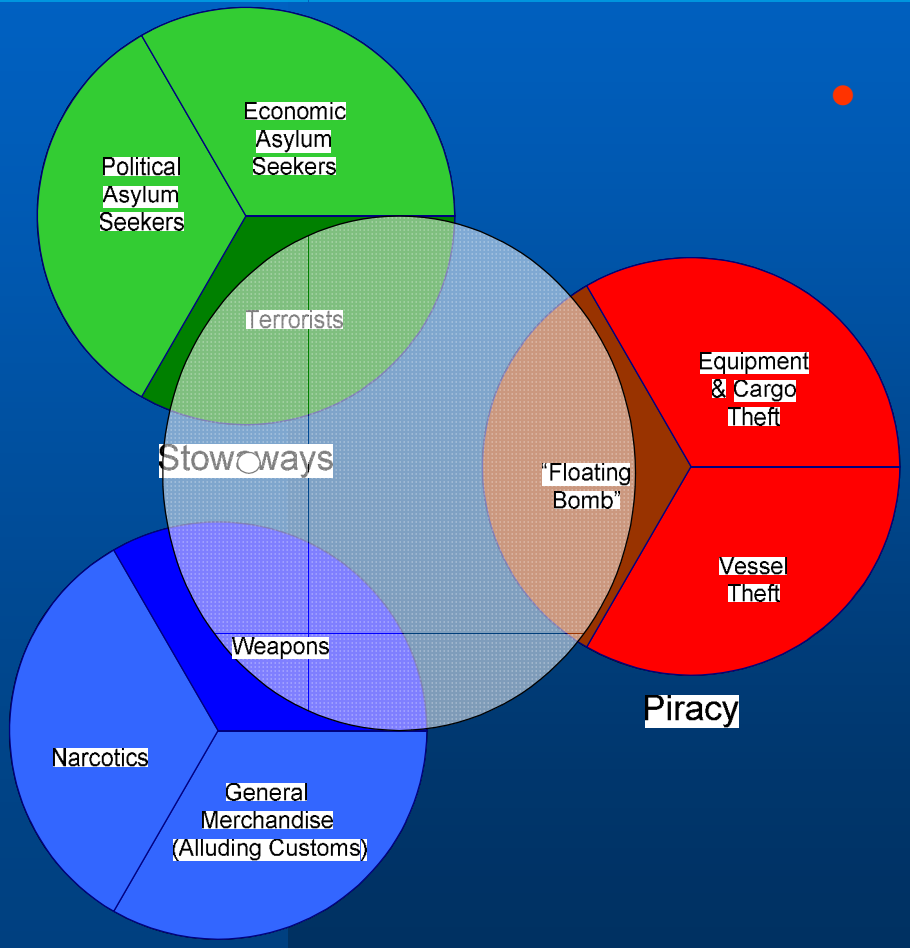
Source: http://ken.mit.edu/images/posters/8.pdf

Framework and Limitations

- **Framework: 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 for**
  - empty or loaded containers,
  - all modes of transportation, and
  - any iteration of carrier to port interface.

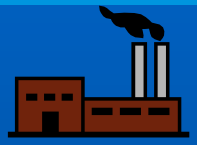
- **Limitations: The following scenarios have been omitted from the analysis due to available information and time constraints.**
  - Use of container other than "sealable containers".
  - Containers without means to seal (ie. open top, flat rack, and platform containers) have not been specifically addressed.
  - Presence of inter-governmental agreements (ie. NAFTA, EU, etc.) that precede international and national security regulations (ie. ISPS & MTSA)
  - Variations for changes in security levels
  - Attacker scenario

Boundary

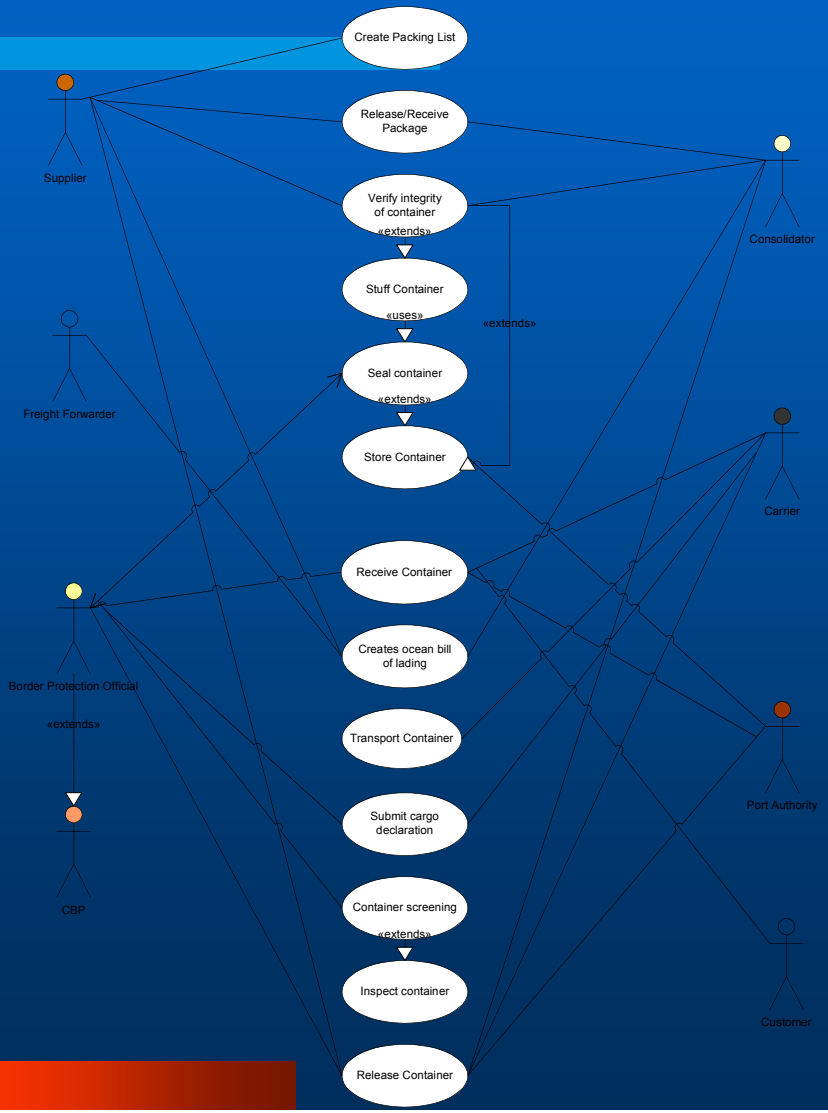


- **Boundary: Since it is only a high level representation it does not include specific use case details. In order to allow modularity, the use cases represent commonalities throughout varying types of carriers and national requirements. The scope is limited only to the security aspects of container 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.**

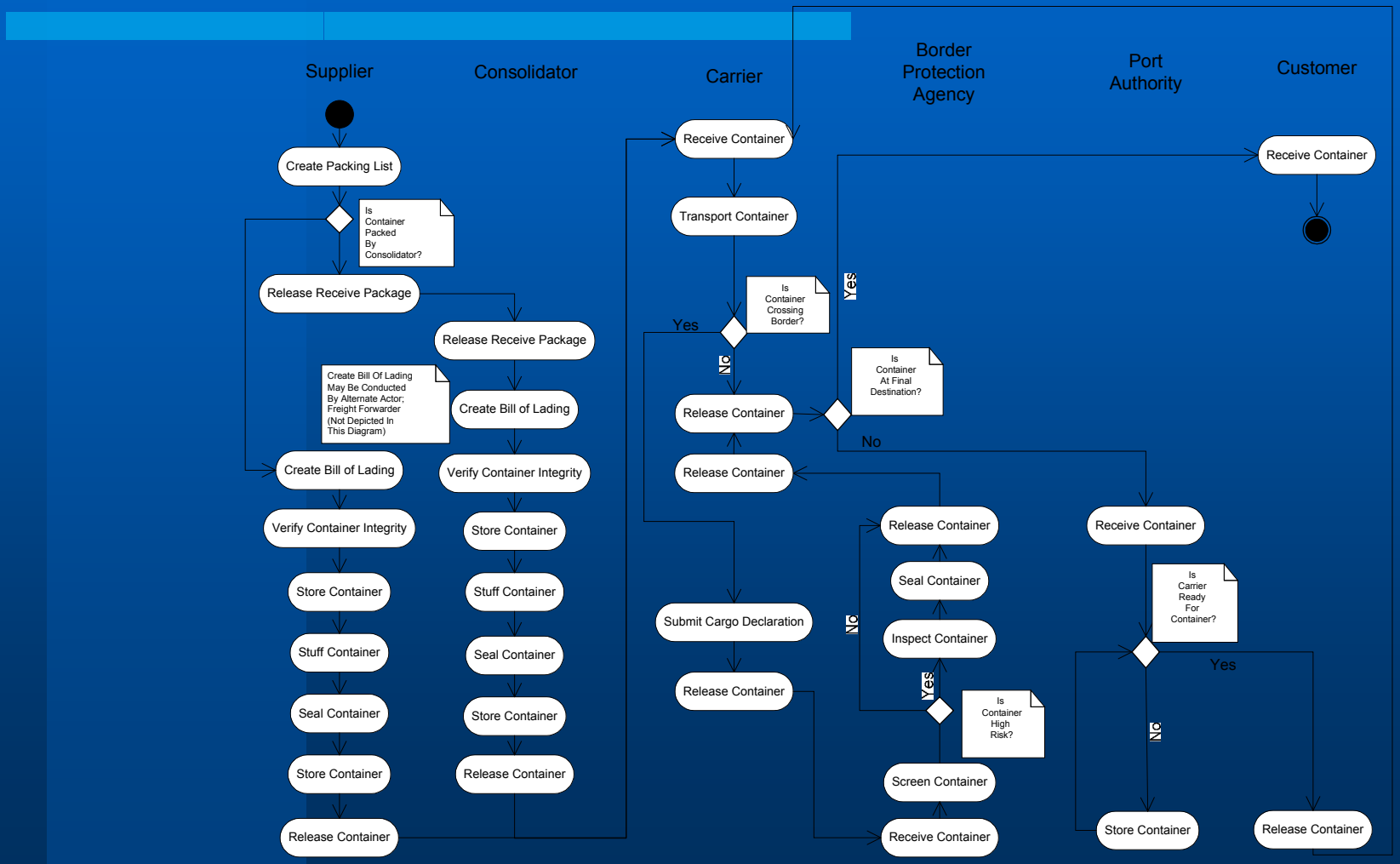
Use Case; Actors

- Supplier 
- Carrier   
- Port Authority 
- Border Protection Official 
- Customer 

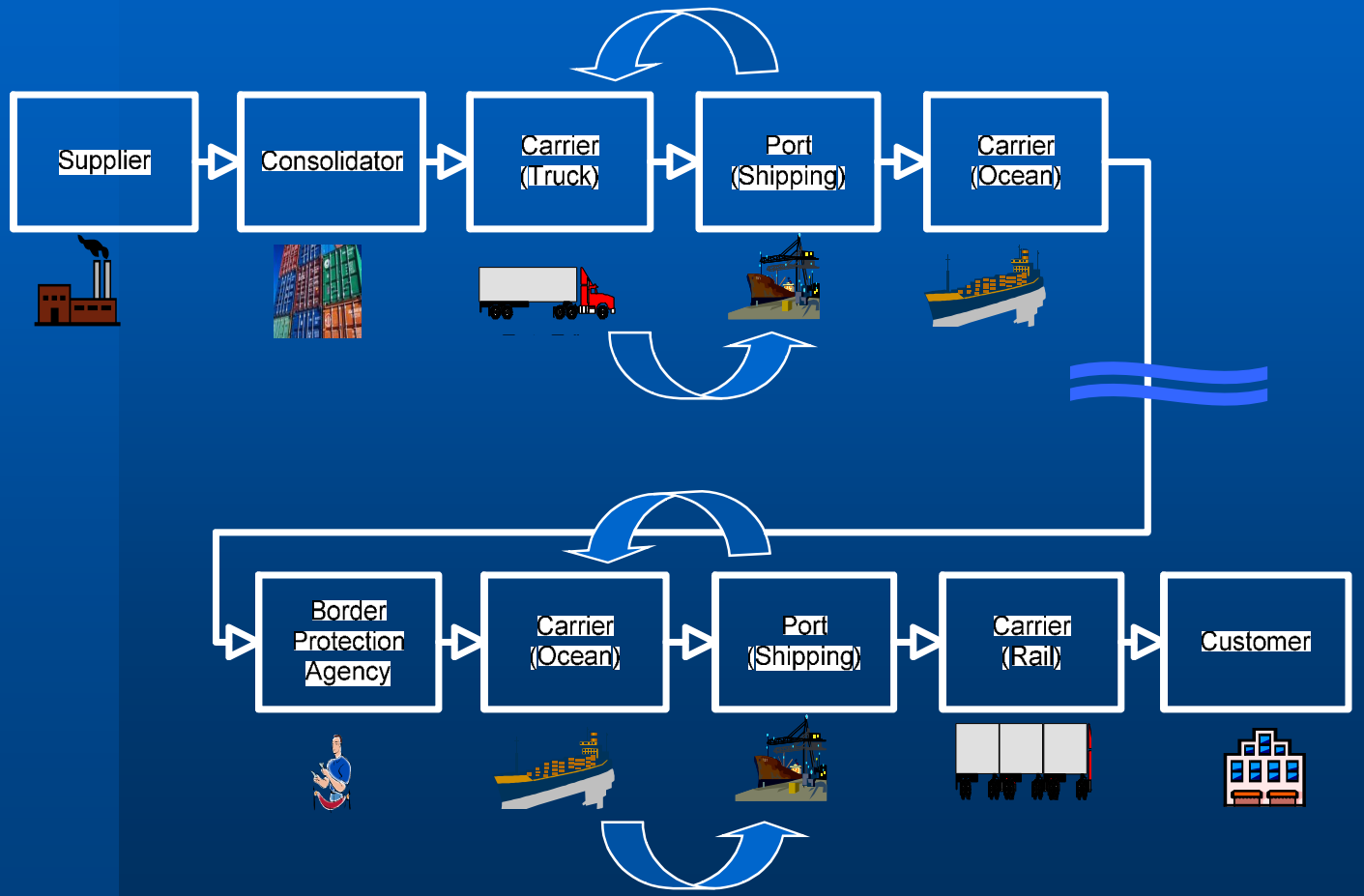
High Level Use Case Diagram



High Level Activity Diagram



Basic Scenario



Goal

- **Ensure security throughout the lifecycle of containerized commerce.**

High Level Requirements

- At least one packing list should be created for every container
- If a supplier uses a consolidator, there must be a legal agreement between the supplier and the consolidator
- The Supplier, Consolidator or Freight Forwarder creates the Bill of Lading (BOL)
- The container is verified in a facility appropriate to enable container inspections
- When stuffing the container, security must be maintained
- All stuffed containers must be sealed
- Storage and transport facilities for containers must be secure
- Document the storage details of the container
- Procedures are in place to ensure that the information is accurate
- The parties releasing and receiving the container must be positively identified
- Container documentation must be verified
- All discrepancies must be addressed prior to receiving or releasing container
- The carrier must securely transports the container to its destination
- The carrier must follow all BPA regulations
- Incoming cargo as detailed by the container's destination government and determine its security risk
- Incoming cargo as detailed by the container's destination government if the container is identified as high risk

Traceability Matrix

Requirement		Use Case												
		01	02	03	04	05	06	07	08	09	10	11	12	13
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												*	

Verification using LTSA

- LTSA is a verification tool for concurrent systems. It mechanically checks that the specification of a concurrent system satisfies the properties required of its behavior. In addition, LTSA supports specification animation to facilitate interactive exploration of system 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. More formally, 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.

Source: http;//www.doc.ic.ac.uk/ltsa

MSC Plug-in

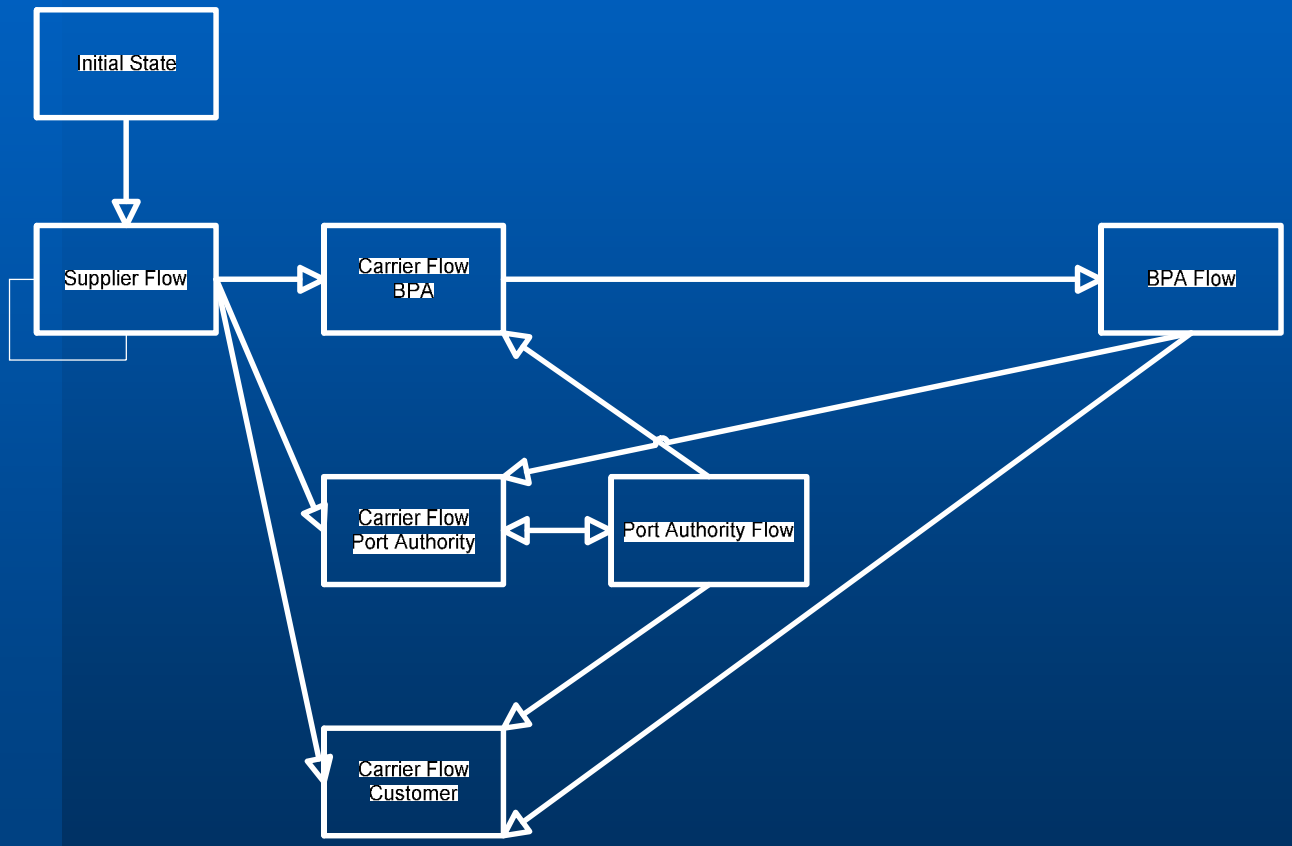
- The MSC plug-in is an extension to the Labeled Transition System Analyzers (LTSA) which allows models to be described by graphically editing sets of scenarios in the form of message sequence charts. The LTSA can be used to detect the presence of *implied scenarios* in the system as part of an iterative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

Source: http;//www.doc.ic.ac.uk/ltsa/msc

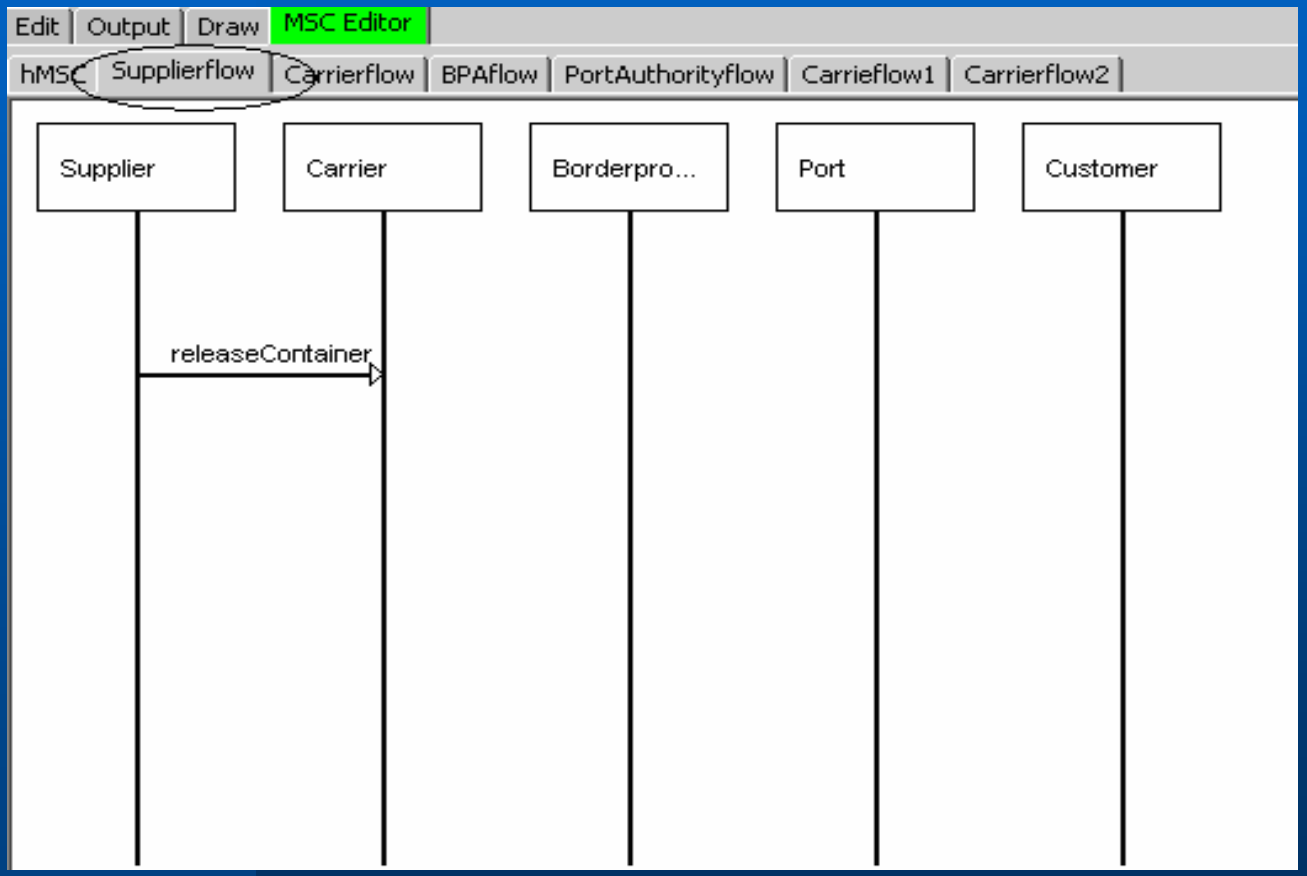
Message Sequence Charts

- Scenario-based specifications
- hMSC– high level Message Sequence Chart
- bMSC– base Message Sequence Chart

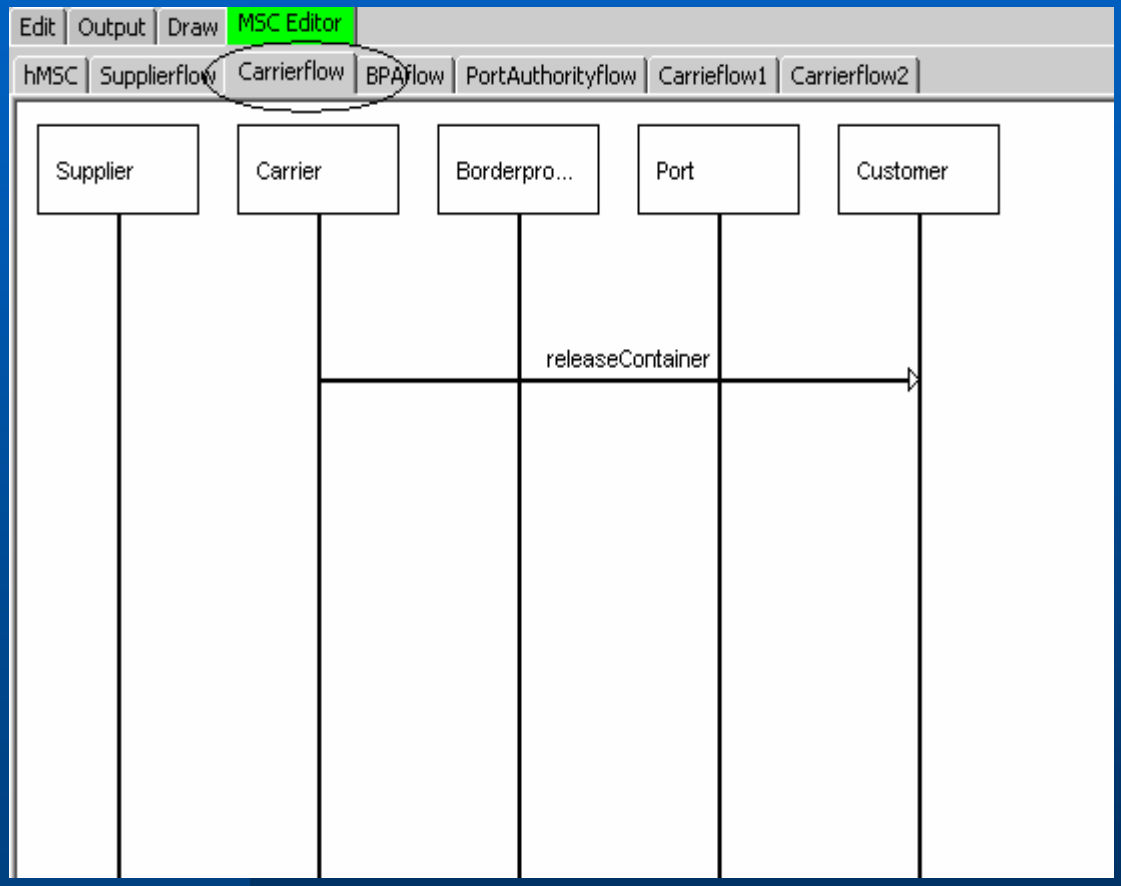
High Level MSC



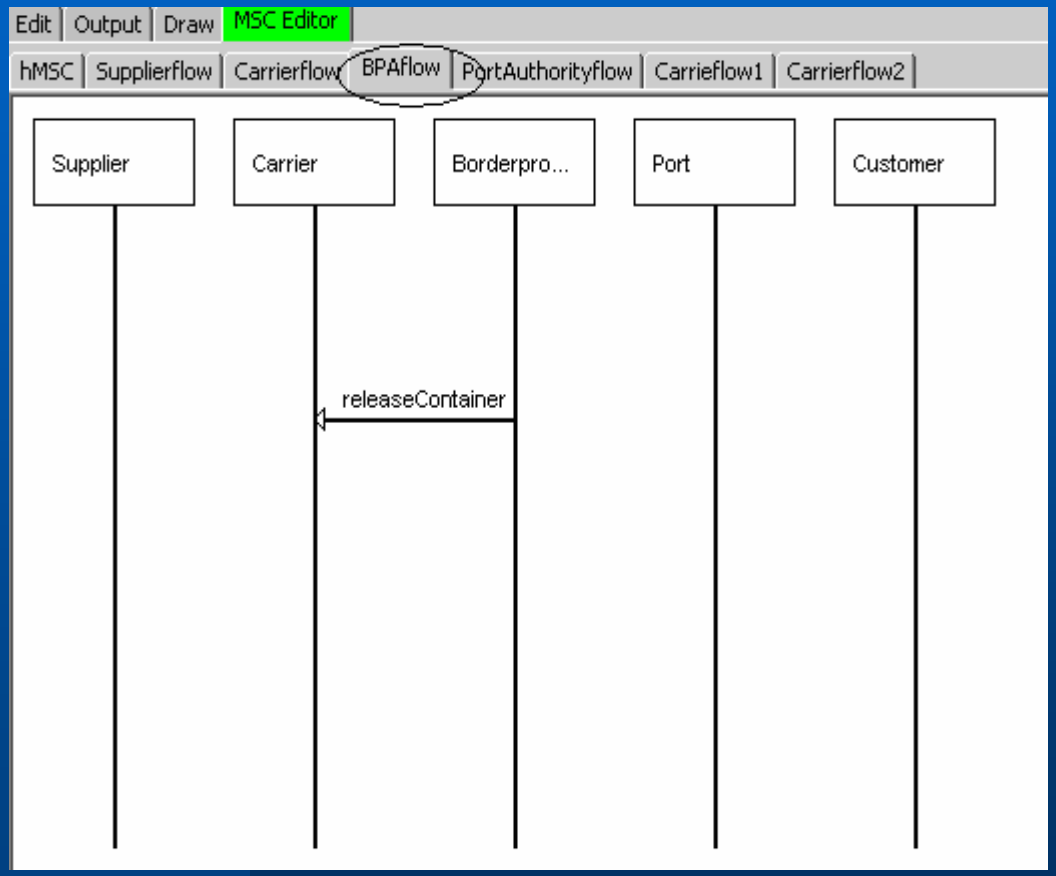
Supplier bMSC



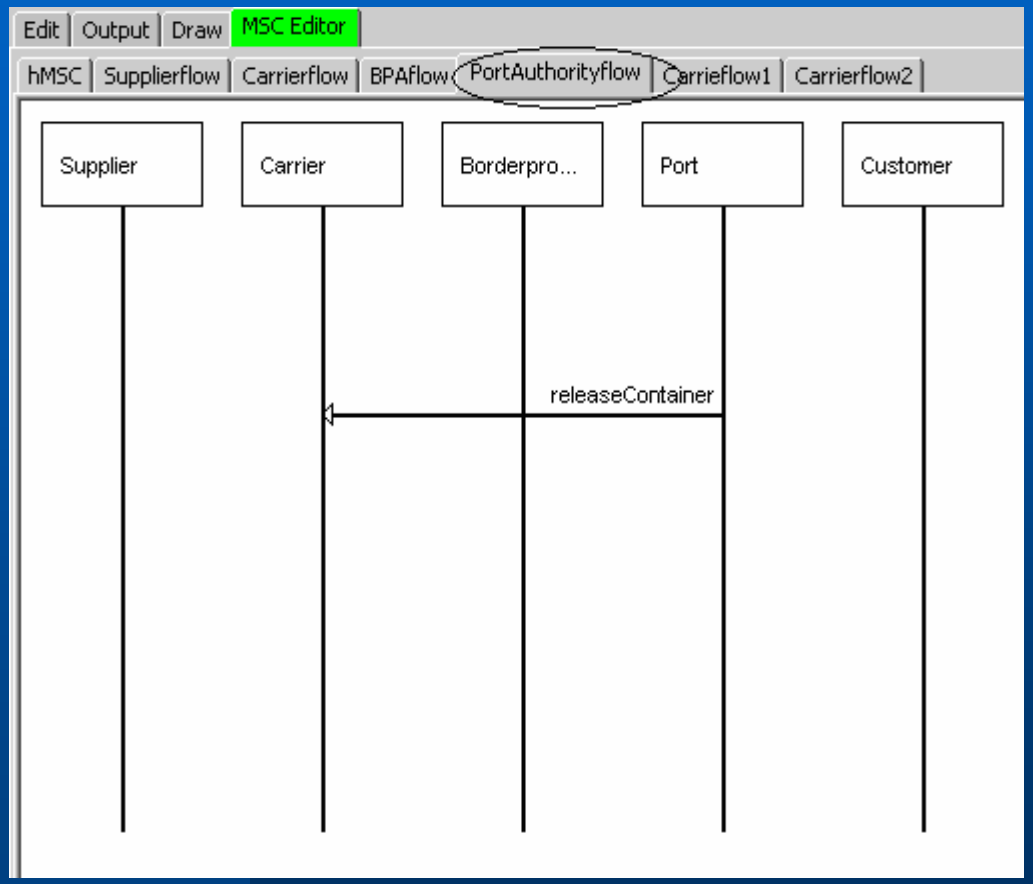
Carrier to Customer bMSC



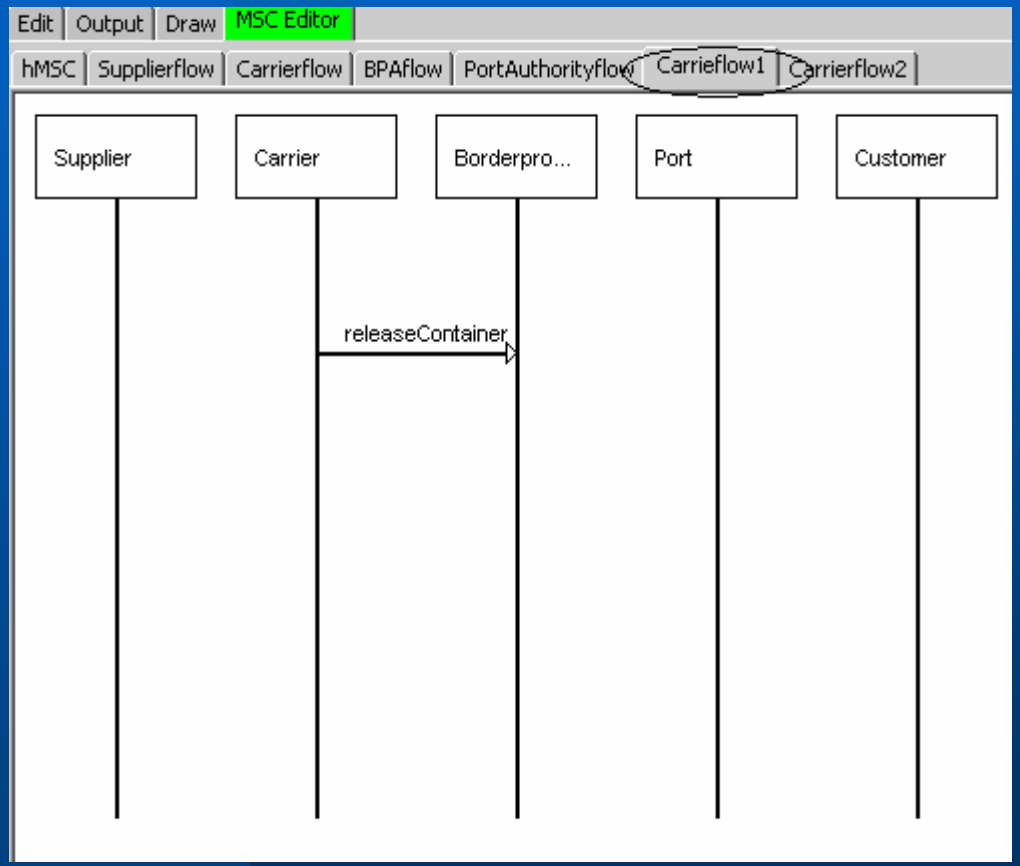
Border Protection to Carrier bMSC



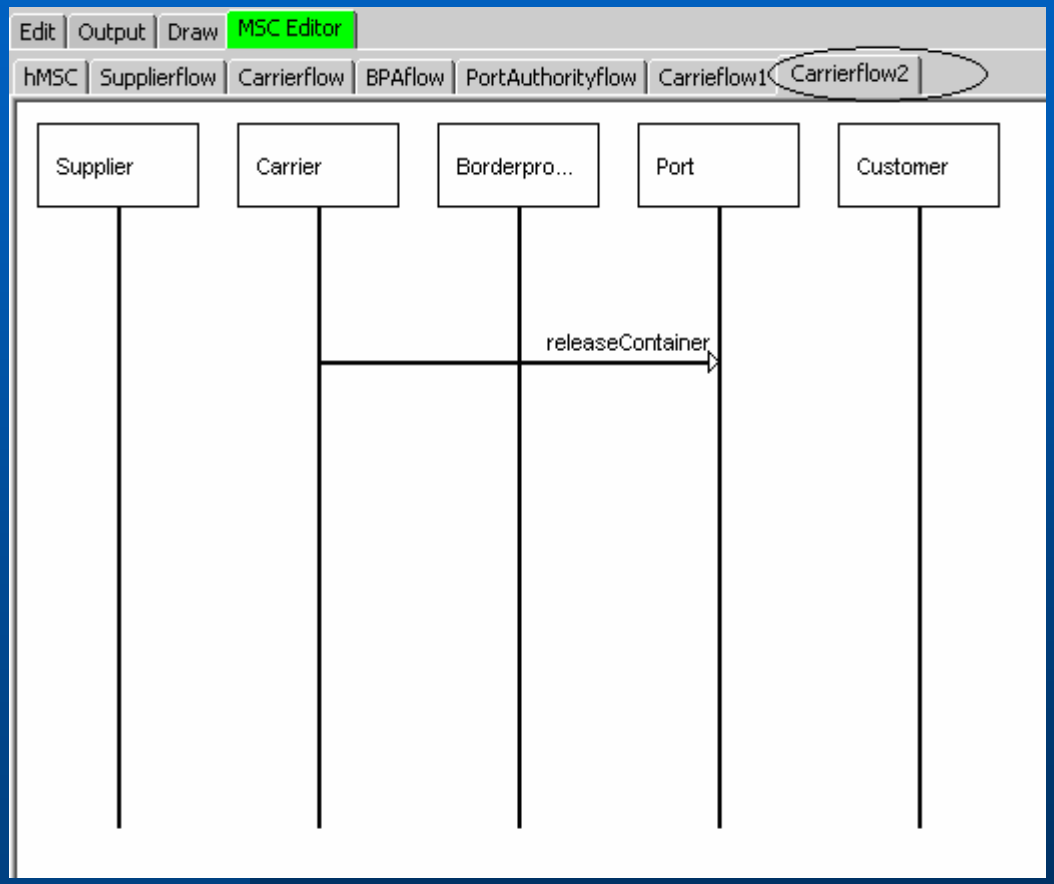
Port Authority to Carrier bMSC



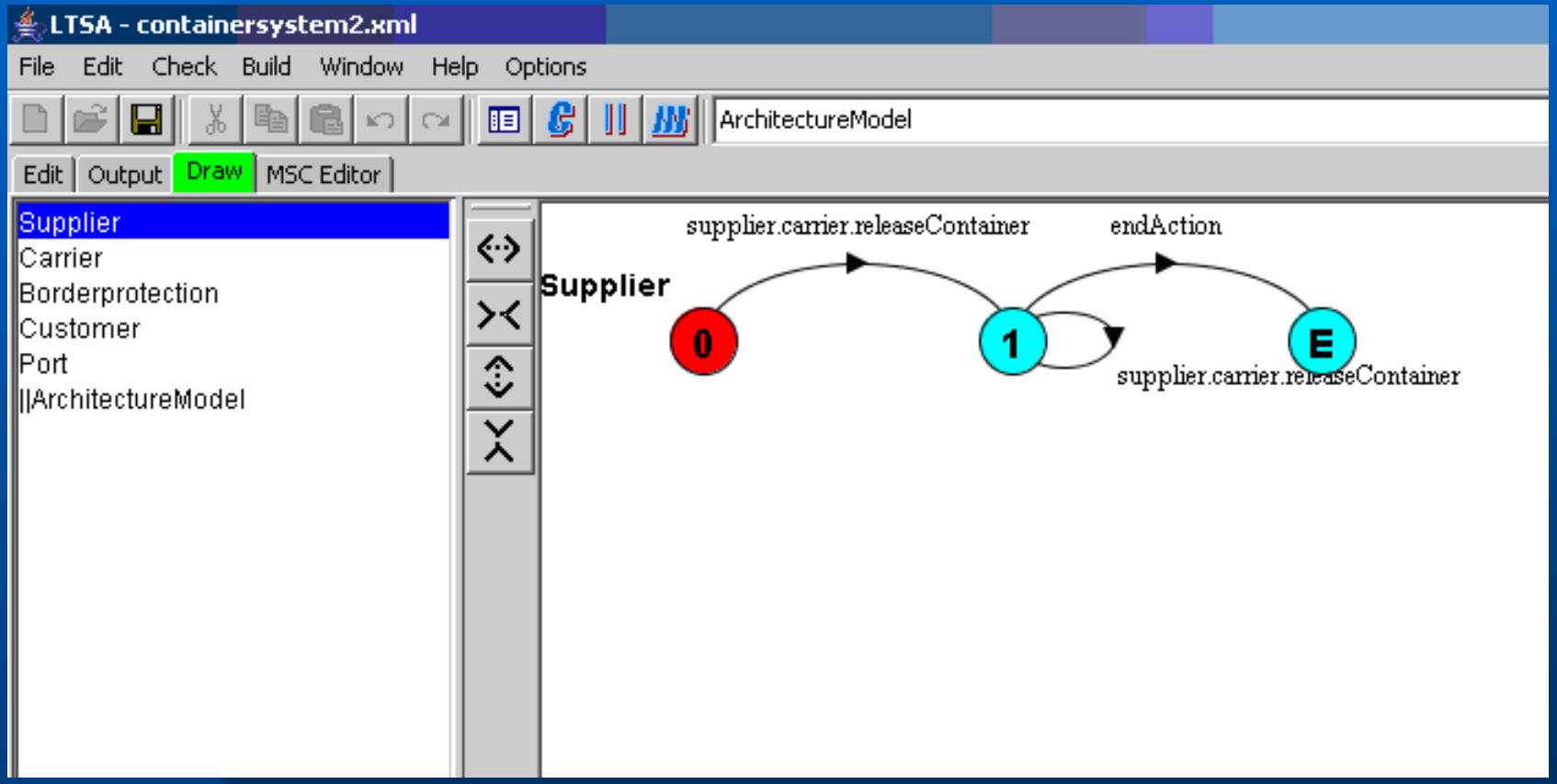
Carrier to Border Protection bMSC



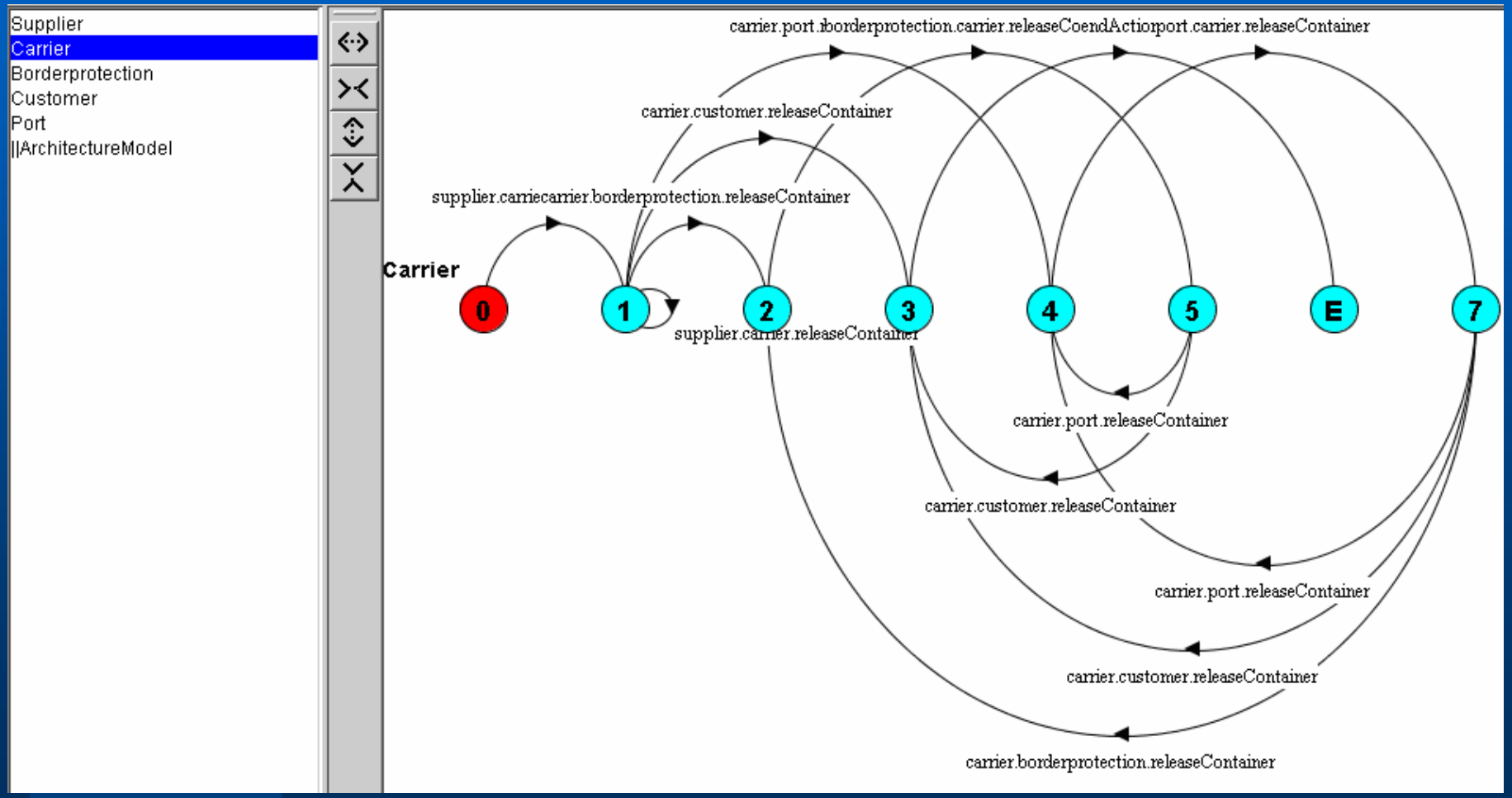
Carrier to Port bMSC



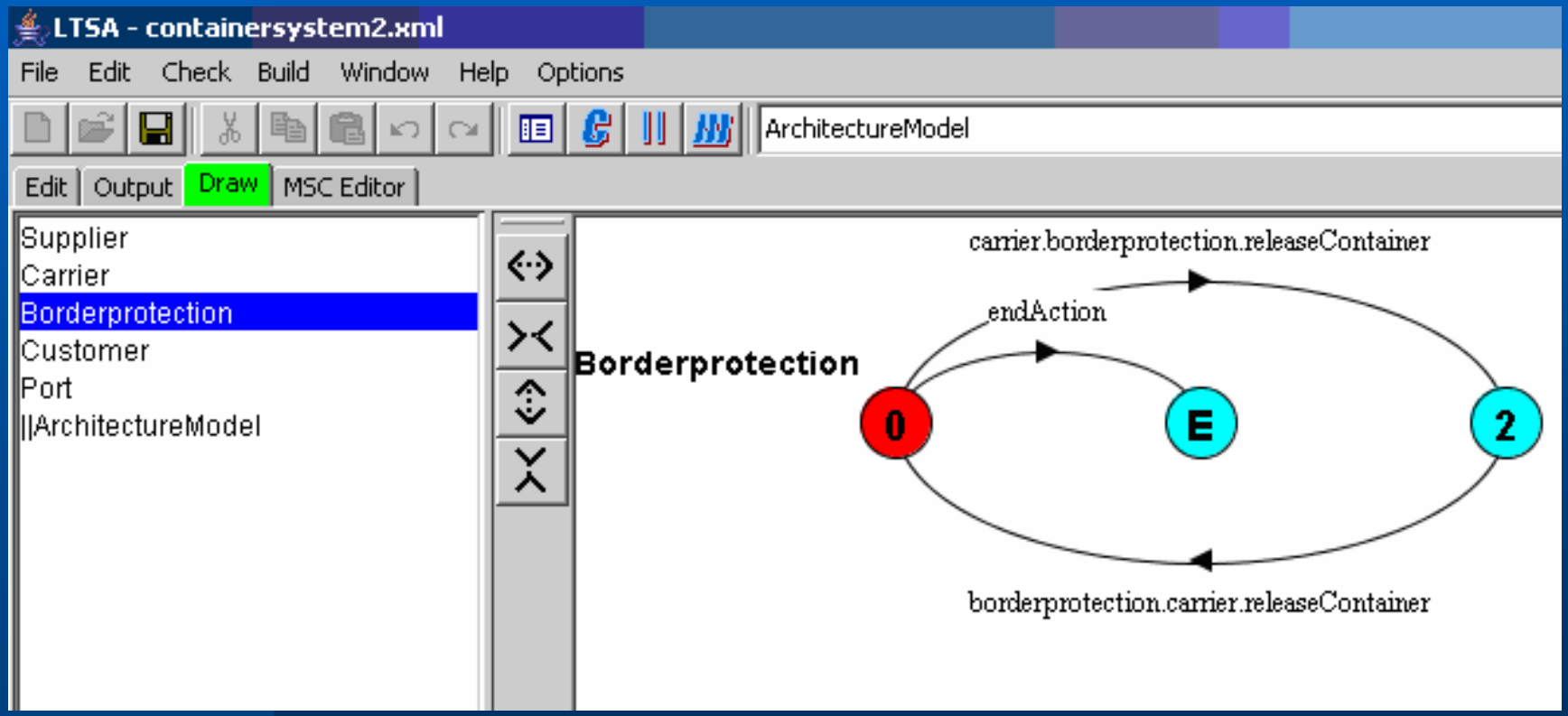
Supplier LTS



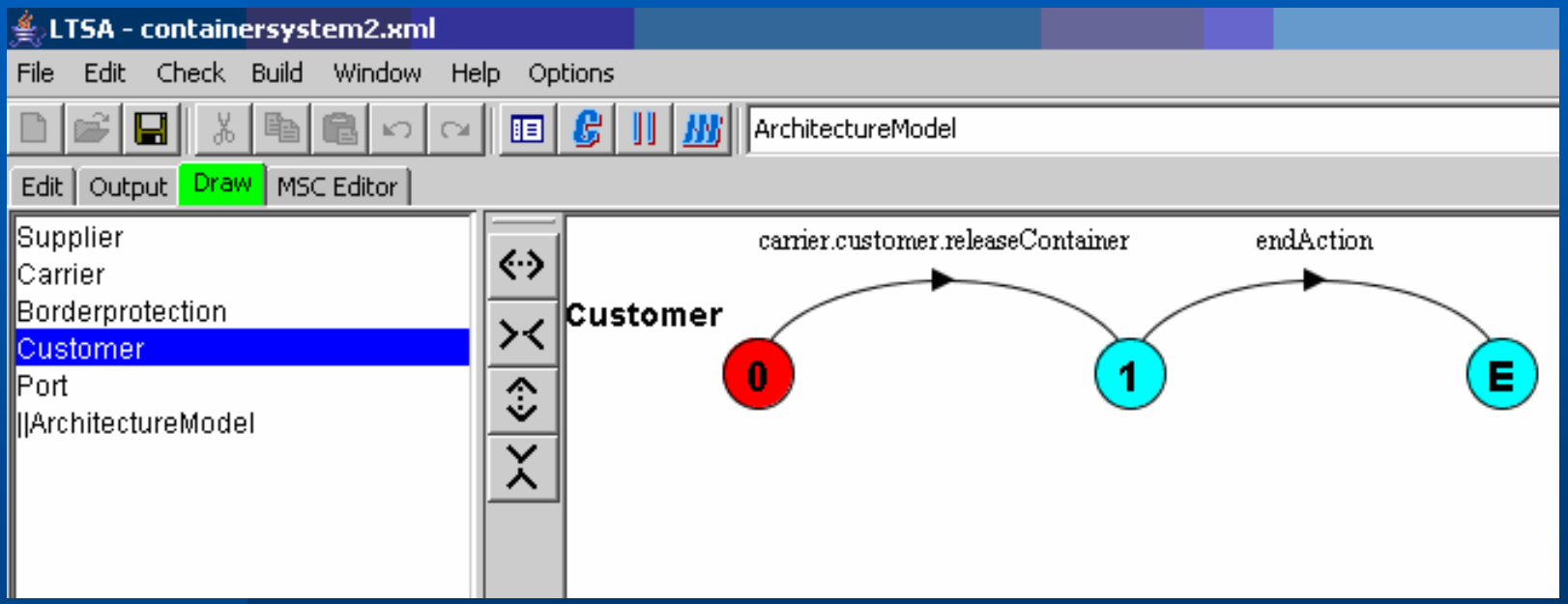
Carrier LTS



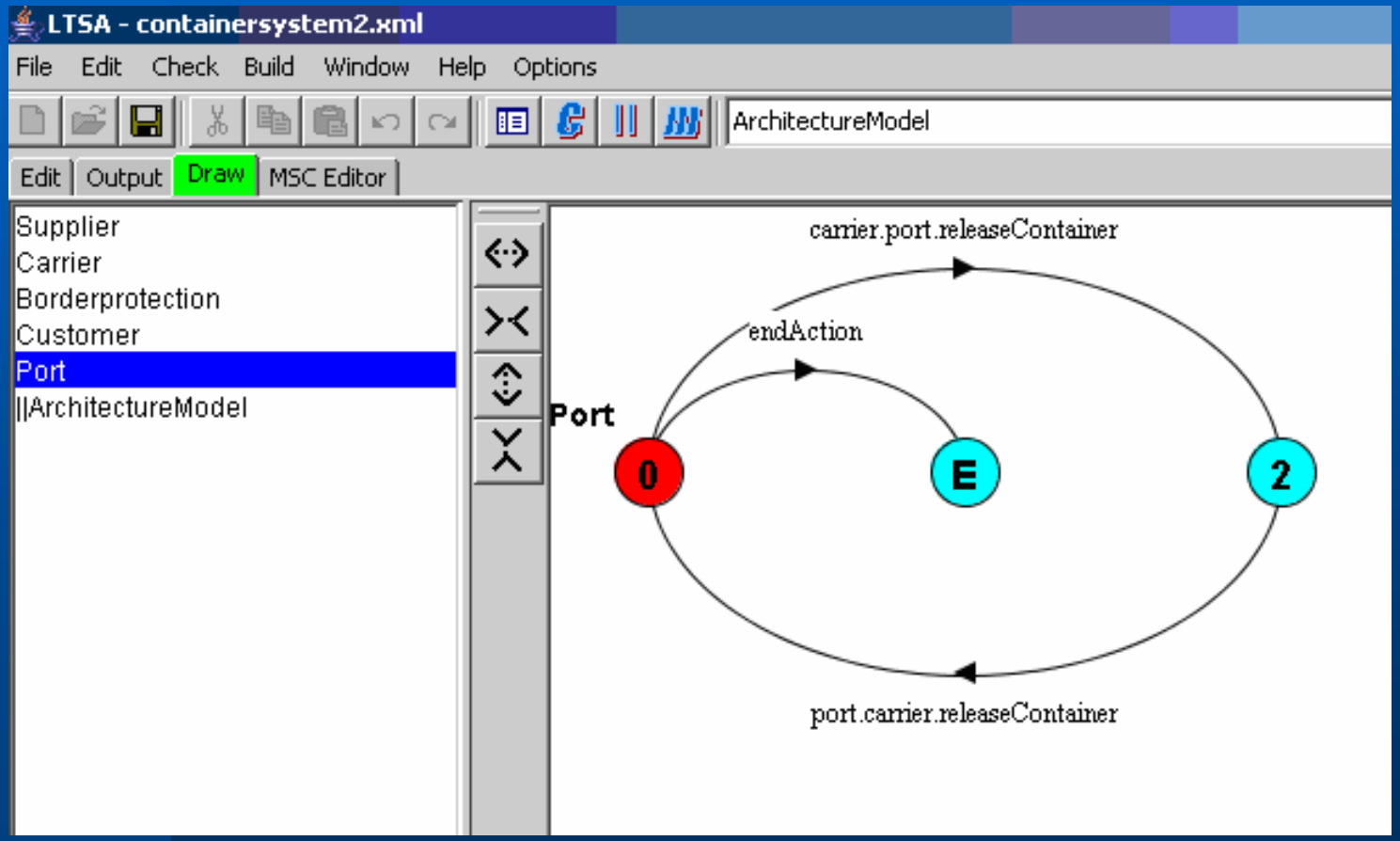
Border Protection LTS



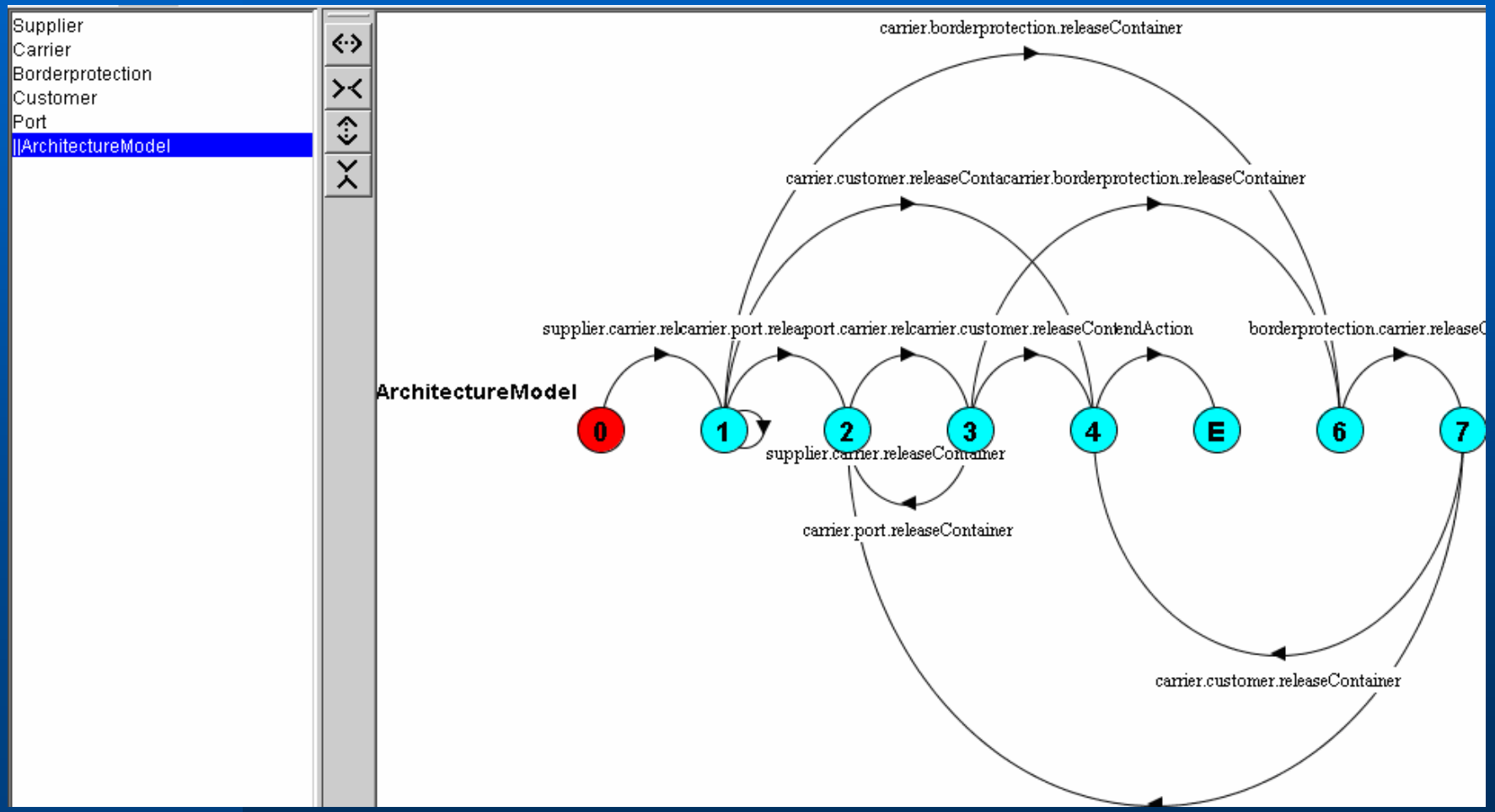
Customer LTS



Port LTS



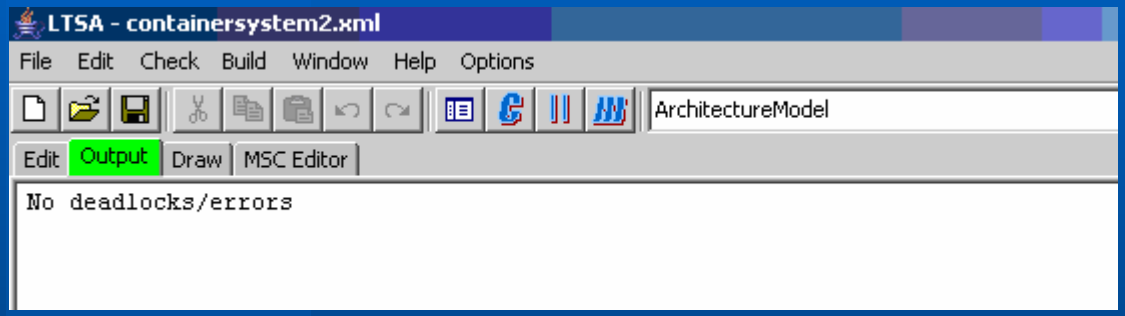
Architecture Model - LTS



Validation and Verification using LTSA (contd.)

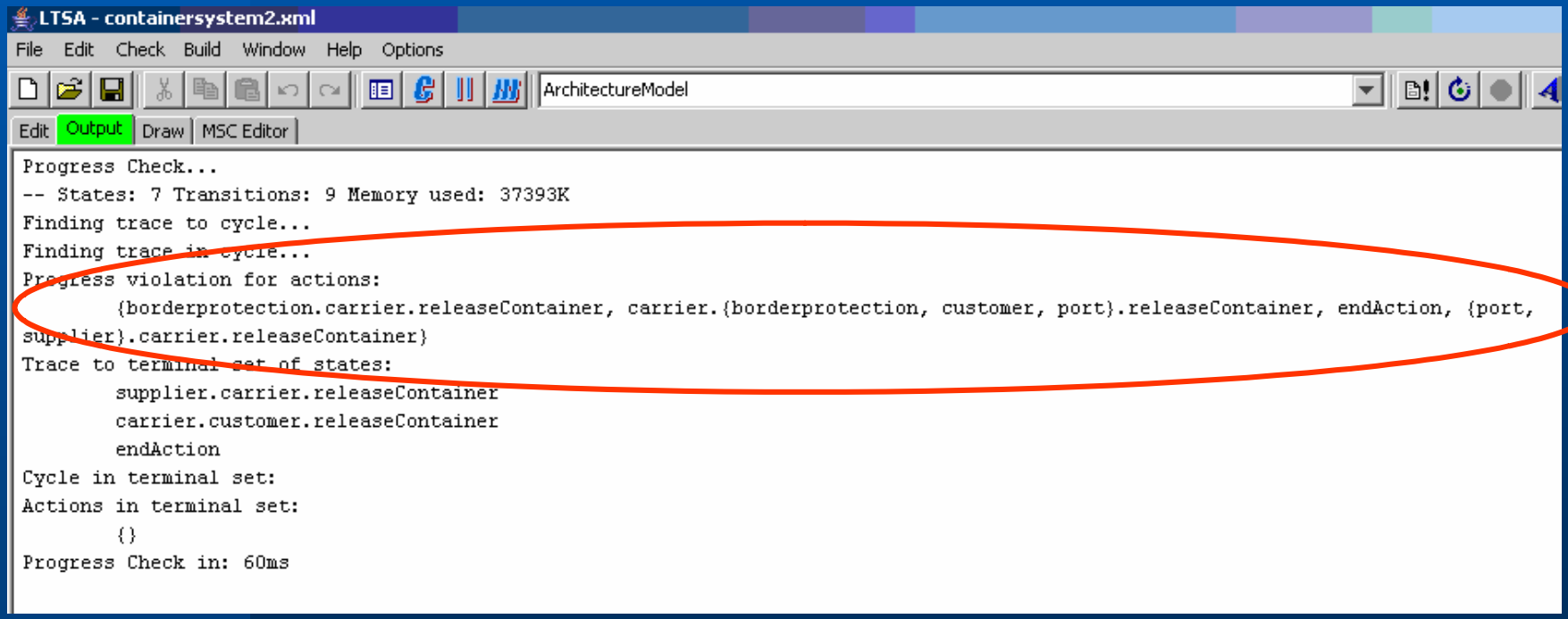
- **Properties we are checking using LTSA**
  - **Deadlock (safety)**
  - **Progress (liveness)**
  - **Implied Scenarios**

Deadlocks



Progress

- The progress check shows violation for a sequence of actions because of the loops between the carrier, the BPA and the Port. But, in this system, the progress property will not be violated because depending upon the number of loops that need to be traversed, the container will be finally delivered to the customer.



Implied Scenarios

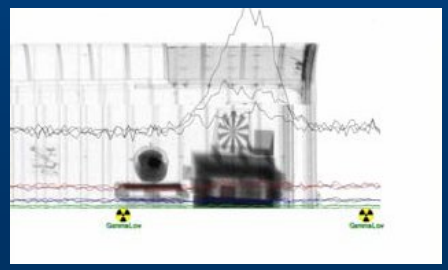
- **The plug-in didn't detect any implied scenarios.**

Manual LTS Verification

- **Currently working on verifying the LTS generated using MSC plug-in by creating an LTS manually**

Advancements & Technology

- **RFID** – Radio Frequency Identification
  - **Active vs. Passive**
  - **Smart Seals**
- **NII** – Non Intrusive Inspection
  - **X-Ray Scans**
  - **Radiation Detectors**
- **Standards**
  - **ISPS** – International Ship & Port Facility Security Code
  - **MTSA** – Maritime Transportation Security Act



Source: www.ops.fhwa.dot.gov

Future Work

- Incorporate attacker scenario
- Incorporate “un-sealable containers”
- Incorporate variations for changes in security levels
- Incorporate most recent system tool development
- Differentiate country specific regulations
- Drill down to explicit threats
- Develop test case for identified requirements

Questions