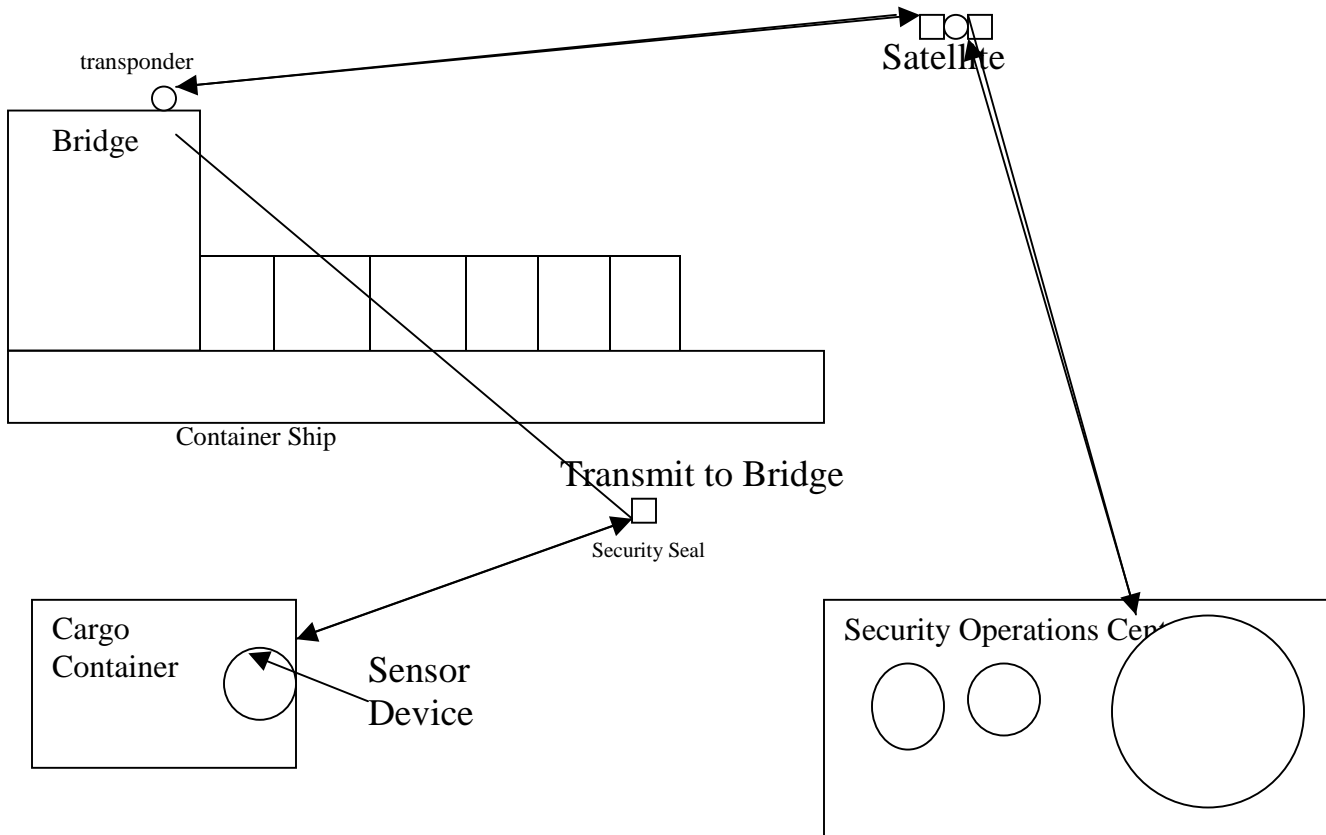


Cargo Tracking System

This concept is an approach to tracking cargo that is shipped from overseas via container ships into the United States. The basic principal is to somehow tag the boxes or crates as they are being loaded into the containers and then to maintain a real time observance of them as they are in transit. While the idea was focused on container ships, the entire notion can be applied to railroad cars, tractor-trailers or even delivery trucks. The main purpose is, of course, to not only deny terrorists the possible access to containers that could be modified enroute to their destination and the contents switched to some sort of destructive material, but also to prevent pilfering and theft of goods.

The technology is not new, it is available and not cost prohibitive. However, the process described here is new and is the intellectual property of its designers. Anyone having access to the paper must execute a non-disclosure agreement and prevent the inadvertent disclosure of the information to others.

The following diagram sketches out our concept and the explanation follows:



We will use a microdot-type device (RFID) to be attached directly to the individual items that are put into a package or packing carton. These devices shall be passive IRIDs. Meanwhile we will attach an active IRID device to the carton that will end up in the shipping container. Our investigations have revealed multiple shapes and sizes of both the active and the passive device and at this time we are looking at one set that is about 3mm square. The method of attachment has yet to be confirmed; however that is a relatively easy solution. As the package is placed inside the carton, its passive IRID is read and the tracking number is recorded on an active IRID which will be placed on the outside of the carton. The cartons are now moved to a container passing through a scanning device enroute that records its collected information re: the carton contents. It is “read” into a laptop computer or a handheld device and the information from that active IRID is stored in its memory. We can, at this point, encrypt the data quite easily if that is an essential factor. Once the contents of the container has been “read” into the computer, we will move the information to an auxiliary storage device known as a flash memory, or a thumb memory or a stick memory. These miniature devices are plugged into a USB port on the computer and can store massive amounts of information up to, at the present time, 256 MB of data. This is a very large amount of information and should it not be enough, we can use two of them to completely inventory the contents of the individual container.

Next, the flash device is removed from the computer and plugged into a specially built package which we call the “seal”. This seal is fashioned to look like a padlock or locking device for the storage container. The container is now sealed with the remote sensor and electronic inventory contained therein. The inventory list also is duplicated in the laptop or handheld computer and is provided with a date/time group and control number prior to the container being loaded onto the ship. A second flash memory can be created or the computer can transmit the information in real time to the Security Operations Center (SOC) which is shown on the right in the diagram above. Presumably both will be performed for backup purposes. All of the data will remain encrypted during this phase so no information is capable of being intercepted for whatever reason such as a terrorist attempting to alter the manifest data.

In the SOC, a logistics analyst can have real time access to the security device on the front of the container by sensing it via a satellite link. This will protect the container from being tampered with while the vessel is at sea or in the case of a railroad car, while it is in transit. Any tampering with the locking device will cause the generation of a signal to the SOC alerting the operator that a possible breach has taken place. Immediately, the operator will

flag the container as being suspect, alert the Coast Guard before the vessel enters U.S. waters and the ship can be intercepted at a safe distance from our shores, boarded and inspected.

Assuming that the vessel is allowed to dock, the containers are then removed and placed aboard trucks for transfer to a distribution site. At this point, the containers are still unopened and the tracking device is still intact as evidenced by the lack of alarms being set off during transit. Prior to being loaded on the truck, the SOC can query the sensor just to insure that the contents have not been tampered with and that the sensor is in fact still working. The trucks or railroad cars which are now in transit can be queried remotely again just as was done on the ship. Since we have not removed the sensor, any attempt to open the container and pilfer the contents will set off an alarm in the SOC thus informing the operator that a theft is under way and authorities can be dispatched immediately.

Upon arrival at the destination, the container can be opened and a message to that effect sent to the SOC using a codeword, password or other authentication device and the merchandise is now in the hands of the distributor. After removing the sensor, the distributor can now check the contents of the container by viewing the inventory that has been stored in the locking device in the form of a flash memory. If the information has been encrypted, the SOC can provide the encryption key to unlock the information and the distributor can verify that in fact his delivery is intact.

If pilfering has occurred, the serial number of the missing element will become apparent when the unloading manifest is checked on the computer. An alarm can be sent to the SOC who now sends an alert to the authorities with the serial number and description of the missing article. Meanwhile the rest of the shipment is distributed to the various outlets or stores that have ordered it and placed on the shelf or utilized as appropriate. The merchandise is still under surveillance as it travels from the warehouse to the outlet. Using the information stored on the flash memory and a hand-held PC, the bill of lading for each truck can be generated and a new inventory list prepared. The information on the flash memory can be transmitted directly to the outlet via normal Internet means and made available before the truckload of merchandise actually arrives.

There is some concern that having the microdot device still attached to the merchandise after it is sold to the consumer. There are two schools of thought there. If the merchandise is something like a TV or Stereo or even an automobile, we now have a built in tracking device should the merchandise be stolen from the consumer. The advantages or disadvantages of this have yet to be explored.

Additional Information

As we were investigating and researching this concept, we have introduced extra ideas that are based on some of the facts we uncovered during our visits with other companies and the discussions that were held between some of the principal investigators. Rather than discuss these at great length, I will provide some of the findings and throw them out for discussion.

1. If the “seal” is tampered with, it will send an alert to the bridge monitoring device which will automatically send an alert via satellite to the SOC.
2. I was concerned about dead spots in satellite coverage with the ships at sea. I have since learned that there are no more of these and unless someone has better information, let us assume that is true.
3. In the information gleaned from the RFID newsletter, I learned that the passive IRID can be read “through a brick wall”. While this may or may not be true, I am assuming we can read it through a cardboard carton.
4. It has been suggested that we provide the ability for each container on the ship to communicate with each other. The importance of this is that apparently some containers cannot be placed in proximity with others and if we could know what is inside each one and develop a stacking algorithm we could perform a necessary task for the cargo loaders.
5. We need to investigate a sensor that will be inside of the container to detect any ABC threat. I believe I can locate a company that has the capability to do that. What we want to do here is prevent terrorists from drilling through the container and inserting a dirty bomb, biological agents or other forms of destructive agents.
6. We will also need to consider a method for detecting a terrorist evacuating the contents while the ship is at sea and inserting himself along with elements of life support in order to be smuggled into the country.
7. If the seal detects a tampering at sea, it sends an alert to the bridge box which then sends a message to the SOC via the satellite link.
8. While in transit, the bridge transponder will send a DTG and GPS coordinates message to the SOC whenever it is polled. The SOC can keep a situation log through this method detailing every port of call that the ship makes.
9. The Piracy problem which is occurring in the North China Sea and in the Caribbean will be curtailed since any tampering with the boxes or any course deviation detected via polling from the SOC will alert the SOC operator who in turn can notify the proper authorities.
10. Also, any cargo which is hijacked can be tracked down through the use of a scanner which will cause the active and perhaps even the passive IRID’s to generate a signal. In essence we will have a sea-going Lomax System.

Some other essential items we learned and need to investigate further are:

1. We need to study the level of automation used in the shipping industry today.
2. Containers are owned by a company that leases them out to the shippers. Are they our targets?
3. Can we build the “seal” device into the container itself? What about the antenna problem?
4. What kind of a beating do the containers have to stand up to?
5. What is the relationship between manufacturers and shipping companies? Do the manufacturers call up and order a number of containers to be available on such and such a date and who handles all of this logistic problem?
6. What Communications capabilities exist on board today and how can we integrate our systems into it?
7. Who really runs the ports and who is in charge of cargo handling?
8. How do we communicate between containers and can we build a self generating network?
9. Containers appear to be leased to the shippers. Many points of vulnerability for terrorists to have access.

What happens when we unload the containers onto trucks or trains.

Once the ship arrives in port, the Bridge Unit can interrogate the seal acquiring the inventory that resides there in the flash memory. When offloaded at the dock:

- Verify that the seal is still unbroken and verify that it has not been tampered with.
- Open the seal and remove the flash memory. Insert it into another computer to check the inventory, printing out a list of merchandise (if this is necessary at this stage).
- Restore the flash memory to the seal box and reset it, handing the list of contents to the driver. Load container onto the truck and deliver to its destination
- At destination break open the seal read the flash and compare it to the original order. IF the information is still encrypted, and it should be, contact the SOC for the cipher code to open the file.
- If all is O.K. move merchandise to inventory

