TRANSPORTATION SECURITY RESPONSE, RELIABILITY, SAFETY AND PERFORMANCE ISSUES

Ernst G. Frankel

Massachusetts Institute of Technology, Department of Ocean Engineering
77 Massachusetts Avenue, Building 5-222, Cambridge, MA 02139-4307, USA
Phone: 617 253 6763, Fax: 617 253 8125, E-mail: efrankel@mit.edu

Abstract

Since the introduction of technology, its performance, reliability and safety have been our major concerns. Performance is expressed in terms of usefulness effectiveness, and costs; reliability in teams of instant and uptime availability to perform; and safety in terms of its ability to assure user, operator, and the environment protection from any ill effects. These three major characteristics of technology were improved by using design and operational data to identify opportunities for advancement, and today we can generally assume that technology, and particularly transport technology, will perform to its design standards, achieve a high level of reliability, and be safe in use for users and the environment in which it works.

In recent years we were forced to confront anew issue not of serious concern before - security of and in the use of technology. While the basic concerns mentioned above were all dependent on the design, manufacture, use, operation, and the environment in which the technology worked and were therefore imbedded reactive characteristics, security is an externally imposed danger. Protection against security impacts cannot be provided by making technology more efficient, reliable or even safe, bur by introducing detection, barrier, fail proofing, and various proactive measures designed to protect the technology from purposely disruptive and destructive actions.

In this presentation we will discuss approaches to proactive and preventative measures under development designed to improve the security of transportation. We will note that these measures cannot be based on historic performance but must consider an array of potential interventions.

1. INTRODUCTION

Since the terrorist attacks of September 11th, security in transportation has become an ever serious concern and both national governments and international organizations have introduced major policies and requirements to assure safer transportation of goods and people. Although basic safety measures were in place before, most of these were designed to respond to problems introduced by physical faults, acts of God or human errors and not terrorism. The new phenomena of purposeful attacks that often include suicide of the perpetrator need a different approach to which organizations and agencies are only now trying to respond in a meaningful, organized way in the U.S. Intelligence, law enforcement, and security activities by government have traditionally been widely dispersed among numerous federal and local agencies with little coordination or information sharing among them. In fact, many of these agencies worked at cross-purposes.

International enforcement of safety and security measures is mainly by agencies of the United Nations such as the International Maritime Organization, UN Conference on Trade and Development, World Health Organization, and more.

Another issue is the development of safety and security requirements by countries that often reorganize their national security apparatus now. I will attempt to present the status of policies, initiatives, and measures current at this time, fully recognizing that the whole process is in a flux and subject to change as governments, organizations, and agencies at all levels and under various jurisdictions gain experience and converge on enforceable, defined rules, requirements, and measures.

1.1. Security Threats

General

Transportation security is a global confidence, tracking, inspection, and control problem that requires technological hardware and software as well as sophisticated confidence, personal evaluation, and effective background and current performance checks. Enormous relations and object oriented data bases are required, supported by reliable real time physical checks and tracking as well as effective analytical software for such problems including order entry checking, final destination, end use or user confirmation, driver, vehicle, and cargo consistency verification, cargo code standard verification, and more. Although physical threats dominate there are links between psychological and confidence measures as well as physical tracking and inspection. A global system for transportation security must include supply chain wide security measures from origin to destination and integrate cooperating standardized networks of confidence checks, tracking, inspection, and control procedures and technology use. Current weaknesses and needs for development of confidence building and tracking or inspection technology are identified and potential approaches to the solution of current gaps or problems are proposed, including increasing concerns with

- Piracy incidents are becoming more frequent. The connection between piracy and terrorism is alarming. Many actions can be taken to present acts of piracy and deter attacks on vessels.
- Harbor robbery incidents in many underdeveloped countries are becoming more frequent. Many actions can be taken to prevent acts of robbery and deter attacks on vessels and their cargo, including cargo transiting ports.
- The problem of stowaways is not new but the scope of the current problem is. The possibility of terrorist stowaways using ships for infiltration is even more alarming, particularly on containerships.
- Airports, docks, and harbor piers are the easiest way to access restricted areas. For some reason, one assumes that the water creates a well-protected barrier. The opposite is true, since water creates opportunities for stealthy penetration.
- Container cargo security has become a focal issue. The potential of import of nuclear, biological, and toxic materials and agents is on the increase and effective methods of detection and neutralization must be found and introduced.
- Port and port terminal security has become an important issue and effective means for boundary protection and area security must be developed to prevent sabotage and other criminal acts.
- Port and air terminal information and communication systems must be secured and protected from unauthorized access and manipulation.
- Port, air terminal, aircraft, and ship personnel and others with legitimate access to ports, aircraft, and ships must be more effectively scrutinized and access effectively controlled, and restricted to only those thoroughly checked, identified, and admitted to areas and facilities for legitimate purposes. Access and regress must be controlled, recorded, and reviewed.
- Port and airport equipment and facilities are complex, large, and expensive. Access, particularly to major equipment, must be strictly controlled and managed. Only specifically identified persons must have access.
- Aircraft, vehicles, and ships receive and discharge gaseous, dry, and liquid substances such as fuel, waste liquids, ballast water, etc. Effective monitors and other controls are required to assure that such transactions to not result in dangerous emissions, pollution, poisoning or environmentally harmful discharges and/or transfer of potential weapons of mass destruction.

- Shipboard and aircraft staff live and work in isolated quarters and could readily be incapacitated by gas or other toxic material intrusions designed to take over vessels or otherwise attain control of a ship. Similarly, operators of port and airport equipment are subject to potential attack and incapacitation, which can cause huge damage and/or penetration by terrorist threats.
- Aircraft high-jacking, demolishers, as well as truck or rail deviation is an increasingly important threat.

Considering security threats, more specifically as they relate to ports and port operations, the following lists of security threats and policies/technologies designed to guard against them is presented.

Air and Seaport Security Threats

1. Unsafe Ships and Aircraft: Aircraft and ships that constitute fire, explosion or toxic pollution hazards that can be triggered by terrorists, crew, as well as by external attacks.
2. Cargo: Hidden hazardous cargo in containers, boxes, holds or tanks such as nuclear, explosive, biological or toxic substances that when released or triggered cause large damage, loss of life, and an unsafe environment.
3. Air and Seaport Facilities: Penetrable, unsafe port fences, and boundaries including access from the waterside that is seldom controlled. Overflight and easy road access, high voltage lines crossing port areas, inflammable storage facilities, tanks, and other hazardous storage facilities.
4. Equipment: Easy access to critical port equipment controls. Access to rails, cables, wires, controls, and guides of major critical port equipment.
5. Air and Seaport Personnel and Persons in Ports: Ports require strict access and exit controls and effective port identification. Ports must have enforceable rules of admission and restrict all access to vicinity of critical equipment, operations, and storage except by essential people.
6. Air and Seaport Boundaries and Potential Penetrations: In addition to port fences and physical boundaries, ports are vulnerable to penetration by thrown or missive explosives, flammables, toxics, poisons, lubricants, etc. Similarly, port supplies such as power, communications, water, air, etc. can be interrupted, corrupted, etc.
7. Environmental (Air, Water, Distributed Systems) Attacks: Ports distributed systems including water, sewage, telephone, power, air, etc. are vulnerable to attack, corruption, interruption, and pollution.
8. Air and Seaport Information and Communication Security: Hand communications are today critical in port operations and management, as ports increasingly serve as info hubs for major supply chains. Much of modern port operations and equipment are digitally (electronically) controlled often using wireless LAN networks that can be penetrated by terrorists and others if not well designed and managed.

1.2. Security Measures and Policies

1. Direct threat recognition and terrorist risk analysis.
2. National laws and regulations and their impact on the possible solutions to be proposed.
3. International standards and conventions regulating marine trade and transit and their impact on the possible solutions proposed.

4. International perimeter environment - assessment of possible risks and "soft belly" areas.
5. External environment to the defined port perimeter - assessment of possible risks
6. Cargo security (incoming and outgoing)
   a. cargo profiling
   b. inventory of existing technologies covering bulk screening and sub-pressure simulations
   c. bulk explosive trace detection
   d. non-conventional (chemical, biological, and nuclear) threat
7. Aircraft and ships security
   a. ground protection
   b. air and sea protection
   c. catering and supplies screening
   d. sensitive carriers
   e. crew screening (incoming and outgoing)
   f. documentation screening and forgery detection
8. Transport personnel, worker, crew passenger security
   a. crew, port worker, passenger identification
   b. checking and security measures
   c. passenger handling procedures
   d. existing protocols
   e. existing training programs
   f. documentation
9. Access control
   a. definition of restricted areas
   b. vehicles control
   c. system for worker, crew, passenger recognition
   d. permit policy
10. Communications infrastructure
    a. examination of command and control communication facilities
    b. examination of contingency existing plans
    c. examination of existing communications protocols with security official services (police, FBI, others); identification of possible loopholes in case of emergencies.
11. Human resources
    a. examination of the human resources employed for serving the security needs of the ports
    b. training programs
12. Parking lots
13. Access roads
14. Obligatory checkpoints
15. Technology
16. Direct and indirect observations
17. Auditing policy

Data Security

a. Protection and security of the system's data itself
b. Data availability in real time
c. Vital elements running the Command and Control Center of any serious security system
d. Identifying vulnerability of data systems. Cyber terrorism and/or computers and data vandalism are real concerns.

Countering Security Threats in Ports

Steps in Developing Transport Security Management Systems

- System and specific risk assessment
- Building of protection and defense programs
- Mapping of computer systems, signaling sensitivity and access rights
- Planning and building of computer secured topology covering prevention, discovery, warning, and recovery
- Contingency plans in case of system collapse
- Simulation of cyber attacks to discover weaknesses of the system
- Simulation of physical penetration to discover weaknesses of the system
- Implementation of the program
- Auditing
- Training

2. TRANSPORT SECURITY TECHNOLOGY INITIATIVES

Governments and industry have recognized the need for new technology for transportation security. Among the technologies of concern are:

- non-intrusive luggage, cargo, and container inspection machines
- effective, secure, and reliable cargo and container tracking devices including content tracking
- container sealing devices
- container identification devices
- air and sea port boundary protection (land, air, water)
- ship hull protection against unauthorized pirate/terrorist boarding at sea, anchor or in port
- crew and port workers identification and access control
- secure wireless local port area networks – Port Info/Communications Security
- secure electronic data transmission storage and use
- biological terrorist attack prevention
- nuclear terrorist attack security
- port equipment securing devices
- security of port power, water, bunker supply, etc. systems

One of the issues of concern is that shippers in, and shipping to, the U.S. will be required to affix a high security manual or electronic seals to containers immediately upon the conclusion of the container stuffing process. An internationally accepted standard for such seals has been approved, and C-TPAT ocean carriers are encouraging their customers to affix such seals.

Carriers support expanding such a practice from a voluntary practice to a government requirement (Table 1).

Table 1. Container Seal Technology

Group	Technology
Sftvi Technology, Sunnyvale, CA	Electronic seals and smart cargo containers
NaviTag Technologies, North Quincy, MA	Electronic seals and tracking devices that use satellites
Isotwg, Addison, TX	Chemical-based intrusion detection using seals and handheld sensors
Argonnc National Laboratory, Argonne, IL	New detector to find nuclear materials in containers
MIT, Cambridge, MA	Radiation detector with imaging capability

Unlike high security manual seals, there is no agreed standard for e-seals, and the substantial difficulties in establishing such a standard have made it clear that such a standard is highly unlikely in the near future. Further, e-seal's limitations are becoming clearer. As the Los Alamos National Laboratory has concluded, e-seals can be defeated as easily as manual seals, and contrary to some of the marketing arguments for them, they cannot and do not inform about what a container's actual contents any more effectively than the carrier's manifest. They do not deter entry into a container any more effectively than a high security manual seal. Furthermore, as technology is developing, e-seals may be overtaken by other technologies that can provide better information, more economically. For example, some technology being tested would indicate whether the container doors have been opened, which while not perfect security information, would provide better security information than whether the seal on the container is the same seal that was originally affixed by the shipper. Furthermore, there is growing interest in sensors that might be economically placed in a container that could detect various security risks and monitor container contents.

The principal container security issue is: what has been loaded into the container? - not what does someone say was loaded in the container, and not whether the seal on the container is intact. Technology, in the form of non-intrusive inspection equipment, is a substantial step forward. Regarding technologies that might be attached to a container, it is important to recognize that ocean shipping containers do not operate in closed or dedicated services for a particular company or geography, but are interchangeable and are globally mobile.

What we may need is an intelligent container seal which can receive an alert signal generated as a data mining application flashing a warning with this alert indicator then used to flag boxes that should be scanned, non intrusively, with x-rays and gamma rays. Containers flagged for inspection should be stowed together. Technology such as SAIC and Heimann could in future scan entire boxes in 1 minute, thereby promising throughput rates of 50-60 boxes per hour, as well as increased revenues from Customs collection. The portability of the huge scanners is improving, enabling them to be quickly moved around a large yard. E-seals can now be permanently installed which use ultra-low power radio "Bluetooth Lite" transmitters.

As opposed to traditional electronic seals, this system will use a single globally available ratio frequency band, which is license-free. Since ALL-Track uses low cost Readers the reading infrastructure will apparently be cost efficient. The small size and high flexibility of the AllTrack Reader permits connection to a standard mobile phone, thus making it a 'mobile' reader.

The new ALLTrack e-Seal can be permanently installed in the container, and by the door hinge a small sensor registers door-opening events. The e-seal also has capabilities to connect a wide variety of external sensors to the inside of the container, enabling future 'smart

container' capability at the same time without duplication of cost. A ten-year battery assures that e-seal will last for the entire lifetime of the container.

Considering scanning of containers, there are a number of x-ray, gamma ray, and pulsed neutron scanners now available. These are expensive, bulky, and heavy equipment and can be installed in drive-through facilities or truck mounted. There are now studies to develop container spreader-mounted scanners to permit use of the time a container is suspended on a spreader (usually 30-50 seconds) for scanning.

Active-pulsed neutron scanners (for nuclear, etc. material detection) obviously requires significant shielding. American Science and Engineering developed a low price ($2m) container inspection system that combines on a truck-mounted platform x-ray scanners with a highly sensitive array of radiation monitors able to register both gamma rays and neutrons. Most existing scanners cannot see through a container full of dense materials. An exception is the VACIS system (Science Application International Corp.). Scanners today are becoming more sophisticated, effectively dealing with back scatter and include detection software that spots anomalies in shipping manifests and minimizes failing layered systems.

Recent developments are to permit scanning from some distance and capturing content, etc. and valuation against listed contents. Effective container identification is part of the requirements. Different marking systems are now being listed.

Radio Frequency Identification hardware and software for item level trucking of containers (EFID) developed by Savi Technology is one approach. Containers uniquely identified with bar code or RF tag that are scanned at every milestone is another approach. There are now alternative data capture devices available that are fully web enabled. There are also magnetic container record markets that can be scanned for container content, origin, destination, and next/previous transfer point that again can be wen hosted (Tren-Star or Trencor Container System).

In addition various handheld testing and scanning equipment are now available from CO_2 testers to check container air samples to prevent illegal immigrant or terrorist border crossing to portable nuclear, biological, toxin, poison, and explosive material testing devices, The main issue in security technology development is in addition to effectiveness that it does not slow the flow of goods and/or introduce unacceptable costs.

Another issue that is being addressed is the problem of information tracking, checking, and updating that must include exception reporting. This must include monitoring of transport forwarders and consolidators in addition to shippers (a responsibility which is moving from the Federal Maritime Commission to U.S. Customs) as well as NVCCs which are consolidators and should also submit manifests to U.S. Customs (Automated Manifest System (AMS)). Finally, as containers are increasingly leased and not owned and therefore move among operators, lessor responsibility must be included,

CSI aims at tightening reporting requirements for all cargo coming into the U.S. with the 24 hour advance cargo manifest declaration rule. These security measures now act as a catalyst that forces all companies involved in the supply chain to adopt information technology and standards that will ultimately lead to more efficient business practices. We may find it attractive to extent this to the adoption of already developed e-commerce technology with a home port portal such as APL's GTN (Global Transport Network) portal that is already used by 12 carriers.

2.1. Transportation Security Strategy Consideration

The various maritime transportation and supply chain security initiatives both at the policy and strategy as well as at the technology level are in a flux. The new Department of Homeland Security is still trying to organize itself. International collaboration and support is being

organized but is far from being defined. In the area of aircraft, vessel, and port security, international support has been demonstrated and implementation of new international rules as the best way to implement statutory requirements for aircraft, vessels, and ports.

In the area of container security, CSI agreements will be expected to transition from a sound concept to an effective operation. A lot needs to be done and greater clarity is required in terms of requirements and responsibilities. Most importantly, major improvements in technology are needed if we are to develop a secure and operationally efficient system. We must now perform

- assessment and analysis of the existing programs
- focused management on strengthening those aspects of existing initiatives that need improvement or more resources
- public explanation and demonstration of progress and results
- identify and support new technological opportunities

The various air transport maritime and supply chain security strategies clearly require greater international support if they are to work effectively.

Ride assessment of security threats requires a unique analytical and statistical approach. Cause and effect and resulting failure mode analysis provide a basis but serve only as a structure. While the effects of security threats or causes can be identified and effects even quantified, the problem is determination of threat identification and probabilities. Threats, as noted before, are externally generated and independent of a transport systems technology, condition, application or performance. They are therefore identified as independent chance events with consequences. They are, furthermore, increasingly independent of geographic location or even ownership of transport. Threats are invoked or acted not just to cause damage and loss of life but as political means for undermining social, political, and economic systems.

Security threats in transportation are usually common cause events causing system failure that arc often catastrophic. Analytical network methods such as fault tree analysis are being investigated to develop rational approaches to relate primary threats and resulting failure events to common cause failures, using failure mode and effect analysis.

The main problem is the lack of predictive information on the type, likelihood, location, and timing of security threats that force us to continuously update or invent arrays of possible threats and their consequences. Yet there is no choice as security threats have become the single most important factor affecting transportation systems reliability, safety, and performance.

3. CONCLUSIONS

The performance and safety of all modes of transportation systems are today largely affected by security threats that must be considered in the planning, design, construction, and operation of transportation systems. This requires a different approach from that used in traditional safety and reliability analysis because it is based on completely random human actions with objectives to cause significant property, life, and political damage. There is no historic or performance data that allows meaningful prediction of such events.