Delft University of Technology
Faculty Mechanical, Maritime and Materials Engineering
Transport Technology

B.W. Hoekstra *Cargo Security Technologies*
Literature survey, Report 2005.TL.6947, Transport Engineering and Logistics.

This report discusses the threats that face cargo and the technologies to protect them against these threats. The transportation system is based on openness and accessibility to allow efficient, organized, and fast movement of cargo. Because of these characteristics, cargo is very vulnerable to theft, pilferage, smuggling, and terrorist misuse.

Cargo theft creates enormous economic losses. The direct cost of cargo theft is 30 to 50 billion euro per year worldwide. The events of 9-11 showed that the terrorist's main goal is to disrupt the economy. The successful detonation of a weapon of mass destruction or an explosive device in a container or trailer at a logistic hub could easily cause an economic impact of over 1 trillion euro.

Many government regulations have been implemented to protect the supply chain and cargo. In many cases, they affect trade worldwide. Governments have formed, with the private sector, public-private partnerships to stimulate the research, development, and implementation of new security technologies. Companies must implement security technologies to comply with the regulations. The implementation of cargo security measures not only increases security but will also increase the efficiency of the logistic processes. Security technologies, such as Tracking and Tracing and Radio Frequency Identification, will provide a better visibility into the supply chain and increase by this means efficiency.

The first step to secure cargo is securing cargo handling and storage facilities. The perimeter security is the first obstacle for unauthorized access. A physical barrier like a fence, wall or water will hinder or delay intruders. With the use of adequate lighting, alarm intrusion sensors, gates and closed-circuit television the security is further increased.

Every mode of the transportation system employs many people involved with handling cargo or its documentation. Access Control is needed to ensure that only authorized people have access. This first step for an adequate Access Control system is background investigations and protocols for all personnel handling cargo and employed in ports, terminals, storage areas, etc. Access Control replaces the standard key with an intelligent permit system, usually in the form of a badge or a plastic laminated card. To verify the user and his ID card, biometric information systems are available.

Locks and or seals provide a way to secure the cargo. Locks are used on containers, rail cars, trailers or other transport conveyance to deter, slow down or deny entry to the cargo. Indicative seals have the sole purpose to indicate whether an unauthorized access attempt has been made. Barrier seals provide physical security to the cargo. They also give evidence of tampering or an attempt to gain access. Electronic seals are a combination of a mechanical seal and electronic components. An electronic seal provides tamper evidence, physical security, and data management. Electronic seals can be divided into four groups: radio frequency identification, infrared, direct contact, and very long range cellular or satellite (GPS). All except for the simplest solutions are capable of reporting sensor information and data that goes beyond seal status and identification of the seal.

A very promising technology to secure the cargo and its transport is the use of tracking and tracing (T&T). The T&T systems are integrated with all kinds of communication technologies like satellite communication, radio frequency (RF), and cellular. T&T systems can give a time-to-time or a continuous update on the cargo's position. There are also systems that signal status-changes, like the opening of the door or movement within the container. Short-range is the tracking and tracing of cargo or the conveyance transporting within a certain area. This area can be a warehouse, shipyard, or a smaller area like a gate. Long-range tracking and tracing is not restricted to a certain area, the position can be determined wherever the cargo is. There are new sensor systems available that use sensors attached to or embedded in an asset, mostly containers, which communicate using wireless mesh networks. These wireless networks can be integrated with other sensors to monitor different aspects of the asset. The tracking information does not only provide more security, it also facilitates and identifies problem areas of the supply chain.

Internal sensors provide a container or trailer with the ability to detect intrusion and monitor the integrity. All these sensors are or can be integrated with a wireless communication device to send an alarm to an operator. The sensors enable the operators, authorities, and other involved parties, to pinpoint the conveyance that needs inspection. There are recent developments for an Advanced Container Security Device (ACSD). The ACSD is installed within a maritime shipping container and is equipped with all kinds of internal sensors and communication systems.

Inspection technologies are used by customs to inspect cargo for the presence of contraband, narcotics, people, weapons, explosives, and other illegal materials. The technologies provide the means to inspect cargo without opening it. The primary function of cargo inspection is to quickly clear the overwhelming number of legitimate cargo while maintaining a high level of security. Some of these technologies will give a signal when a threat material is detected. The other technologies, specifically those who produce an image, rely on an operator's interpretation of the produced inspection result.

The transportation of cargo from origin to destination is accompanied with lots hand-of points where either paper has to change hands or an Electronic Data Interchange message set is exchanged. The internet is becoming the primary means to exchange information regarding the different aspects of cargo. This system, however, may be vulnerable. The information stored on databases and exchanged between parties can be stolen by a cyberattack. The internet offers access to high-tech software, which, with high-tech hardware, can be used to produce fraudulent shipment papers. To protect the information systems against attacks and fraud, different technologies are available. Some protect the actual databases, for example, firewalls and access

control software. Others protect the exchange of information with the use of encryption software, digital signatures, or a Virtual Private Network.

Integration and combination of technologies increase the security level. This integration is possible with the use of security-integrated software. The maximum feasible security is achieved with a layered security system. The great benefit is that the technologies provide a backup for one another. Of course, there will be always a change that the system is defeated, there is no guaranty for 100% security. However, the use of information systems and integration of technologies enables quick identification of weak spots to ensure that adequate measures can be implemented.

Reports on Transport Engineering and Logistics (in Dutch)

Modified: 2005.09.13; logistics@3mE.tudelft.nl , TU Delft / 3mE / TT / LT.
