Port- and Supply Chain Security
25th IAPH World Ports Conference, Houston 2007

Werner Krüdewagen
Director Sector Sales Siemens Security
May 2007
werner.kruedewagen@siemens.com
Scope of Security Measures in the Container Logistics Chain

Places in the logistics chain in “Maritime Cargo”

Source: OECD, 2003
A „Macro-View“: Security for Ports and Supply Chain

* Secure Communication:
  - Intrusion Detection
  - Anti Virus
  - Content Security
Container Logistics Flow: Participants in the Value Chain

- EU
- National Governments
- WCO
- DHS/TSA

- Customs
- Customs (CBP)
- Carriers Shipping Lines

- Port Operators
- Terminal Operators
- Container Operators
- Logistics Service Providers
- Exporter

- Warehousing/Wholesale
- Manufacturer/Exporter
- Retailer
- Terminal Operators
- Container Operators
- Logistics Service Provider
- Importer

Manufacturer/Exporter

May 2007

Werner Krüdewagen/Siemens

IAPH Houston
Major Fields of Technology Applications in Cargo-Security

Container Security Devices/Container Seals/Container Sensors
- Assuring container integrity throughout the supply chain
- Passive/active RFID
- Special sensors (semi-electronic, electronic) which create real time alerts or communicate with a secure device (i.e. transponder seal) to record events

Detectors at Port/Land Communication Junctures
- Screening & Scanning of Containers (problem for speedy flow of goods)
- Nuclear Detection, X-Ray etc.

Traceability of Containers
- Possible combination of seals, RFID, GPRS, GPS
- Reader-infrastructure, satellites, GPRS infrastructure etc.

Smart Video and Access Control
- Optical Character Recognition (OCR)/Damage Control
- Smart Cards/Biometrics

Information Systems
- Standardize and computerize bill of lading
- Interfaces to SCM-software of industrial players, customs/authorities

Authorized Sealing and Intervention
- Sealing Process at the point of authorized/certified loading
- Monitoring, Intervention throughout the Supply Chain

Additional Aspects
- Combination with other sensor types i.e. temperature, shock, environmental conditions which are beneficial for sensitive goods (pharma, food etc.)
The "Smart Container": a multi-Concept/Technology case?

Danger Management Station

In case of intrusion alarm on site or cross-country

Container Security Device
RFID (CSD)

⇒ Inside of container

GPS / GSM-Modem

Mobile solution

In case of intrusion or other sensor alarm outside of sites (WAN)

Within a country
Cross-country

Container ID
(RFID-tag)

OCR
Optical Character Recognition
Damage Inspection

⇒ Inside of container
(e.g. temperature, bio, chem, volume, shock)

Sensors

⇒ Or / and connection to CSD

Mechanical Seal
E-seal
Port- & Container Security: A shift towards integrated solutions

Relevant Places and Regulations in Port-/Supply Chain Security

Standard Solutions and highly integrated Process Solutions are required

Standard Systems & Solutions

Integrated Process Solutions

May 2007
Werner Krüdewagen/Siemens
IAPH Houston 7
Building Technologies
Terminal Gates: Central Security and Data Nods
Potential synergies between the SC actors

- Screening & Scanning
- Container Security Device / RFID-Reading
- Damage Inspection
- License Plate Recognition
- Container ID Recognition
- Truck Measures, Weight etc.
- Authorization, access and area control
- Data Integration and Interface with Terminal Management Systems

RFID-based Container Security
Smart Terminal Gates

Example: Nuclear Detection Solution
Dutch Customs - Port of Rotterdam

Example: „CommerceGuard“ Joint Venture
RFID-based Container Security and Traceability

Container Security Device (CSD)
Radiation Detection at the Port of Rotterdam
Combination of terminal gate processes with data management
Radiation Detection Project Port of Rotterdam
Automated Terminal Gate Systems
The future brings combined Sensors, Data and Images

Driver passes through portal and stops at Data Entry Gatestand

Equipment is electronically scanned while passing through portal.

Gate operator may review images for damage while driver inputs data. Transaction is processed and equipment is released automatically. Operator only intervenes when there are exceptions.

Driver uses Finger Print for Identification

Driver follows easy to use menus to enter data.
Example: RFID-CSD utilization by Starbucks
Example CSD (CommerceGuard):
Security Data can increase efficiency

EvSS administration

- Read shipment records through a convenient Internet interface
- Rely on secured data
- Select approved levels of information for authorized users
- Extract data for business needs

User • Date • Time • Location • Container ID • Seal number • CSD number
The ICSO was founded on July 29, 2006 in Brussels as a non-profit organisation, which will develop and publish global standards for container security devices (CSDs) and related systems.

**Founding Members**

- Founding members of ICSO include **General Electric Company, GreenLine Systems, JPMorgan Chase, Mitsubishi Corporation, Siemens AG, and Unisys Corporation**. There are already several other leading companies interested in joining ICSO.
- Membership of ICSO is possible for businesses, official agencies, and individuals who are committed to rapidly developing standards for new and emerging technologies for container security devices.
- These member companies share the objective of rapidly improving in-transit container security by quickly defining global standards to help protect international commerce.
- More information under [www.containersecurity.org](http://www.containersecurity.org)
Summary: Key Factors for Port- and Supply Chain Security

“Technology meets Processes”
- Technology-applications are vital but will not be efficient without standard processes
- Actors in the Supply Chain have to harmonize processes

Information Systems of actors will stay based on a heterogeneous landscape
- Data Management and controlled Data Sharing are vital
- Data protection is as important as data sharing
- “Middle-Ware” approach: find a common denominator for interoperability

Information Carriers (like RFID chips) will mainly refer to information sources
- Devices will carry only selected critical data
- Interfaces to Supply Chain software and IT are key

Port Terminals
- Port Terminals will be major security and data nodes
- Terminal concepts of operators (efficiency) and/or customs (security/information)?

Slicing the elephant
- Start with “realistic” action clusters which are open for enhancements

Authorized Economic Operator Concept is vital
- Loading and Sealing Process
- Monitoring, Intervention throughout the Supply Chain

Standardization
- Speed is needed as industry is deploying solutions
- Standards on interoperability are needed (protocols, data management etc.)