STANDARDS AND REQUIREMENTS FOR A CONTAINER SECURITY DEVICE FOR USE IN A GLOBAL SECURE SUPPLY CHAIN

A Presentation for ECITL

14 Oct 2011

Gisele Bennett, PhD
Regents' Researcher /Director, Electro-Optical Systems Laboratory
Professor, School of Electrical and Computer Engineering

+1.404.407.6155 / Gisele.bennett@gtri.gatech.edu

Outline

- ➜ Who we are
- Our Cargo Security Experience
- Standards
- E-Seals
- Things to consider

Four Pillars of Georgia Tech:
a Great Complement, a Greater Synergy

Georgia Tech Research Institute

GTRI is an integral part of Georgia Tech, where research and academics combine to provide unmatched expertise, capabilities, and know-how in solving some of the toughest problems facing government and industry.

Georgia Tech Research Institute

Georgia Tech Enterprise Innovation Institute

Georgia Institute of Technology

Georgia Tech®
Global Learning Center
A PROFESSIONAL MEETING AND LEARNING FACILITY

Georgia Tech Research Institute

Georgia Institute of Technology

SOLVING PROBLEMS GLOBALLY

Georgia Tech Research and Education Centers

UNITED STATES OF AMERICA
Atlanta, GA | Huntsville, AL
16 GTRI Locations Nationwide)

ATHLONE, IRELAND

PANAMA CITY, PANAMA

SAN JOSE, COSTA RICA

SHANGHAI, CHINA

SINGAPORE

Georgia Tech Joint and Dual Degree Programs

BEIJING, CHINA
PEKING UNIVERSITY

DAEJEON, SOUTH KOREA
KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY

MILAN & TURIN, ITALY
POLITECHNICO DI TORINO
POLITECHNICO DI MILANO

MUNICH, GERMANY
TECHNICAL UNIVERSITY OF MUNICH

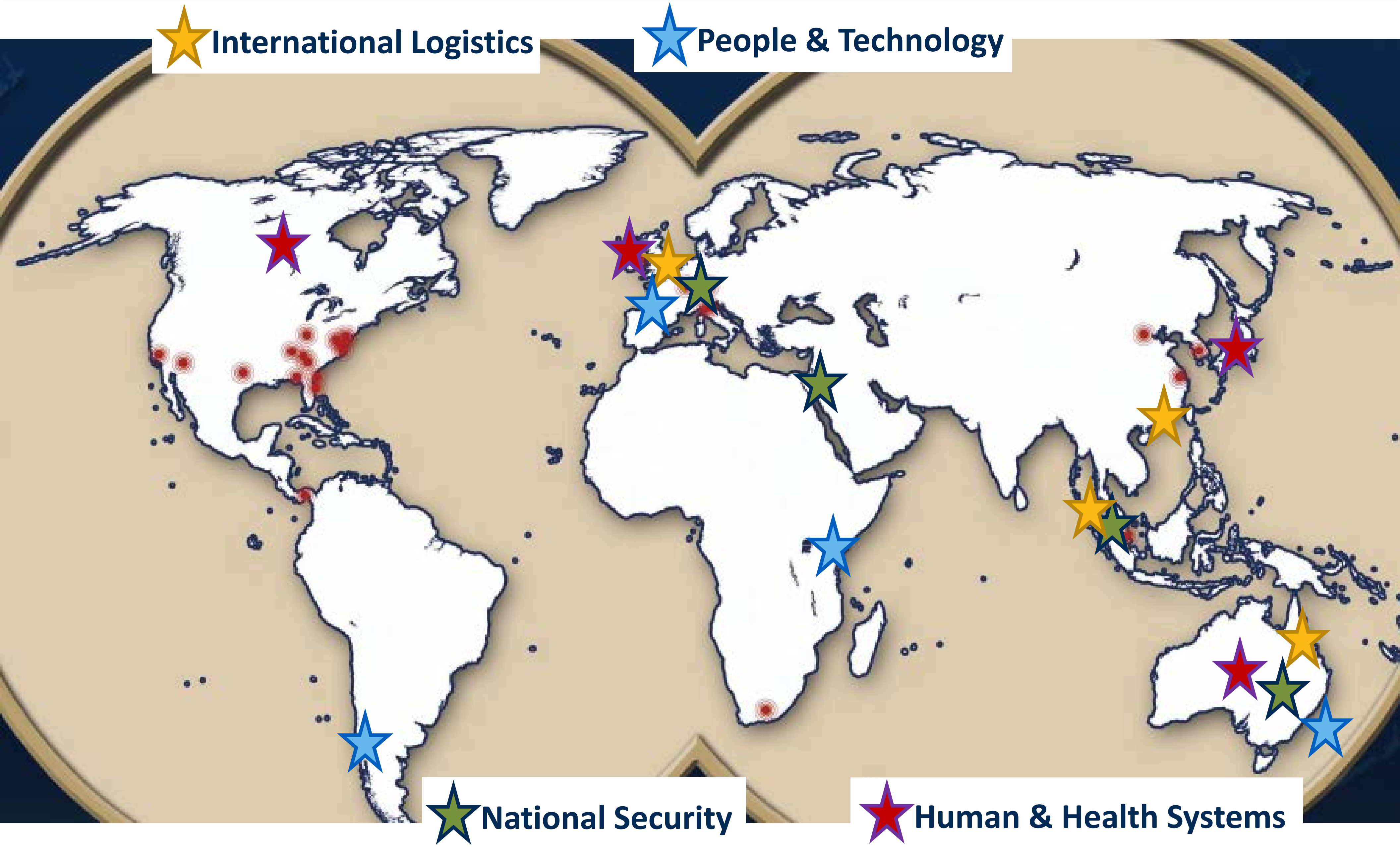
PRETORIA, SOUTH AFRICA
UNIVERSITY OF PRETORIA

Georgia Tech Campuses

UNITED STATES OF AMERICA
ATLANTA & SAVANNAH, GEORGIA

METZ, FRANCE

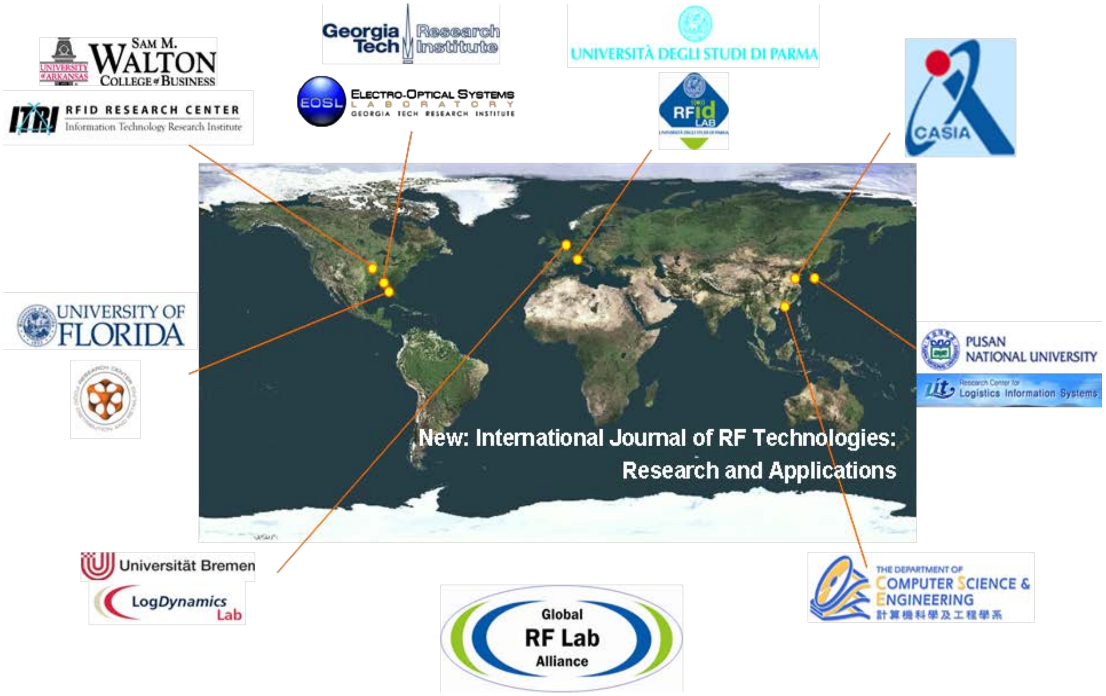
GTRI's Global Research Footprint



Global Outreach and Technology Transfer

- GTRI is part of a Global RF Lab Alliance (GRFLA) – a network of international RF labs that foster international collaborations

- GTRI facilities in Athlone, Ireland and Georgia Tech Metz, France provide EU-based footprint for broader research and collaboration

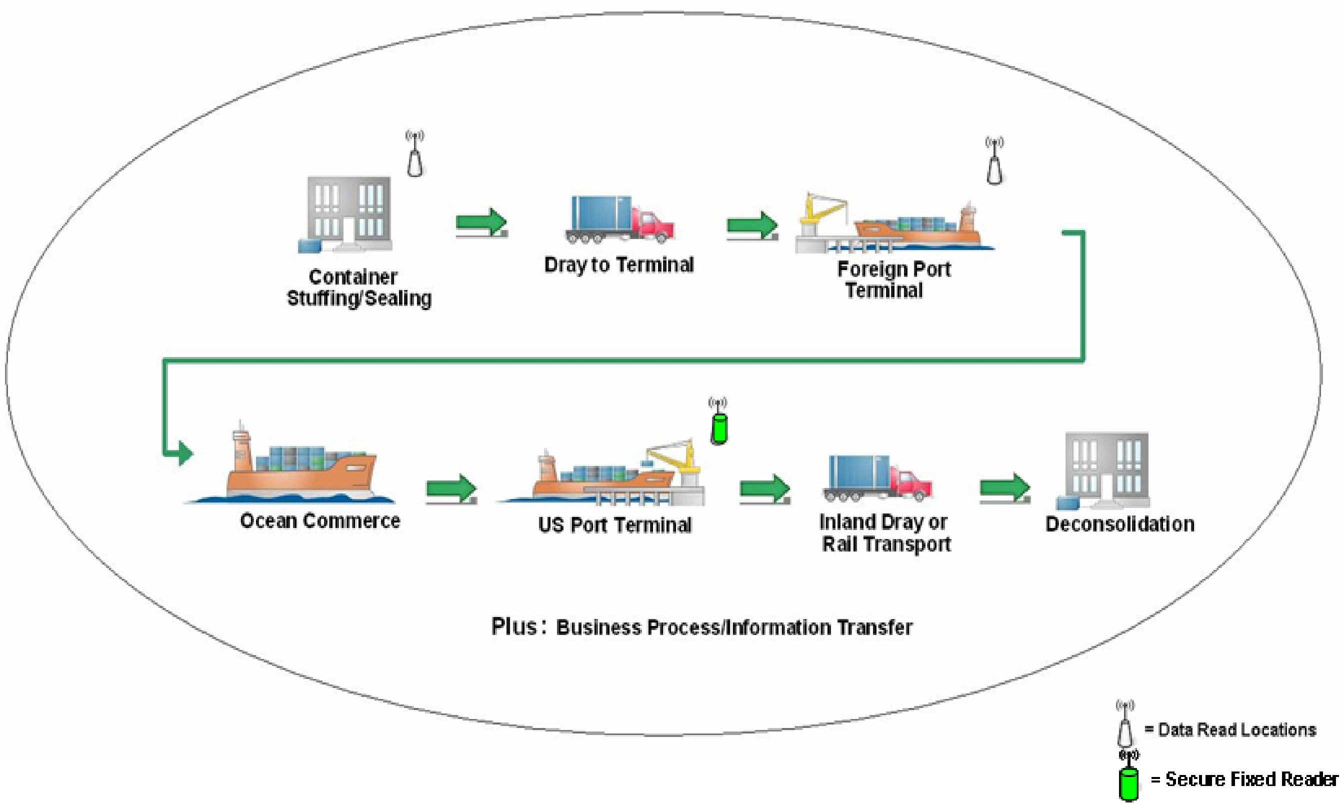


Outline

- ✓ Who we are
- → Our Cargo Security Experience
- Standards
- Things to consider

Meeting Cargo Security Challenges

- Secure supply chain that meets the demands of homeland security while providing value added to the commercial sector through asset visibility (e.g. condition, location, status – SECURITY)
- Open and interoperable global communications (outlined by DHS), multi-vender, multi-functional devices can all interface with each other to use a common global infrastructure for data transmission.



GTRI Role in Cargo Security

- Developing technologies for tracking containers and monitoring condition since the late 90's- developing ruggedized systems that are needed for the global supply chain
- Department of Homeland Security Science & Technology Directorate (DHS S&T) Program Experience:
  - 2004 – Competitively selected to develop a 6-sided Advanced Container Security Device (ACSD)
    - Container Security Device (CSD) evolved from this effort
  - 2006 – Initial contract to develop CSD to detect and report 2" door openings – only commercial CSD to meet DHS requirements to date
  - 2009 – GTRI ACSD 6-side sensor grid design chosen for integration into a DHS composite container
  - 2010 - Shanghai- China to Savannah, GA Global Secure Supply Chain pilot for testing CSD
  - 2011 – Develop Secure Hybrid Composite Container (teamed with University of Maine)
- Member, WCO committee on e-seals

Successful Testing

- CSD delivered and passed initial DHS testing at Sandia National Labs.
- CSD operation demonstrated to DoD, State, Federal, Industrial, and International community members in August 2009 simulating a supply chain route.
- Now ready for field testing
  http://www.gtri.gatech.edu/media/726

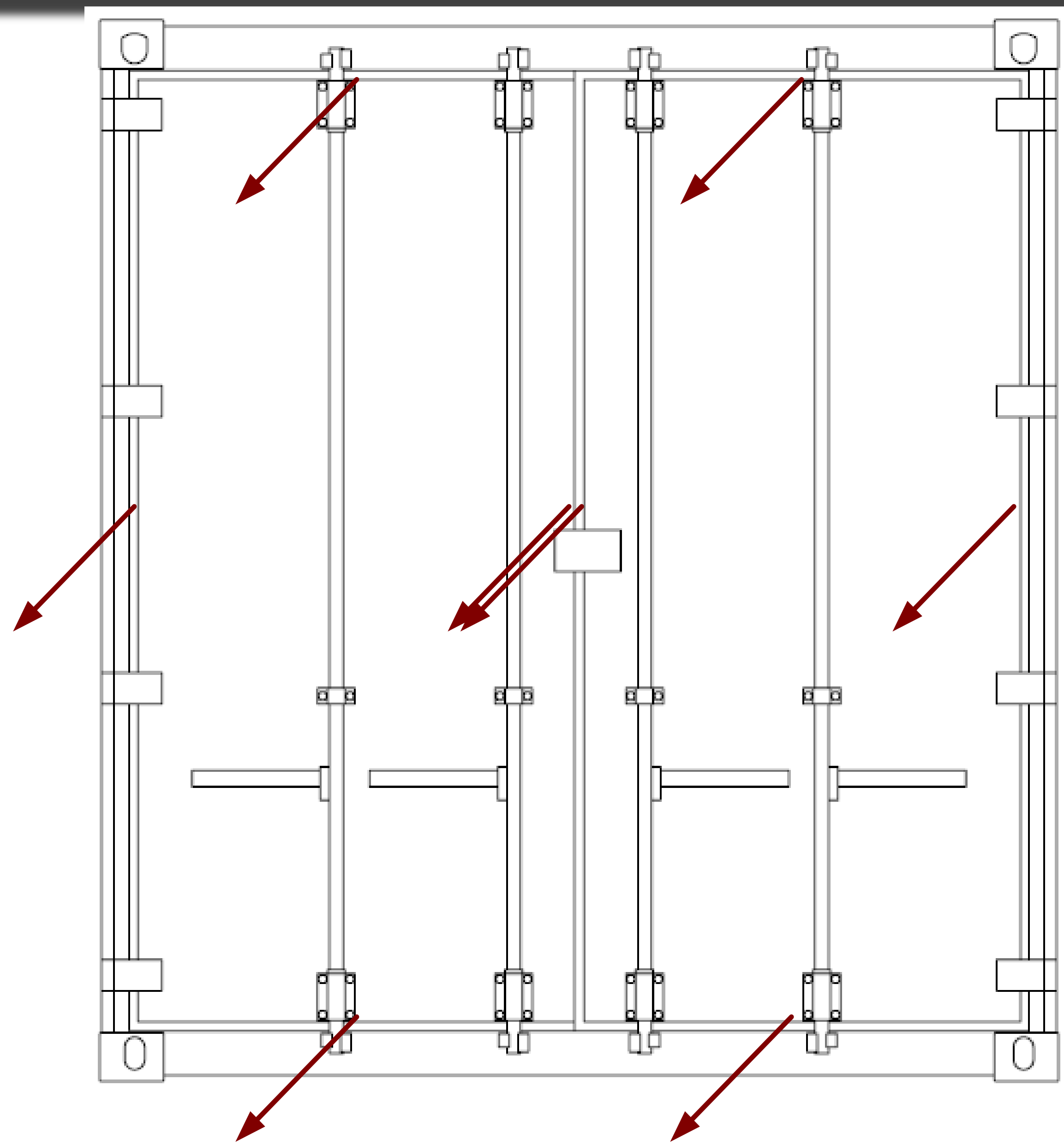
Featured on National Geographic Channel Special

Container Security Device: Door Alarm Functionality and Conditions

- **“Any surface experiencing 2” inches of movement” on all axes**
- Eight potential degrees of movement not just two

A simple home magnetic door device will not work

Certain e-seals are easily defeated

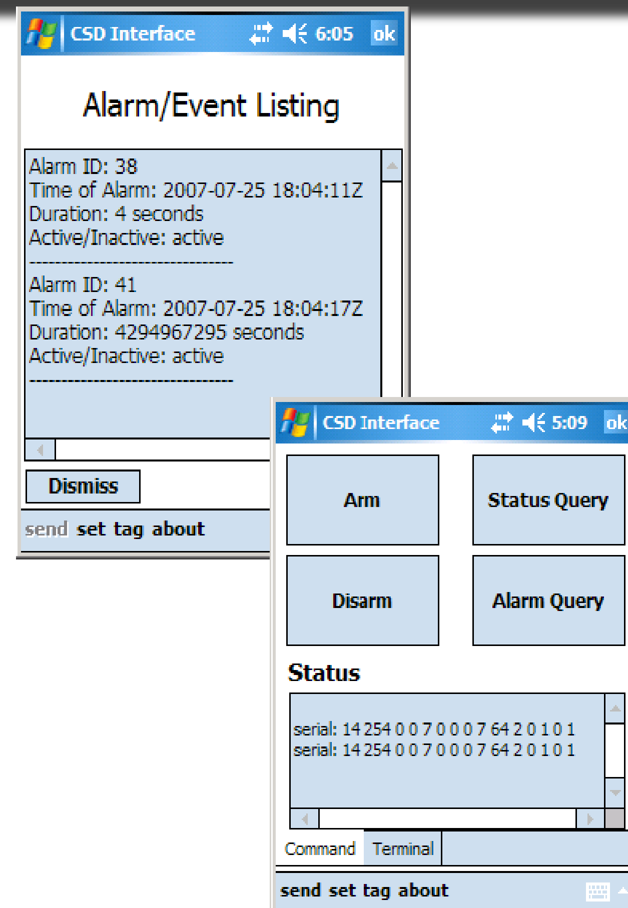


Container Security Device and Breach Detection

Georgia Tech Research Institute

Key Features and Functions:

- Easy installation
- Flexible reuse options
  (one time use or multi-use)
- Cost effective
- Easy battery replacement
- Low false alarm rate
- Located inside container without cargo space interference
- High probability of detection
  (10s of thousands of controlled laboratory testing)
- Robust sensor design with strong immunity to tampering
- Low power consumption



EOSL LABORATORY GEORGIA TECH RESEARCH INSTITUTE

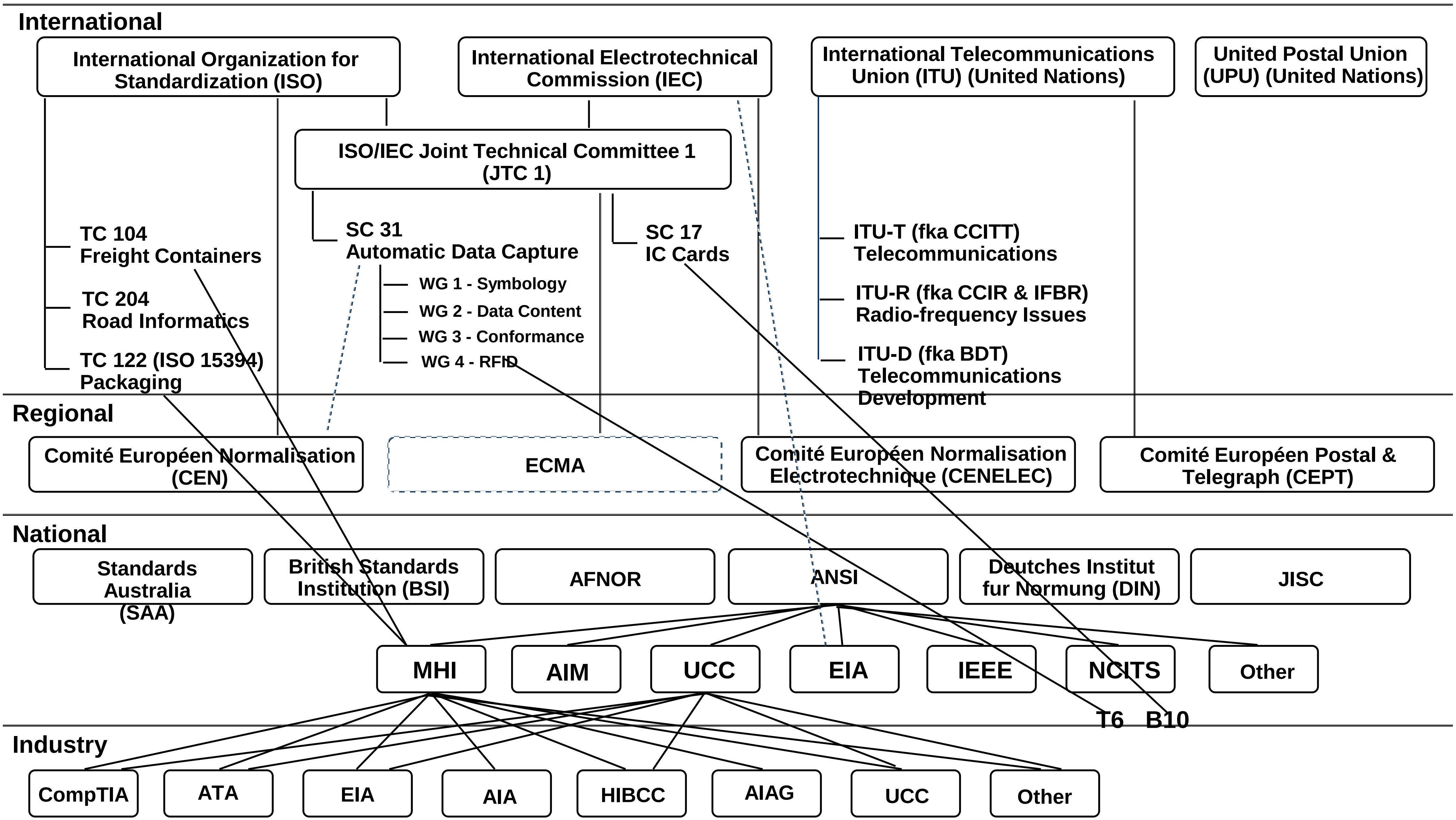
Challenge

- Develop Secure Supply Chain
  - Container Security Device – Monitors door openings
  - Breach Security Device – Detects 3” hole in any of the 6 sides of the container
- Difficulties:
  - Harsh environment
  - Policy
  - International Regulations
  - Interoperability
- Other efforts
  - Hybrid Composite Container – 25% lighter; can integrate security system

Outline

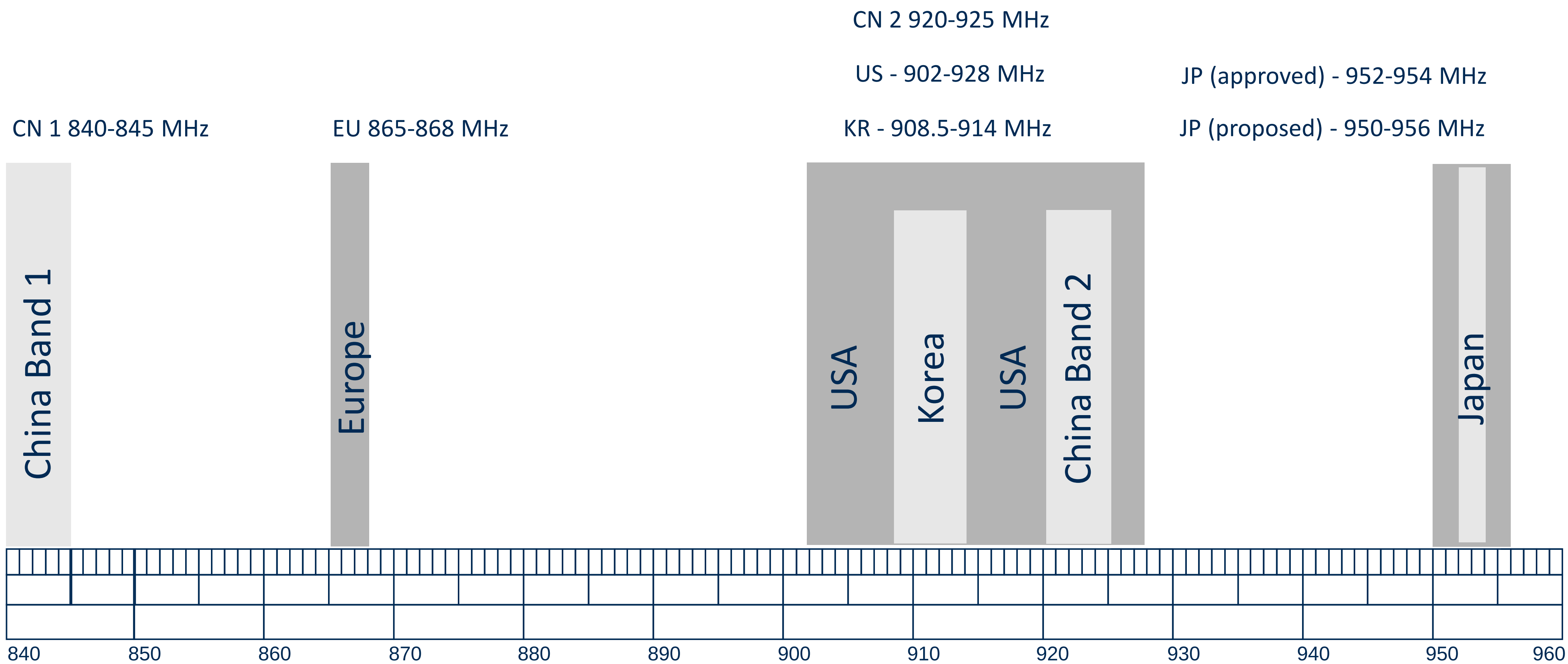
- ✓ Who we are
- ✓ Our Cargo Security Experience
- → Standards
- Things to consider

Standards Organizations*



* Slide Compliments of Craig Harmon, QED Systems

Global Frequency Bands



Reference Documents & Standards

Georgia Tech Research Institute

- International Maritime Organization (IMO) Safety of Life at Sea (SOLAS) Regulation 54.2.2 “Sources of Ignition”
- 802.15.4 – Zigbee
- Certification for radio operations globally
- Data Standards

Environmental Requirements

- Temperature:
  - Operate: -40ºC to +70ºC (IEC 60721-3-2 Table 1)
  - Survive: -50ºC to -40ºC and +70ºC to +85ºC (**IEC 60721-3-2** as above, and **IEC 60721-3-2** Class 2K5 (modified low end to -50ºC)
- Thermal Shock
  - As listed in **IEC 60721-3-2**, Table 1, Class 2K4:
    - from 20ºC to -40ºC in 4 minutes maximum
    - from -40ºC to 20ºC in 4 minutes maximum
    - from 20ºC to 70ºC in 4 minutes maximum
    - from 70ºC to 20ºC in 4 minutes maximum

Environmental Requirements

Georgia Tech Research Institute

- Humidity:
  - 95% humidity over the temperature range from -40^{o}C to +70^{o}C (from IEC 60721-3-2, Table 1)
- Structural Vibration and Mechanical Shock Environments
  - Shock: 10' empty container drop & 5' fully-loaded container drop (from IEC 60721-1, Table 1, Item No. 6.1.3)
  - Vibration (from IEC 60721-3-2, Table 5):
    - 3 m^2/s^3 from 10-200 Hz
    - 1 m^2/s^3 from 250-2000 Hz
- Precipitation
  - Salt Mist, Rain, Impacting Water/Water from sources other than rain, Frost/Ice, Sand & Dust, Fungus (From IEC 60721-1 and IEC 60721-3-6)

Environmental Requirements

- Radiation and Electromagnetic Environments
  - Radiated emissions shall not exceed the limits given in 47 CFR Part 15 (UC FCC Rules on radio frequency devices).
  - Radiated emissions shall not exceed the emission limits for enclosure port type (please see Appendix B for specifics on enclosure ports) equipment installed in the bridge and deck zone of a ship or in the general power distribution zone of a ship, from IEC 60533, Tables 2 and 3, consolidated in the table below.

Frequency Range	Limits
150 kHz to 300 kHz	80 dBµV/m to 52 dBµV/m
300 kHz to 30 MHz	52 dBµV/m to 34 dBµV/m
30 MHz to 2 GHz	54 dBµV/m
Except 156 MHz to 165 MHz	24 dBµV/m

Breach Detection Requirements

Objectives	Requirements
Size of hole to be detected in the container	≥ 3 inch diameter circle
Probability of Detection (P_d)	95%
Probability of False Alarm & Critical Failure (P_{fa})	0.2%
Time to detect and report a hole in the container	≤ 1 second
Alarm Detection Latency	≤ 1 minute
Lifetime Power Source Duration Continuous enabled time	≥ 3,600 hours ≥ 1,680 hours

Requirements Definition – Breach Detection

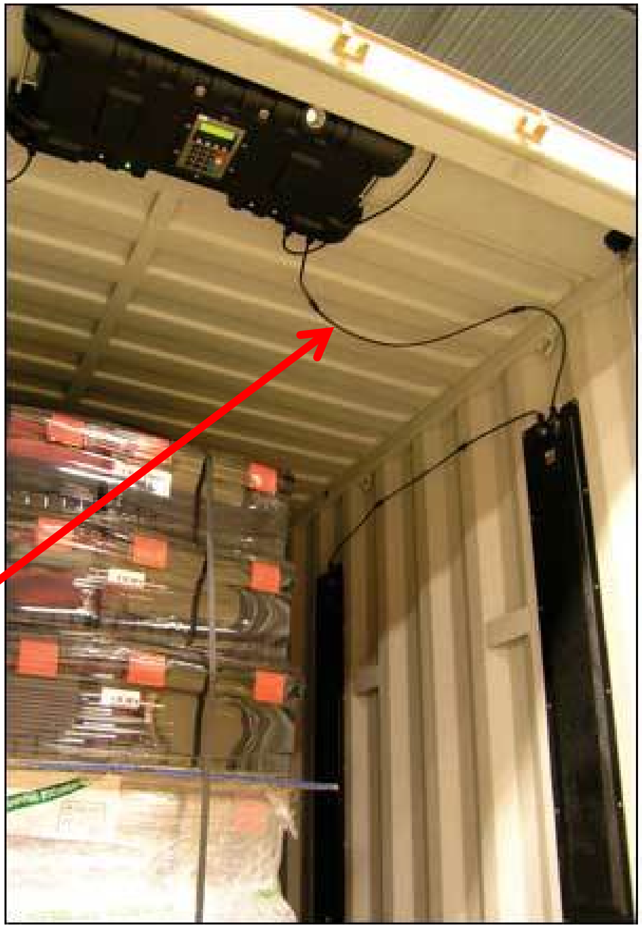
Georgia Tech Research Institute

- A "Hole in the Container" is an opening that was not part of the original container design or construction, that was created during container monitoring, and that provides access to the interior volume of the container.
- "Alarm Detection Latency" is the elapsed time between occurrence of an alarm event and communication relay of alarm status.
  - E.g., time from detection of a breach by a subsystem of the BSD to successfully communicating the breach to the CSD.
- "Lifetime Power Source Duration" is defined as the length of time during which no maintenance of the power source is required and only includes time in the armed state.
  - E.g., This includes enabled time and time from testing of the container to stuffing in a disabled but powered state.

System Installation

- Cables
- Connectors
- Housings

What not to do

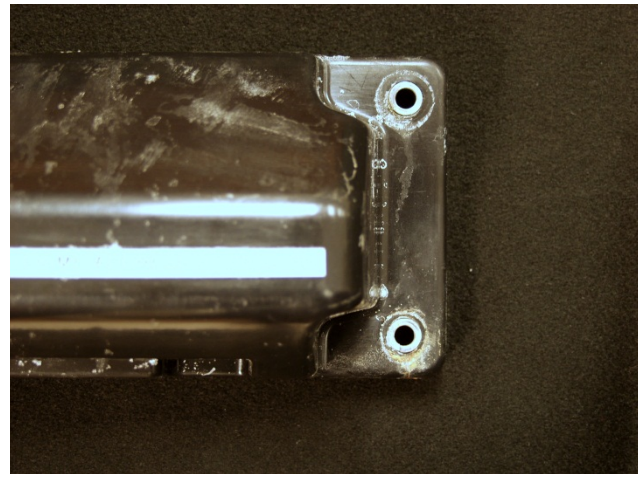


Outline

- ✓ Who we are
- ✓ Our Cargo Security Experience
- ✓ Standards
- → Things to consider

Things to consider

- Testing
  - How do you test Pd & Pfa
- Regulations and Certifications
- Data control
- Upgradability & Interoperability
  - Add sensors, e.g. chemical
  - Mix and match vendor products – no dependency on a single source



How do we test?
E.g. RF Performance Test Standards

Georgia Tech Research Institute

Tag tests:

✓ Tag turn-on performance (ISO 18046-3)

No specific field test guidance

✓ Tag scattering (ISO 18047-6)

ΔRCS: ±2 dB [Pouzin2008]

Reader tests:

× Backscatter sensitivity

No 900 MHz test standards

× Interference rejection

No 900 MHz test standards

- **Current Standards:**
  - ISO 18046-2 (2011)
    - “Test methods for interrogator performance”
  - ISO 18046-3 (2007)
    - “Test methods for tag performance”
  - ISO 18047-6 (2011)
    - “Test methods for air interface communications” (860-960 MHz *con*formance)

Building on the CSD for a Secure Supply Chain

Georgia Tech Research Institute

What next?

- CSD as data source to support better risk assessment?
- Combining CSD data with NII, manifest information, etc to develop an architecture for secure supply chains
- Pilots for the the future can test architecture as well as provide large scale environment for technology applications
- Focus on open standards, global interoperability

Questions?