

2nd Annual Infrastructure Protection and Security Forum

Plan, Prevent, Protect
Melbourne, Victoria, Australia
30th & 31st July 2007

***“Maritime Transportation Infrastructure
Safety & Security From All Hazards”***

National Infrastructure Institute –
Center for Infrastructure Expertise (www.ni2cie.org)
Dale Ferriere, Deputy Director, CDR, USCGR

Presentation Outline

- What are "ALL HAZARDS"?
- WHAT is "Maritime Transportation Critical Infrastructure (CI)"?
- HOW can we protect Maritime Transportation CI?
- RISK Management Applications
- COUNTERMEASURES
- LEGISLATIVE Overview
- Mitigating Risk Public-Private Partnership Example:
"Canada US Cargo Security Project"

ALL HAZARDS

- Heavy Weather (high winds, fog, rain, snow, ice storms, hail, flooding)
- Seismic Events (earthquakes, tsunamis)
- Wild Fires
- Man-made Explosions & Fire
 - Industrial Accidents (Texas City, Halifax)
 - Intentional (Terrorism & Criminal Activity)
- Terrorism (IEDs, EFPs, CBRNE, Toxic Chem-Bio Releases)
- Insanity (Oklahoma City Federal Building, Columbine High School, Virginia Tech. University)

Q? - What is Maritime Transportation CI?

ANS - Physical marine structures, transportation and information systems & people through which a nation's economy operates.

- Dredged & piloted shipping channels & waterways
- Seaports & Their Cities – “seaport came first”
- Marine Facilities (Port Facilities)
- Maritime Cargo & Maritime Commerce
- Intricate Systems & Networks of People Resulting in Exports & Imports
- Maritime Transportation System
- Cargo Ships
- Support Vessels
- Seafarers
- Waterfront Workers
- Other Associated Transportation & Workers (rail, trucking, air)

HOW CAN WE PROTECT MARITIME TRANSPORTATION CI?

- Define & Prioritize CI.
 - Agreed upon risk management applications.
 - Public sector involvement - they own & operate most of it!
- Establish public-private partnerships.
- Improve first responder interoperability, inclusive of privately owned & operated CI.
- Build & develop resilient infrastructure.
- Establish user transparency.

Two months prior to KATRINA, USCG Commandant ADM Thomas Collins said, “Standards are risk driven, not resource driven”.

What is RISK?



Risk Management (RM) Approaches:

- ISO (Aspects & Impacts).
- LOSS PREVENTION.
- THREAT & VULNERABILITY ASSESSMENTS.
- TARGET ANALYSIS (CARVER, CARVER2).
- Comprehensive: Consider all RM approaches.

RM Application: ISO 9001/14001/Physical Security Standards? (Aspects & Impacts)

- **Considers engineering & administrative controls.**
- **Determine RELATIVE RISK using consensus-based decision-making from subject matter experts.**
- **Assigns numeric weights to scenarios (ASPECTS).**
- **Results in determining high probability and high consequence incidents (IMPACTS)**
 e.g., Loss of life, debilitating injuries, environmental & natural resource damages, property damages.

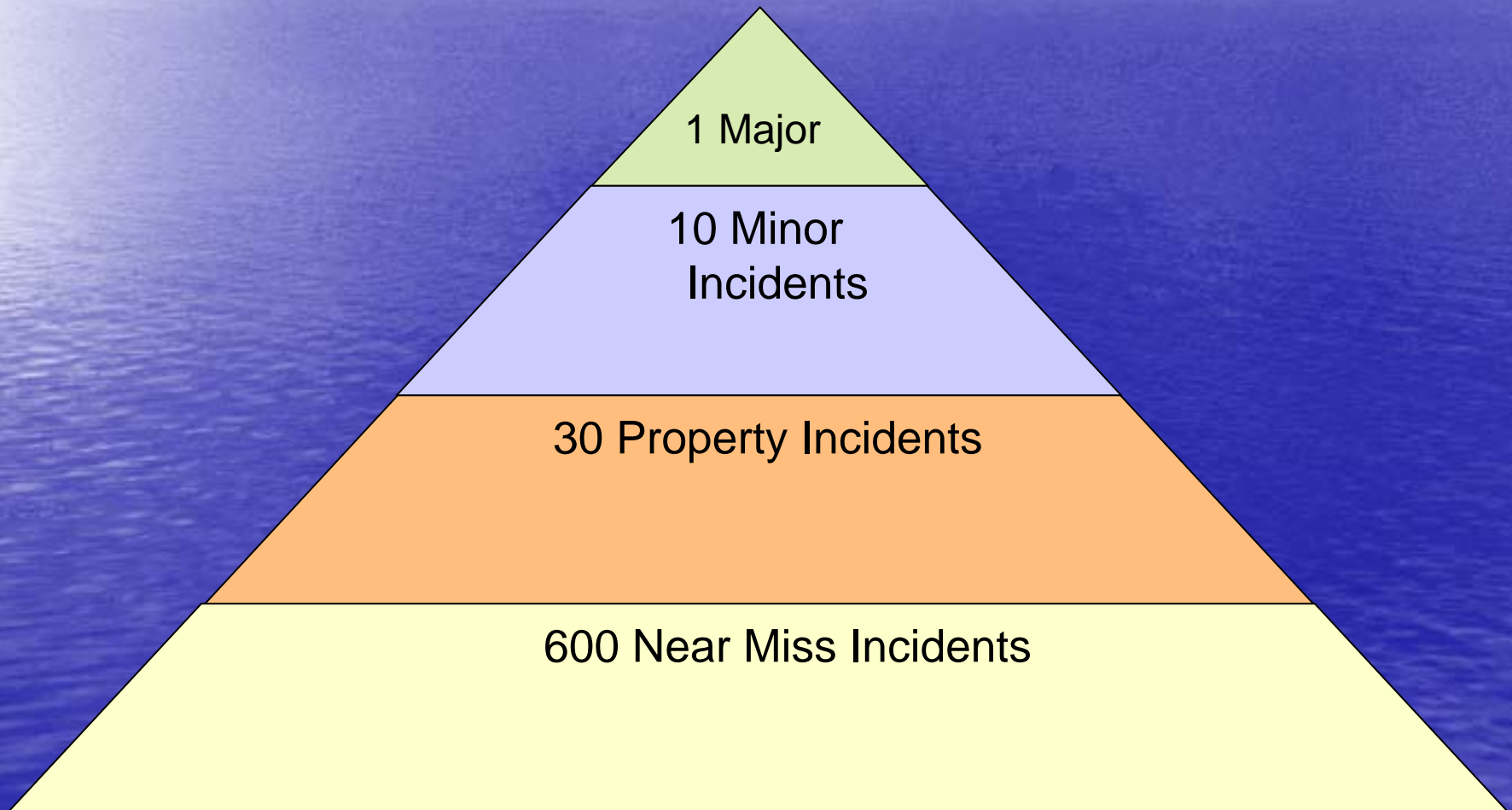
RM Application – ISO 9001/14001 (continued):

- **RISK = Probability X Consequence**
- **Uses Grid Assessment**
- **Low=1, Moderate=2, High=3 Probability (Y-Axis)**
- **Low=1, Moderate=2, High=3 Consequence (X-Axis)**
- **Agree to risk acceptability criteria based on government, industry & corporate standards (as low as reasonably practical - ALARP)**
- **e.g., If RELETIVE RISK = 6 or above then additional controls & countermeasures are required.**
- **Evaluate (assign numeric value) of RISK for each prescribed scenario.**

ISO Approach: Aspects & Impacts – Pro's & Con's

- **Susceptible to “Can’t happen to me” Syndrome.**
- **Won’t fully consider lowest common denominator regarding human factors.**
- **Subjective & consensus based (no scientific units for RISK).**
- **Susceptible to inflating appreciation for pre-existing controls.**
- **If correctly done, then identifies areas of concern.**
- **If correctly done, then includes consideration for legislative compliance, non-compliance & associated liability.**
- **If correctly done, then considers all hazards: industrial accidents, terrorism, heavy weather, management incompetence & corruption.**

RM Application: Loss Prevention Theory: Human & Environmental Factors



RM Application: Loss Prevention Theory – Pro's & Con's

- **When successfully implemented enables an organization to predict & prevent worst case incidents.**
- **Insurance Actuaries do it successfully and for profit, why not maritime transportation companies & government regulators?**
- **Requires time, commitment & consistency.**
- **Favorable results are not initially obvious and therefore subject to criticism.**
- **Won't satisfy impatient executives.**
- **Helps satisfy strict compliance re ISM Code Section 9.2.**

RM Application: Loss Prevention Theory – Organizational Requirements:

- Executive management put “truth” of incident investigations above performance measures (& bonuses).
- Honesty & integrity.
- Standard incident investigation methodology.
- Determine and distinguish immediate & root causes.
- Discipline “Anti-leaders” unwilling to self-critique their personal role in accidents.
- Collaboration & cooperation across areas of subject matter & operational expertise.
- Managers hold a strict liability perspective of risk.

Post 9/11 Revision: $RISK = \frac{\text{Threat} * \text{Vulnerability} * \text{Consequence}}{\text{Countermeasures}}$

- Threat is an unknown hazard over which we have little or no control
e.g., terrorism, heavy weather, criminal activity. To detect & pre-empt emerging threats requires Maritime Domain Awareness & Effective information & intelligence gathering & sharing (See Canada US Cargo Security Project).
- Vulnerability is where & how built infrastructure and systems which CI supports are susceptible to hazards.
e.g., maritime transportation system & its corresponding CI.
- How to compare & prioritize TARGETs (see CARVER & CARVER2)?
- Consequence is resulting losses to people, property & processes.
- Countermeasures are actions taken to minimize vulnerabilities.

RM Application:
Distinguishing CARVER2 from CARVER

- **C2 Identifies relative "worth" of each key asset and ranks and rates assets across sector lines.**
- **C2 alters traditional CARVER analysis by forcing users to ask the same security questions about all assets regardless of sector type.**
- **C2 is non-technical, uses open source information, and is designed for use with less than one hour of training.**
- **C2 identifies inter-relationships between various infrastructures.**
- **C2 may also be used when doing an analysis based on structural attack, including from natural hazards or following a chemical or biological attack.**
- **C2 is not a replacement for traditional target analysis.**

Maritime Transportation Infrastructure Safety & Security From All Hazards



NI² Center for Infrastructure Expertise

CARVER²

SCORE : 0 - 0

Inspector

Inspector

Organization

Asset Name

Address

Sector

Asset Identification Number

GPS

GIS

Subtype

Criticality

Impact of Loss of Asset

Users Affected

Direct Economic Loss
and Cost to Rebuild (\$)

Potential Deaths from Attack

Accessibility

Ease at which terrorists can enter infrastructure
to cause its destruction

Remote Site?

Yes No

Recoverability

Time needed to replace
infrastructure, if possible

Vulnerability

Susceptibility of infrastructure to destruction

Choose

Blast

Chem/Bio

Espyability

Is the infrastructure an "icon" - representing more
than a physical structure, i.e. national monument

(Notoriety)

Redundancy

Are there "back up" facilities/equipment
that will offset the infrastructure loss

Interdependency

Additional CI Sectors Affected by Loss of Asset

Agriculture

Public Health

Defense Industry

Transportation

Post Office, Shipping

Food

Emergency Services

Information/Telecom

Bank Finance

Icon

Water

Government

Energy

Chemical, Hazard Mat'l

New

Save

Delete

Go to Record Number:

Go

Refresh

Record 1 of 1



RM Application - After C2 Assessment perform following for prioritized CI:

- Assume each hazard type is IMMINENT.
- Then identify most vulnerable aspects.
- Determine what hazard type each CI is most vulnerable to:
 - heavy weather
 - seismic events
 - man-made events
- Consider exposure type & route of entry (CBRNE, projectiles, heat, etc.), then assess resulting consequences. Are these consequences acceptable? If "no" then requires action.
- Re-consider objectives (protection & recovery)
- Identify applicable & cost-effective administrative controls & countermeasures.

RM Application: Terrorism Threat Vectors

Post 9/11 Revision: $RISK = \frac{Threat * Vulnerability * Consequence}{Countermeasures}$

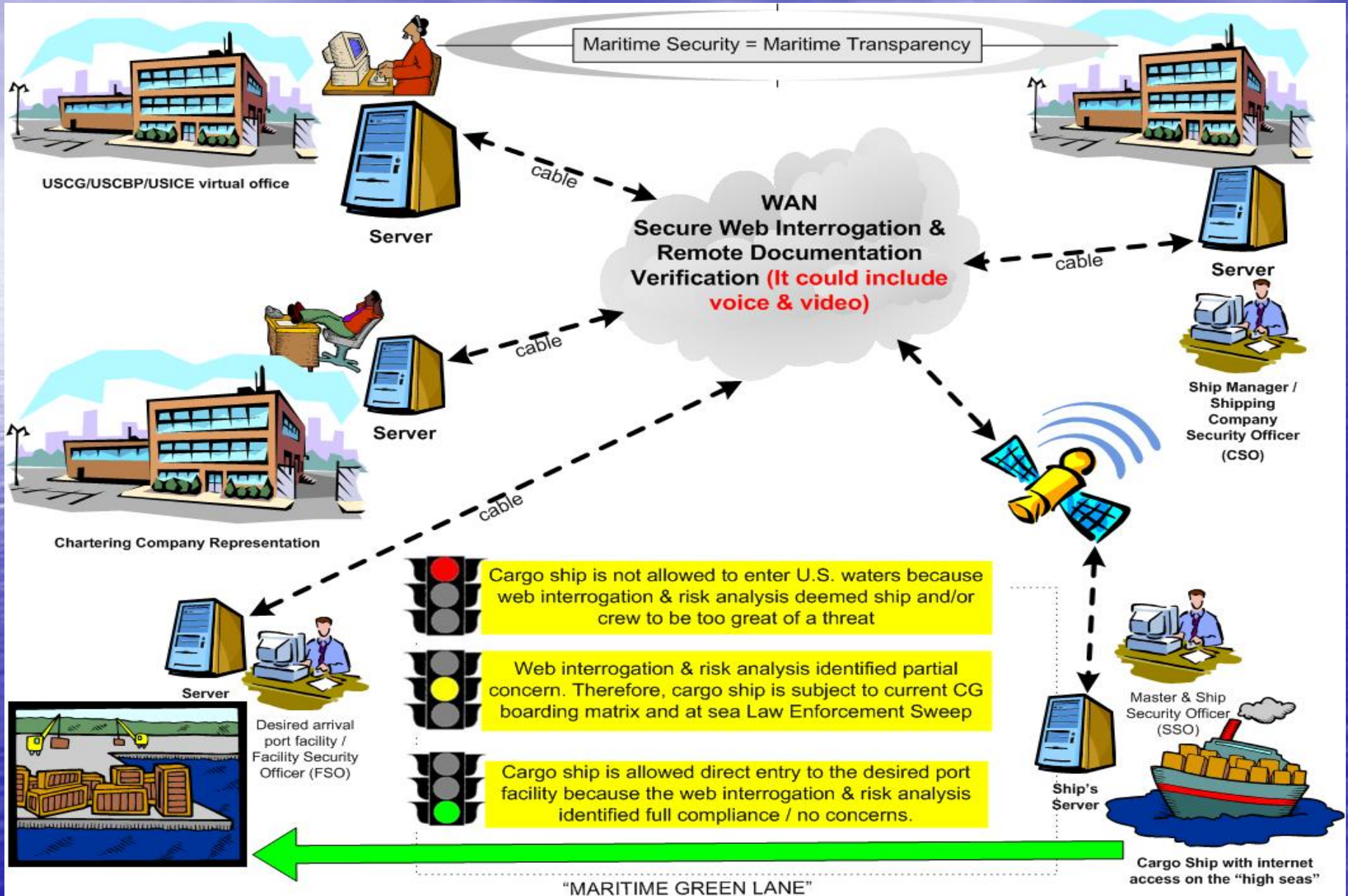
- **Terrorism – Maritime Transportation CI Threat Vectors:**
 - people
 - waterborne vessels & ships
 - underwater vehicles & divers
 - shore-side vehicles
 - airborne vehicles
 - marine & domestic commerce
- **Terrorists and/or criminals leveraging inter-modal cargo, bulk cargo, commercial ships, seafarers, waterfront workers, pilots, government regulators as means for their devastating ends.**

Countermeasures

- **Access Control Technologies (waterside & shore-side)**
 - real & virtual fencing
 - CCTV networks
 - sensor networks
 - radar
 - sonar
 - other
- **Smart & Intelligent Technologies**
 - Instrumented inter-modal cargo containers
 - Shipboard sensor networks
 - Port facility sensor networks
 - Worker Credentialing & Biometrics
- **Ship & Cargo Targeting Systems Using AI**
- **Virtual Sea Border**
- **Virtual Seaport Fusion Centers**
- **Financial & Legal Incentives**

Maritime Transportation Infrastructure Safety & Security From All Hazards

USVSB



Maritime Security Legislative Protocols ISPS CODE & MTSA Pros & Cons

- **Establishes structure & organization**
e.g., Ship Security Plans, (Port) Facility Security Plans, Company Security Officer, Ship Security Officer, (Port) Facility Security Officer.
- **Establishes shipboard & facility security protocols.**
e.g., How to raise security levels (MARSEC), How to notify the port state following a security breach, etc.
- **HOWEVER, Accountability & Liability for security breaches are weakly defined (Who pays? Who is the responsible party?)**
- **HENCE, Maritime industry is reluctant to take ownership of security & Innovation is subsequently driven by government.**

INTER-MODAL CARGO CONTAINERS:

■ Threats:

- People (terrorists), weapons, WMD components, contraband – smuggling – stolen & missing containers – both in-bound and out-bound transportation risk exposure.

■ Vulnerability:

- Lack of supply chain linkage accountability – too many unknown entities – easy to infiltrate – easy to corrupt – portal scanning technology is not fool-proof – cannot visually inspect every container – can government resolve without supply chain industry collaboration? – What to do?

Canada US Cargo Security Project -

- WHAT IS IT? Private-public partnership & collaboration.
- In-container sensor network & satellite supported communication system.
- Real-time report of sensor outputs to user's desk-top computer.
- Sensor types – accelerometer, thermometer, barometer, geo-position, radiation detection, ultra wide band radar.
- RESULTS?
- Demonstrated i-Containers are feasible.
- Future is now: Integrating in-container sensor networks with global cargo information network will make each supply chain link (human node) completely transparent & therefore threat resistant.
- COSTS & BENEFITS?
- Won't move forward until there is clear financial incentive e.g., potential for unlimited liability for breach of security resulting in terrorism.



Canada-US Cargo Security Project



Kique Romero
UWB Radar Research and Development
Lawrence Livermore National Laboratory, University Of
California

(925) 423-2830, romero29@llnl.gov

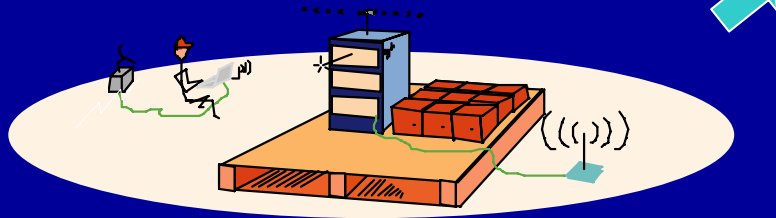
September, 2006

University of California

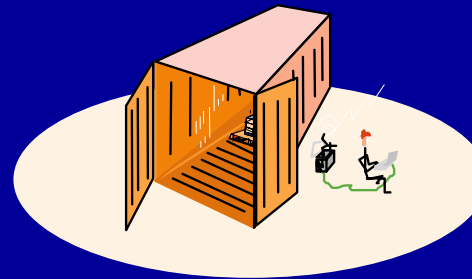
This work was performed under the auspices of the
Department of Energy by the Lawrence Livermore National
Laboratory under contract W-7405-Eng-48

System explored the ability to track and monitor over the complete shipping cycle

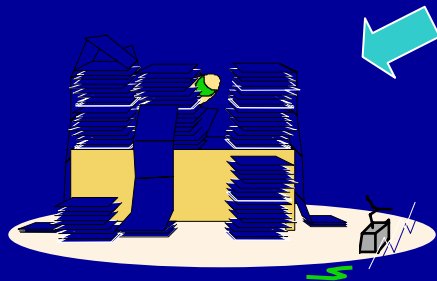
1) Build & test prototype package



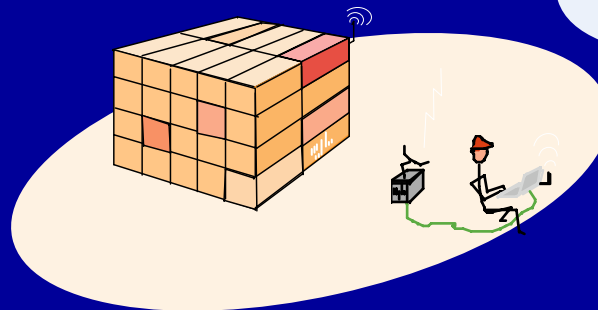
2) Install & verify package and scan at load point



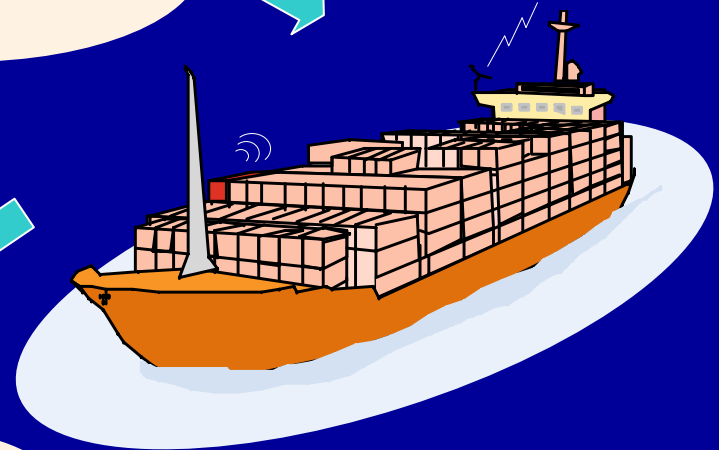
5) Compare logged and real-time data



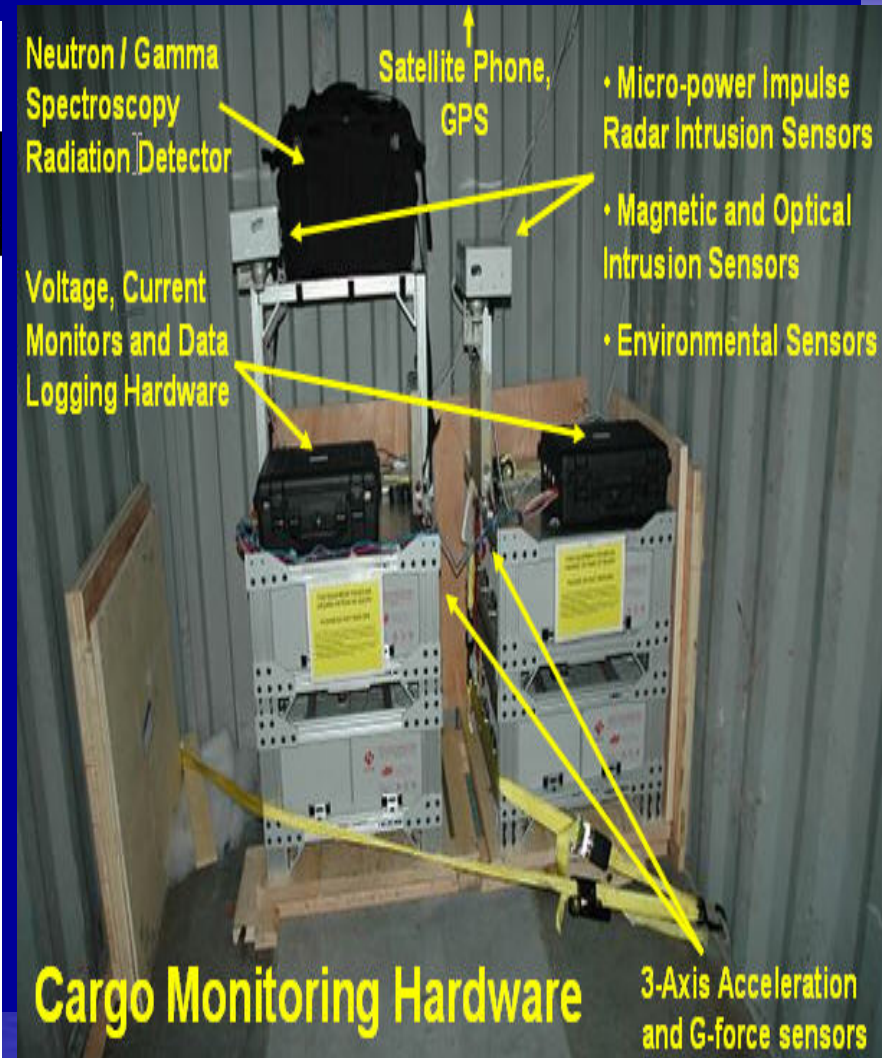
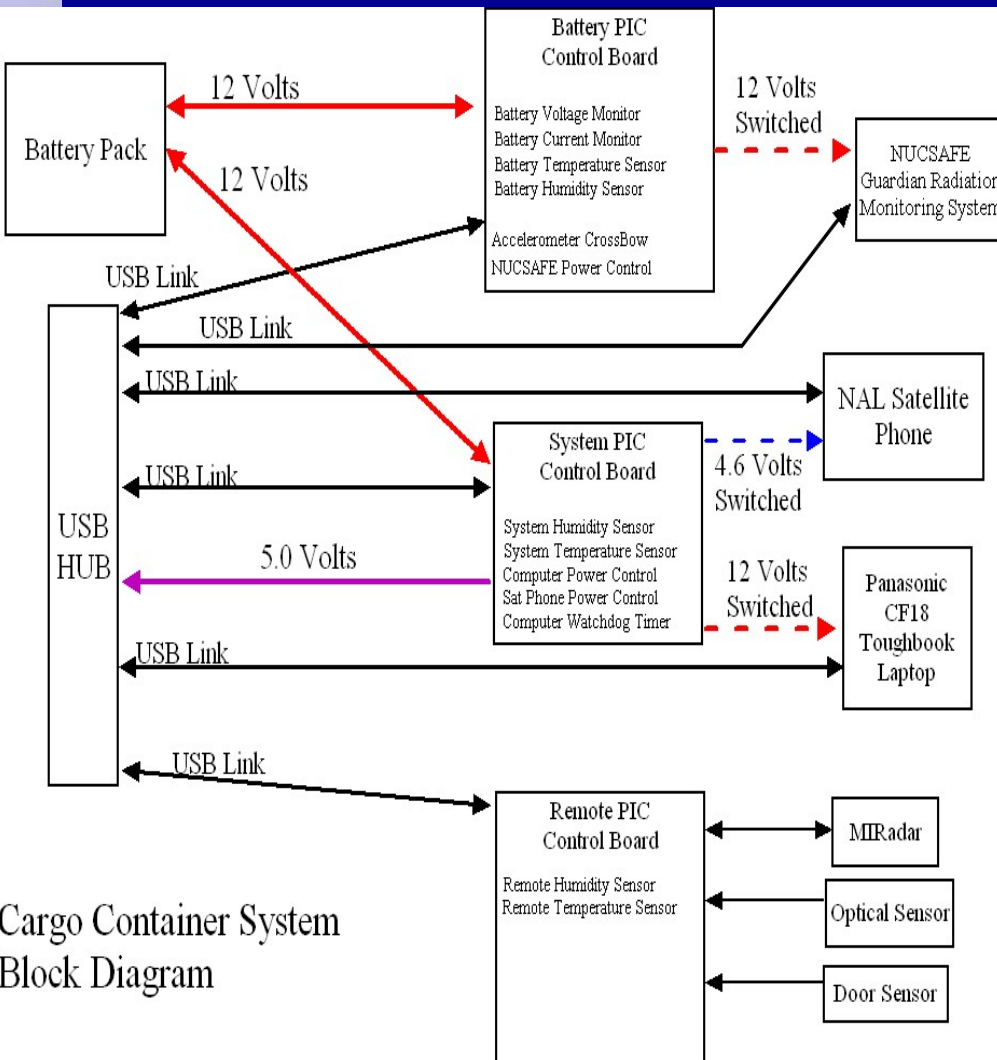
4) Scan at transshipment points



3) Track shipment, log data & report status to website



The system will characterize the environmental data and event data



Secure, real time, adaptive communications will transmit data

