
Department of Homeland Security Control Systems Security Program Transportation Sector

David Sawin – Program Manager

**Bob Hoaglund, CSSP - Maritime Transportation Modal Lead
Control Systems Security Program / ICS-CERT**



**Homeland
Security**

Agenda

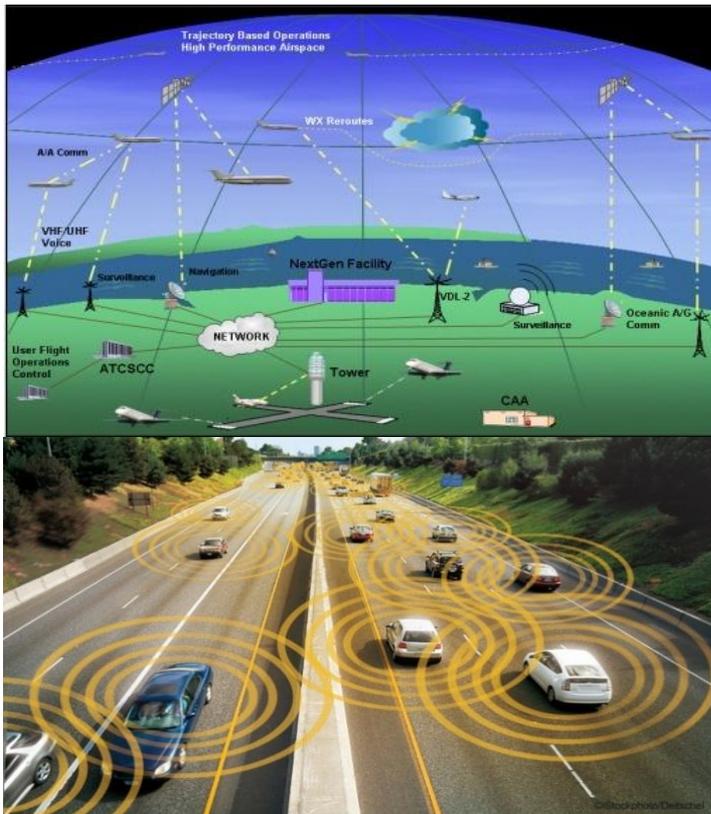
- Overview of Department of Homeland Security Control Systems Security Program (DHS CSSP) Transportation Sector
- Discussion of risks/vulnerabilities, opportunities within the maritime industry
- Next steps for Maritime



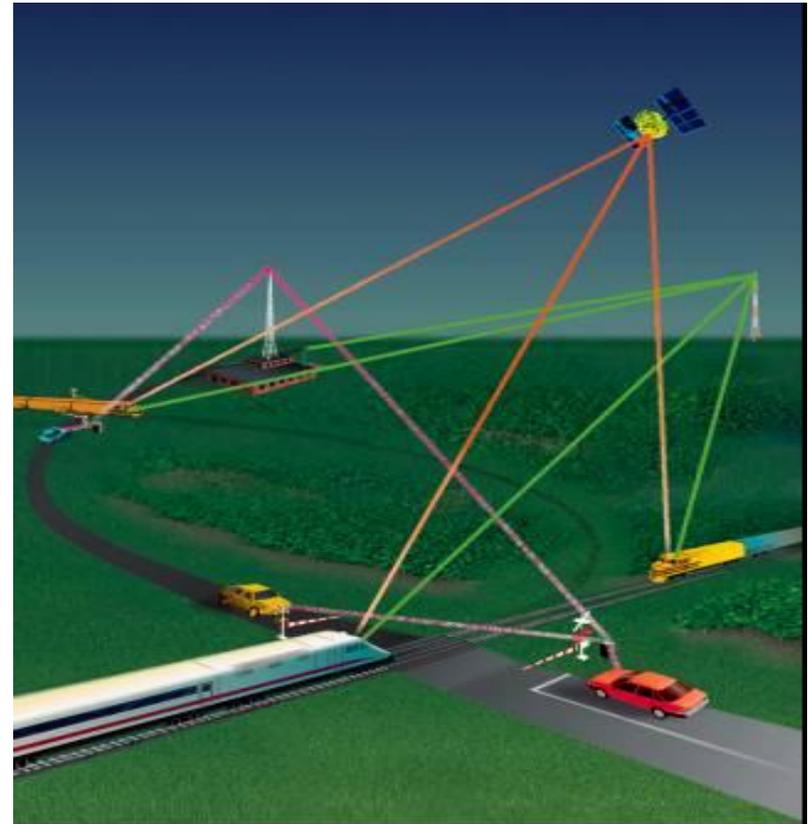
Homeland
Security

Transportation Control Systems Are Highly Connected

- Transportation is increasingly interdependent using wireless communications



Any printed version of this picture should include: ©iStockphoto/Detschel
Photo number 7201240 should be purchased for each project in which this image is used.



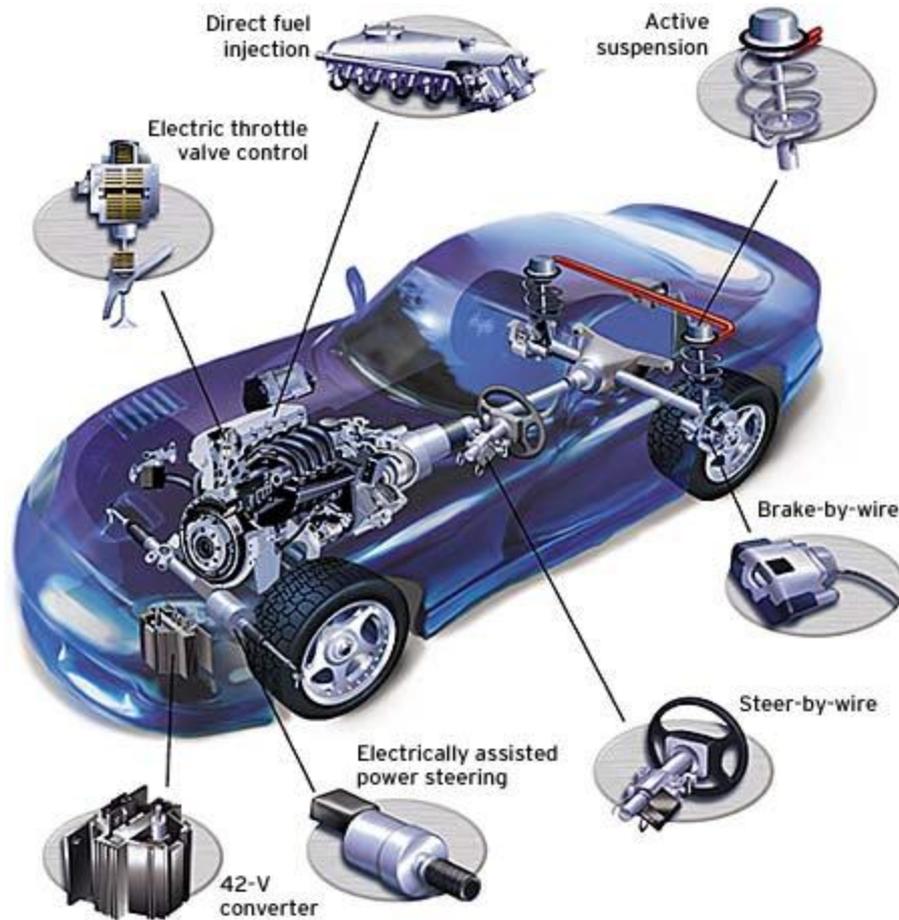
Homeland
Security

E-enabled vehicles are now the norm...



Homeland
Security

...for all of us!



Homeland
Security

Control Systems Security Challenges

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus & Mobile Code	Common & widely used	Uncommon and can be difficult to deploy
Support Technology Lifetime	3-5 years	Up to 20 years
Outsourcing	Common/widely used	Rarely used (vendor only)
Application of Patches	Regular/scheduled	Slow (vendor specific)
Change Management	Regular/scheduled	Legacy based – unsuitable for modern security
Time Critical Content	Delays are usually accepted	Critical due to safety
Availability	Delays are usually accepted	24 x 7 x 365 x forever
Security Awareness	Good in private and public sector	Generally poor regarding cyber security
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages / audit
Physical Security	Secure	Remote and unmanned



18 Critical Infrastructure Sectors

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S. critical infrastructure into the following 18 CIKR sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- **Transportation**
- Water and Water Treatment



Many of the processes controlled by computerized control systems have advanced to the point that they can no longer be operated without the control system



**Homeland
Security**

Partnership Between DHS and DOT/Volpe

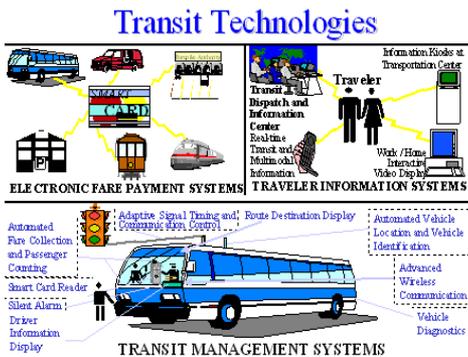
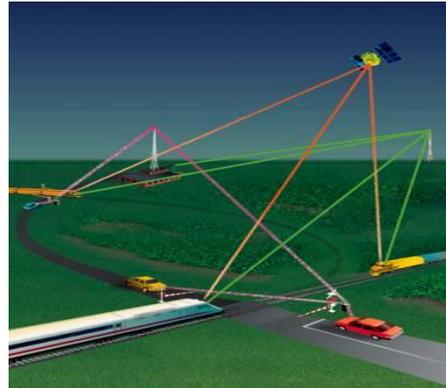
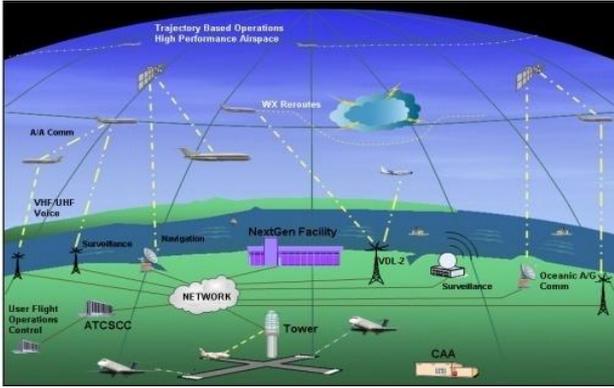


- Outreach
- Site Assessments
 - Cyber Security Evaluation Tool (CSET)
- Standards, best practices, training
- Transportation Sector Control System Security Roadmap



Homeland
Security

Growing Dependencies Could Increase Risk



Homeland Security

Maritime Automated Systems



Homeland
Security

Terminal Automation

➤ Information Technology

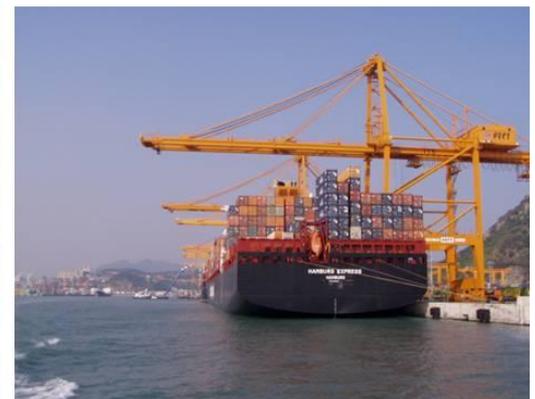
- Terminal Operation System (TOS)
- Container Terminal Management System (CTMS)
- Payroll, other back office systems

➤ Communications

- E-mail, cargo messages
- Website, cargo tracking
- Wireless, cargo apps

➤ Access Control

- Security / ID Card system
- CCTV
- Truck gates
- Personnel gates



Terminal Automation

- **Scheduling Software**
 - Vessels
 - Yard equipment
 - Maintenance
- **Control Systems**
 - Seaside cranes
 - Yard Cranes
 - Other Yard Equipment
 - Remote monitoring
 - Buildings
 - Gates



Vessel Automation

➤ Navigation

- Radar
- Automatic Identification System (AIS)
- Electronic Charts (ECDIS)
- GPS

➤ Communications

- Radio
- Satellite
- Broadband
- Internet, E-mail

➤ Integrated bridge

- All systems interconnected
- Auto Helm



Automated Container Terminal Entrance

- Optical Character Recognition Reads Vehicle & Container ID
- Imaging can also detect container damage, lock system



Driverless Vehicle

Hamburg Germany. Driverless vehicle moving 40' container to automated storage crane.



Homeland
Security

Crane Accident

Oakland, CA. Dropped cargo container too early. Is this a result of a Control System failure?

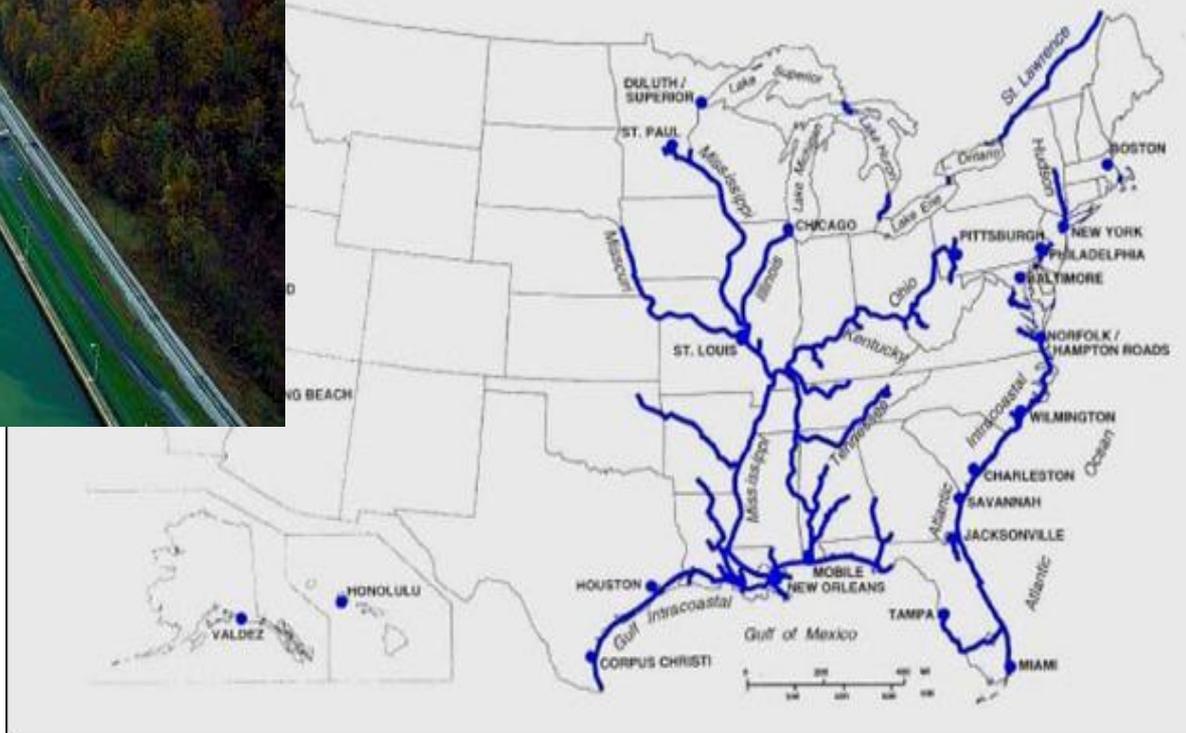


Homeland
Security

Inland Waterway System



Ports and Navigable Waterways of the United States



Fire Onboard

- Could bad planning software have made it worse?
- Hazmat too close together?



Navigation Malfunction

- Human error or equipment malfunction?



Navigation Error

- Rotterdam. Human error or equipment malfunction?



Vessel Balance Accident

Liberia. Vessel storage usually planned with bay planning software.



Homeland
Security

Rollover Accident

- Antwerp 2007. Vessel instability due to ballast tanks?
- Software or human error?



Vessel Accident – Bayplan Software

- MV Annabella
- Load plan/bayplan software did not recognize 30' containers and assumed all were 40'.
- 7 stacked 30' containers weighed 225 tons – no alarm
- Bayplan would alarm if 40' container stack weighed 240 tons.
- Stack collapsed during voyage.
- 26 Feb '07



Vessel Accident

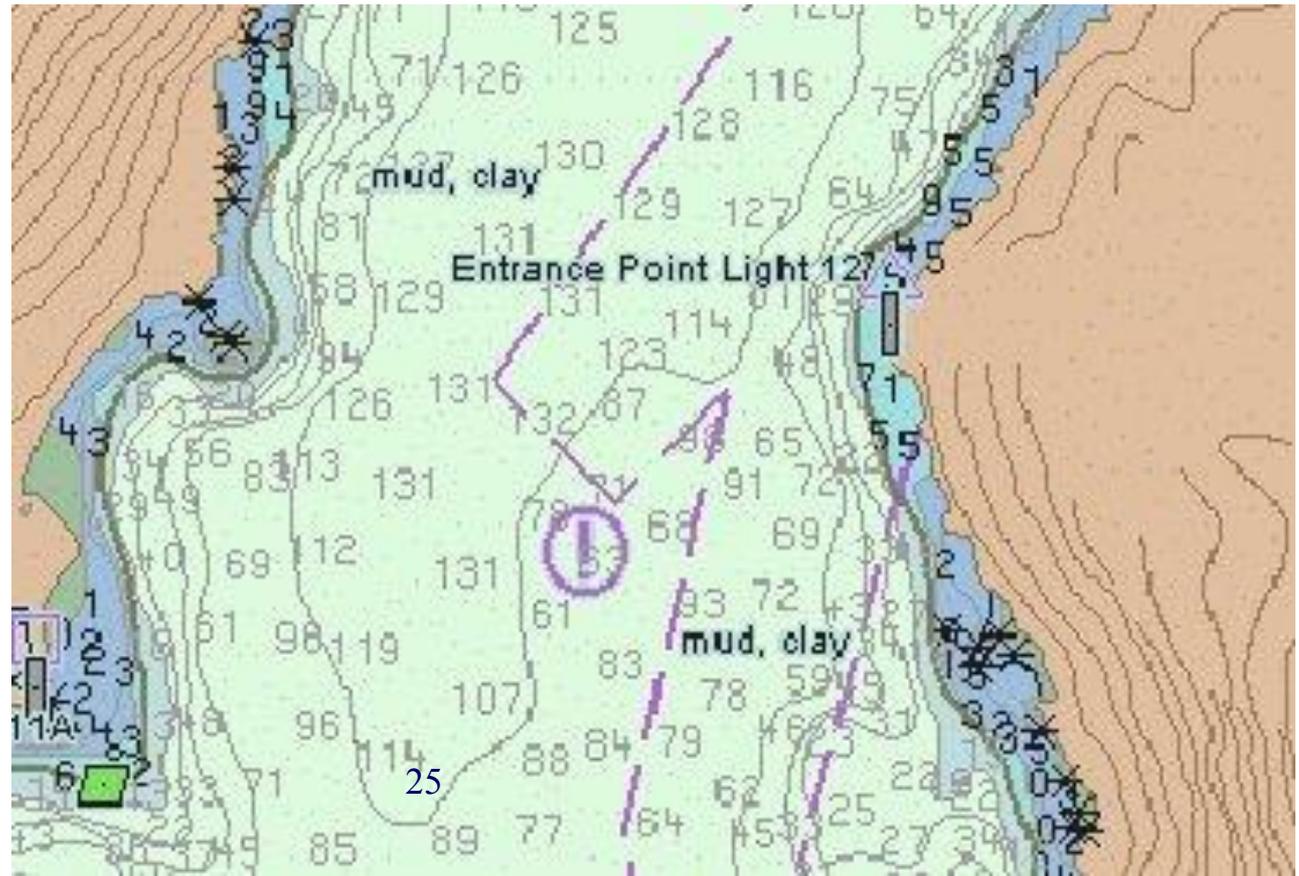
- MV Royal Majesty – Bermuda to Boston
- Integrated bridge, 2 GPS & electronic charts (ECDIS)
- Antenna line broke and GPS registered Dead Reckoning (DR) for 30 hours. DR is estimated position based on speed and heading.
- Crew didn't notice DR indicator light or 2nd GPS



Vessel Vulnerability

Resolution of Electronic Charts

- Electronic chart display system (ECDIS)
- Systems may show different underwater hazard
- Wrecks, rocks, & other underwater obstructions.



Homeland
Security

Dry-dock Malfunction

Dubai. Opened sea gate while workers were under vessel resulting in 27 deaths and the loss of 2 vessels.



Countryman & McDaniel



Homeland
Security

Maritime Mode Progress to Date

Surveyed

- 3 vessels docked on the east coast
- 2 container terminals on the east coast
- 1 in the Gulf of Mexico

CSET Assessments

- 3 at southern US Port

Outreach to over 15 Maritime organizations

3 Site briefings scheduled

Cruise Industry



Need Strategies to Strengthen Security

- Cybersecurity requires a lifecycle approach



Risk assessments
Standards
Design practices
Certification
Monitoring
CIA



**Homeland
Security**

Next Steps for CSSP-Transportation



- Expanding CSSP assistance to all transportation modes
- Help industry define cybersecurity issues
- Transportation Roadmap



Cybersecurity is a Shared Responsibility

Report cyber incidents and vulnerabilities to:

www.us-cert.gov

Or send e-mail to:

soc@us-cert.gov,

ics-cert@dhs.gov

Or call:

877-776-7585 (ICS-CERT)

888-282-0870 (US-CERT)

Get more information at: www.us-cert.gov/control_systems



**Homeland
Security**

Questions / Feedback

Bob Hoaglund - CSSP

US Department of Transportation

Volpe National Transportation Systems Center

(617) 494-3653

Robert.Hoaglund@dot.gov



**Homeland
Security**



Homeland Security