Control Systems Security Program - Transportation

DHS CSSP

ICSJWG Conference – Seattle

October 27, 2010

David Sawin

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation

Research and Innovative Technology Administration

Cyber Security is a National Issue

Howard Schmidt
White House Cyber Security Coordinator

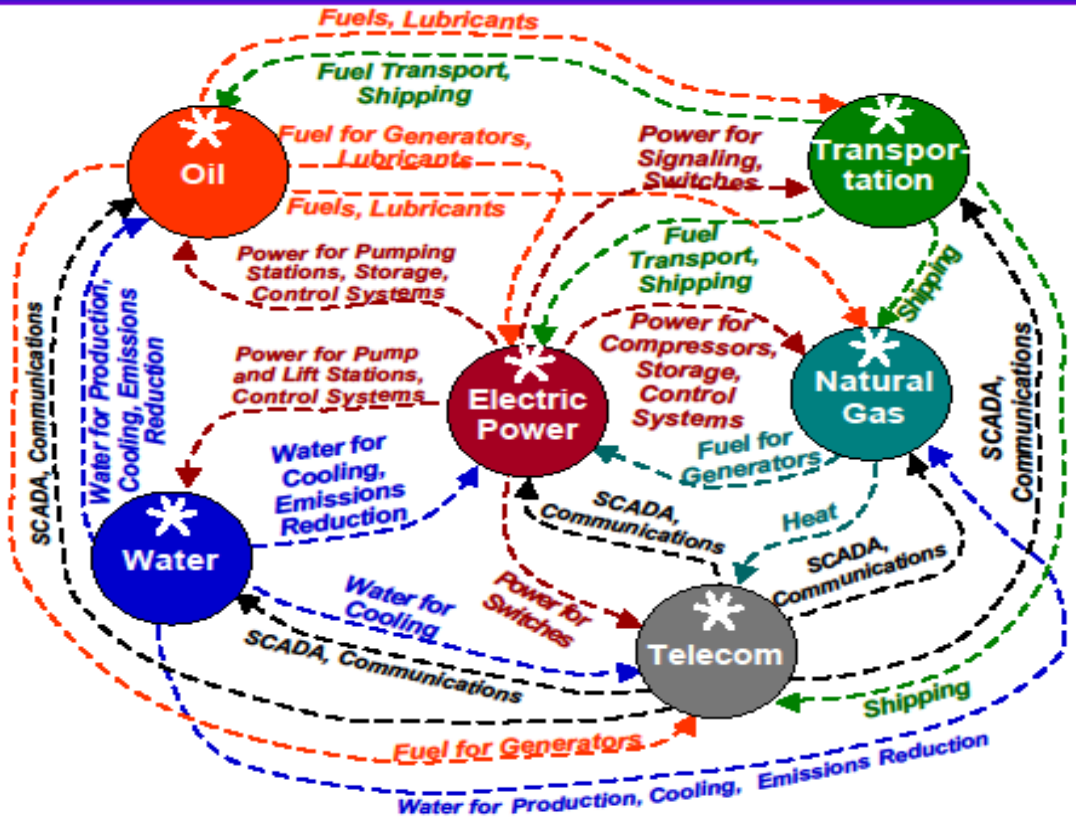
- Howard Schmidt appointed White House Cyber Security Coordinator, Dec. 2009
- 2010 Protecting Cyberspace as a National Asset
- PDD63 – Critical Infrastructure

18 Critical Infrastructure Sectors

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified & categorized U.S. Critical Infrastructure into the following 18 Critical Infrastructure & Key Resources Sectors

1. *Agriculture & Food*
2. *Banking & Finance*
3. *Chemical*
4. *Commercial Facilities*
5. *Dams*
6. *Defense Industrial Base*
7. *Emergency Services*
8. *Energy*
9. *Government Facilities*
10. *Information Technology*
11. *National Monuments & Icons*
12. *Nuclear Reactors, Materials, & Waste*
13. *Postal & Shipping*
14. *Public Health & Healthcare*
15. *Telecommunications*
16. ***Transportation***
17. *Water*
18. *Critical Manufacturing**

Examples of Infrastructure Interdependencies



Source: Heller, M (2001). Interdependencies of Civil Infrastructure Systems. *The Bridge*, a publication of the Nation Academy of Engineering. V. $, #31, 2001

The John A. Volpe National Transportation Systems Center

U.S. DOT strategic goals

- Safety/Security
- State of good repair
- Economic competitiveness
- Livable communities
- Environmental sustainability

Photo courtesy of the Volpe Center

Volpe Center mission, vision and capabilities

Mission and vision

- A world-recognized Federal center of excellence and leader in transportation
- Trusted enabler of critical improvements to transportation and logistics systems
- Leader in government, industry, and academic cooperation

Unique capabilities

- Institutional knowledge of the global transportation systems
- Awareness of Federal responsibilities, objectives, and activities in the public interest
- Experience with the full spectrum of technologies and disciplines relevant to transportation system improvements

Centers of Innovation at the Volpe Center

- Multimodal Systems Research and Analysis
- Safety Management Systems
- Environmental and Energy Systems
- **Freight Logistics and Transportation Systems**
- Physical Infrastructure Systems
- Communication, Navigation, Surveillance and Traffic Management Systems
- Human Factors Research and System Applications
- Advanced Vehicle and Information Network Systems

Volpe Center Cyber Security Life Cycle Support

Volpe Center Cyber Security Life Cycle Support

FAA

- National Airspace System (NAS) Vulnerability Assessment for PDD-63
- ~ 50 C&A's and Penetration Testing for the National Airspace System
- GPS Vulnerability Assessment
- Cyber Security Awareness Training & Workshops
- Cyber Security Incident Response Center (CSIRC)
- Airborne Network IA Support (Security/Safety R&D studies, RTCA SC-216)
- B-787 Security Certification and Cyber Training Support
- Aerospace Network Security Simulator
- WebCM – C&A, Operational Support, Configuration Management Tools

Volpe Center Cyber Security Life Cycle Support

USAF/TSWG

- Joint USAF/Civil AN R&D Plans for Secure Airborne Networks
- AN Workshops (US and UK)
- Electronic Flight Bag Security Use Case/Risk Assessment
- Commercial Derivative Aircraft Cyber Papers

OTHER

- NASA – Airborne Network IA Research Studies
- TSA – Transportation Worker Identification Card C&A
- Maryland Intelligent Transportation System Cyber Security Assessment
- DOT Intelligent Transportation System JPO - Trust Model for *Intellidrive*

Volpe Center Supporting DHS Control System Security Program in Transportation

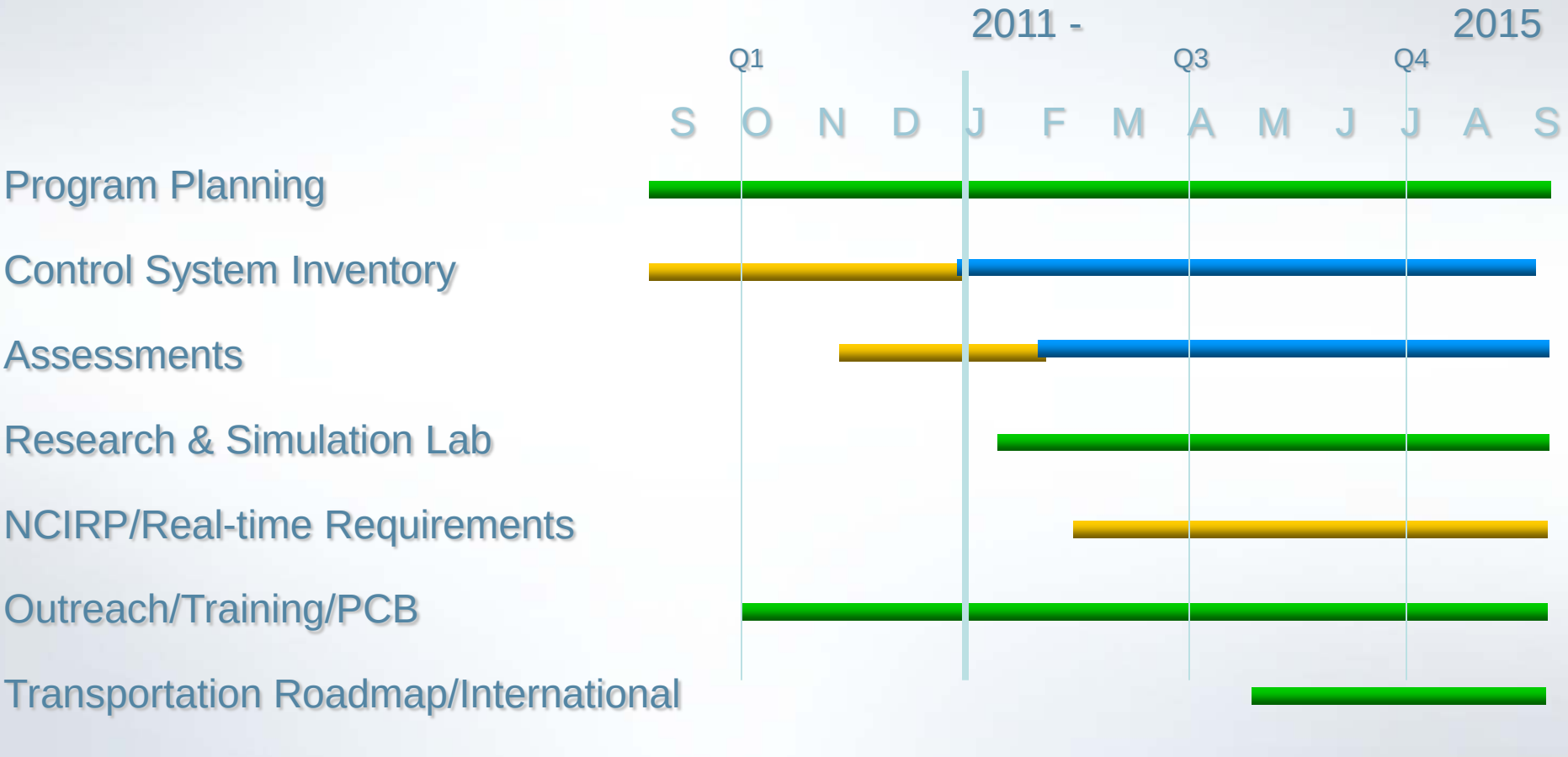






- Control system inventory
- Threat and vulnerability assessments
- Research and simulation laboratory
- National Cyber Incident Response Plan
- Real-time reporting concepts
- Outreach, training and professional capacity building
- Transportation Control System Security Roadmap
- International Collaboration

Planned Engagement of Modes

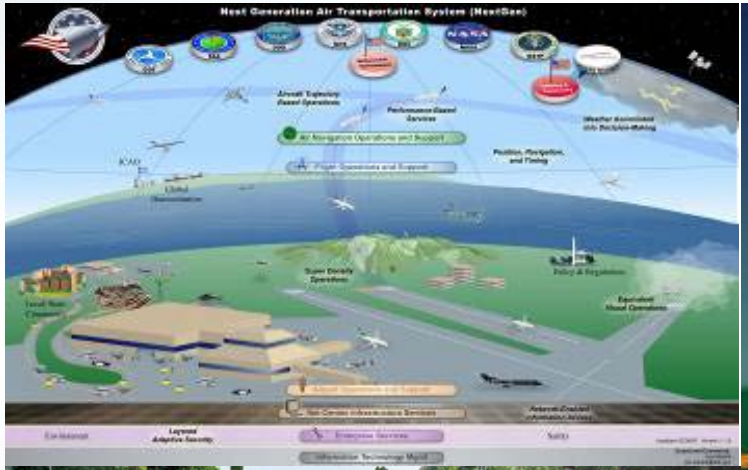


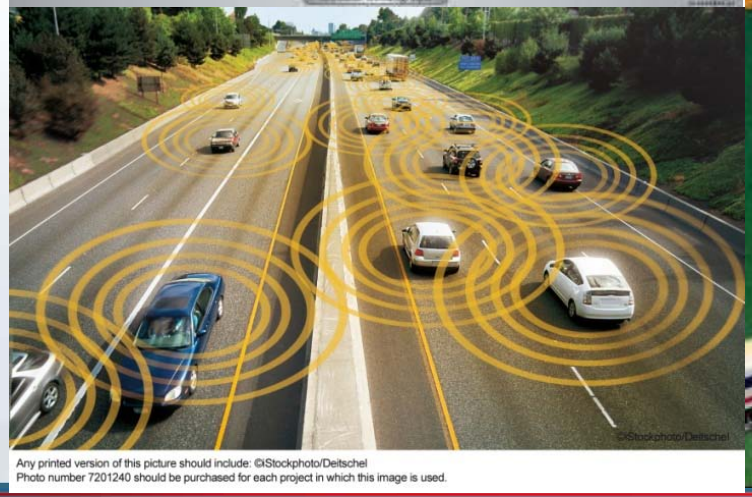
All Transportation Modes - Rail & Aviation - Highway, Pipeline, Maritime, Non-rail Transit & Intermodal -

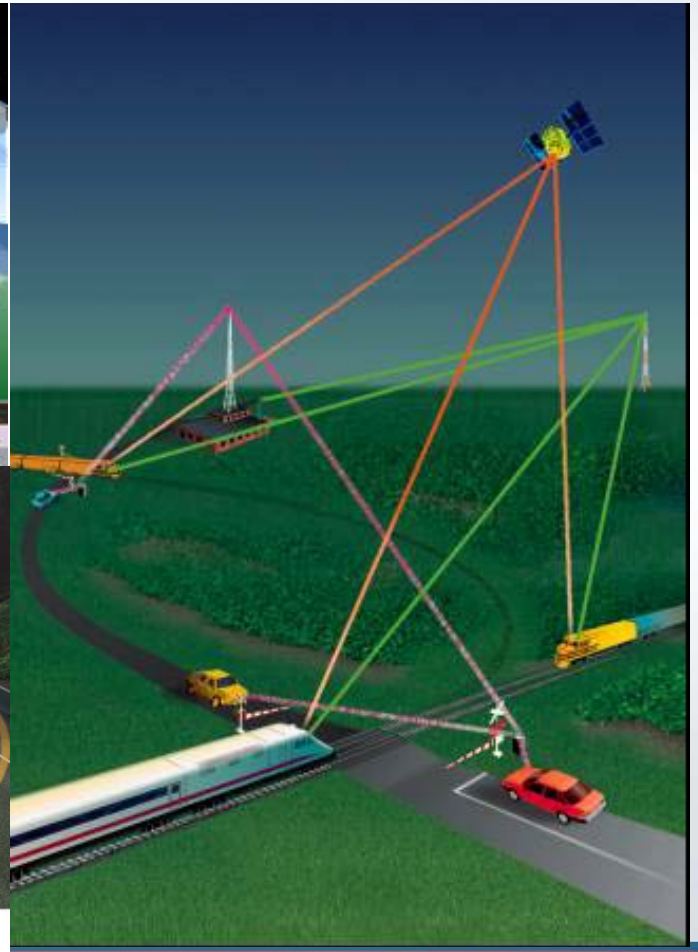
Volpe Center Supporting DHS Control System Security Program in Transportation

- Major players
  - DHS CSSP Joint Working Group, conferences & workshops
  - DHS TSA Joint Working Group
  - American Public Transportation Association, Amtrak, Association of American Railroads, Union Pacific, FTA, FRA
  - Surface Transportation/Public Transportation ISACS,
  - FAA, Highway, Pipeline, Maritime
  - Many others

Transportation Systems Are Becoming Increasingly Dependent on Information Technology



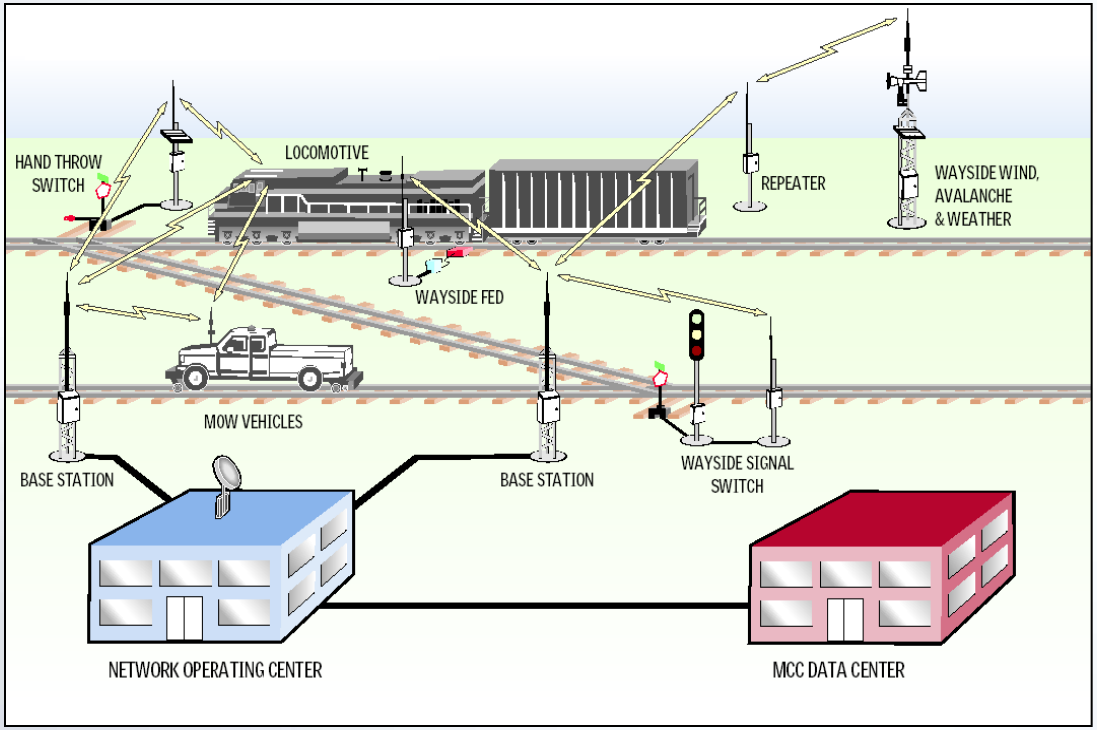


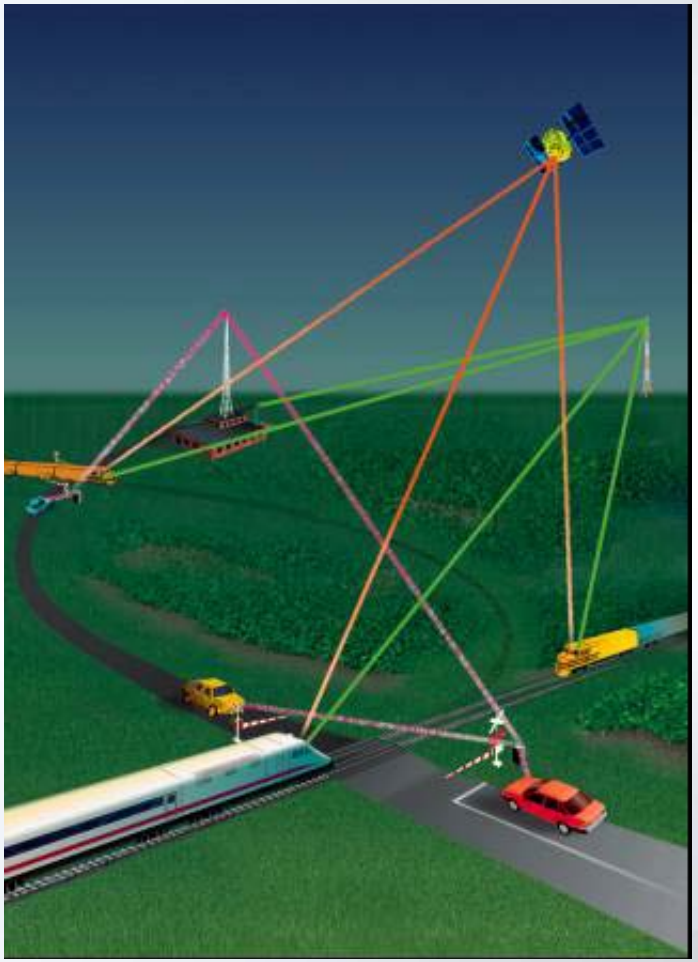


14 Year Old Boy Derails Polish Trams with Modified TV Remote

Source: Telegraph.co.uk, 11 January 2008

Future Positive Train Control Systems





Intelligent Transportation System Vulnerabilities: Variable Message Signs on Highways Hacked

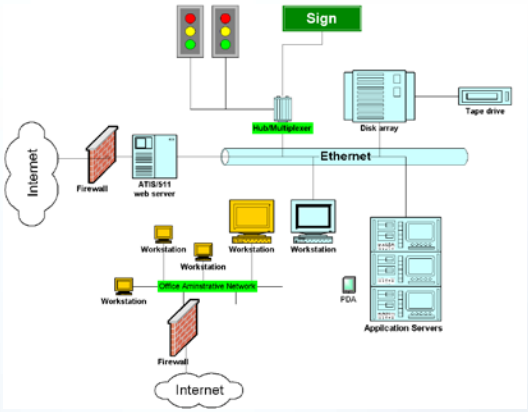
Hacking instructions were available on i-hacked.com.

Traffic Management System Vulnerabilities

Traffic signal computer crash & power failure in Maryland delays thousands.

Source: Washington Post, November 5, 2009

Disgruntled employee hacked into traffic control computer in Los Angeles; shut down signals at key points causing delays for four days in 2006.



Traffic management centers vulnerable to malware and hacking

Cyber-physical Systems in Automobiles Vulnerable

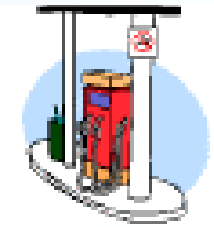
Key vehicle systems controlled by hacker teams from U. of Washington and UCSD

Tire sensor hacking kit developed by University of South Carolina and Rutgers U.

Source: MIT Technology Review, August 10, 2010

Future Intelligent Transportation System: Intellidrive

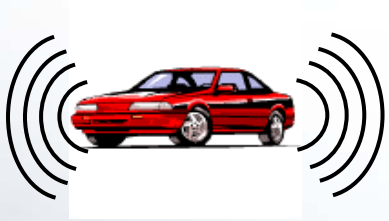
E-payment Transactions



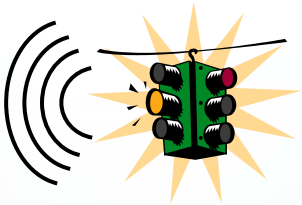
"The Network"

Opportunity for Innovation

V2V Safety Messages



Signal Phase and Timing Information

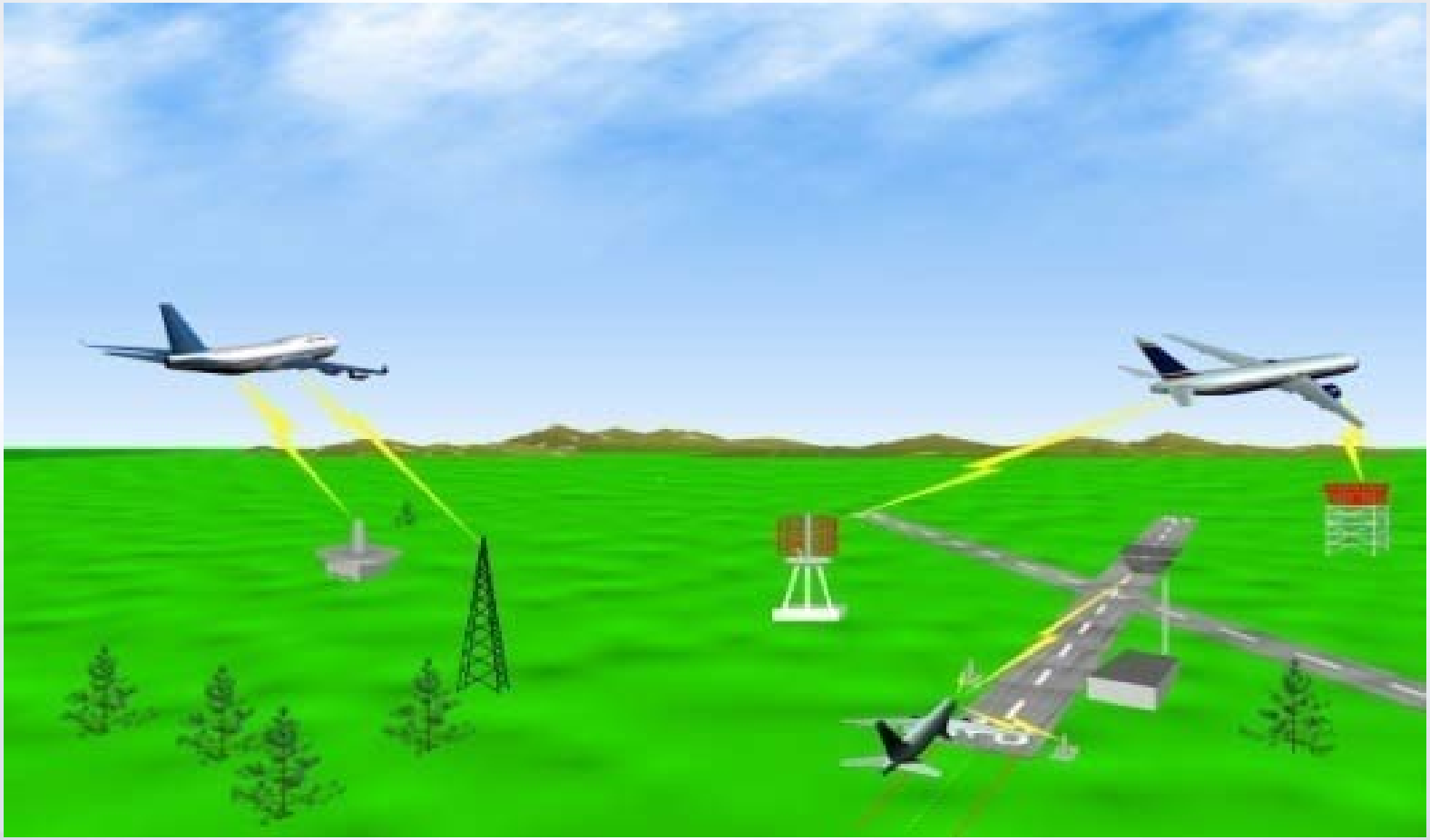


- Real Time Network Data

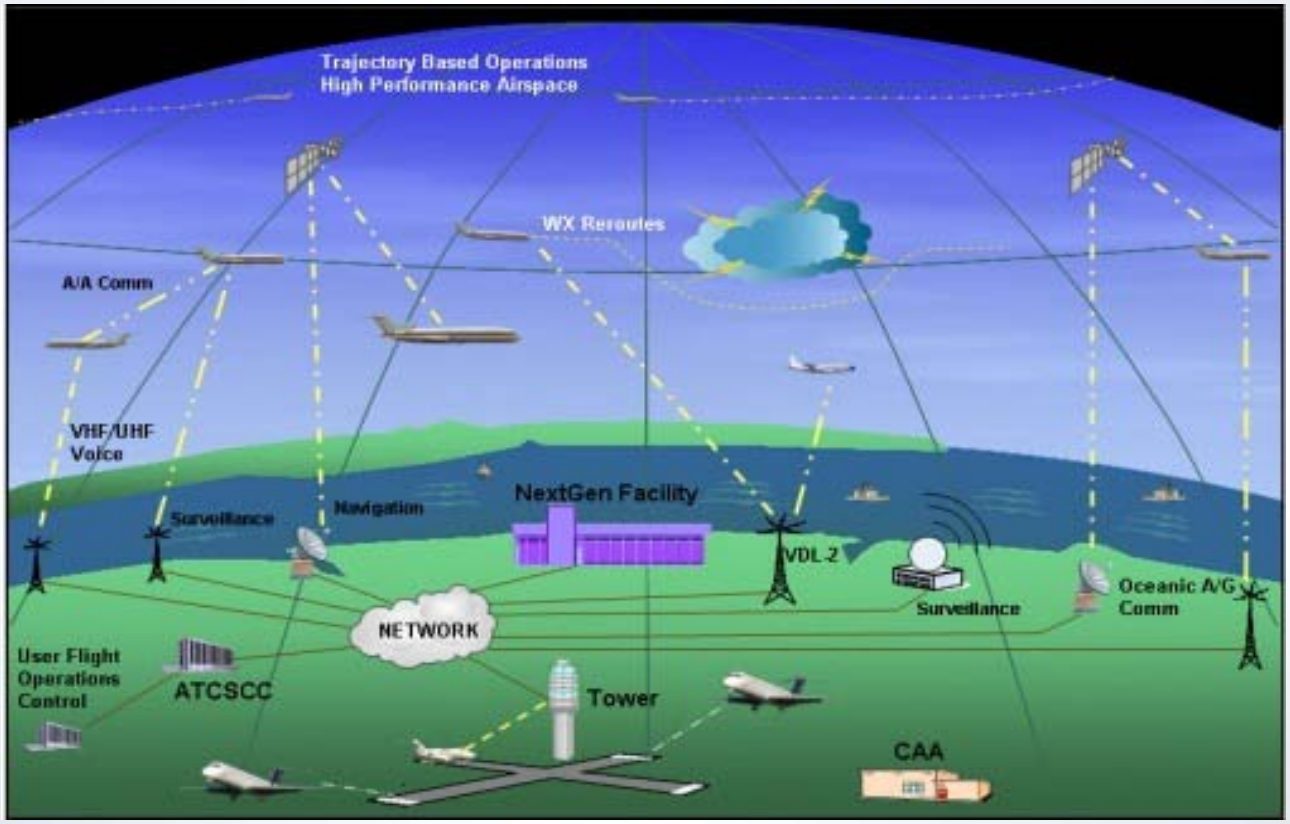
V2V Crash avoidance

Probe Data

Today's Air Traffic Control System

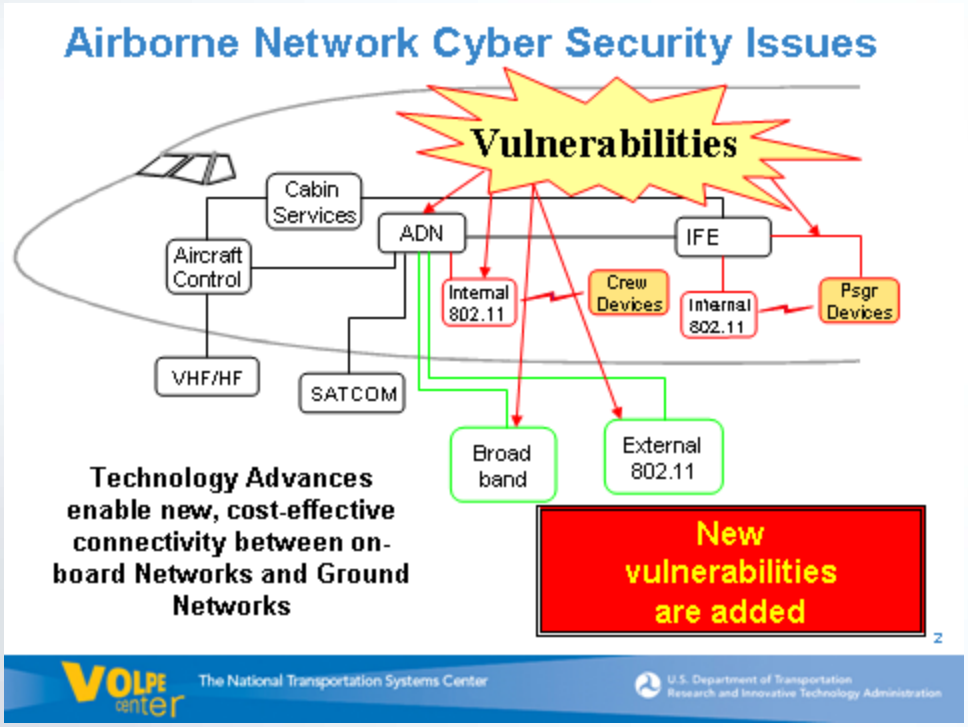


NextGen Air Traffic Control System



"NextGen: Security = Safety"

Coordinated Collaboration Among All Stakeholders

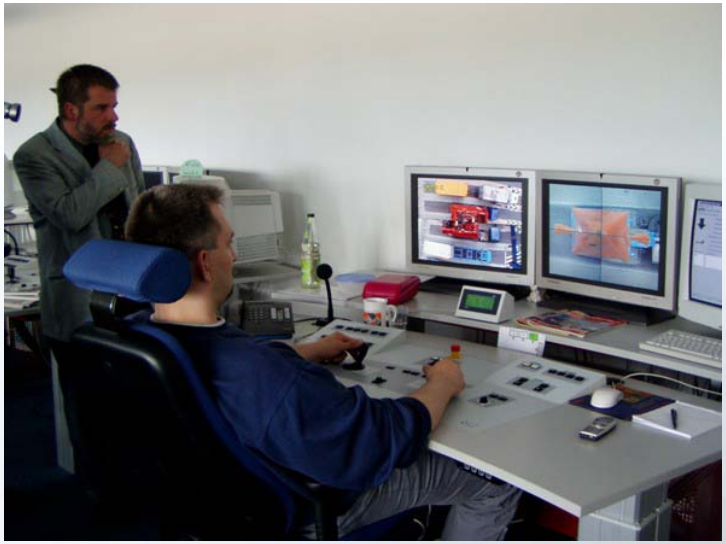


Example: Airborne Network Security

- Designers & manufacturers
- Equipment suppliers
- System integrators
- University & government researchers
- Testing organizations
- Users
- Infrastructure operators
- Standards organizations
- Regulators

Today's Automated Maritime Systems

- Today's maritime environment includes automation throughout our nation's ports
  - Automated entry systems
  - Wireless cargo tracking
  - Driverless cranes and other vehicles



Driverless Vehicle

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

Crane Accident

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

Vessel Balance Accident

- Liberia. Vessel storage usually executed by Control System “Bay Plan”. Several onboard ship systems are Control Systems

Hazardous Cargo

- Guam. Water activated cargo. Not all hazardous cargo is coded correctly resulting in inaccurate manifest

Navigation Malfunction

- Oakland, CA. Steering or navigation malfunction.

Dry-dock Malfunction

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

Pipeline Explosions

Next Steps = Collaboration

- We would like to communicate and learn from all of you
  - What's been done?
  - What are the…
    - Lessons learned and Methodologies
- For Transportation
  - Control system inventory
  - Threat, vulnerability and assessments
  - Research and simulation laboratory
  - National Cyber Incident Response Plan
  - Real-time reporting concept
  - Outreach, Training and Professional Capacity Building
  - Transportation Roadmap
  - International Collaboration

Contact Information

David Sawin
Program Manager, Information Assurance (Control Systems)
617 494 2206
David.sawin@dot.gov

Rod Cook
Chief, Intermodal Infrastructure Security and Operations
617 494 2203
Rodney.cook@dot.gov