

Introduction to Cyber Security Issues for Transportation

T3 Webinar – December 7, 2011

Michael G. Dinning

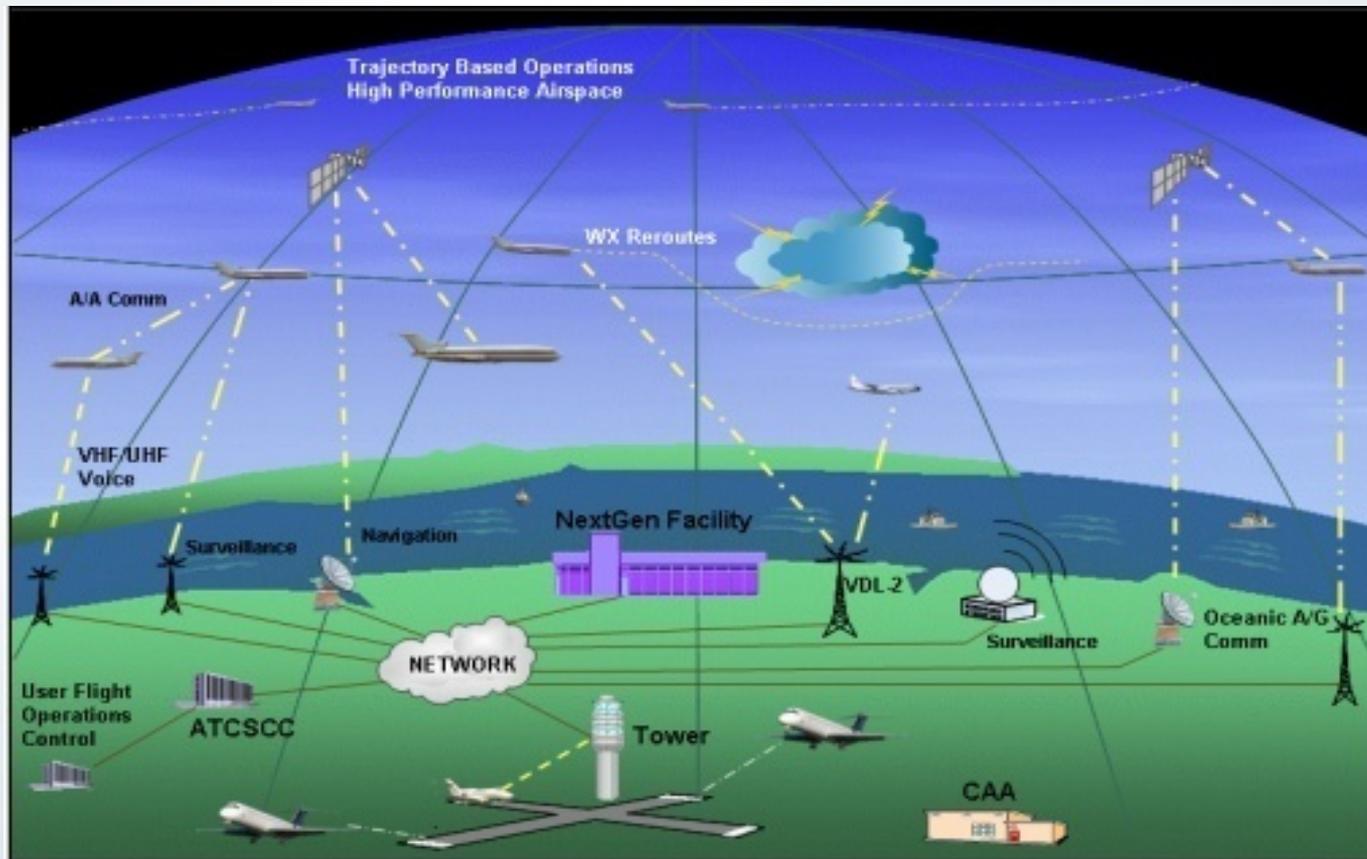


Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

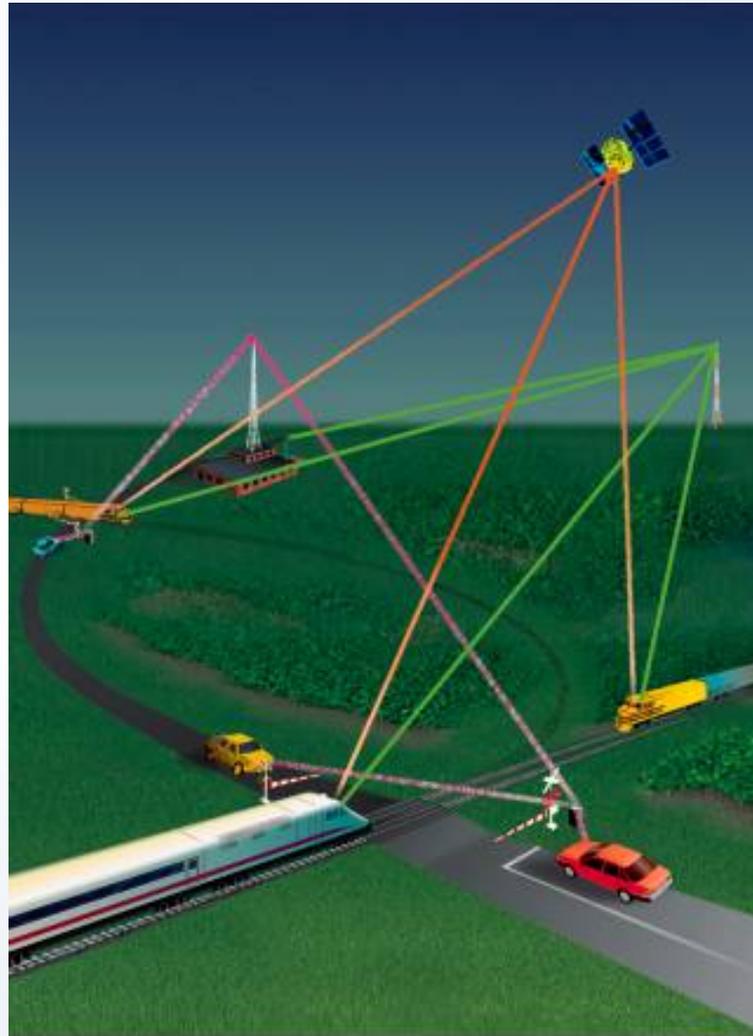


We're Increasingly Dependent on the Digital Infrastructure

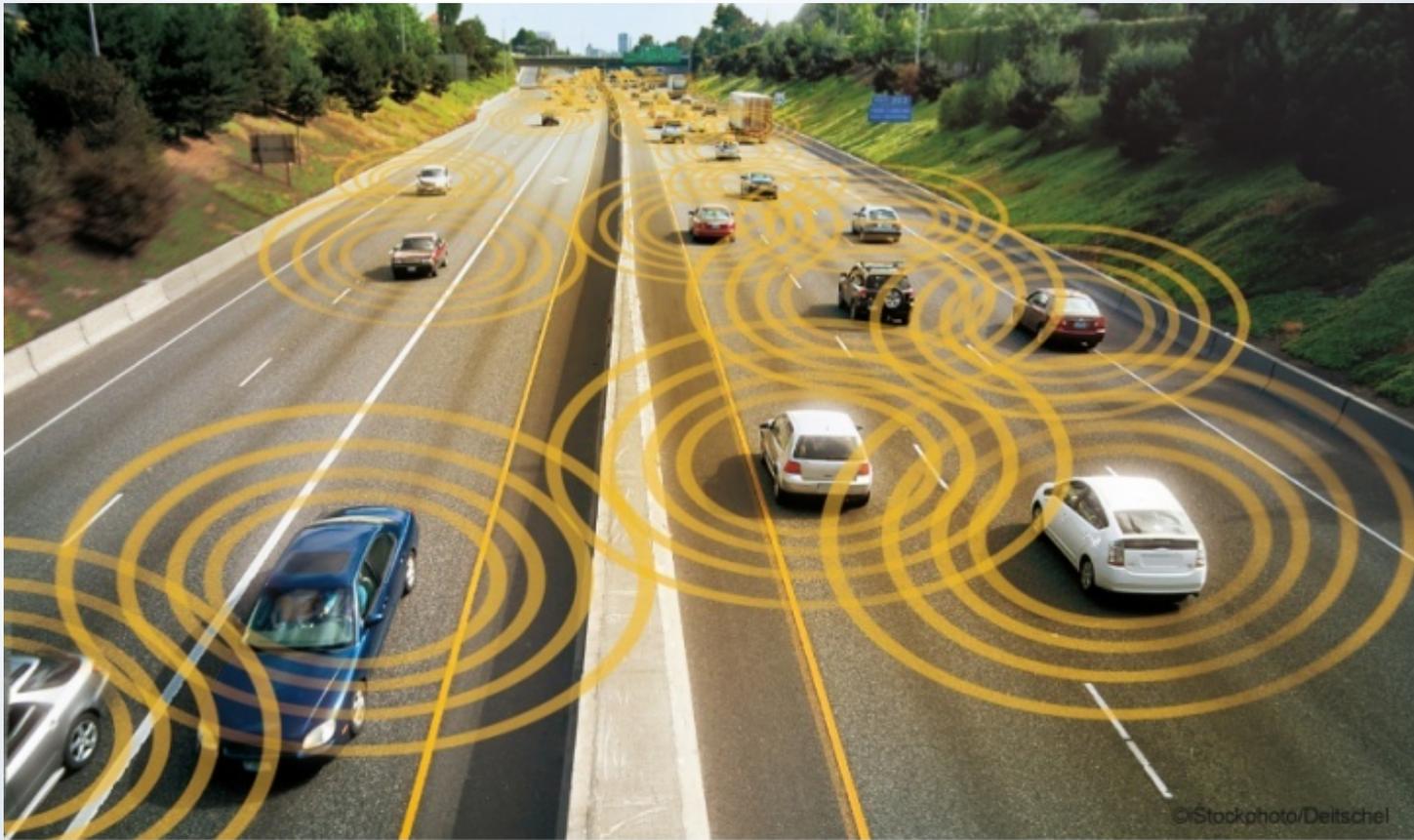


In NextGen Air Traffic Control Systems....

...Positive Train Control



...Intelligent Transportation Systems



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



...Intermodal Ports



Terminal Operations & Management



Automated Gates



Physical Security



Crane Monitoring and Control



Wireless Devices & Tracking

E-enabled Vehicles Are Now the Norm



Transit Vehicles are E-enabled

RF Cellular Wi-Fi WiMAX DSRC

Control Domain

Vehicle Controls

Vehicle Diagnostics

Traffic Signal Priority

Video Surveillance

Duress Alarms

Vehicle Immobilizers



Operations Domain

Automated Dispatching

Vehicle Location

Route/Schedule Status

Passenger Counters

Stop Annunciation

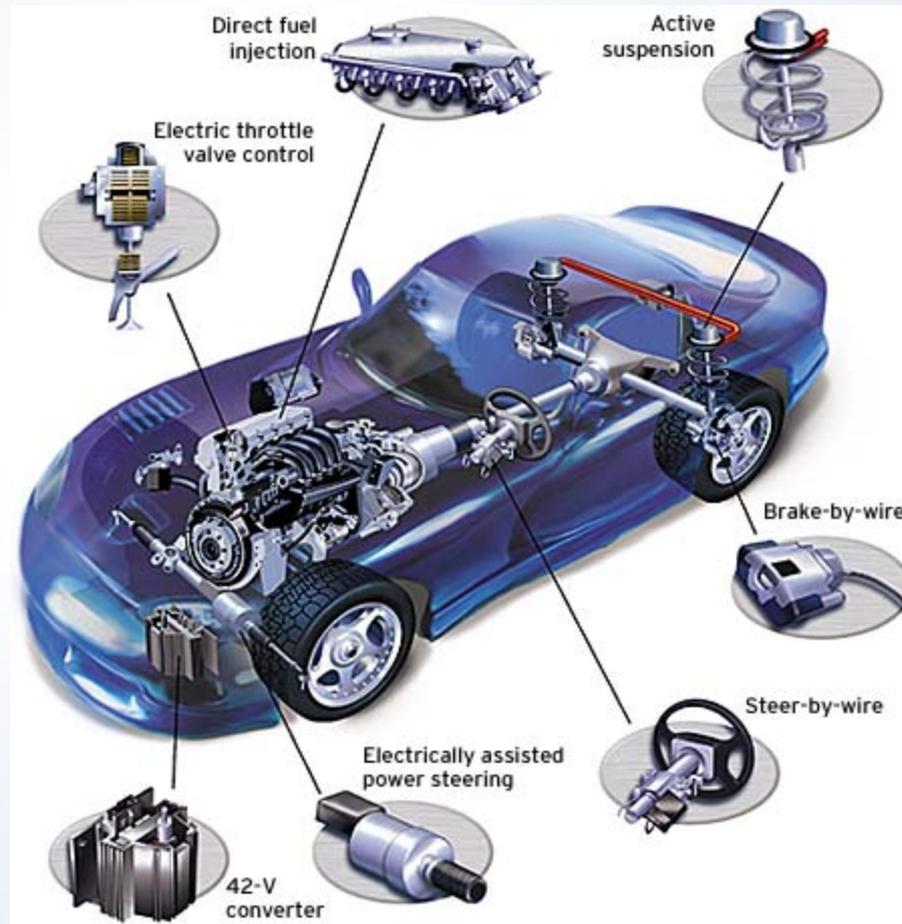
Electronic Payments

Infotainment Domain

Customer use of Wi-Fi and WiMAX

Real-time Travel Info & Trip Planning

Automobiles and Trucks Are E-enabled



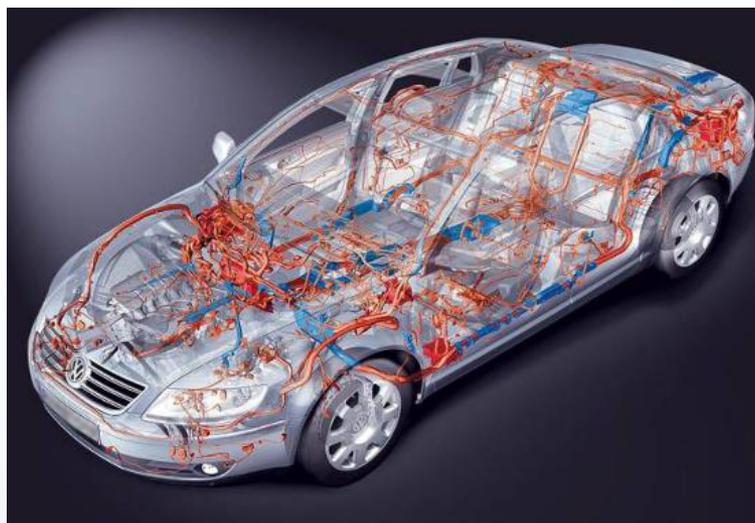
Source: aa1car.com

We're Demanding Connectivity and Increasing the Potential Attack Surface

Satellite Cellular WiFi Radio DSRC

Blue Tooth
& RF

Wireless
Sensors



CD & MP3

Mechanics'
Diagnostic
Tools

Cyber Security Threats are Increasing



ANONYMOUS



Stuxnet & Duku

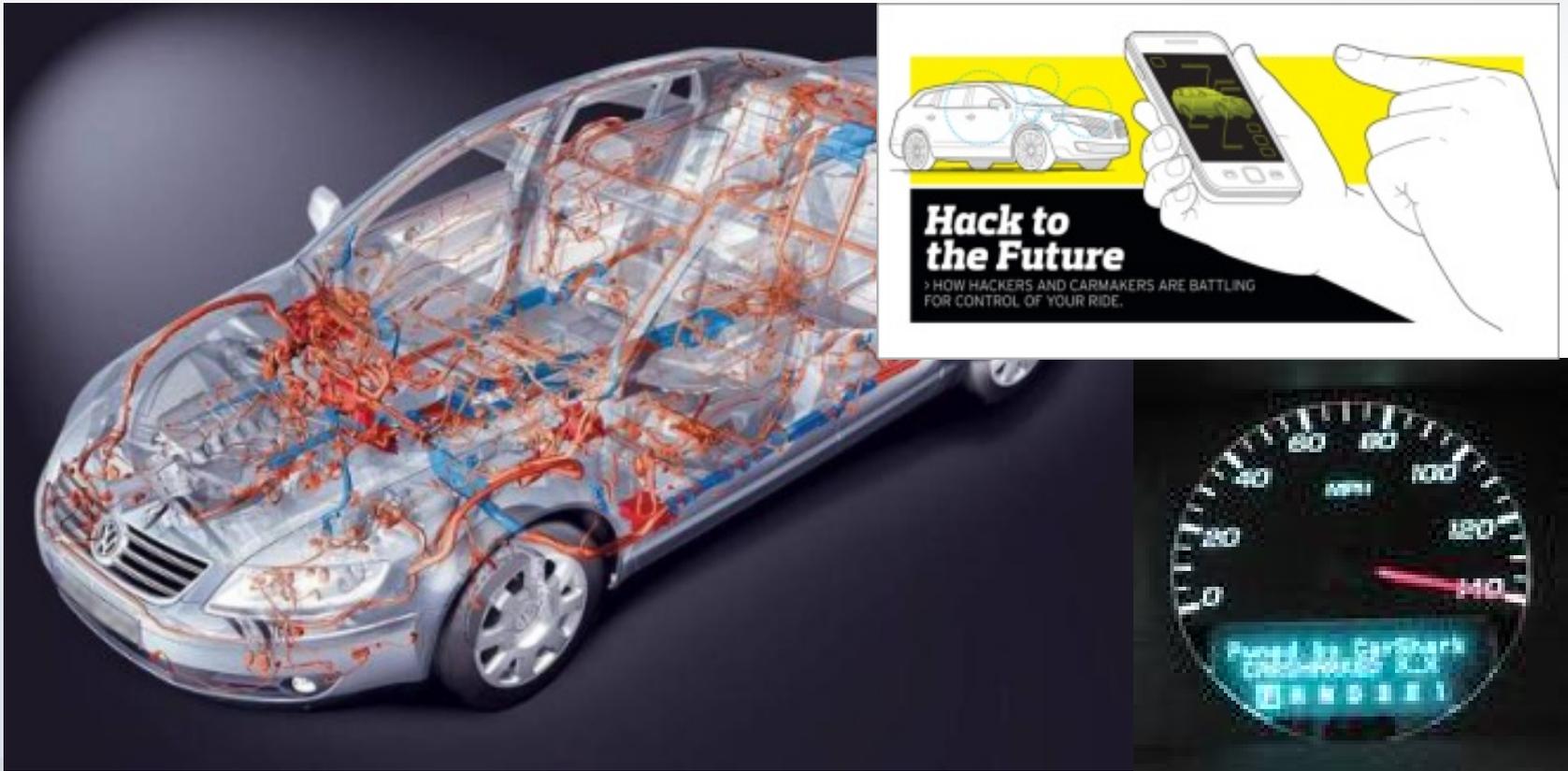
Frequent Hacks Into Highway Dynamic Message Signs



Insider Threat Impacted Traffic Management Center & Signaling



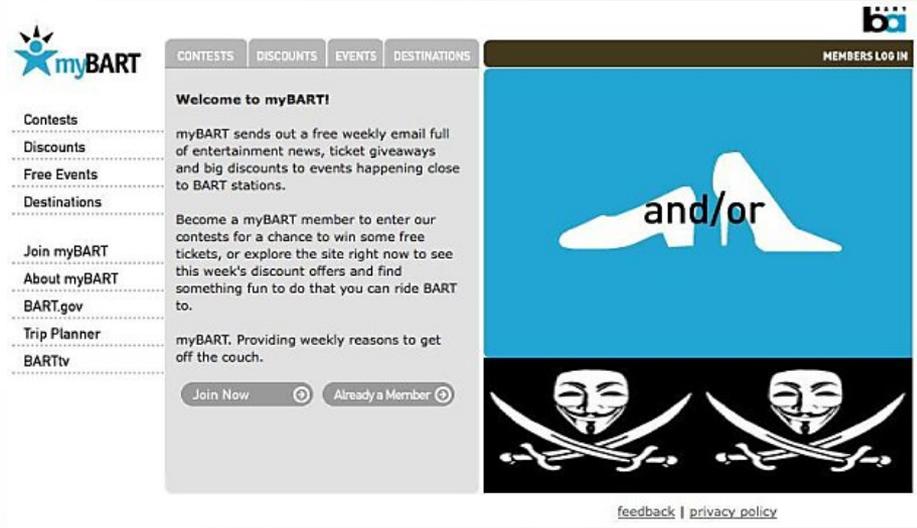
Researchers Revealed Potential Vulnerabilities in Automobiles



Recent Hybrid Attacks on Transit

“No Justice No BART” – Physical Attacks

“Anonymous” – Cyber Attacks



Even “Isolated” Legacy Systems Are Vulnerable

14 Year Old Boy Derails Polish Trams, January 2008

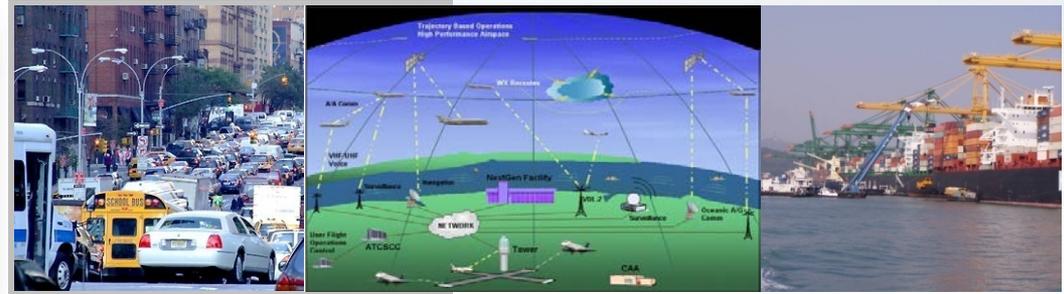


- 4 light rail trains derailed, 12 people hurt
- Used modified television remote controller
- Locks disabling switch when vehicle present not installed

Need a Complete Understanding of the Systems, Interdependencies & Importance



Cyber-physical Control Systems



Traffic Control & Operations Management Systems



Safety Management Systems



Traveler & Operator Services: 511, E-commerce, E-payment

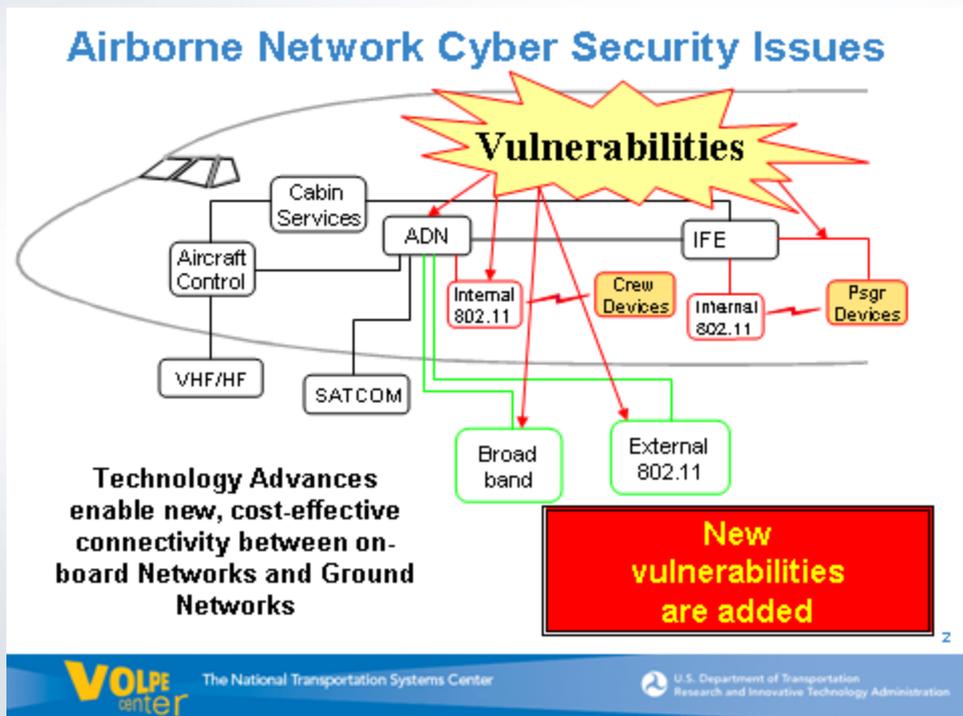
Must Understand Dependencies on Critical Information

Example: Fatal SpanAir Crash



- Cause: pilot error
 - Failed to deploy flaps
 - Warning disabled
- Related factor: Virus in management system
 - Virus had slowed maintenance management system
 - Data not entered
 - Would have grounded plane

Understanding and Risk Mitigation Requires Collaboration



- Designers & manufacturers
- Equipment suppliers
- System integrators
- Expert consultants
- University & government researchers
- Testing organizations
- Users (airlines)
- Infrastructure operators
- Standards organizations
- Certifiers and regulators

Example: Airborne Network Security

Best Practice: Collaboration on Airborne Network Security

Manufacturing



Airbus, Boeing, Bombardier, Astronautics, ARINC, CMC Electronics, Curtiss-Wright, General Electric, Panasonic, Rockwell-Collins, Thales

Airline Operations



American Airlines, British Airways, Delta Airlines, Lufthansa, United Airlines

Airborne Network



Security Simulator

Equipment / Engineering

Funding / Strategic Direction

Subject Matter Experts

Research / Facilities



Government

FAA, U.S. Air Force, Defense Information Systems Agency, Dept of Homeland Security (DHS), DOT Volpe Center, UK Center for Protection of National Infrastructure, UK Computer and Electronic Security Group

Wichita State University, Louisiana Tech University



Academia



We Must Build Security Into the Process to Ensure the Resilience of the Overall System



Risk assessments
Standards
Design practices
Certification
Maintenance & Ops



Goals: systems safety, security, reliability and resilience

Create a Cyber Security Eco System: Incorporate Security Into the Design Process, SMS's & the Safety Culture

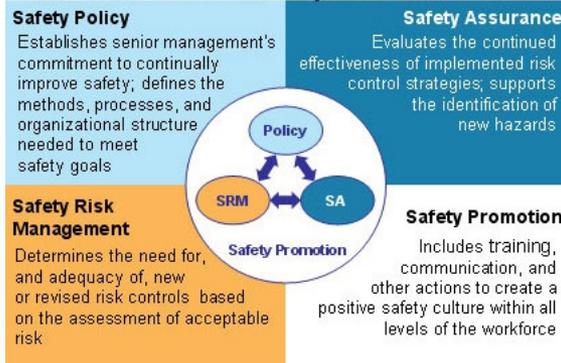


Systems engineering process



Cyber risk management throughout the systems development life cycle

The Four SMS Components



System security/safety process, management systems and culture



Certification process

Strategy Must Address Life Cycle

Create a cyber security eco-system (like Fire Safety)

- Identify systems, connections & interdependencies
- Assess vulnerabilities and risks
- Identify and use best practices and standards
- Include cyber security in design specs and acquisitions
- Collaborate with IT, physical security & other groups
- Develop policies and procedures for cyber security
- Motivate employees with training, exercises & “hot triggers”
- Make sure that systems and operations are resilient (i.e. layers, detection, incident response, COOP)
- Develop organization-wide strategic plan linked to funding



Cyber Security Resources and Tools

- TSA Transportation Systems Sector Cyber Working Group
 - Newsletter, monthly meetings, summit, training, case studies
- DHS Control System Security Program - Transportation
 - Assessments (i.e. CSET), information sharing, standards, training
- Industry associations
 - APTA Control & Communications Security Working Group
 - AAR Rail Information Security Committee
 - SAE Automotive Systems Security Committee
 - RTCA SC216 Aeronautical System Security Committee
 - AAPA Security Committee
- TRB Transportation Cyber Security Sub Committee
- Information Sharing and Analysis Centers & Computer Emergency Response Teams
- DOT Volpe Center Transportation Cyber Security Team/Lab



Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!

