



eEnabled Aircraft Operational Cyber Security Working Group (eEACSec)

Presented by: John Pawlicki and Vince Rakauskas
(DOT/Volpe)

June 7, 2011

Agenda

- eEnabled Aircraft Security Issues – Vince Rakauskas
- eEACSeC WG Overview – John Pawlicki

Eighteen (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**



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

Volpe Center Mission, Vision & Capabilities

John A. Volpe National Transportation Systems Center

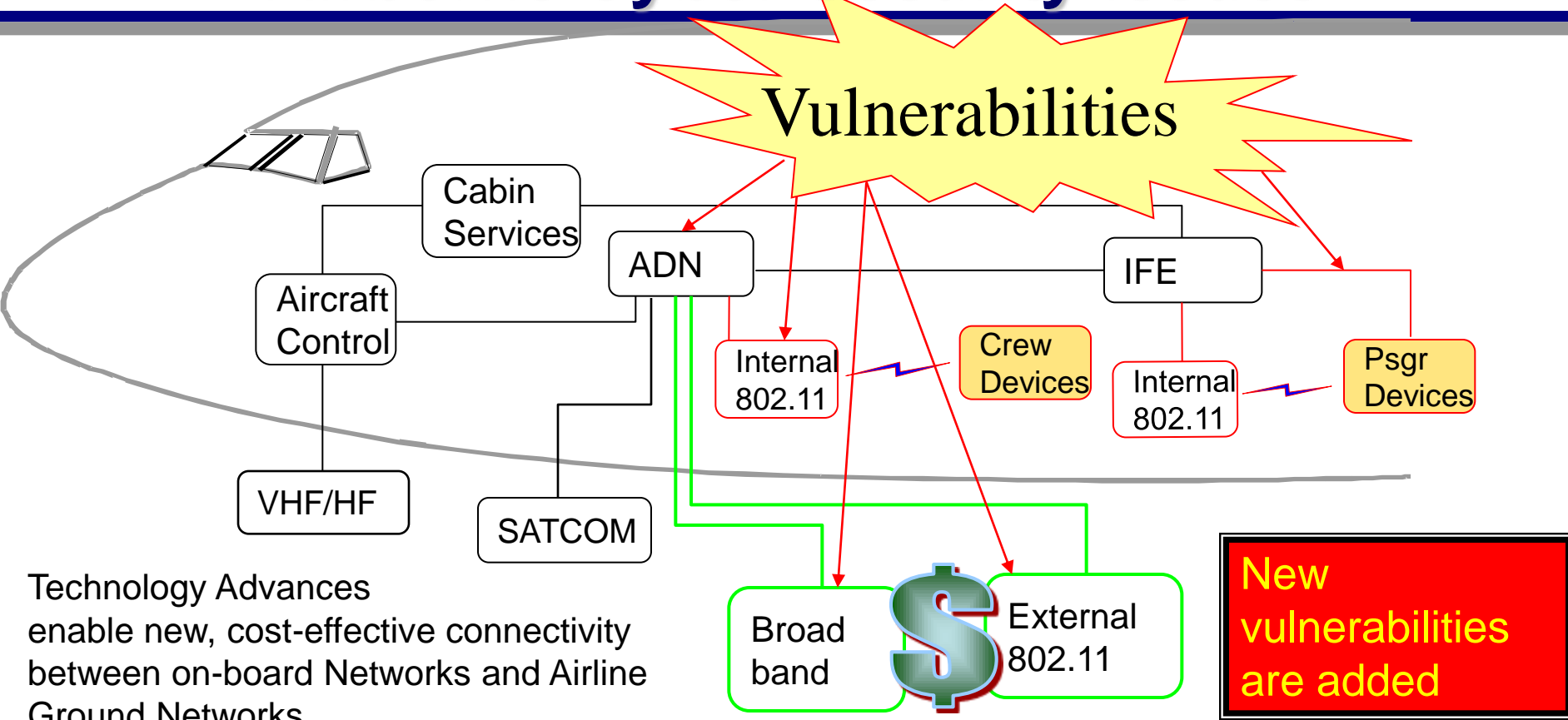


U.S. Department of Transportation
Research and Innovative Technology
Administration



- 578 Federal Employees representing a full spectrum of disciplines from engineering to physical and social sciences
- 261 Advanced Degrees (66 PhDs and 195 Masters)
- More than 60 Federal Career Interns and Co-op Students
- More than 1,000 contractors
- A world-recognized Federal center of excellence and leader in transportation technical, operational, institutional, and managerial innovation
- Trusted enabler of critical improvements to transportation and logistics systems
- Leader in government, industry, and academic cooperation; Research and simulation laboratory

Airborne Cyber Security Issues

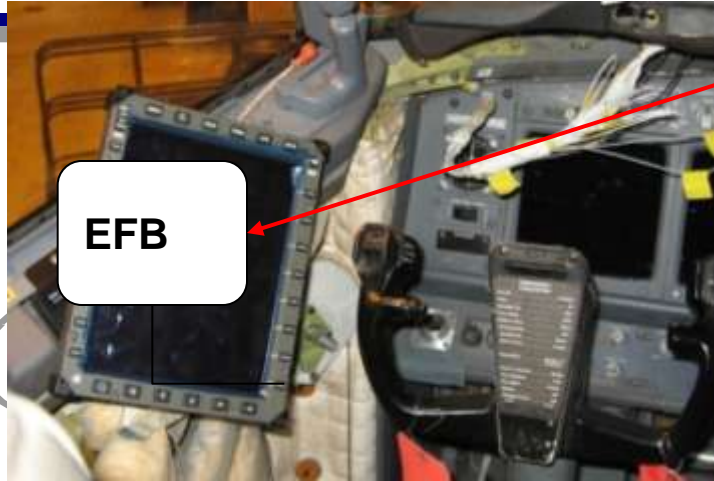


Technology Advances enable new, cost-effective connectivity between on-board Networks and Airline Ground Networks

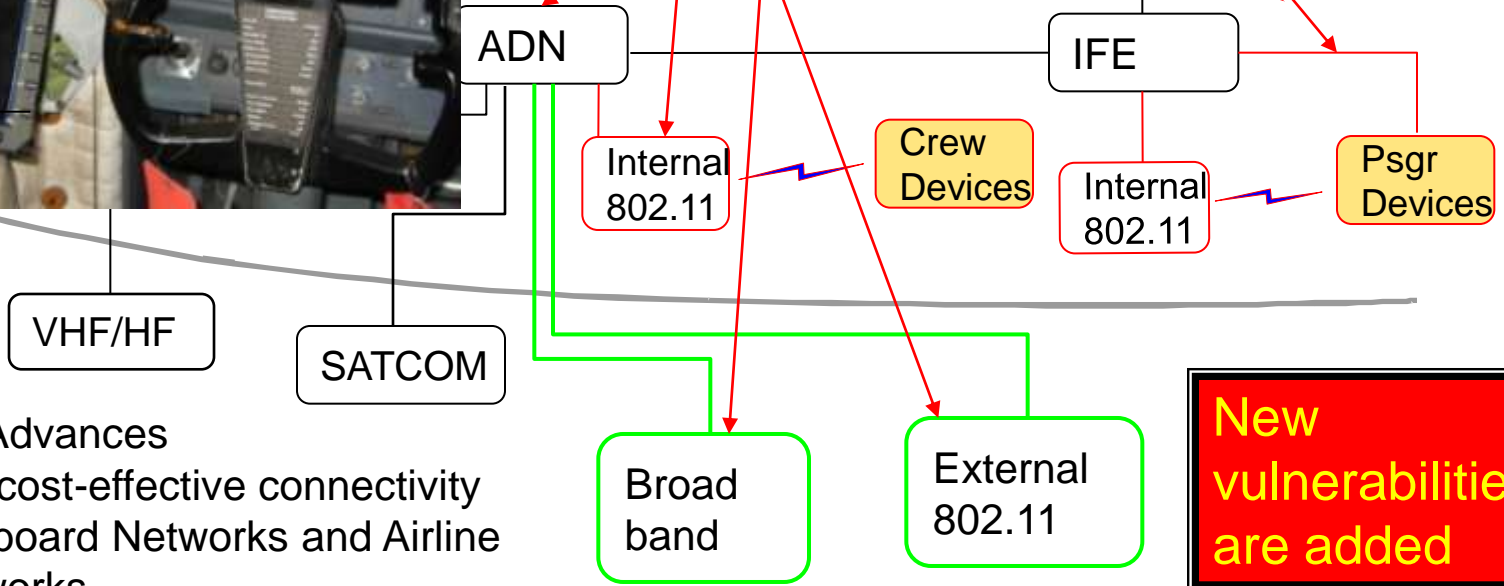
Airlines will use Broadband Internet connectivity to support passenger services then use existing bandwidth to support operations.

Revenue from passenger services provides funding for increased infrastructure costs

Airborne Cyber Security Issues



Vulnerabilities

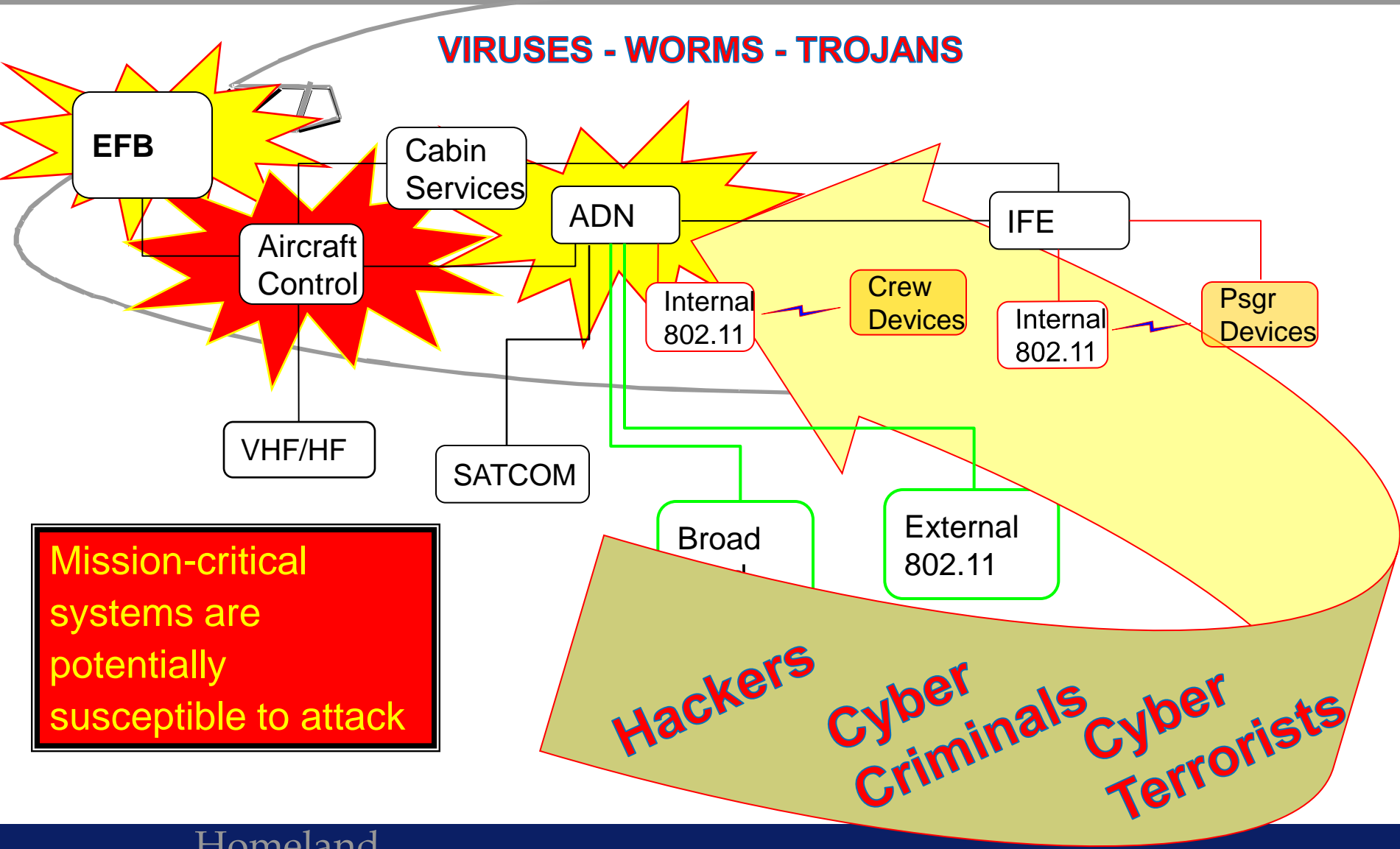


Technology Advances enable new, cost-effective connectivity between on-board Networks and Airline Ground Networks

Airlines will use Broadband Internet connectivity to support passenger services then use existing bandwidth to support operations.

Revenue from passenger services provides funding for increased infrastructure costs

Airborne Cyber Security Issues



Airborne Cyber Security Issues

- These cyber security vulnerabilities were not only new but were not anticipated.
- Since it has not been a concern in the past, the existing Code of Federal Regulations does not specifically address cyber security vulnerabilities
- Consequently, there are no existing Policies, Certification Criteria or Procedures that provide assurances that cyber security vulnerabilities will not cause unsafe flight conditions
- Cyber security vulnerabilities in the ADN will be irrevocably bound to the safety of flight.
- Unmitigated, these vulnerabilities will have a definite negative effect on the safety of flight

Key Topics Requiring Focus & Resolution

- Safety vs. Security Paradigm
- Documented Certification Criteria and Processes that are acceptable to FAA
- Coordination of NextGen/GIG/Aviation Industry on security architectures and information sharing
- Global naming/addressing
- Global trust paradigm
- Adaptation of controls/best practices to AN

Implementation is the beginning – not the end

- Maintenance and Monitoring
- Incident Response
- Airborne Cyber Security Training

eEACSec WG Overview

eEACSec Working Group

New WG being formed and managed (initially) by the Dept of Transportation's (DOT) Volpe Center and the Dept of Homeland Security (DHS)

Following the lead of the UK's Centre for the Protection of National Infrastructure (CPNI) in forming a US-equivalent to their existing eEACSec working group

- Members included airlines, OEMs/suppliers, service providers, airports and other related industry participants (UK eEACSec formed in Nov 2010)

eEACSec Working Group (WG)

This US-based WG will coordinate with the UK-based eEACSec WG on all efforts, to reduce duplication and increase acceptance of recommendations

The eEACSec WG will work with other industry bodies in a cooperative manner, concentrating on cybersecurity issues facing aircraft/avionics and systems

What We Are Trying to Accomplish

Mission

- Provide a forum to develop security aviation industry operational processes based on current cybersecurity threats in a neutral environment benefiting all participants

Goal

- Identifying and defining new or improved industry standards, best practices, processes or procedures in conjunction with other industry bodies relating to operational aspects of the industry in respect to cybersecurity issues

Background

- The new generation of “eEnabled” commercial aircraft have increased electronic capabilities which result in new and increased levels of threat to the security (and therefore the safety) of the aircraft.
- OEMs are taking steps to produce aircraft which are secure and can be operated securely.
- However, airlines, MROs, airports and aviation service providers can introduce security problems through inappropriate operational processes and procedures.
- The new processes and procedures are sufficiently different than current practice and new risk management & assessment approaches are needed

Current Cyber Security Environment in Aviation

An evolutionary change is occurring

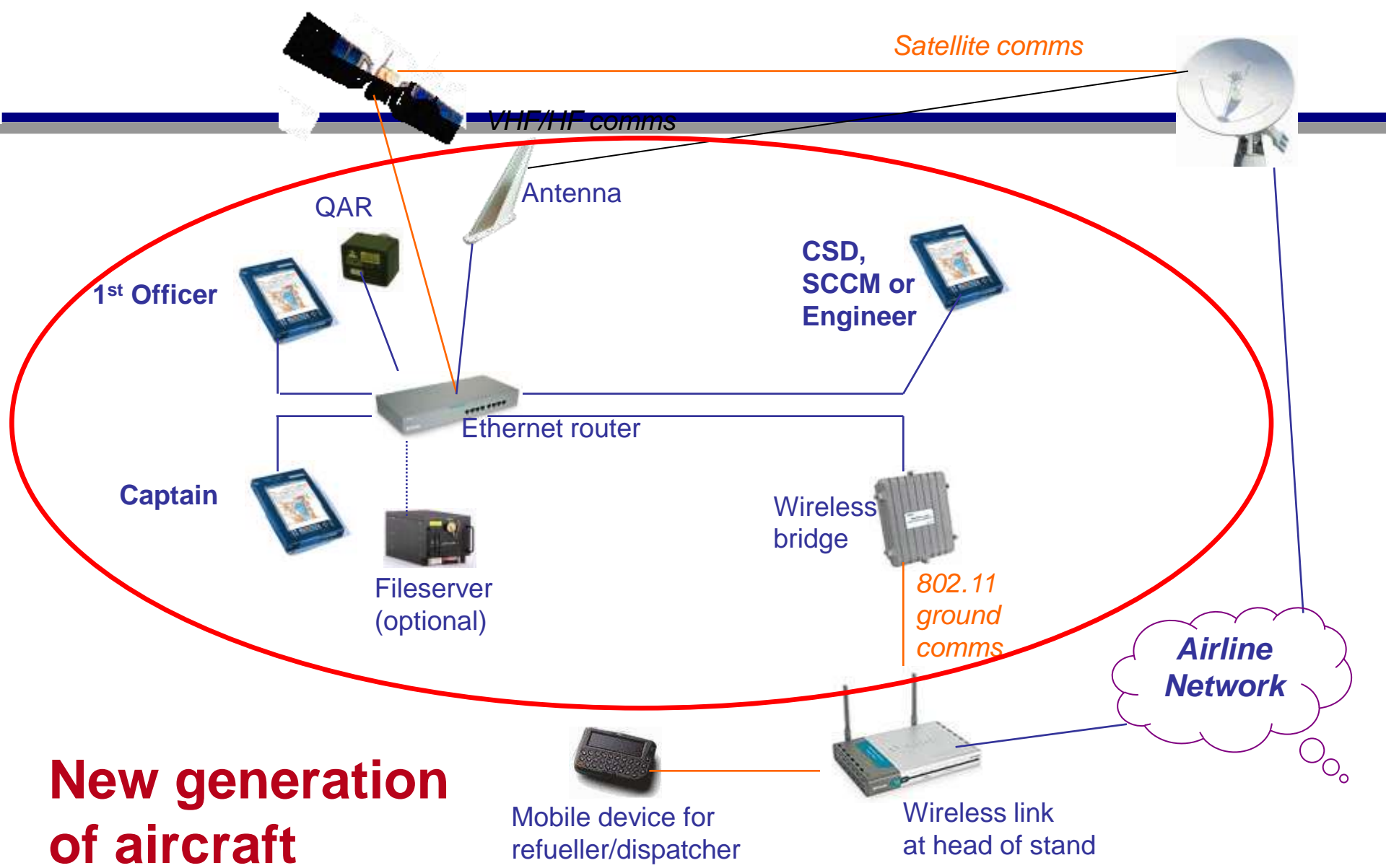
Current Aircraft

- **Internally:** Most aircraft have information backbones associated with avionics speaking to each other on dedicated connections, with a few exceptions
- **Externally:** Aircraft are operated using voice, with data communications as a secondary mechanism; IFE, SatCom and other communications are not typically integrated into the aircraft's
- **Support:** Majority of aircraft are supported by off-line data loaders, test systems, and reasonably secure proprietary equipment

Emerging (or already here) eEnabled Aircraft

- **Internally:** Most aircraft have information backbones based upon AFDX (Ethernet) bus, and many avionics and another systems will interface to the cockpit via a singular network
- **Externally:** Aircraft will be operated using data communications (GPS, ADS-B, etc) primarily in NextGen, and voice will be a secondary option
- **Support:** Wireless systems such as Gatelink, and fully-connected ground-support systems at airlines/MRO facilities will connect via networks to other data sources or targets

Aviation infrastructure becomes more vulnerable to cyber attacks due to expanded communications capabilities



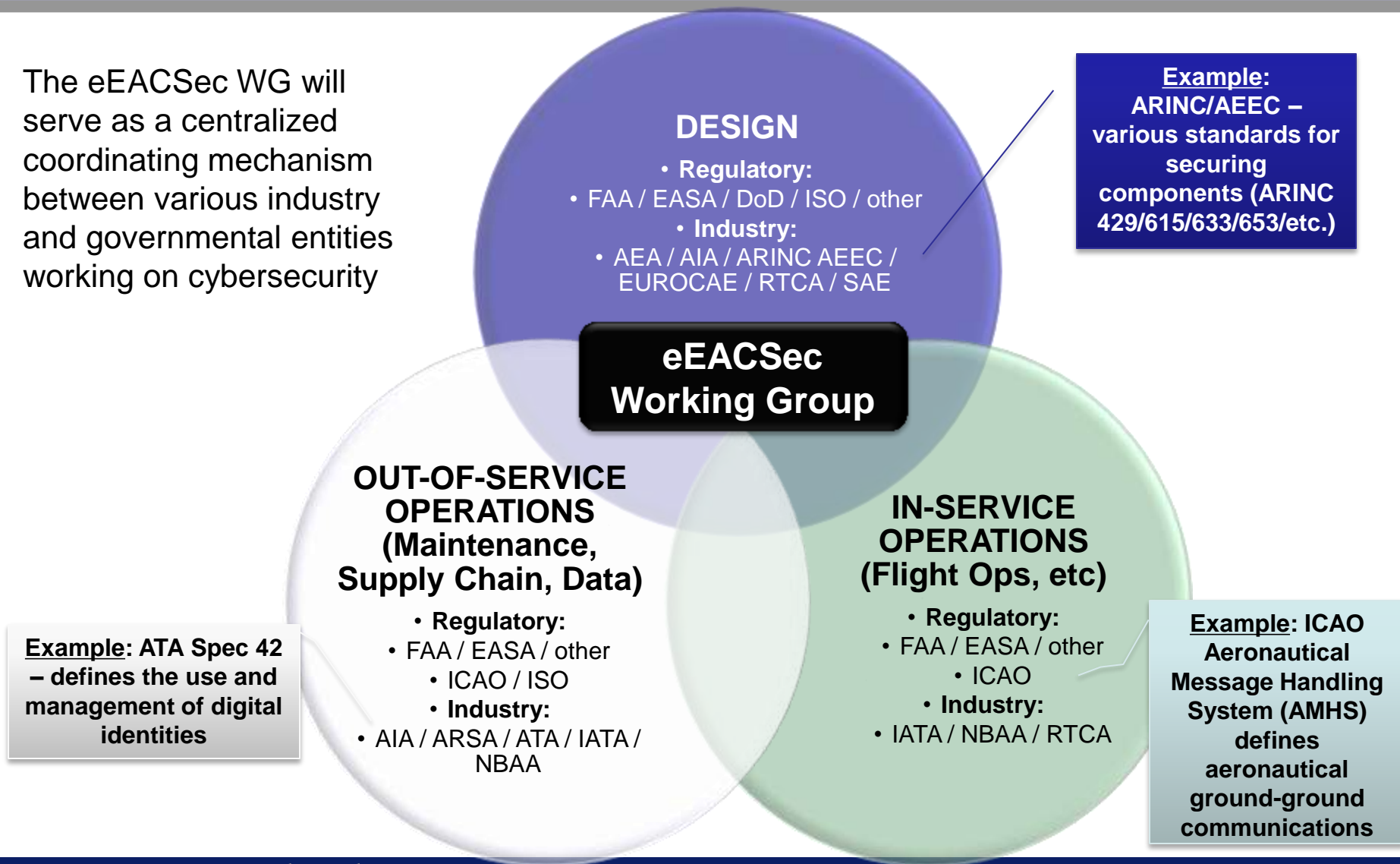
New generation of aircraft

Changes to Secure eEnabled Aircraft & Support Systems

- Effort required is not just related to securing avionics and/or networks
 - As the Internet has shown, this is not enough
- Processes and procedures relating to information processing and communications must change as well
 - As any organization with Internet connectivity has learned simply adding more network security equipment will not solve the problem alone
 - Strong cybersecurity standards, processes and procedures need to be enforced, e.g.:
 1. Locking out certain types of websites and applications
 2. Implementing strong passwords, changed on a regular basis
 3. Protecting data by not allowing access via uncontrolled means
 4. Ensuring data backups or replication is done on a timely basis to minimize impact if an event occurs
 5. Issuing digital identities for use in authenticating personnel/assets
 6. Using encrypted data for certain transactions
 7. Monitoring and responding to security audit logs

Existing Cybersecurity Standards Bodies & Groups

The eEACSec WG will serve as a centralized coordinating mechanism between various industry and governmental entities working on cybersecurity



Do We Actually Need Another Industry Working Group & Why?

- **Safety versus Security**

- Design/build/operations/maintenance currently dominated by safety analysis, certification and inspection regimes
- **Safety \neq Security**
- **Safety + Malice = Security**
- We cannot rely on past experience, since security issues are rather new, and still evolving

- Without a concentrated effort to bring together (or coordinate) security issues among disparate operational areas (flight, maintenance, supply chain, design, etc.) the industry will continue to have ad hoc, differing solutions to digital security issues as they arise
 - Identified issues may not always be handled by other operational areas, thus creating gaps
- Some degree of coordination is needed to better address new standards approaches globally

Initial UK eEACSec Issues Identified

TOPIC DISCUSSED	ISSUE
Not have enough input from airlines, MROs and Aviation Service Providers	There are concerns that current standards work does not have enough input from airlines, MROs and Aviation Service Providers, and may be excessively influenced by US regulators (FAA). This could result in a standard which does not fit with the current approaches of UK operators, and which would require operational changes
Airplane Leasing Organisations	The involvement of airplane leasing organisations was raised, in both the working group and in WG72 and SC216
Gatelink Security	Airports should be involved, since they will be providing connectivity services for the airplanes (one key issue will be Gatelink and assuring it has been configured securely)
Airline and MRO (Secure State)	The initial issue that needs to be dealt with in this context is the ability of airlines and MROs to maintain and operate the airplanes in a secure state.
Security Added to the Safety Culture	The safety culture which currently exists in aviation electronics is not sufficient in this context, since it precludes malicious acts. Therefore information security needs to be added to the safety culture (and to the physical security culture).
Cybersecurity Standards (Airline & MROs)	The proposed solution to this situation is to promote standards for information security across the whole aviation industry, and in particular covering airlines and maintenance operations. These would be written by and for industry, but would also be usable by regulators where they see fit.
RTCA SC-216 ICA Overlap	SC-216 ICA SG4: Some of these standards will cover the ICAs needed for type certification and the requirements for Flight Standards certification.

Next Steps

- 1. Identify an 'Industry Chairperson' from an airline/operator for the group**
- 2. Volpe Center will continue defining the framework and TOR for the WG**
 - Coordination with the existing UK eEACSec group
- 3. Expect to continue outreach to existing Standards groups and industry entities**
- 4. Kick-off meeting expected in summer 2011**
 - Follow-on quarterly or bi-monthly meetings afterwards

If interested in participating, or, monitoring progress, please contact:

- Kevin Harnett – Volpe Center Cyber Security Project Manager - 617-699-7086 (cell)
- John Pawlicki – Volpe Center consultant – 424-254-8450 – john.pawlicki@vsintl.net
- For information on the UK eEACSec WG: Peter Davis, UK CPNI (contact Kevin Harnett, Volpe)