Many thanks for the help, support, and slide material from:

- Brian Verna, AFS-360
- Steve Paasch, AIR-134
- Varun Khanna, ANM-111
ASISP Topics

- A rose by any other name...
- Background
- e-Enabled Aircraft
- Potential Risks
- AVS Security Scope
- U.S. Government Services
- Non-Government Services
- Regulations, Policy, Standards and Guidance
- Future Direction of ASISP
- ARP 4754A
A rose by any other name...

- We’ve used several terms for security from electronic attacks on networks and systems: network security, information security, systems security, and cyber security

- These terms are often used interchangeably, which may cause confusion as to their intended meaning
A rose by any other name...

- We are now trying to standardize on the term *Aircraft Systems Information Security Protection* (ASISP)...
  - ...to indicate security from electronic attacks on aircraft networks and systems

- We’re talking here only about aircraft: not air traffic services and providers
  - U.S. governmental services have their own programs for information security
Background

- Prior to the availability of e-Enabled technologies, legacy aircraft have used architectures with limited wired or wireless connectivity to non-governmental service providers.
- This is rapidly changing as aircraft are incorporating Wi-Fi, Electronic Flight Bags, wireless Field Loadable Software, real-time aircraft health monitoring and reporting, and Passenger Information and Entertainment Systems.
Background

- Aircraft operators and manufacturers have identified potential economic and safety benefits using e-Enabled technology and software applications
- e-Enabled applications will mean increased aircraft connectivity to non-governmental service providers
Background

Aircraft operators have the option to include a wireless network on e-Enabled aircraft to:

- Remotely upload software parts, aeronautical charts, airplane flight manuals, electronic checklists, performance information, flight plan information etc., to aircraft systems located anywhere in the world.
- Continuously monitor health information from aircraft systems and record data to an onboard maintenance computer and send information to airlines in real-time.
e-Enabled Aircraft, Domains and Connectivity

- Aircraft control
  - Flight & Embedded Control Functions
  - Cabin Core Functions
  - Air / Ground (Network ?) Interface

- Airline Information Services
  - Administrative Functions
  - Flight Support Functions
  - Cabin Support Functions
  - Maintenance Support Functions
  - Role-specific Functions
  - Air / Ground Network Interface

- Passenger Info & Entertainment Services
  - Embedded IFE Functions
  - Passenger Internet Portal
  - Onboard Passenger Web
  - Passenger Device Interface
  - Air / Ground Network Interface

- Non-Government Services

- Control the Airplane
- Operate the Airline
- Entertain the Passengers

- CNS/ATM Network
  - Terminal
  - En Route
  - Command Center
  - Tower

- A/C External threat
- A/C Internal threat
- CNS/ATM connectivity

- Internet
- External Networks
Potential Risks

Examples of potential ASISP risks:

- Erroneous maintenance messages
- Corrupted software loads to aircraft systems
- Malware to infect an aircraft system
- An attacker to use onboard wireless to access aircraft system interfaces
Potential Risks

Examples of potential ASISP risks:

- Denial of service of wireless interfaces
- Misuse of personal devices that access aircraft systems
- Misuse of off-board network connections to access aircraft system interfaces
- Denial of service of safety critical systems
Potential Risks

Vulnerabilities

Technology advances enable new connectivity between on-board networks and airline ground networks, including internet.
AVS Security Scope

- Recent designs for aircraft systems include connectivity to non-governmental services such as the internet, portable electronic devices, and commercial-off-the-shelf technologies that have not been certified and accredited for secure operations by a government authority.
  - These designs can introduce ASISP vulnerabilities beyond the scope of current airworthiness regulations and traditional systems safety assessment methods typically used to show compliance with the airworthiness requirements located in Title 14 CFR.
AVS Security Scope

- e-Enabled technologies should be evaluated to ensure that the security controls are as good as, or better than, the aircraft networks, systems, and procedures that they are replacing.
U.S. Government Services

- U.S. governmental Air Traffic Services
  - Have been certified and accredited in accordance with the Federal Information Security Management Act (FISMA), FAA Order 1370.82A Information Systems Security Program and the FAA Information Systems Authorization Handbook
  - For purposes of ASISP, we consider U.S. government Air Traffic Services to be secure
Examples of government services:
- Global Navigation Satellite Systems (GNSS)
- Automatic Dependent Surveillance – Broadcast (ADS-B)
- Ground Based Navigation Aids
- Instrument Landing Systems (ILS)
- Air Traffic Data and Voice Communications
Non-Government Services

Examples of non-government service providers

- Airline Networks (Airline Operations Centers)
- Airport Networks (e.g., GATELINK)
- Public Networks (e.g., Internet)
- Data Loaders (e.g., FLS and Databases)
- Wireless Aircraft Sensors and Sensor Networks
- Ground Support Equipment
- Universal Serial Bus (USB) devices
- Portable Electronic Flight Bags
- Cellular Networks
Regulations, Policy, Standards, and Guidance

Regulations

- The following regulations do not specifically address security requirements for aircraft networks and systems
  - § xx.1301 Function and Installation
  - § xx.1309 Equipment, Systems, and Installation
- EASA published a pre-Regulatory Impact Assessment (RIA); FAA commented; EASA reaction was positive
  - We have an approved Aviation Rulemaking Advisory Committee which will convene during March 2015
Aviation Rulemaking Advisory Committee

ARAC

- As a result of the December 18, 2014 ARAC meeting, the FAA assigned the ARAC a new task to provide recommendations regarding ASISP rulemaking, policy and guidance on best practices for aircraft systems including both certification and continued airworthiness.

- This new ARAC activity is soliciting membership for the new ASISP working group.
Policy

The FAA issued a Policy Statement for ASISP:

- PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security, March 6, 2014
Regulations, Policy, Standards and Guidance

Policy

- PS-AIR-21.16-02 quote:
  - “The Federal Aviation Administration (FAA) will issue special conditions for initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications for aircraft systems that directly connect to external services and networks under………
Policy

PS-AIR-21.16-02 quote:

- ………the following conditions:
  1. The external service or network is non-governmental;
  2. The aircraft system receives information from the non-governmental service or network; and,
  3. The failure effect classification of the aircraft system is “major” or higher.”
Regulations, Policy, Standards and Guidance

Policy

- PS-AIR-21.16-02
  - Does not require the issuance of special conditions for airworthiness and operational approval of field loadable software (FLS), aeronautical data bases, and the Aircraft Communications Addressing and Reporting System (ACARS); other policies, standards, and guidance apply
Regulations, Policy, Standards and Guidance

Policy

- We’re focusing in, for the most part, on connectivity to the outside
Standards and Guidance

- There are many information processing standards and guidance that might be able to be used in the ASISP context
  - Federal Information Processing Standards (FIPS)
  - National Institute of Standards and Technology (NIST)
  - International Standards Organization (ISO)
Regulations, Policy, Standards and Guidance

Standards and Guidance

- There are industry activities such as:
  - ARINC 811 Commercial Aircraft Information Security Concept of Operation and Process
    - ARINC 822 Aircraft/Ground IP Communication (GATELINK822)
    - ARINC 834-2 Aircraft Data Interface Function (ADF) for Aircraft Interface Device
    - ARINC 835 Guidance for Field Loadable Software Using Digital Signatures
    - ARINC 842 Guidance for Using Digital Certificates
    - ARINC Network Infrastructure and Security (NIS) Subcommittee (drafts/reports)
    - ARINC AGIE/MAGIC Subcommittee (drafts/reports)
Regulations, Policy, Standards and Guidance

Standards and Guidance

- There are industry activities such as:
  - A4A (formerly ATA) Spec 42 Aviation Industry Standards for Digital Information Security
Regulations, Policy, Standards and Guidance

Standards and Guidance

- RTCA SC-216 produced the following standard:
  - DO-355 *Information Security Guidance for Continuing Airworthiness*
  - AFS-300 plans to invoke the guidance in DO-355
Regulations, Policy, Standards and Guidance

Standards and Guidance

- RTCA SC-216 also produced the following standard:
    - Contains guidance for Aircraft Certification to address information security threats to aircraft safety
    - Applies only to part 25, Transport Category Airplanes, with a passenger seating configuration of more than 19 seats
    - Invocation likely limited to part 25 Special Conditions in the near future
Standards and Guidance

- RTCA SC-216 also produced the following standard:
  - DO-356 *Airworthiness Security Methods and Considerations*
    - A methods companion doc to DO-326A
    - As with DO-326A, applies only to part 25, Transport Category Airplanes, with a passenger seating configuration of more than 19 seats
    - Invocation also likely limited to part 25 Special Conditions
Future Direction for ASISP

AVS Strategic ASISP Plan (AKA 5 Year Plan) Current Draft

- Obtain recommendations for rulemaking and best practices for FAR Part 23, 25, 27, 29, including Instructions for continued airworthiness
  - GAMA has established an AD-HOC working group to develop industry recommended best practices for general aviation
  - Also need to obtain recommendations on the use of existing industry standards
Future Direction for ASISP

AVS Strategic ASISP Plan Current Draft

- Obtain recommendations for rulemaking and recommended best practices for FAR Parts 23, 25, 27, 29, including Instructions for Continued Airworthiness
  - For example, possibly on best practices for wireless Field Loadable Software (FLS) security, automatic fault logging and reporting for ASISP, and EFB / iPADS security considerations
Future Direction for ASISP

AVS Strategic ASISP Plan Current Draft

- Obtain recommendations for rulemaking and recommended best practices for FAR Part 23, 25, 27, 29, including Instructions for Continued Airworthiness
  - Instructions for Continued Airworthiness (ICA) for Transport Category Airplanes
Future Direction for ASISP

AVS Strategic ASISP Plan Current Draft

- Update Policy Statement PS-AIR-21.16-02, *Establishment of Special Conditions for Cyber-Security* per accepted recommendations
- Revise Special Conditions and Companion Issue Papers per recommendations
- Define RTCA Documents Applicability for ASISP
- Support RTCA follow-on activities for ASISP
- Develop and publish Designee Management guidance and criteria for ASISP
Future Direction for ASISP

AVS Strategic ASISP Plan Current Draft

- Support Research and Development for ASISP
- Develop and publish training materials for ASISP
Future Direction for ASISP

Deciding ASISP placement in the development of aircraft systems requirements

- A separate process on its own, so to speak?
- Or not separate: part of the processes in Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A, Certification Considerations for Highly Integrated or Complex Aircraft Systems?
ARP 4754A

Describes the Aircraft Systems Engineering Process

- Requirements Capture
- Allocation of Requirements
- Architectural Considerations
- Software Design Assurance Level Determination
- Hardware Level Assurance Level Determination
- Integration
ARP 4754A

Describes the Aircraft Systems Engineering Process

- Safety Assessment Process (high level)
  - Functional Hazard Assessment (FHA)
  - Preliminary System Safety Assessment
  - System Safety Assessment, etc. (e.g., CCA)
- Requirements Validation
- System Verification
ARP 4754A

Safety Assessment Process Guidelines & Methods (ARP 4761)

Intended Aircraft Function

Function, Failure System & Safety Design Information Information

Aircraft & System Development Processes (ARP 4754 / ED-79)

Guidelines for Integrated Modular Avionics (DO-297/ED-124)

Electronic Hardware Development Life-Cycle (DO-254 / ED-80)

Software Development Life-Cycle (DO-178B/ED-12B)

Development Phase

Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)

Safety Assessment Process

Functional System

Operation

In-Service/Operational Phase
Discussion, Questions, Wrap-up

Contact information:
Peter Skaves, FAA Chief Scientific and Technical Advisor for Advanced Avionics
Peter.skaves@faa.gov
(425) 802 0395