Cybersecurity – Civil Aircraft

• Since 2005, FAA has been addressing cyber vulnerabilities during certification using Special Conditions (SCs).
  – First “e-enabled” aircraft was the B-787.
  – After-market modifications that have vulnerabilities also use SCs.
  – Question: Are the SCs sufficient?

• FAA asked Aviation Rulemaking Advisory Committee (ARAC) to form a Working Group to develop recommendations on protecting aircraft systems from cyber vulnerabilities.

• December 2014, ARAC approved the Aircraft Systems Information Security and Protection (ASISP) working group to provide recommendations for potential rulemaking, policy/guidance, and best practices.
ASISP Working Group Membership

- U.S. Government – DOT/FAA, DOD, DHS, USCG
- U.S. Manufacturers – GE, Boeing, Honeywell and BendixKing, Panasonic, Textron, Rockwell-Collins, Gulfstream, Garmin, Bell Helicopter
- Foreign Manufacturers – Embraer, Sagem, Thales, Dassault, Airbus
- Operators – FedEx, United, American
- Standards Developers – ASTM Intnl., RTCA, SAE
- Organizations – GAMA, AFA
- Observers: TCCA, EASA and ANAC
Working Group Report

• Delivered to the ARAC on September 15, 2016.

• ARAC forwarded the report to FAA on October 3, 2016.

• 30 recommendations:
  – Ranging from rulemaking to developing best practices;
  – Applicable to large airplanes, small airplanes, rotorcraft and engines.
ASISP Recommendations

Eight Areas:

1. Rulemaking for airworthiness standards;

2. Other rulemaking;

3. Adoption of existing standards, updating existing standards, development of best practices, and MOC to support new regulations;

4. Update of FAA’s current cybersec policy;
ASISP Recommendations, cont.

5. Continued Operational Safety;
6. Specific Technologies, TSOs;
7. Standards for designees; and
8. R&D.
Most Important Cybersecurity Rec

• The FAA work closely with… certifying authorities to achieve harmonization for the airworthiness standards and guidance for aircraft… security and protection.
• The importance of harmonization can not be emphasized too much.
• Having the same regulatory framework for ASISP airworthiness standards is vital.
Conclusion

• ASISP working group delivered a very thorough, comprehensive report... the easy part?

• Implementation will be difficult.
  – FAA’s limited capacity for rulemaking.
  – Lots of moving parts.
  – FAA’s limited resources.

• To adequately address cybersecurity, we need to leverage the expertise of our international partners, ICAO and standards development organizations, like SAE.
Questions