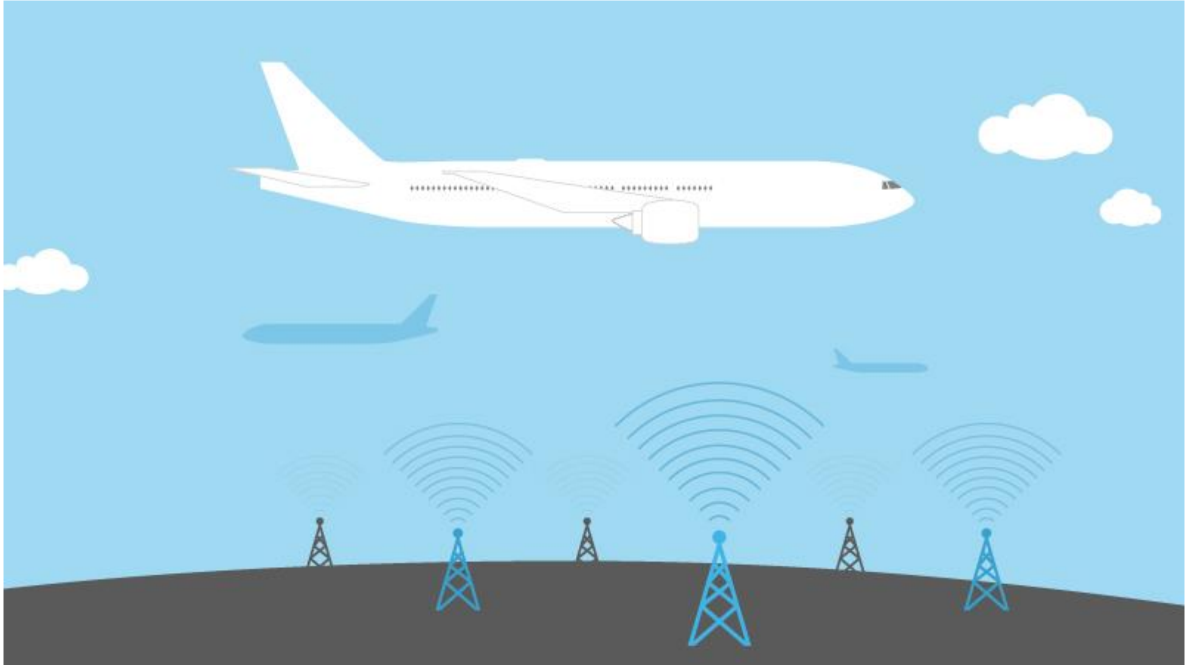
Network Security Program Proposed to Improve Aircraft Cyber Security

Woodrow Bellamy III

[Avionics Today 06-25-2015] Under a new draft Advisory Circular (AC), the FAA has proposed a set of requirements for airspace users to create an Airborne Network Security Program (ANSP). The AC lays out "an acceptable means" for operators to obtain operational approval for securing the onboard computer networks of certified aircraft.



Air to ground aircraft connectivity concept of operations. Photo: Gogo.

Within the AC, the FAA highlights the need for an ANSP to address current onboard architecture of aircraft that feature Transmission Control Protocol (TCP) / Internet Protocol (IP) connectivity. This is opposed to previous aircraft designs that utilized ARINC 429 or MIL-STD data bus transmissions to connect flight-critical avionics systems.

"The transmission of critical data necessitates the need for an ANSP. A comprehensive ANSP ensures network security onboard the aircraft, the off-airport supporting infrastructure (corporate offices), and everything in between," the draft AC states.

The FAA also specifically states that the AC describes an acceptable means "but not the only means" of obtaining operational approval for an aircraft certified with a special condition related to security of the onboard computer network." However, if the means defined in the AC were used to obtain approval, operators would then be required to conform to all of the listed requirements.

To create an ANSP, the AC assigns responsibility to the Design Approval Holder (DAH) to identify communication systems designed with TCP/IP protocol and submit network security guidance to the FAA Aircraft Certification Office for approval (ACO).

Thompson Aerospace CEO Mark Thompson, whose company sells unique aircraft connectivity and data management technology designed with specific security protocols that would prevent unspecified access to aircraft broadband radios, told *Avionics Magazine* that the AC is a step in the right direction. He also references some of the requirements that the FAA mandated as operational specifications on previous Boeing and Airbus aircraft, including the 787 and A350.

"Basically they're saying that they're going to require in the future, if someone is going to do anything based on IP traffic, they have to have a security plan," said Thompson. "Previously the only time that the security plan was invoked was for aircraft that were [Avionics Full Duplex Switched Ethernet] AFDX enabled."

Thompson also supported the draft AC's requirement for creating a General Maintenance Manual, which lays out how to control access to the Loadable Software Airplane Part (LSAP) librarian resource for an aircraft. The majority of today's airplane software loadable parts are uploaded onto an aircraft through an airborne data loader.

"We agree wholeheartedly that every airline should have a aircraft security network policy, and that's basically what the FAA is saying with this proposed ANSP. Not just the 787, or A350 because we have had ACARS on the aircraft for a long time and ACARS has always been susceptible to people doing malicious things," said Thompson. "In the AC they also address the airborne data loader, which is a big risk item. The airborne data loader is the device they walk to the plane with to put data on the plane and take data off. If that device or the individual carrying that device has been compromised, then the reality is the aircraft can be compromised."

The **draft AC** has been released following the FBI's detaining of Chris Roberts, a computer researcher who claims to have hacked into a Thrust Management Computer (TMC) on an unspecified Boeing aircraft through the cabin-based In-flight Entertainment (IFE) system. Since the release of an FBI affidavit detailing Roberts' claims, the public has been inundated with reports of cyber security risks associated with modern aircraft with onboard networks that have become increasingly digital and ever-more connected to the Internet.

During the recent **2015 Global Connected Aircraft Summit**, aviation experts **discussed these and other cyber security risks associated with today's aircraft**.

Currently, the draft AC No. 119-ANSP is available for industry comments until July 6, 2015, an FAA representative has confirmed with *Avionics Magazine*.
- See more at: http://www.aviationtoday.com/av/topstories/Network-Security-Program-Proposed-to-Improve-Aircraft-Cyber-Security_85398.html#.VwPcmaQrKUk