

criteria have been developed for this aircraft certification program, specific to this airplane's network architecture and design, providing initial guidance on an acceptable means of compliance for the 787. Additionally, the FAA intends to participate in an industry committee chartered with developing acceptable means of compliance to address aircraft network security issues, and hopes to endorse the results of the work of that committee by issuing an advisory circular (AC). Until such time as guidance is developed for a general means of compliance for network security protection, these special conditions and the agreed-to guidance are imposed on this specific network architecture and design.

- *AIRBUS Comment (a)*: Airbus stated that the requirement in the proposed special conditions is not "high level" enough because it considers a solution or an architecture. Airbus believes that criteria or assumptions for defining the domains are missing (for example, systems criticality, interfaces, rationale for the need to protect one domain from another one, trust levels * * *). The commenter maintained that the Aircraft Control Domain (ACD), Airline Information Domain (AID) and Passenger Information and Entertainment Domain (PIED) need to be precisely defined.

FAA Response: We do not agree that the requirement in the proposed special conditions prescribes a solution or an architecture. These special conditions and the acceptable means of compliance were developed based on the Boeing-proposed 787 network architecture and connectivity between the Passenger Information and Entertainment Domain and the Aircraft Control Domain and Airline Information Domain. The applicant is responsible for the design of the airplane network and systems architecture and for ensuring that potential security vulnerabilities of providing passenger access to airplane networks and systems are mitigated to an appropriate level of assurance, depending on the potential risk to the airplane and occupant safety. This responsibility is similar to that entailed in the current system safety assessment process of 14 CFR 25.1309. (See also AC 25.1309-1A and the ARAC-recommended Arsenal version of this AC, which can be found at http://www.faa.gov/regulations_policies/rulemaking/committees/arac/media/tae/TAE_SDA_T2.pdf, and SAE (Society of Automotive Engineers) ARP (Aerospace Recommended Practice) 4754). We believe the general definitions for the airplane network

"domains" are sufficient for these special conditions.

- *AIRBUS Comment (b)*: Airbus stated that in the sentence "The design shall prevent all inadvertent or malicious changes to, and all adverse impacts * * *", the wording "shall prevent ALL" can be interpreted as a zero allowance. According to the commenter, demonstration of compliance with such a requirement during the entire life cycle of the aircraft is quite impossible because security threats evolve very rapidly. The only possible solution to such a requirement would be to physically segregate the Passenger Information and Entertainment Domain from the other domains. This would mean, for example, no shared resources like SATCOM (satellite communications), and no network connections. Airbus maintained that such a solution is not technically and operationally viable, saying that a minimum of communications is always necessary. Airbus preferred a less categorical requirement which allows more flexibility and does not prevent possible residual vulnerabilities if they are assessed as acceptable from a safety point of view. Airbus said this security assessment could be based on a security risk analysis process during the design, validation, and verification of the systems architecture that assesses risks as either acceptable or requiring mitigations even through operational procedures if necessary. Airbus noted that this process, based on similarities with the SAE ARP 4754 safety process, is already proposed by the European Organization for Civil Aviation Equipment (EUROCAE) Working Group 72 for consideration of safety risks posed by security threats or by the FAA through the document "National Airspace System Communication System Safety Hazard Analysis and Security Threat Analysis," version v1.0, dated Feb. 21, 2006. Airbus said such a security risk analysis process could be used as an acceptable means of compliance addressed by an advisory circular.

FAA Response: We agree that Airbus's interpretation of zero allowance for any "inadvertent or malicious changes to, and all adverse impacts" to airplane systems, networks, hardware, software, and data is correct. However, this does not prevent allowing appropriate access if the design incorporates robust security protection means and procedures to prevent inadvertent and intentional actions that could adversely impact airplane systems, functionality, and airworthiness. Airbus commented that "a minimum of communications is

always necessary." Unauthorized users, however, must not be allowed communication access to aircraft systems and equipment in such a way that inadvertent or intentional actions can have any adverse impact on the aircraft systems, equipment, and data. Technology exists which allows sharing of resources without allowing unauthorized access and inappropriate actions to systems and data. As previously mentioned, detailed compliance guidelines and criteria, specific to the 787 network architecture, have been developed into an acceptable means of compliance for this airplane certification program. In addition, we intend to participate in future related industry committees (such as SAE S-18, which is currently revising ARP 4754, EUROCAE Working Group 72, and RTCA (RTCA, Incorporated; formerly Radio Technical Commission for Aeronautics) Special Committee 216). These groups will be developing additional aircraft network security guidance, and we hope to be able to endorse the results of their efforts as an acceptable means of compliance for network security issues on future aircraft certification programs.

- *AIRBUS Comment (c)*: Airbus said that this requirement is limited to the design ("The design shall prevent all inadvertent or malicious changes * * *"), but security solutions are always dependent on organizational procedures. Airbus said that because the efficiency of a security solution relies on the weakest link in the overall chain (design, operations, organizations, processes, * * *), the robustness of the design may be impaired (by, for instance, cabin crew interfaces being used by unauthorized passengers) if equivalent security requirements are not mandated for other involved parties, as, for example, through an operational or maintenance approval.

FAA Response: The applicant is responsible for developing a design compliant with these special conditions and other applicable regulations. The design may include specific technology and architecture features, as well as operator requirements, operational procedures and security measures, and maintenance procedures and requirements, to ensure an appropriate implementation that can be properly used and maintained to ensure safe operations and continued operational safety. These special conditions do not preclude organizational, process, operational, monitoring, or maintenance procedures and requirements from being part of the design to ensure security protection. As with other aircraft models, the operator is obligated to