CyTRAP Labs GmbH

Roentgenstrasse 49 Street
CH-8005 Zuerich Zip Code
Switzerland Country

+41(0)44 272 1876 Voice
+41(0)76 200 7778 Cell

www.CyTRAP.eu URL
info@CyTRAP.eu E-Mail

ComMetrics Indicators

3 January 2008

[Federal Register: January 2, 2008 (Volume 73, Number 1)]
[Rules and Regulations]
[Page 27-29]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr02ja08-5]

[[Page 27]]

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 25

[Docket No. NM364 Special Conditions No. 25-356-SC]

Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security--Isolation or Protection From Unauthorized Passenger Domain Systems Access

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final special conditions.

SUMMARY: These special conditions are issued for the Boeing Model 787-8 airplane. This airplane will have novel or unusual design features when compared to the state of technology envisioned in the airworthiness standards for transport category airplanes. These novel or unusual design features are associated with connectivity of the passenger

domain computer systems to the airplane critical systems and data networks. For these design features, the applicable airworthiness regulations do not contain adequate or appropriate safety standards for protection and security of airplane systems and data networks against unauthorized access. These special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing standards. Additional special conditions will be issued for other novel or unusual design features of the Boeing Model 787-8 airplanes.

DATES: Effective Date: February 1, 2008.

FOR FURTHER INFORMATION CONTACT: Will Struck, FAA, Airplane and Flight Crew Interface, ANM-111, Transport Airplane Directorate, Aircraft Certification Service, 1601 Lind Avenue SW., Renton, Washington 98057-3356; telephone (425) 227-2764; facsimile (425) 227-1149.

SUPPLEMENTARY INFORMATION:

Background

On March 28, 2003, Boeing applied for an FAA type certificate for its new Boeing Model 787-8 passenger airplane. The Boeing Model 787-8 airplane will be an all-new, two-engine jet transport airplane with a two-aisle cabin. The maximum takeoff weight will be 476,000 pounds, with a maximum passenger count of 381 passengers.

Type Certification Basis

Under provisions of 14 Code of Federal Regulations (CFR) 21.17, Boeing must show that Boeing Model 787-8 airplanes (hereafter referred to as ``the 787'') meet the applicable provisions of 14 CFR part 25, as amended by Amendments 25-1 through 25-117, except Sec. Sec. 25.809(a) and 25.812, which will remain at Amendment 25-115. If the Administrator finds that the applicable airworthiness regulations do not contain adequate or appropriate safety standards for the 787 because of a novel or unusual design feature, special conditions are prescribed under provisions of 14 CFR 21.16.

In addition to the applicable airworthiness regulations and special conditions, the 787 must comply with the fuel vent and exhaust emission requirements of 14 CFR part 34 and the noise certification requirements of part 36. The FAA must also issue a finding of regulatory adequacy pursuant to section 611 of Public Law 92-574, the ``Noise Control Act of 1972.''

The FAA issues special conditions, as defined in Sec. 11.19, under Sec. 11.38, and they become part of the type certification basis under Sec. 21.17(a)(2).

Special conditions are initially applicable to the model for which they are issued. Should the type certificate for that model be amended later to include any other model that incorporates the same or similar novel or unusual design feature, the special conditions would also apply to the other model under Sec. 21.101.

Novel or Unusual Design Features

The digital systems architecture for the 787 consists of several networks connected by electronics and embedded software. This proposed network architecture is used for a diverse set of functions, including the following:

1. Flight-safety-related control and navigation and required systems (Aircraft Control Domain).
2. Airline business and administrative support (Airline Information Domain).
3. Passenger entertainment, information, and Internet services (Passenger Information and Entertainment Domain).

The proposed architecture of the 787 is different from that of existing production (and retrofitted) airplanes. It allows new kinds of passenger connectivity to previously isolated data networks connected to systems that perform functions required for the safe operation of the airplane. Because of this new passenger connectivity, the proposed data network design and integration may result in security vulnerabilities from intentional or unintentional corruption of data and systems critical to the safety and maintenance of the airplane. The existing regulations and guidance material did not anticipate this type of system architecture or electronic access to aircraft systems that provide flight critical functions. Furthermore, 14 CFR regulations and current system safety assessment policy and techniques do not address potential security vulnerabilities that could be caused by unauthorized access to aircraft data buses and servers. Therefore, special conditions are imposed to ensure that security, integrity, and availability of the aircraft systems and data networks are not compromised by certain wired or wireless electronic connections between airplane data buses and networks.

Discussion of Comments

Notice of Proposed Special Conditions No. 25-07-01-SC for the 787 was published in the Federal Register on April 13, 2007 (72 FR 18597). One comment was received from the Air Line Pilots Association, International (ALPA) and several from Airbus.

ALPA Comment: ALPA strongly recommended that a backup means must also be provided for the flightcrew to disable passengers' ability to connect to these specific systems.

FAA Response: These special conditions apply to the design of airplane systems and networks, and would not preclude a security

mitigation strategy that provides a means for the flightcrew to disable passenger connectivity to the networks or to disable access to specific systems connected to the airplane networks. However, the FAA would prefer not to dictate specific design features to the applicant but rather to allow applicants the flexibility to determine the appropriate security protections and means to address all potential vulnerabilities and risks posed by allowing this access. For example, the security protection response to a suspected network security violation could result in--

The system automatically disabling passenger access to the network or certain functions,

Flight deck annunciation and flightcrew disabling of passenger access to certain systems or capabilities, or

Various combinations of the above.

AIRBUS General Comment 1: In Airbus's opinion these special conditions leave too much room for interpretation, and related guidance and acceptable means of compliance should be developed in an advisory circular for use by future applicants.

FAA Response: We agree that guidance is necessary and specific, detailed compliance guidelines and

[[Page 28]]

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

CyTRAP Labs GmbH

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

[[Page 29]]

operate and maintain the aircraft in conformance with regulations and with requirements for operation and maintenance of the product.

AIRBUS Comment (d): Airbus noted that the special

conditions consider only interference between the Passenger Information and Entertainment Domain (PIED) and the Airline Information Domain or Aircraft Control Domain. It notes there is no requirement for protecting the Aircraft Control Domain from the Airline Information Domain, if this one is considered less trusted than the Aircraft Control Domain. As an example, it said that the Airline Information Domain could implement portable electronic flight bags.

FAA Response: These special conditions address only the interfaces between the passenger domain (PIED) and other aircraft systems and networks. Other interfaces and accesses are addressed by current regulations and policy, and by another proposed special conditions.

AIRBUS Comment (e): Airbus said that, depending on the meaning of ``unauthorized external access,'' these special conditions may be redundant to proposed special conditions 25-07-02-SC (see comment ``b'' about 25-07-02-SC).

FAA Response: These special conditions are not redundant. The passenger PIED and its security implementation are part of the airplane model and type design, and are not considered ``external'' to the aircraft. In reviewing the Boeing-proposed 787 network architecture and design during development of these special conditions, we determined the need for two separate special conditions. To ensure appropriate security protection of the aircraft and its systems, one special condition was needed for access from the passenger domain, and one for access from sources external to the airplane.

AIRBUS proposed text revision: Airbus proposed the following revised wording for these special conditions.

The applicant shall ensure that security threats from all points within the Passenger Information and Entertainment Domain, are identified and risk mitigation strategies are implemented to protect the Aircraft Control Domain and Airline Information Services Domain from adverse impacts reducing the aircraft safety.

FAA Response: As noted previously, the purpose of these special conditions is to ensure security protection from all inadvertent or malicious changes to, and all adverse impacts to, airplane systems, networks, hardware, software, and data from accesses through the passenger domain. We do not believe the commenter's proposal is specific enough to achieve this purpose, and we will retain the current wording.

Applicability

As discussed above, these special conditions are applicable to the 787. Should Boeing apply at a later date for a change to the type certificate to include another model on the same type certificate incorporating the same novel or unusual design features, these special conditions would apply to that model as well.

CyTRAP Labs GmbH

Conclusion

This action affects only certain novel or unusual design features of the 787. It is not a rule of general applicability.

List of Subjects in 14 CFR Part 25

Aircraft, Aviation safety, Reporting and recordkeeping requirements.

0
The authority citation for these special conditions is as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701, 44702, 44704.

The Special Conditions

Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for the Boeing Model 787-8 airplane.

The design shall prevent all inadvertent or malicious changes to, and all adverse impacts upon, all systems, networks, hardware, software, and data in the Aircraft Control Domain and in the Airline Information Domain from all points within the Passenger Information and Entertainment Domain.

Issued in Renton, Washington, on December 21, 2007.
Ali Bahrami,
Manager, Transport Airplane Directorate, Aircraft Certification Service.
[FR Doc. E7-25467 Filed 12-31-07; 8:45 am]

BILLING CODE 4910-13-P