Federal Aviation Administration

Memorandum

Date: February 15, 2008

From: Manager, Small Airplane Directorate, ACE-100

To: Pilatus PC-12/47E Project File and ELOS File

Prepared by: Doug Rudolph, Aerospace Engineer, ACE-112

Subject: Equivalent Level of Safety to 14 CFR, Part 23, § 23.1357(b); Pilatus PC-12/47E, Finding No. ACE-08-02

This memorandum requests your office to review and provide concurrence with the proposed finding of Equivalent Level of Safety (ELOS) to the Circuit Protective Devices 14 CFR, part 23, § 23.1357(b).

BACKGROUND

The Pilatus PC-12/47E is a 10,450-pound single-engine, nine-passenger airplane powered by a new 1,200 shaft horsepower (SHP) Pratt & Whitney PT6A-67P turboprop engine. The PC-12/47E is an upgrade of the certified PC-12/47 model airplane with the following improvements:

- APEX New Cockpit and Avionics System (Honeywell)
- PGDS Power Generation and Distribution System
- CPCS Cabin Pressurization and Control System
- ECS Environmental Control System
- ENGINE Pratt & Whitney PT6A-67P
- ESIS Electronic Standby Instrument System

As part of this new model certification, the certification basis for the areas not affected by the modification should remain the same from the PC-12/47 model, unless an unsafe condition exists. This includes one ELOS that was granted for the PC-12/47 and the one ELOS that was extended for that model.

APPLICABLE REGULATIONS

Section 23.1357(b) requires:

(b) A protective device for a circuit essential to flight safety may not be used to protect any other circuit.

REGULATIONS REQUIRING AN ELOS

Pilatus Aircraft Ltd. is seeking certification of the PC-12/47E aircraft with an installed Honeywell Primus Apex™ Integrated Modular Avionics (IMA) system. This IMA system consists of one Modular Avionics Unit (MAU) with 2 channels. The MAU contains maximum 12 user modules with individual avionics functions that support many essential roles at the aircraft level.

Electrical power is supplied to each MAU channel from two aircraft electrical buses via two conventional circuit breakers.

Per 14 CFR, part 23, §23.1357(b), this regulation requires that a protective device for a circuit essential to flight safety may not protect any other circuit. For today's modern integrated systems, it is difficult or impossible to show compliance to this rule, even if the level of safety often exceeds those of legacy federated system.

Therefore an Equivalent Level of Safety is requested by the applicant to cover this technological evolution.

The Federal Office of Civil Aviation (FOCA) has issued an ELOS to this regulation for the corresponding European Aviation Safety Agency (EASA) type certificate (TC), per FOCA Certification Review Item (CRI) F-10 stage 3.2, "closed", dated September 11, 2007. The Federal Aviation Administration (FAA) has determined that an appropriate level of safety can be provided by the issuance of an ELOS, in accordance with the provisions of 14 CFR, part 21, § 21.21(b)(1).

DESCRIPTION OF COMPENSATING FEATURES

Discussion

The FAA added 14 CFR part 23 § 23.1357(b) in 1977 with the amendment 23-20, when only federated equipments were installed in aircraft. Safety analysis came along in 1990 with the amendment 23-41 of the 14 CFR, part 23, § 23.1309. Guidance material Advisory Circular (AC) AC-23.1309-1A had been provided 2 years later in 1992.

With the Notice of Proposed Rule Making (NPRM) 75-23 dating back to 1975, FOCA understands that the definition of an essential circuit in the FAR 23.1357(b) can only be seen as a federated essential function at the aircraft level. The intention of the rule was to avoid the loss of more than one essential function at the aircraft level when a protective device pops up, or that a non-essential function in failure condition does not switch off an essential function. With this rule the regulator imposed an electrical architecture in response to a simple safety analysis. It

cannot be accepted that the definition of "essential circuit" is reduced to a "box" that needs one power supply from the aircraft electrical bus.

Since the technology has evolved and large integration of functions is available in today's IMA avionics, an equivalent level of safety shall be provided.

FOCA Position from FOCA CRI F-10 stage 3.2:

The applicant shall demonstrate through a design analysis that each function or combination of functions (i.e. COM-NAV) at the aircraft level is equivalent (or exceed) in safety to a federated architecture that complies with 14 CFR, part 23, § 23.1357(b). The objective of the analysis is to stress the design for single point of failure or common causes. The FOCA CRI intent is not to show an equivalent reliability to a federated system (i.e. the IMA circuit breaker (C/B) is as reliable as both COM + NAV C/Bs). Therefore, the failure of each C/B that powers a component of the IMA cabinet shall be analysed for their impact on aircraft safety in case of failure.

With the Equivalent level of safety and considering the electrical power supply to the IMA system, the safety assessment shall address the following points:

1. Care should be taken to ensure that single failure either on the backplane or line replaceable modules (LRM) that can lead to the loss of a complete MAU channel are minimized.
2. A specific protection shall be provided for the cooling fan circuits, so that a short circuit on the 30 VDC supply does not lead to the loss of a MAU channel.
3. As part of an overall IMA system design analysis, provided to comply with the above mentioned objectives, the following events shall be considered:
    a. Isolation (segregation) of LRM's with duplicated power supplies to minimize the possibility of the loss of both channels following a failure on one channel.
    b. In case a LRM generates short circuits, how should a pilot determine which MAU channel is to be disconnected, if at all possible and necessary? In case the electrical power cannot be removed on the appropriate MAU channel for an operational or a system design reason, the consequences in flight shall be analysed.
    c. The effects of external 28 VDC shorting to the MAU case or backplane along with any possible cooling fan 30 VDC wiring failure occurring within the MAU.
    d. Any audio or visual alerts generated for power supply channel failures shall be made adequate to the flying crew in order to minimize confusion and reduce workload in trouble shooting task. This also applies for cooling fan failure and the consequences of only partial cooling operation.
    e. Verification that the MAU is not powered with circuit protective devices that are under control of the MAU itself.

f. Combinations of MAU power supplies failures that could result from common mode failures shall be analysed. In this regards, significant electrical transients, as for example improper generator regulation, engine flame out or relight, the availability of critical functions shall ensure continuous safe flight and landing. Even when the both generating system are isolated from each other, it shall be demonstrated that the transients do not propagate through LRM modules.

g. All the analysis should be supported by practical tests including flight tests. This is necessary to confirm the effects of the failures in a complex and high integrated environment.

4. If an automatic overheat protection feature is employed by any LRM in the MAU, this facility shall not be able to be reset in flight, unless it can be assessed that in all the cases, such a reset would not lead to any subsequent risk of fire, smoke or other failure that may reduce the capability of the flight crew to cope with adverse operating conditions. Pilatus shall also be aware that circuit breaker resets will not be an acceptable means to resolve infrequent problems that require a "cold start".

Applicant's Position from FOCA CRI F-10 Stage 3.2:

The MAU cabinet is divided into two channels hosting a variety of line replaceable modules (LRM). The dual channel architecture of the MAU allows functions to be distributed, so that no single failure will cause the loss of all functions. More specifically:

- each channel duplicates the other channel's essential functions
- each channel is powered independently
- each channel is protected by its dedicated circuit breaker

Consequently, a single MAU channel does not represent an essential load. A loss of a single MAU channel will be annunciated to the pilot, however, all essential functions will still be provided by the remaining channel.

Furthermore, the battery-backed electrical system #1 LH bus bars provide power to MAU channels - the Essential bus to channel "A" and the Standby bus to channel "B". These busses have the highest level of integrity in the PC-12 /47E electrical power system. In order to ensure full MAU availability in case of an individual bus failure, each MAU channel is additionally powered from the Main bus (part of electrical system #2, RH side). As a result, a failure of the primary power distribution path will cause an automatic switch-over of the MAU power to the secondary system (no pilot action required).

Pilatus believes that this method of supplying power independently to both MAU channels, with automatic reversion to a secondary power system, plus providing independent circuit protection to both MAU channels offers an Equivalent Level of Safety, thereby satisfying the intent of § 23.1357(b).

Pilatus response to the six items raised in the "FOCA position" section in the above referenced FOCA CRI is as follows:

1. Noted.
2. Pilatus agrees with the FOCA position that a short circuit in the 30 VDC cooling fan circuits should not result in an immediate loss of a MAU channel, either by design or by specific protection.
3. Pilatus will establish criticality objectives through a structured, top-down safety analysis approach, following the guidance provided in the Pilatus Engineering Report ("Safety Analysis Philosophy"). System Safety Assessments will demonstrate how each system component satisfies these objectives, if required. With respect to the specific concerns listed by FOCA, the Pilatus position is as follows:
    a. Noted.
    b. In case of a short circuit inside the MAU, the aircraft circuit protection device (circuit breaker) associated with the affected MAU channel will remove power from that channel. Failure of a MAU channel will be annunciated to the crew.
    c. Short circuits of external 28VDC power to the MAU or backplane will be analysed. Failure of MAU cooling fan wiring inside the MAU will be analysed separately.
    d. Noted.
    e. There are no internal circuit breakers or fuses in the MAU cabinet. However, each MAU Power Supply Module (PSM) has a thermally-controlled shut-down feature that can remove power from only that supply. The crew will be notified in the event a PSM shuts down due to an overheat condition.
    f. Continuity of the supply of aircraft electrical power to the MAU cabinet will be analysed for the following conditions: single generator failure, in flight engine shutdown (dual generator failure), in flight engine relight. Continued availability of critical functions during common cause events affecting the supply of electrical power to aircraft equipment will be addressed in System Safety Assessments. The susceptibility of the MAU to variations in electrical power input quality will be addressed through environmental qualification of the equipment.
    g. Practical tests, including system bench/rig tests, ground tests and flight tests, will be conducted as required to show compliance with the applicable airworthiness requirements.
4. The MAU and its modules contain several automatic overheat protection features. All of these will automatically reset in flight after the temperature falls below a safe reset threshold. There are no means for the crew to manually force a reset. The overheat protection features in the MAU are identical to the ones applied in existing Honeywell Primus Epic systems.

Related Regulatory Material

14 CFR, part 23, § 23.1309 and § 23.1357

Guidance material Advisory Circular AC 23.1309-1C.

APPLICANT POSITION

Based on the information provided in the previous sections, Pilatus is of the opinion the PC-12/47E Primus Apex™, as implemented on the PC-12/47E aircraft, it meets the intent of the 14 CFR, part 23, § 23.1357(b) rule and provides an equivalent level of safety.

FOCA/EASA POSITION

FOCA concurs that the Honeywell Primus Apex™, as implemented on the PC-12/47E aircraft, provides an equivalent level of safety as envisioned in the regulations and, therefore, meets the requirements of 14 CFR, part 23, § 23.1357(b) and FOCA has issued an Equivalent Level of Safety on behalf of EASA by the closing of FOCA CRI F-10, stage 3.2.

FOCA is requesting a corresponding FAA ELOS be granted for the validated U.S. Type Certificate.

FAA Position

The above is from the FOCA developed CRI F-10 stage 3.2. The FAA documented this FOCA CRI and coordinated FAA agreement on FAA Issue Paper E-3.

The FAA is in full agreement with FOCA/EASA position on this issue.

There have been no unsafe conditions documented to this data that would warrant not issuing this ELOS for this airplane.

RECOMMENDATION

The FAA recommends approval of the applicant's proposal.

CONCURRED BY

Margaret Kline *12-14-07*
Manager, Project Support Office, ACE-112 Date

Steven W. Thompson for *2-15-08*
Manager, Standards Office, ACE-110 Date

David R. Showers for *2-15-08*
Manager, Small Airplane Directorate, ACE-100 Date

K ace112dr/Pilatus/new model pc-12/45e and pc-12/47e/ace-08-02 elos 23.1357b IMA individual circuit protection pc-12-47e.doc

K:/ACE-110/masterdoc/issued/8100-5/ACE-08-02 ELOS 23.1357b IMA individual circuit protection PC-12-47E.doc/dlr:tjl:2-15-08