



Federal Aviation Administration

Memorandum

Date: November 20, 2015

To: Manager, Boeing Aviation Safety Oversight Office, ANM-100B

From: Manager, Transport Airplane Directorate, ANM-100

Prepared by: Jim Voytilla, ANM-100B

Subject: INFORMATION: Equivalent Level of Safety Finding for Flight Control System Failure Criteria on the Boeing Company Model 787-8/-9/-10 (Project Nos. TC6918SE-T, PS06-0496, PS06-0497, PS13-0546 and PS14-1031)

ELOS Memo#: TC6918SE-T-SF-1

Regulatory Ref: § 25.671(c)(2)

The purpose of this memorandum is to inform the certificate management aircraft certification office of an evaluation made by the Transport Airplane Directorate (TAD) on the establishment of an equivalent level of safety (ELOS) finding for the Model 787-8 airplane.

This memo was subsequently revised to extend this ELOS to the Boeing Model 787-9 and 787-10 airplanes.

Background

The 787 model airplane must be shown capable of continued safe flight and landing, without requiring exceptional piloting skill or strength, for single failures and certain combinations of failures not shown to be extremely improbable. The requirements for the consideration of failure conditions in the flight control systems are covered specifically by §25.671 and in general by §25.1309.

Boeing has proposed an equivalent level of safety with §25.671(c)(2) based on the proposal from the Flight Controls Harmonization Working Group (FCHWG) Aviation Rulemaking Advisory Committee (ARAC) and the draft harmonized AC/AMJ 25.1309 ("ARSENAL" version) from the System Design and Analysis Harmonization Working Group (SDAHWG). The proposal provides guidelines on what should be an acceptable risk level after the occurrence of any single failure in the flight control system.

Applicable regulation(s)

§§21.21(b), 25.671(c)(2), 25.1309

Regulation(s) requiring an ELOS

§25.671(c)(2)

Description of compensating design features or alternative standards which allow the granting of the ELOS (including design changes, limitations or equipment need for equivalency)

Boeing will demonstrate compliance of the Model 787 airplane flight control system and equipment with 14 CFR 25.671(c)(2), Amendment 114 by following the draft harmonized 25.671(c)(2) rule from the FCHWG ARAC report, dated May 17, 2002, and utilizing the means of compliance guidance in the associated draft harmonized Advisory Circular/Advisory Material Joint (AC/AMJ) for 25.671 and the draft harmonized AC/AMJ 25.1309 (“ARSENAL” version), dated June 10, 2002, from the SDAHWG.

The current §25.671(c) rule states:

“§25.671(c) The airplane must be shown by analysis, tests, or both, to be capable of continued safe flight and landing after any of the following failures or jamming, in the flight control system and surfaces (including trim, lift, drag, and feel systems), within the normal flight envelope, without requiring exceptional piloting skill or strength. Probable malfunctions must have only minor effects on control system operation and must be capable of being readily counteracted by the pilot...”

(2) Any combination of failures not shown to be extremely improbable, excluding jamming (for example, dual electrical or hydraulic system failures, or any single failure in combination with any probable hydraulic or electrical failure).”

The draft harmonized rule states:

“§25.671(c) The airplane must be shown by analysis, tests, or both, to be capable of continued safe flight and landing after any of the following failures, including jamming, in the flight control system and surfaces (including trim, lift, drag, and feel systems), within the normal flight envelope, without requiring exceptional piloting skill or strength. Probable failures must have only minor effects and must be capable of being readily counteracted by the pilot...”

(2) Any combination of failures not shown to be extremely improbable. Furthermore, in the presence of any single failure in the flight control system, any additional failure states that could prevent continued safe flight and landing shall have a combined probability of less than 1 in 1000. This paragraph excludes failures of the type defined in (c)(3)[jams].”

Compliance with the draft harmonized 25.671(c)(2) rule will be shown by safety analysis, simulation, airplane ground, and airplane flight testing. The system safety analysis will include a Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis. Pilot assessments will be conducted in the simulator and during airplane ground and flight testing to evaluate the acceptability of handling qualities following different failure conditions. The pilot assessments will be based on pilot evaluation utilizing AC 25-7A Flight Test Guide for Critical Transport Category Airplanes, Appendix 7, FAA Handling Qualities Rating Method (HQRM) as guidance. The safety analysis will identify various flight control system and equipment failure conditions. Boeing, FAA, and EASA specialists will review the safety analysis and agree on the specific failure conditions that require a handling qualities assessment. Transient response and delay times as discussed in draft harmonized AC/AMJ for 25.671 will be considered, and where appropriate adopted as part of the handling qualities assessments.

In addition to above, the following summarizes the additional steps proposed for the safety analysis:

- 1) In the safety analysis, highlight all significant latent failures that could leave the airplane one failure away from a catastrophic failure condition.
- 2) Discuss all significant latent failures with the FAA and EASA as soon as possible after significant latent failures are identified.
- 3) In the safety analysis, document that in the presence of any single failure in the flight control system (excluding jams), any additional failure states that could prevent continued safe flight and landing have a combined probability of less than 1 in 1000.

Explanation of how design features or alternative standards provide an equivalent level of safety to the level of safety intended by the regulation

Paragraph §25.671(c)(2), as proposed by the ARAC Recommendation provides a definition of acceptable risk level for subsequent failures. The FAA accepts this definition of acceptable risk level for subsequent failures; however, the FAA does not agree that this definition by itself is sufficient to provide an equivalent level of safety to the existing §25.671(c)(2). Therefore, the following additional criteria was added:

Failure conditions that are classified as catastrophic and that occur as a result of two failures, either of which are latent, must be highlighted in the system safety assessment, subject to review by the FAA. This review will ensure that any such failure conditions are, in fact, extremely improbable by assessing the failure rates and service history of each component, the inspection type and interval for any component whose failure would be latent, and any possible common cause or cascading failure modes.

These criteria are derived from guidance material recently developed by ARAC for use in the proposed revision to AC 25.1309. This guidance states, “The use of periodic maintenance or flight crew checks to detect significant latent failures when they occur is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications. Where this is not accomplished, the system safety assessment should highlight all those significant latent failures that leave the airplane one failure away from a failure condition classified as catastrophic. These cases should be discussed with the FAA as early as possible after identification.”

FAA approval and documentation of the ELOS

The FAA has approved the aforementioned ELOS finding in project Issue Paper SF-1 or Administrative Collector Issue Paper G-6. This memorandum provides standardized documentation of the ELOS that is non-proprietary and can be made available to the public. The TAD has assigned a unique ELOS Memorandum number (see front page) to facilitate archiving and retrieval of this ELOS. This ELOS Memorandum number should be listed in the type certificate data sheet under the Certification Basis section. An example of an appropriate statement is provided below.

Equivalent Safety Findings have been made for the following regulation(s):
§ 25.671(c)(2), "Flight Control System Failure Criteria" (documented in TAD ELOS Memo TC6918SE-T-SF-1).



Transport Airplane Directorate,
Aircraft Certification Service

12/3/2015

Date

ELOS Originated by ACO:	Doug Tsuji	ANM-130S
----------------------------	------------	----------