



421 Aviation Way
Frederick, Maryland 21701

T. 301-695-2000
F. 301-695-2375

www.aopa.org

December 8, 2016

Ms. Dorenda Baker
Director, Aircraft Certification Service
Orville Wright Bldg. (FOB10A)
FAA National Headquarters
800 Independence Ave. SW
Washington, D.C. 20591

Dear Ms. Baker:

We are writing today to highlight the central barriers which are inhibiting the certification and approval of low-cost, modern technology for the existing general aviation (GA) fleet, and offer solutions for removing those obstacles.

The Aircraft Owners and Pilots Association (AOPA) has previously stressed to the FAA the critical need for a comprehensive policy to modernize the existing GA fleet. That means understanding the major fundamental barriers preventing companies from seeking affordable FAA certification and approval of their products, and working collaboratively to address those issues without compromising safety.

While progress has been made, AOPA still believes there is substantial work remaining. AOPA has worked extensively with the FAA, industry stakeholders, and companies to understand those challenges. With this letter, AOPA offers four specific recommendations for reforming existing FAA policy and encouraging more companies to enter the market for retrofitting type-certificated aircraft in a cost-effective and safe manner.

1. Increase the focus on properly classifying failure conditions during the functional hazard assessment (FHA), particularly relating to the GA fleet.

As you know, an applicant for a supplemental type certificate (STC) must comply with 14 CFR § 23.1309¹ to make a major change to type design and install new equipment into a type-certificated airplane. (§ 21.101(a).) Under § 23.1309, an STC applicant must ensure the proposed equipment is designed and installed so that the airplane performs as intended under the airplane's operating and environmental limitations. The new equipment must also not adversely affect the safety of the airplane, its systems, or its occupants. These standards ensure the design and installation of the equipment meets an acceptable level of safety.

To demonstrate compliance with § 23.1309, the FAA requires the STC applicant to conduct a thorough system safety analysis, consisting of a functional hazard assessment (FHA),

¹ All references to parts or sections shall hereinafter refer to Title 14 of the Code of Federal Regulations, unless otherwise stated.

verification of both complex hardware and electronic software designs, and a system safety assessment (SSA). (*See* Advisory Circular (AC) 23.1309-1E.)

The FHA requires the STC applicant to identify all functions of the equipment proposed to be installed into the airplane. For each function, the applicant identifies and classifies all potential failure conditions as either: no safety effect, minor, major, hazardous, and catastrophic. The classification of the failure conditions determines the complex hardware development assurance level (DAL), software DAL, and the acceptable level of safety to which the equipment's design must satisfy. (AC 23.1309-1E, at 23.) A SSA is then performed to validate the safety of the design and ensure it meets the acceptable level of safety.

The FHA, including the classification of failure conditions, is highly important because the complex hardware DAL, software DAL, acceptable level of safety, and SSA are dependent upon those classifications. Given the fact-intensive nature of these classifications, the FAA has relatively minimal guidance on how those classifications are made. AC 23.1309-1E identifies a variety of factors to consider, including the nature of the failure modes, flight crew actions, flight crew workload, performance degradation, reduced operational capability, among others. (AC 23.1309-1E, at 27.) The FAA also emphasizes the consideration of mitigating or alleviating factors which reduce the severity of a failure condition. (*Id.* at 27–28.)

AOPA is concerned, however, that the failure conditions are not being properly classified. In many instances, the FAA determines a major, hazardous, or catastrophic failure condition exists when there may only be a minor failure condition. Improper failure condition classifications lead to a more demanding complex hardware DAL and software DAL, and a higher acceptable level of safety. This *unnecessary* extensive analysis of the equipment's design drives certification costs higher.

AOPA urges the FAA to ensure that failure conditions are being properly classified, especially for equipment intended to be installed in the existing GA fleet. Small airplanes under 6,000 pounds comprise the large majority of the aging GA fleet which needs modernization. For equipment intended for installation in these airplanes, the FAA should expand the written guidance in AC 23.1309-1E and incorporate factors into the FHA analysis which are unique to this segment of the fleet, such as the reliability and safety of the system being replaced, and service history of the article. A concerted effort to reduce the severity of the failure condition classification, where possible, will reduce certification costs.

2. Electronic software should not be developed in accordance with DO-178B if the software is simple and isolated from the aircraft's systems.

The FAA requires equipment containing electronic software to be developed in accordance with RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*. DO-178B contains different software design standards depending upon the classified failure condition during the FHA. For instance, software must be developed in accordance with software DAL A in DO-178B for equipment classified as having a catastrophic failure condition. A minor failure condition means the software must be developed in accordance

with software DAL D in DO-178B. DO-178B sets higher design standards for equipment with more severe failure conditions.

Currently, all equipment containing software must be developed in accordance with DO-178B, regardless of whether the equipment is installed in a transport or normal category airplane. This is consistent with the requirements set forth in FAA technical standard orders (TSO). A sample review of TSOs for equipment sought by the GA industry indicates the FAA directs all software development to DO-178B, regardless of any other considerations.

TSO No.	Equipment	Software Qualification Requirements
TSO-C48a	Carbon Monoxide Detector Instruments	Develop per DO-178B
TSO-C55a	Fuel and Oil Quantity Instruments	Develop per DO-178B
TSO-C113a	Airborne Multipurpose Electronic Displays	Develop per DO-178B
TSO-C151c	Terrain Awareness and Warning Systems (TAWS)	Develop per DO-178B
TSO-C165a	Electronic Map Display Equipment for Graphical Depiction of Aircraft Position	Develop per DO-178B
TSO-C198	Automatic Flight Guidance and Control System (AFGCS) Equipment	Develop per DO-178B
TSO-C209	Electronic Flight Instrument System (EFIS) Display	Develop per DO-178B/C

These TSOs are consistent with the FAA's internal order, which makes compliance with DO-178B for software development standard in every TSO. (*See* Order 8150.1C, at G-3.) Although the FAA allows deviations from existing policy and the TSO requirements, the FAA has not defined or explained the alternatives to DO-178B which would be permitted and under what circumstances.

There are several reasons why the FAA must fundamentally shift away from DO-178B for verifying software in modern, safety-enhancing equipment in certain applications.

First, DO-178B dramatically increases certification costs and the price of the equipment. Companies required to develop its software through DO-178B often use designated engineering representatives (DER) with experience in DO-178B compliance. DERs may charge at least hundreds of thousands of dollars for software verification. The entire single-engine piston airplane market consists of only 126,036 airplanes. (*2015 General Aviation Statistical Databook & 2016 Industry Outlook*, at 23.) The market is not large enough to give a manufacturer a reasonable possibility of recovering these costs, making DO-178B a non-starter for many companies.

Second, the NORSEE policy, which the FAA has touted as a means of incorporating safety-enhancing equipment into the existing fleet, is significantly limited. Although it does not require DO-178B software verification, NORSEE only applies to non-required equipment which has a minor failure condition and constitutes a minor change in type design. This means companies seeking an STC for their product cannot utilize the NORSEE policy. The FAA should

create an alternative pathway to DO-178B for manufacturers to make a major change in type design.

Third, alternatives to DO-178B have been developed. ASTM F3153-15, *Standard Specification for Verification of Avionics Systems*, is a relatively new industry standard developed under the ASTM F39 Committee. F3153-15 allows for system-level testing of an avionics system to verify its intended function and compliance with safety objectives. The FAA has allowed the use of this standard in certain applications in lieu of DO-178B, and AOPA urges the FAA to expand its use even further. If necessary, the FAA could engage with the industry to develop additional requirements beyond F3153-15 which satisfy the agency's safety objective.

Finally, DO-178B contemplates situations where its software verification processes may not need to be applied. DO-178B states: "There are situations where the software component of an airborne system or equipment is *simple and isolated* such that the set of inputs and outputs can be bounded. If so, it may be possible to demonstrate that exhaustive testing of this input space can be substituted for one or more of the software verification process activities identified in section 6." (DO-178B, at 86 (emphasis added).) Thus, DO-178B even recognizes that the rigorous processes identified in the standard may be unnecessary in certain circumstances.

AOPA recommends that companies not be required to develop its software in accordance with DO-178B if the software is simple and isolated from the aircraft's systems. Applying DO-178B to *all* electronic software, regardless of the failure condition, complexity of the software, and integration of the equipment, is not warranted. And applying the same design standards for electronic software in both transport and normal category airplanes is also inconsistent with the FAA's risk-based approach to aircraft certification.

The FAA is advancing a safety continuum philosophy, the concept that one level of safety may not be appropriate for all certification levels. The proposed part 23 rewrite exemplified that approach. The FAA must now incorporate this important philosophy into means of compliance, including electronic software verification. That can be achieved by limiting the use of DO-178B in applications where the software is simple and isolated from other systems.

3. Implement a risk-based approach toward granting production approval.

Production approval can be granted through either a production certificate (PC), parts manufacturer approval (PMA), or a TSO authorization (TSOA). (§ 21.1(b)(7).) Part 21 outlines the requirements that the applicant must satisfy to obtain production approval. A major requirement is for a manufacturer to have a "quality system" that addresses all the items listed in § 21.137, including design data control, document control, supplier control, inspections and testing, among other components. These requirements are identical for a manufacturer pursuing production approval through a PC, PMA, or TSOA. (§§ 21.137, 21.307, 21.607.)

The existing production approval requirements were originally promulgated through a final rule in October 2009. (74 Fed. Reg. 53368 (Oct. 16, 2009).) During that rulemaking, the FAA standardized and implemented identical quality system requirements for each of the three

production approvals (PC, PMA, and TSOA). (74 Fed. Reg. at 53368–69.) However, the FAA emphasized that the quality system requirements were meant to be scalable:

“Our requirements are consistent for all manufacturers, but they will be scalable and commensurate to the size of the company and the complexity of the product or article produced. For example, we would expect a large aircraft manufacturer to have a well-developed, complex quality system. In contrast, a small parts manufacturer producing a non-complex article could have a less complex quality system.” (74 Fed. Reg. at 53371.)

The original intent of current part 21 was for the FAA to create a scalable structure dependent upon company size and product or article complexity. The scalable approach, unfortunately, has not been reflected in current FAA guidance and practice. Only minimal reference has been made to the quality system requirements being dependent upon the size of the business and complexity of the product. (*See, e.g.*, AC 21-43A, at 2-1 [“PAH quality systems are scalable to the size and complexity of the product or article being produced.”].)

AOPA strongly believes that the requirements for production approval should be dependent upon the risk that product or article poses to the safety of flight. The FAA has already proposed a risk-based approach to the design approval of airplanes under part 23. (81 Fed. Reg. 13452 (Mar. 14, 2016).) That approach to design approval is predicated on the FAA’s safety continuum philosophy. AOPA believes this philosophy should be applied to production approval.

The FAA already evaluates the risk of an article to the safety of flight during the design approval process. The FAA should leverage the analyses performed during the system safety analysis to determine the appropriate requirements for the manufacturer’s quality system. In other words, the risk analysis performed during the design approval process should guide the requirements of the quality system. That would prevent aircraft certification offices (ACOs) and manufacturing inspection district offices (MIDOs) from duplicating efforts or arriving at inconsistent conclusions on the risk of the article.

4. Increase the use of industry standards for issuing production approval.

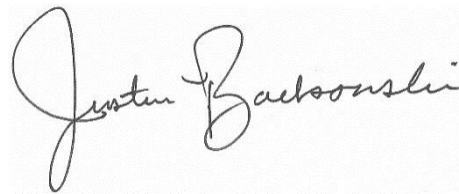
A critical aspect to retrofitting the existing fleet is encouraging new manufacturers to enter the certified market. Many new manufacturers, which are not in the GA industry or are only developing products for the experimental market, are unfamiliar with the FAA’s production approval process. Notwithstanding, those same manufacturers have oftentimes already implemented a quality system in accordance with International Organization for Standardization (ISO) 9001, *Quality Management Systems—Requirements* (ISO 9001), and Society of Automotive Engineers, Inc., International AS9100, *Quality Systems—Aerospace—Model for Quality Assurance in Design, Development, Production, Installation, and Servicing* (AS9100).

The FAA should make it easier for many of these new manufacturers to make the transition by enabling the use of industry standards which meet the intent of the FAA’s quality system requirements in part 21, such as ISO 9001, AS9100, and others. The FAA has already

suggested that these types of international standards satisfy the quality system standards set in part 21. (*See* 71 Fed. Reg. 58914, 58916 (Oct. 5, 2006); 74 Fed. Reg. at 53371.) The FAA's recognition of these and other standards as a means of obtaining production approval would encourage and make it easier for additional manufacturers to enter the certified market. Alternatively, the FAA could define what additional requirements would be necessary, if any, for the manufacturer to transition from an industry-approved quality system to a quality system approved by the FAA.

AOPA appreciates the FAA's efforts thus far to streamline certification and approval requirements for modernizing the existing GA fleet. AOPA stands ready, willing, and able to assist the FAA and industry in any way possible to address the remaining work needed to bring more modern equipment to the certified market.

Sincerely,

A handwritten signature in black ink that reads "Justin T. Barkowski". The signature is written in a cursive style with a large initial "J" and "B".

Justin T. Barkowski
Director, Regulatory Affairs