Original 737 Max Design Non-compliances with 14 CFR Part 25

MCAS-only design issues – Safety Issues #1, #2, and #3

Other design issues – Safety Issues #4, #5, and #6

Safety Issue #7 is a maintenance issue – Not discussed here

According to the "Summary of the FAA's Review of the Boeing 737 Max", subtitled, "Return to Service of the Boeing 737 Max Aircraft", dated November 18, 2020 (Page 76-78), six design issues (and one maintenance issue) were identified to correct the unsafe condition and return the 737 Max to service:

> ***13. FAA Conclusion***
> ***Following a thorough, transparent and inclusive process, the FAA determined that Boeing's changes to the 737 MAX design, flightcrew procedures and maintenance procedures effectively mitigate the airplane-related safety issues that contributed to the Flight 610 and Flight 302 accidents.***
> ***…***
>
> ***13.1 Safety Issue #1: Use of Single Angle of Attack (AOA) Sensor***
> ***In the original design, erroneous data from a single AOA sensor activated MCAS [Maneuvering Characteristics Augmentation System] and subsequently caused airplane nose-down trim of the horizontal stabilizer. In the new design, Boeing eliminated MCAS reliance on a single AOA sensor signal by using both AOA sensor inputs and through flight-control law changes that include safeguards against failed or erroneous AOA indications. The updated FCC [Flight Control Computer] software with revised flight-control laws uses inputs from both AOA sensors to activate MCAS. This is in contrast to the original MCAS design, which relied on data from only one sensor at a time, and allowed repeated MCAS activation as a result of input from a single AOA sensor. The updated FCC software compares the inputs from the two sensors to detect a failed AOA sensor. If the difference between the AOA sensor inputs is above a calculated threshold, the FCC will disable the STS [speed trim system], including its MCAS function, for the remainder of that flight and provide a corresponding indication of such deactivation on the flight deck.***
>
> ***13.2 Safety Issue #2: MCAS Reset Generates Repetitive MCAS Commands***
> ***In the original design, when a continuous erroneous high AOA sensor value existed, the MCAS control law used pilot release of the electric trim switch to reset MCAS activation. Once reset, the MCAS system would make another airplane nose-down stabilizer trim command after five seconds. This scenario would repeat each time the MCAS made a command and the pilot made an electric trim command of any duration and released the trim switch. In the new design, Boeing included flight-control law changes to ensure that MCAS will not command repeated movements of the horizontal stabilizer. The revised flight-control laws allow only one activation of MCAS per sensed high-AOA event. A subsequent activation of MCAS is only possible after the airplane returns to a low-AOA state, below the threshold that would cause MCAS activation.***

13.3 Safety Issue #3 MCAS Trim Authority

In the original design, all MCAS commands were incremental commands, which moved the horizontal stabilizer a fixed amount regardless of the current position of the stabilizer. Therefore, multiple MCAS commands resulted in a significant horizontal stabilizer mistrim condition, which the flightcrew could not counter using only elevator control. In the new design, Boeing included flight-control law changes that limit the magnitude of any MCAS command to move the horizontal stabilizer, so that the final horizontal stabilizer position (after the MCAS command) preserves the flightcrew's ability to control the airplane pitch by using only the control column.

Issues #1, #2, and #3 point to a non-compliance with 25.671(c)(1), which requires the airplane to be capable of continued safe flight after single failures without exceptional piloting skill or strength. Additionally, most would argue that a single AOA sensor failure is "probable", which further requires only "minor" effects on control system operation.

> (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.
> (1) Any single failure, excluding jamming (for example, disconnection or failure of mechanical elements, or structural failure of hydraulic components, such as actuators, control spool housing, and valves).

Issues 1-3 also point to a non-compliance with 25.672(c), where the automatic system (MCAS) encountered a single failure which led to unsafe flight and which was not adequately described in the Airplane Flight Manual.

> If the functioning of stability augmentation or other automatic or power-operated systems is necessary to show compliance with the flight characteristics requirements of this part, such systems must comply with Sec. 25.671 and the following:
> (c) It must be shown that after any single failure of the stability augmentation system or any other automatic or power-operated system--
> (1) The airplane is safely controllable when the failure or malfunction occurs at any speed or altitude within the approved

operating limitations that is critical for the type of failure being considered;
(2) The controllability and maneuverability requirements of this part are met within a practical operational flight envelope (for example, speed, altitude, normal acceleration, and airplane configurations) which is described in the Airplane Flight Manual; and
(3) The trim, stability, and stall characteristics are not impaired below a level needed to permit continued safe flight and landing.

A third non-compliance is 25.1309(b), where the "probable" failure of a single AOA sensor precluded the ability of the crew to cope with adverse operating conditions.

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that--
(1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and
(2) The occurrence of any other failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.

13.4 Safety Issue #4 Flightcrew Recognition and Response
FDR data from both accidents show that the flightcrews were unable to effectively manage the stabilizer movement and multiple flight-deck effects that occurred as a result of the single AOA sensor failure. In the new design, Boeing revised eight non-normal flightcrew procedures and proposed additional training. The revised flightcrew procedures and pilot training provide the pilot with additional information to recognize erroneous stabilizer movement and the effects of AOA sensor failures.

Issue #4 indicates that enhanced flightcrew procedures and training are being used in lieu of design changes that meet the latest amendment to 25.1322.

13.5 Safety Issue #5 AOA DISAGREE Message
In the originally delivered configuration, the AOA DISAGREE alert message on the Primary Flight Display was not functional unless the airline chose the AOA indicator option. This alert message is intended to be standard on all 737MAX airplanes. In the new design, Boeing revised the AOA DISAGREE implementation to maintain the original design intent to be standard on all 737 MAX aircraft. The FAA is requiring an additional software update that alerts the flightcrew to a disagreement between the two AOA sensors due to a sensor failure or calibration issues. The updated software

implements an AOA DISAGREE alert message on all 737 MAX airplanes. While the lack of an AOA DISAGREE alert message is not an unsafe condition itself, the FAA is mandating this software update because the flightcrew procedures now rely on this alert message to guide flightcrew action.

Issue #5 highlights four non-compliances. 25.672(a), 25.1302(b), 25.1309(c), and 25.1322(a) require clearly distinguishable, unambiguous flightcrew information if failures lead to an unsafe condition.

25.672(a):

If the functioning of stability augmentation or other automatic or power-operated systems is necessary to show compliance with the flight characteristics requirements of this part, such systems must comply with Sec. 25.671 and the following:
(a) A warning which is clearly distinguishable to the pilot under expected flight conditions without requiring his attention must be provided for any failure in the stability augmentation system or in any other automatic or power-operated system which could result in an unsafe condition if the pilot were not aware of the failure. Warning systems must not activate the control systems.

25.1302(b):

(b) Flight deck controls and information intended for the flightcrew's use must:

(1) Be provided in a clear and unambiguous manner at a resolution and precision appropriate to the task;

(2) Be accessible and usable by the flightcrew in a manner consistent with the urgency, frequency, and duration of their tasks; and

(3) Enable flightcrew awareness, if awareness is required for safe operation, of the effects on the airplane or systems resulting from flightcrew actions.

25.1309(c):

(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.

25.1322(a):

[(a) Flightcrew alerts must:

(1) Provide the flightcrew with the information needed to:

(i) Identify non-normal operation or airplane system conditions, and

(ii) Determine the appropriate actions, if any.

(2) Be readily and easily detectable and intelligible by the flightcrew under all foreseeable operating conditions, including conditions where multiple alerts are provided.

(3) Be removed when the alerting condition no longer exists.

13.6 Safety Issue #6 Other Possible Stabilizer Runaway Failures

The FAA and Boeing conducted a comprehensive review of the integrated SSA of the MCAS function. This review identified an extremely remote failure condition that required timely pilot intervention to ensure continued safe flight and landing. In the new design, Boeing has implemented a Cross-FCC Trim Monitor, which can effectively detect and shut down erroneous stabilizer commands from the FCCs. This makes continued safe flight and landing for this type of failure not dependent on pilot reaction time.

Issue #6 indicates non-compliances with 25.671(c)(1), (c)(2), and 25.1309(b)(1), since unsafe flight cannot result from "extremely remote" failures. Unreasonably short pilot response times were erroneously assumed in the original compliance determinations.

25.671(c)(1) & (2):

(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.

(1) Any single failure, excluding jamming (for example, disconnection or failure of mechanical elements, or structural failure of hydraulic components, such as actuators, control spool housing, and valves).
(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).

25.1309(b)(1):

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that--
(1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable