

**NATIONAL TRANSPORTATION SAFETY BOARD  
OFFICE OF AVIATION SAFETY  
WASHINGTON, D.C. 20594**

**August 21, 2019**

**SYSTEM SAFETY AND CERTIFICATION SPECIALIST'S REPORT**

**NTSB ID No.: DCA19RA017**

**A. ACCIDENT:**

Operator: Lion Mentari Airlines (Lion Air)  
Location: Jakarta, Indonesia  
Date: October 28, 2018  
Aircraft: 737 MAX 8, Registration PK-LQP

**B. SUMMARY:**

On October 29, 2018, PT Lion Mentari Airlines (Lion Air) flight 610, a Boeing 737 MAX 8, PK-LQP, crashed in the Java Sea shortly after takeoff from Soekarno-Hatta International Airport, Jakarta, Indonesia. The flight was a scheduled domestic flight from Jakarta to Depati Amir Airport, Pangkal Pinang City, Bangka Belitung Islands Province, Indonesia. All 189 passengers and crew on board died, and the airplane was destroyed. The National Transportation Safety Committee of Indonesia is leading the investigation.<sup>1</sup>

**C. 737 MAX and the Need for MCAS:**

The 737 MAX 8 is a derivative of the 737-800 model and is part of the 737 MAX family (737 MAX 7, 8, and 9<sup>2</sup>). The 737 MAX incorporated the CFM LEAP-1B engine, which has a larger fan diameter and redesigned engine nacelle compared to engines installed on the 737 Next Generation (NG) family. Because the 737-8 is a derivative of the 737-800 model, its certification basis, which was established per 14 CFR 21.101 Changed Product Rule, required Boeing to demonstrate compliance with Amendment 25-136 for significant areas of change at the product level and those areas affected by the significant product level change.

During the preliminary design stage of the 737 MAX 8, Boeing tests and analysis revealed that the addition of the LEAP-1B engine and associated nacelle changes produced an airplane nose-up pitching moment when the airplane was operating at high angles of attack (AOA) and mid Mach numbers. This nose-up pitching moment was deemed likely to affect the stick force per g (FS/g) characteristics required by FAR 25.255 and the controllability and maneuverability requirements of FAR 25.143(f). After the study of various options for addressing this issue, Boeing implemented aerodynamic changes as well as a stability augmentation function called the Maneuvering Characteristics Augmentation System (MCAS), as an extension of the existing Speed

---

<sup>1</sup> The preliminary report on this accident can be found at [https://reports.aviation-safety.net/2018/20181029-0\\_B38M\\_PK-LQP\\_PRELIMINARY.pdf](https://reports.aviation-safety.net/2018/20181029-0_B38M_PK-LQP_PRELIMINARY.pdf).

<sup>2</sup> Both the 737-8 and 737-9 were in service at the time of the accident. The 737-7 and 737-10 are planned future derivatives that have not yet entered service.

Trim System (STS), to improve aircraft handling characteristics and decrease pitch-up tendency at elevated angles of attack.

As the development of the 737 MAX 8 progressed, the MCAS function was expanded to low Mach numbers. MCAS is designed to function only during manual flight (autopilot not engaged), with the airplane's flaps up, at an elevated AOA.

## **D. Speed Trim & MCAS Description:**

To ensure that the 737-600/700/800/900 (737 NG) family of airplanes met the certification requirements for longitudinal static stability (speed stability), the airplanes incorporated a Speed Trim System (STS) to augment the basic airplane's speed stability during certain low speed, high thrust flight conditions by moving the horizontal stabilizer during manual flight (autopilot is not engaged). For the 737 NG family of airplanes, the Speed Trim System included the Speed Trim Function. The STS was carried over to the 737-7/-8/-9 (737 MAX) family of airplanes. Additionally, on 737 MAX airplanes, the MCAS function was added to the STS to address the pitch characteristics described above.

### **D.1 Speed Trim Function:**

The Speed Trim function, which is implemented as a control law within the flight control computer (FCC<sup>3</sup>), commands incremental stabilizer trim through the automatic trim control system circuitry. There are two different stabilizer trim rates depending on whether position of the flaps<sup>4</sup>. A schedule determines the desired incremental stab deviation from the last trimmed position as a function of airspeed and flap position.

According to the Enhanced Digital Flight Control System (EDFCS) system safety analysis (SSA), the worst-case failure mode of the Speed Trim function was considered to be a runaway of the horizontal stabilizer trim actuator (HSTA) as a result of sensor or FCC failures, or FCC-to-stab trim motor (STM) wiring failures. The SSA indicated that during the runaway, the pilot is able to detect the fault by noticing the continuous running of the trim mechanical wheels in the flight deck, or by the change in column force necessary to maintain pitch attitude, or through change in airplane pitch attitude. The SSA indicated that the pilot compensates for the runaway through:

- column input in the direction opposing the uncommanded trim until activation of the column activated trim cutout switches, or
- activation of the main electric trim by either pilot in a direction opposing the uncommanded motion, which overrides the FCC commanded trim runaway, or
- moving the guarded stabilizer trim cutout switches<sup>5</sup> located on the aisle stand to the CUTOUT position, or restraining the stabilizer trim wheel,

---

<sup>3</sup> The flight control computers (FCC) are part of the digital flight control system. There are two autopilots, autopilot A from FCC A and autopilot B from FCC B.

<sup>4</sup> When the flaps are down, the stabilizer rate is three times faster than when the flaps are up.

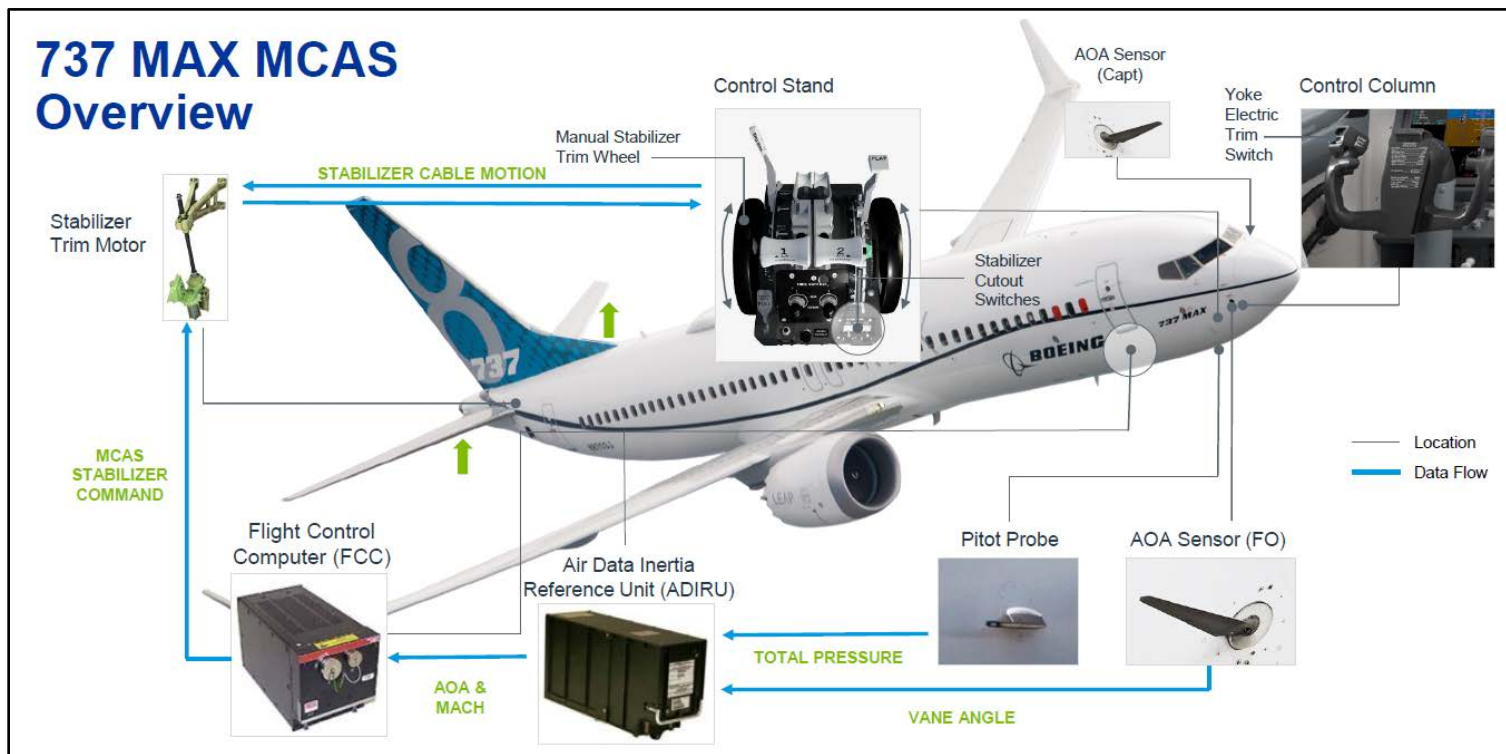
<sup>5</sup> Two stabilizer trim cutout switches on the control stand can be used to stop the main electric and autopilot trim inputs to the stabilizer trim actuator. The switches can be set to NORMAL or CUTOUT. If either switch is moved to CUTOUT, both the electric and autopilot trim inputs are disconnected from the stabilizer trim motor. NORMAL is the default position to enable operation of the electric and autopilot trim.

- Speed/ Stab Trim runaways are limited by the inherent stab trim motor rate and column actuated trim cut-out switches. Sufficient means are available for the pilot to maintain control and recover from the runaway<sup>6</sup>.

## D.2 MCAS Functional – Detailed Description:

The MCAS is a function within the Speed Trim System and, when activated, moves the stabilizer during non-normal flaps up, high angle of attack maneuvers to provide a desirable increase in stick force gradient and a reduced pitch up tendency. Similar to the Speed Trim Function, the MCAS function is also a flight control law<sup>7</sup> contained within each of the two FCCs. MCAS is only active in the master FCC for that flight. At airplane power-up, the master FCC defaults to the left side FCC; and will then alternate between the left and right FCC by flight. The master FCC is not affected by the position of the Flight Director switches. The FCCs receive inputs from several systems including the air data inertial reference system (ADIRS). Reference Figure 1. Specific to the MCAS, the control law commands the stabilizer trim as a function of the following: Air/Ground, Flap position, Angle of attack, Pitch rate, True Airspeed and Mach.

Figure 1 Diagram showing the components of MCAS<sup>8</sup>



The AOA and Mach inputs are provided to each FCC by the associated air data inertial reference unit (ADIRU). Each ADIRU receives AOA information from one of the two resolvers contained within the associated AOA sensor (i.e. the Left ADIRU uses left AOA vane and the Right ADIRU uses the right AOA vane). Information from the other resolver contained within the AOA sensor, along with data from other sources, is provided to the

<sup>6</sup> MCAS failures do allow the stabilizer to move at the flaps down trim rate, even if the flaps are up, but even the flaps down trim rate is a limit, albeit faster than the normal flaps up rate. Column cutout is always available in the forward direction but may not be available in the aft direction for certain MCAS failures.

<sup>7</sup> MCAS is an open loop flight control law.

<sup>8</sup> Reference Boeing 737 MAX MCAS briefing, dated March 25, 2019.

stall management yaw damper computer (SMYD), which is used, along with data from other sources, for the purpose of calculating and sending commands to the Stall Warning System (SWS)<sup>9</sup>.

As originally delivered, the MCAS became active during manual, flaps-up flight (autopilot not engaged) when the AOA value received by the master FCC exceeded a threshold based on Mach number. When activated, the MCAS provided a high rate automatic trim command to move the stabilizer AND. The magnitude of the AND command was based on the AOA and the Mach. After the non-normal maneuver that resulted in the high AOA, and once the AOA fell below a reset threshold, MCAS would move the stabilizer ANU to the original position and reset the system. At any time, the stabilizer inputs could be stopped or reversed by the pilots using their yoke-mounted electric stabilizer trim switches, which also reset the system after a 5 second delay.

The latter behavior is based on the assumption that flight crews use the trim switches to completely return the airplane to neutral trim. In the FCC software version current at the time of the accident, if the original elevated AOA condition persists for more than five seconds following an MCAS flight control law reset, the MCAS flight control law will command another stabilizer nose down trim input (with the magnitude based on the AOA and Mach sensed at that time).

On all 737 models, column cutout switches interrupt stabilizer commands, either from the autoflight system (e.g. FCC) or the electric trim switches in a direction opposite to elevator command. On the 737NG and MAX, two column cutout switching modules, one for each control column, are actuated when the control columns are pushed or pulled away from zero (hands off) column position. When actuated, the column cutout switching modules interrupt the electrical signals to the stabilizer trim motor that are in opposition to the elevator command.

The MCAS function requires the stabilizer to move nose down in opposition to the column commands when approaching high angles of attack. To accommodate MCAS, the column cutout function in the first officer's switching module was modified to inhibit the aft column cutout switch while MCAS is active, allowing aircraft nose-down (AND) stabilizer motion with aircraft nose-up (ANU) column input. Once MCAS is no longer active, the normal column cutout function in the stabilizer nose down direction is re-instated.

## **E. Functional Hazard Assessment and Requirements Generation:**

### **E.1 Functional Hazard Assessment:**

A functional hazard assessment (FHA) is a systematic examination of a system's functions and purpose, and it typically provides the initial, top-level assessment of a design and addresses the operational vulnerabilities of the system function. The FHA is therefore typically used to establish the safety requirements that guide system architecture design decisions. An FHA evaluates what would occur (the "hazard" in FHA) if the function under question was lost or malfunctioned and classifies the severity of that effect. An FHA is conducted early in the design and development cycle to identify hazards and classify them by severity, beginning at the airplane level and working down to individual systems.

Federal Aviation Administration (FAA) Advisory Circular AC 25.1309-1A, dated June 21, 1988 and SAE ARP4761 define the severity classes that are used to classify the effect of loss or malfunction as part of an FHA. AC 25.1309-1A defines the following three severity classes: catastrophic, major and minor, with corresponding acceptable probabilities of extremely improbable (1E-9) or less per flight hour, improbable (1E-5 or less), and no worse than probable (1E-3). European regulations (originally JAR and now EASA) include an additional

---

<sup>9</sup> The SWS operates the control column stick shakers to alert the crew when the airplane is nearing an aerodynamic stall.

category: hazardous, which falls between catastrophic and major and has an associated acceptable probability of 1E-7 or less. The differences among the classes are associated with effects on the airplane, occupants, and crew.

To begin an FHA, engineering judgment is used to identify the failure conditions which require evaluation. According to the FHA sections<sup>10</sup> of Boeing’s 737 NG/MAX Stabilizer Trim Control System Safety Analysis, (Reference section H.2.2 of this report), performance analyses and piloted simulations were accomplished as needed to help define the hazard categories for the identified conditions. Figure 2 shows the criticality categories used in developing the FHA and the corresponding minimum acceptable probabilities of occurrence. The failure conditions defined by the FHA provide the basis for the top-level events analyzed by the Fault Tree Analysis (FTA) to demonstrate compliance with FAR 25.671(c)(2) and 25.1309(b)(1). A fault tree analysis was performed on each failure condition determined to be either Catastrophic or Hazardous. Additionally, Major events are included in the FHA for reference, per FAA/JAA request.

**Figure 2 Failure Effect Categories**

<b>FAR/JAR Failure Effect Category Definitions</b>					
	FAR - AC 25.1309-1A definitions.	No significant degradation of aircraft capability. Crew actions well within their capabilities.	Reduction of the aircraft capability or of the crew ability to cope with adverse operating conditions.		Prevention of continued safe flight and landing of the aircraft.
Effects on aircraft and occupants of the identified failure condition.	AMJ No.1 of JAR 25.1309 definitions.	Slight reduction of safety margins,	Significant reduction in safety margins,	Large reduction in safety margins,	Loss of the aircraft and/or fatalities.
		Slight increase in work load, (e.g. routine changes in flight plan), or  Physical effects but no injury to occupants.	Reduction in the ability of the flight crew to cope with adverse operating conditions impairing their efficiency, or  Injury to occupants.	Physical distress or workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely, or  Serious injury to or death of a relatively small portion of the occupants.	
FAR effect category AC 25.1309-1A.	Minor	Major		Catastrophic	
JAR effect category AMJ No. 1 of JAR 25.1309	Minor	Major	Hazardous	Catastrophic	
Criticality category RTCA DO-178A	Non-essential (Level 3 software)	Essential (Level 2 software)		Critical (Level 1 software)	
Criticality category RTCA DO-178B	Minor (Level D software)	Major (Level C software)	Hazardous (Level B software)	Catastrophic (Level A software)	
FAR qualitative probability terms.	Probable		Improbable		Extremely Improbable
JAR qualitative probability terms.	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
FAR and JAR quantitative probability ranges.	10 <sup>-3</sup>	10 <sup>-5</sup>	10 <sup>-7</sup>	10 <sup>-9</sup>	Probability of Failure Condition (for one flight hour or flight if less than one hour).

<sup>10</sup> The safety analysis contained two sections that discussed hazard analysis; the first FHA was developed for the 737NG in the original release of the analysis (1997) and the second FHA was developed as part of the 737 MAX changes (2016).

As part of the MCAS development phase, in late 2012, Boeing performed a preliminary functional hazard assessment<sup>11</sup> of MCAS using piloted simulations in their full motion Engineering Flight Simulator. Several hazards were assessed at that time, however, this section of the report will focus only on the following two hazards: uncommanded MCAS operation up to its maximum authority (0.6 degrees of airplane nose down stabilizer) and uncommanded MCAS operation equivalent to a three (3) second stabilizer trim runaway<sup>12</sup>. To perform these simulator tests, Boeing induced a stabilizer trim input that would simulate the stabilizer moving at a rate and duration consistent with the MCAS function. Using this method to induce the hazard resulted in the following: motion of the stabilizer trim wheel, increased column forces, and indication that the airplane was moving nose down. Boeing indicated to the NTSB that this evaluation was focused on the pilot response to uncommanded MCAS operation, regardless of underlying cause. Thus, the specific failure modes that could lead to uncommanded MCAS activation, such as an erroneous high AOA input to the MCAS, were not simulated as part of these functional hazard assessment validation tests. As a result, additional flight deck effects (such as IAS DISAGREE and ALT DISAGREE alerts and stick shaker activation) resulting from the same underlying failure (for example, erroneous AOA) were not simulated and were not documented in the stabilizer trim and autoflight safety assessment reports reviewed by the NTSB.

**Table 1 Original results of preliminary hazard assessment**

Hazard	Hazard classification
Uncommanded MCAS operation up to its maximum authority	Major
Uncommanded MCAS function operation equivalent to 3 second mistrim	Major

The FHA evaluations were conducted by Boeing in their Engineering Cab using FAA guidance regarding pilot response to flight control failures requiring trim input that is contained in FAA Advisory Circular AC25.7C<sup>13</sup>. In particular, Boeing uses the following assumptions in its flight controls FHAs:

- Uncommanded system inputs are readily recognizable and can be counteracted by overriding the failure by movement of the flight controls in the normal sense by the flight crew and do not require specific procedures.
- Action to counter the failure shall not require exceptional piloting skill or strength.
- The pilot will take immediate action to reduce or eliminate increased control forces by re-trimming or changing configuration or flight conditions.
- Trained flight crew memory procedures shall be followed to address and eliminate or mitigate the failure.

Boeing advised that these assumptions are used across all Boeing models when performing functional hazard assessments of flight control systems and that these assumptions are consistent with the requirements contained in 14 CFR 25.671 & 25.672 and within the guidance contained in FAA Advisory Circular (AC) 25-7C for compliance evaluation of 14 CFR 25.143<sup>14</sup>.

In March 2016, Boeing determined that MCAS should be revised to improve wings-level, flaps up, low Mach stall characteristics and identification. The MCAS was revised such that depending on AOA, it would be capable

<sup>11</sup> The hazard assessments were developed as part of aircraft certification and based on AC 25.1309-1A.

<sup>12</sup> The two events were assumed to start from a trimmed condition. Boeing also considered the hazard of uncommanded MCAS operation until pilot response. This condition had the same severity as the 3-second case.

<sup>13</sup> FAA advisory circular (AC) 25-7C, titled, "Flight Test Guide for Certification of Transport Category Airplanes," dated October 16, 2012, provides guidance for the flight test evaluation of transport category airplanes.

<sup>14</sup> FAR 25.143(g) Controllability and Maneuverability – General, Requires that changes of gradient that occur with changes of load factor must not cause undue difficulty in maintaining control of the airplane, and local gradients must not be so low as to result in a danger of over-controlling. Reference is made to CFR amendment 25-129 for the described FAR 25.143(g) requirement.

of commanding incremental stabilizer to a maximum of 2.5 degrees at low Mach decreasing to a maximum of 0.65 degrees at high Mach.

The requirements document also indicated that the preliminary functional hazard assessments of MCAS were re-evaluated by pilot assessments in the motion simulator and by engineering analysis and determined to have not changed in hazard classification as a result of the increase in MCAS authority to 2.5 degrees.

**Table 2 Results of preliminary hazard assessment for revised MCAS authority**

Hazard	Hazard classification
Uncommanded MCAS function operation up to its maximum authority	Major*
Uncommanded MCAS function operation equivalent to 3 second mistrim **	Major

**\* Major Classification:**

The uncommanded MCAS command to the maximum nose down authority at low Mach numbers was evaluated in the 737 MAX cab and rated as Minor. The high Mach uncommanded MCAS command and subsequent recovery is the critical flight phase in establishing the hazard rating for erroneous MCAS commands. According to Boeing, engineering analysis determined that the existing high Mach evaluations remain valid as the aerodynamic configuration had not changed significantly since the pre-flight evaluations, and the MCAS authority limit at high Mach did not change significantly in the flight test update. As the ratings for these high Mach evaluations were more severe than for low Mach, the overall flight envelope hazard ratings remain the same as the pre-flight evaluations.

**\*\* Piloted Simulation not Required:**

According to Boeing, Engineering analysis determined no low Mach piloted simulation to be required as this failure is less critical than MCAS function operation to maximum authority. Stabilizer motion for three seconds would not reach maximum authority in low Mach conditions. The existing high Mach evaluations remain valid as the aerodynamic configuration has not changed significantly since the preflight evaluations, and the 3 second stabilizer motion is the same magnitude.

When assessing unintended MCAS activation in the simulator for the FHAs, the function was allowed to perform to its authority and beyond before pilot action was taken to recover. Failures were able to be countered by using elevator alone. Stabilizer trim was available to offload column forces, and stabilizer cutouts were available but not required to counter failures. This was true both for the preliminary FHAs performed in 2012 and for the reassessment of the FHAs in 2016.

In a 2019 presentation to the NTSB, Boeing indicated that the MCAS hazard classification of “major” for uncommanded MCAS function (including up to the new authority limits) in the Normal flight envelope were based on the following conclusions:

- Unintended stabilizer trim inputs are readily recognized by movement of the stab trim wheel, flight path change or increased column forces.
- Aircraft can be returned to steady level flight using available column (elevator) alone or stabilizer trim.
- Continuous unintended nose down stabilizer trim inputs would be recognized as a Stab Trim or Stab Runaway failure and procedure for Stab Runaway would be followed.

Boeing also indicated that as part of the development process, although not formally part of the FHA analysis, engineering personnel and test pilots discussed the scenario of repeated uncommanded MCAS activation due to erroneously high AOA and considered whether a system redesign was necessary to address this issue. As part of this discussion, they discussed the combined flight deck effects (including stick shaker activation, among others), but determined that no redesign was necessary. This conclusion was based in part on the assumption that each activation would be recognized and immediately trimmed out, which is consistent with the regulatory guidance in AC 25-7C that a pilot will take immediate action to trim out reduce or eliminate high control forces by re-trimming or changing configuration or flight conditions.

### **E.1.1 Requirements Generation and Traceability:**

Based on the MCAS pilot assessments using the Engineering Flight Simulator, several system and safety requirements were generated. An NTSB review of these requirements found one requirement related to the probability of an MCAS system hardover. The requirement stated: “The probability of a system hardover, oscillatory failure, and loss of function shall be commensurate with the hazard levels identified by the FHA, which were determined by Pilot simulator assessments of the MCAS failure modes. As previously stated, unintended MCAS operational FHA events were assessed as “Major” in the normal flight envelope, with a corresponding required probability of 1E-5.

The MCAS function is a control law (software) contained within the Flight Control Computer (FCC), which was developed by Rockwell Collins Inc to meet the design specifications contained within a Specification Control Drawing (SCD) provided to them by Boeing<sup>15</sup>. The SCD covers the design, fabrication, performance, qualification, and functional testing requirements for the Enhanced Digital Flight Control System (EDFCS) for use on the Boeing 737. An NTSB review of the SCD revealed that requirements for MCAS were first added to the document at Revision G, dated July 28, 2014.

On December 23, 2015, Boeing released an internal document titled “Engineering Authorization for Incorporation of EDFCS Problem Reports B-1740” to transmit requested changes, safety requirements, into the EDFCS SCD. Of the six new safety requirements, two of them were related to MCAS; One of the safety requirements (3.1.1.5.3.1.1-A) included an upper limit to “The probability of the FCC producing an erroneous flaps up/down discrete output or an erroneous MCAS Engage discrete output without detection.” This requirement was derived from the above-mentioned FHA result that unintended MCAS operation have a probability of less than 1E-5.

An NTSB review of the EDFCS SCD revealed that the MCAS safety requirement 3.1.1.5.3.1.1-A was added to the SCD per Boeing document “B-1740” at Revision J, dated November 3, 2016.

An NTSB review of a December 09, 2016 Rockwell Collins document titled “EDFCS FCC-730 P10.0 Requirement Verification Matrix” was conducted. This document included a “traceability matrix” table that identified the incremental requirements that were changed/added/deleted for the EDFCS FCC-730 P10.0 software development. The document indicated that the traceability matrix had been reviewed by Rockwell and their review found that the requirements affected by the EDFCS FCC-730 P10.0 software development have been correctly allocated, implemented, and verified. The NTSB review of the “traceability matrix” table found that it included all of the safety requirements that were added to the SCD per Boeing document “B-1740, including the MCAS safety requirement 3.1.1.5.3.1.1-A. According to Boeing, the safety requirement would be covered in the

---

<sup>15</sup> Boeing’s Flight Controls –Autoflight (EDFCS/FCC) & Autothrottle Certification Plan CP13474 indicated that the software will be developed by Rockwell Collins and the Software Accomplishment Summary (SAS) document will be a summary of all the design development and verification activities defined in the PSAC that provides the data to substantiate that the objectives of RTCA DO-178B for the appropriate design software level have been met.



EDFCS system safety assessment. A review on the Boeing EDFCS system safety assessment found that the MCAS safety requirement 3.1.1.5.3.1.1-A was addressed.

## **F. Certification:**

In Title 14, Code of Federal Regulations (CFR) United States of America Part 21, the Federal Aviation Administration (FAA) is responsible for certifying aircraft. The certification basis is usually established based on the aircraft configuration and functionalities and any special conditions that deemed necessary. For Boeing 737-8 MAX the certification basis is mainly based on the FAR Part 25. Boeing is responsible to show compliance with the requirements set in the certification basis using a proper and standard procedure<sup>16</sup>.

### **F.1 Type Certification Process and Overview:**

The FAA is responsible for prescribing minimum standards required in the interest of safety for the design, material, construction, quality of work, and performance of aircraft, aircraft engines, and propellers (Ref. 49USC44701). Product certification<sup>17</sup> is a regulatory process administered by the FAA to ensure that an aircraft manufacturer's product complies with Federal Aviation Regulations (FAR). Successful completion of the certification process enables the FAA to issue a type certificate (TC) or an amended type certificate (ATC). To obtain a TC or an ATC, the manufacturer must demonstrate to the FAA that the aircraft or product being submitted for approval complies with all applicable regulations. The FAA determines whether or not the applicant has met its responsibility to show compliance to the applicable regulations.

The Federal regulations that apply to type certification of transport-category airplanes are 14 CFR Part 21, 25, 26, 33, 34, and 36. The Part 25 regulations are those concerned with the airworthiness standards for transport-category airplanes and are organized into subparts A through G. Because regulations are continuously evolving, each airplane is assigned a type certification basis that is established by the FAA based on the regulations in effect on the date of application. These regulations represent the minimum standards for airworthiness; an applicant's design may exceed these standards and the applicant's tests and analyses may be more extensive than required by regulation. The specific applicable regulatory requirements and how compliance will be demonstrated is documented in an FAA accepted certification plan.

### **F.2 Certification Guidance:**

FAA Order 8110.4C, titled "Type Certification", prescribes the responsibilities and procedures the FAA must follow to certify new civil aircraft, aircraft engines, and propellers, or changes thereto, as required by 14 of the Code of Federal Regulations (CFR) Part 21. This order is primarily written for internal use by the FAA, its designees, and delegated organizations. The order provides procedures and policy for the type certification of products and, unless stated otherwise, the type certification process in this order applies to all U.S. TCs, including amended TCs.

### **F.3 Typical Certification Process:**

FAA Order 8110.4C contains a section that presents a high-level flow diagram of the certification events that typically make up the life cycle an aircraft. The diagram is meant to explain the type certification process, not to

---

<sup>16</sup> FAR 21.20 is the provision setting forth the responsibility for showing compliance. Applicable Orders are 8110.4 (Type Certification) and 8110.15 (ODA)

<sup>17</sup> Certification accounts for proper completion of tasks established for flight operations and ground crew maintenance tasks and it relies on decision making and actions being based on an established safety culture.

dictate precisely how the project should flow. Although the model shows the proper sequence of events for certificating a product, the various aspects of the project generally progress through the process at different times and at different rates. The model divides the product's type certification life cycle into phases based on *The FAA and Industry Guide to Product Certification*. For each of the certification events identified on the flow diagram, the Order also provides information describing each event, identifies expectations and develops specific interface procedures between the applicant and the FAA.

During a meeting with the NTSB<sup>18</sup>, the FAA provided a high-level overview of the certification process for an amended type design program. The briefing indicated that the applicant would start by conducting familiarization briefings and submitting the following to the FAA: a certification project notification (CPN), a program notification letter (PNL) and a master certification plan (MCP). These documents detail the changes and identify the regulatory requirements and policies that are applicable; they also identify areas of change associated with the FAA airworthiness directives. As part of the overview, the FAA provided a high-level flow diagram of the certification events that contained similar information as the diagram within Order 8110.4c. (Reference Figure 3)

Figure 3 Diagram of FAA Certification Process



<sup>18</sup> Meeting held at the FAA on February 27, 2019.

During a meeting with the NTSB<sup>19</sup>, the FAA provided the investigation team with a list (Reference table 3) showing a timeline for when certain 737 MAX 8 certification events occurred.

**Table 3 737 MAX Timeline**

Amended Type Certification (ATC) Application	January 2012
General Familiarization Meeting (completed)	March 2012
Technical Familiarization Meetings (completed)	May 2012
Certification Basis Established (G-1 Issue Paper)	February 2014
FAA Acceptance of Master Certification Plan	November 2013
FAA Acceptance of (related) Detailed Certification Plans	November 2016
Type Inspection Authorization Approved	August 2016
FAA Certification Flight Tests Complete	February 2017
ATC Issuance	March 2017*

#### **F.4 FAA Certification Office:**

The FAA has 10 aircraft certification offices (ACO) which are responsible for approving the design certification of aircraft, aircraft engines, propellers, and replacement parts for those products. There are also specialized certification offices which include the Engine Certification Office (ECO), the Military Certification Office (MCO), the Boeing Aviation Safety Oversight Office (BASOO), and the Delegation Systems Certification Office (DSCO). The BASOO is the FAA’s certification office specifically assigned to provide oversight of the certification of Boeing products. It is located in Seattle Washington. BASOOs’ responsibilities include oversight of Boeing’s Organization Designation Authorization (ODA), involvement in certification of safety critical areas as well as novel and unusual designs and assisting foreign Civil Aviation Authorities (CAAs) in validation of Boeing products. The BASOO was responsible for the certification oversight and approval for the 737 MAX.

#### **F.5 Certification Basis:**

According to Type Certificate Data Sheet<sup>20</sup> (TCDS) A16WE, revision 64, dated October 10, 2018, Boeing applied for a transport category amended type certificate (ATC) for the 737-8 airplane on June 30, 2012. The ATC was approved on March 8, 2017. The Boeing 737-8 airplane was added as the most recent model in a series of derivative models (or “changed aeronautical products”) that were approved and added to the Boeing type certificate (TC), originally issued for the Boeing 737-100 on December 15, 1967.

The applicable certification basis for the 737-8 airplane is Title 14, Code of Federal Regulations (14 CFR) part 25 as amended by Amendments 25-0 through 25-137, plus amendment 25-141 with exceptions permitted by 14 CFR 21.101.

<sup>19</sup> Meeting held at the FAA on February 27, 2019.

<sup>20</sup> A Type Certificate Data Sheet (TCDS) is a formal description of the aircraft, engine or propeller. It lists limitations and information required for type certification including airspeed limits, weight limits, thrust limitations, etc.

## **F.6 Certification Basis for Changed Aviation Products:**

The certification basis for changed aeronautical products allows an aircraft manufacturer to introduce a derivative model as a design update on a previously certificated aircraft and add the changed product onto an existing TC. The FAA approves such changes if it finds that the changes are not significant enough to warrant application for a new TC. This process enables a manufacturer to introduce derivative aircraft models without having to resubmit the entire aircraft design for certification review. The manufacturer can use the results of some of the analyses and testing from the original type certification to demonstrate compliance, in which case the regulations that were in effect on the date of the original TC apply.

Title 14 CFR 21.101, Subpart D, specifies the requirements for demonstrating airworthiness compliance for changed aeronautical products. The current revision of 14 CFR 21.101, amendment 21.92, which became effective on April 16, 2011, states that an application for a changed aeronautical product to be added to a TC “must show that the changed product complies with the airworthiness requirements applicable to the category of the product in effect on the date of the application.” This regulation is more specific than previous revisions regarding what can be used from the original certification basis in an application for a derivative model involving a major change.

On April 25, 2003, the FAA issued FAA Order 8110.48, *How to Establish the Certification Basis for Changed Aeronautical Products*, which provides the procedures that the FAA and its designees utilize for determining the certification basis for changes to type certificated products including changes made through an amended Type Certificate which was the method utilized for the 737 MAX. The handbook refers to FAA Advisory Circular 21.101-1, *Establishing the Certification Basis of Changed Aeronautical Products*, which contains an acceptable means, but not the only means, to comply with 14 CFR 21.101. On July 21, 2017, this Order 8110.48 was cancelled and replaced by Order 8110.48A.

## **G. System Safety Assessment Process - General:**

### **G.1 Overview:**

The process for developing and certifying a safety-critical system must provide assurance that all significant single failure conditions have been identified and that all combinations of failures which lead to hazardous or catastrophic airplane level effects have been considered and appropriately mitigated. Aircraft manufacturers provide this assurance through their safety assessment processes.

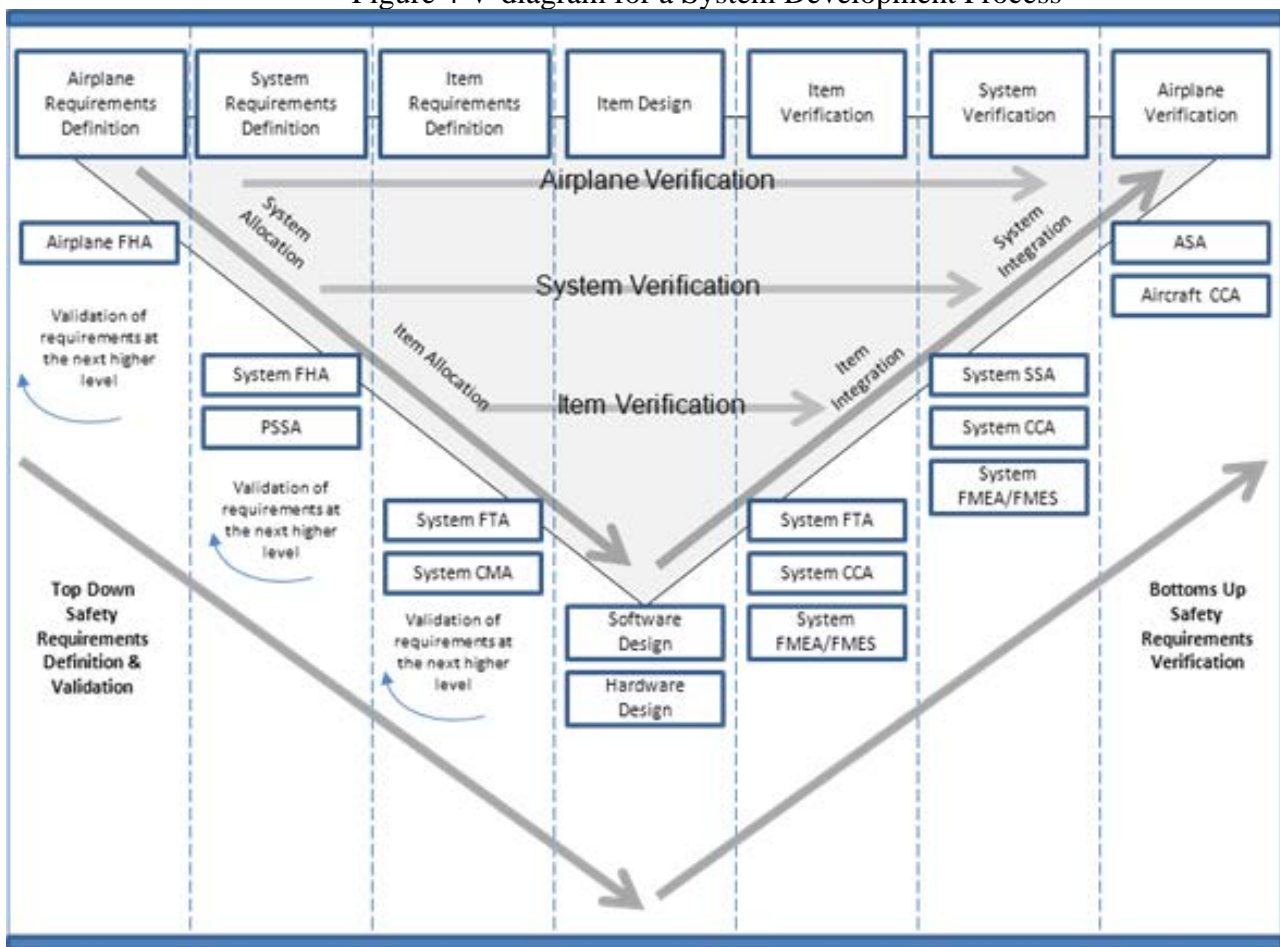
The safety assessment process is divided into two parts; the airplane level safety assessment and the individual system safety assessments. The airplane safety assessment assures the robustness of the overall airplane system design that implements the required airplane functions. The individual system safety assessments assure the system designs meet their safety requirements and support the airplane level safety assessment.

The airplane assessment process begins by identifying the airplane functions and determining which airplane functions are required for continued safe flight and landing. A Functional Hazard Assessment (FHA) is performed on the functions required for safe flight and landing to identify potentially catastrophic and hazardous failure conditions. For each failure condition, the airplane architecture (i.e. systems) which implements the function is identified and the high-level system failure conditions are determined. An engineering assessment is performed to verify system failure conditions are being addressed by the individual systems.

The basic structure of a system development process can be represented by a V-diagram, where time is represented horizontally (left to right) and system hierarchy is represented vertically (Reference Figure 4). Initially (top left), the top-level design requirements (payload, range, passenger capacity, performance, etc) for the aircraft are selected. The airplane requirements are then broken down into airplane-level functions (e.g. control airplane in the air); airplane-level functions to system functions (e.g. control pitch, yaw and roll); system-level functions to systems (e.g. stabilizer system control); systems to subsystems (e.g. MCAS) in a top-down process. Following this system development process, requirements for each part item or piece of equipment are identified with each level providing validation of the level above. Validation is the process of ensuring that the requirements are sufficiently correct and complete. The right side of the V diagram involves a series of bottom-up evaluation activities to ensure the requirements are verified as met at each level in integration of the final product. Verification is the process of ensuring that the final product meets the design requirements. Verification activities may include analysis and testing the individual item of equipment (e.g. flight control computer software) and then progressively integrating the equipment into a complete system and even flight testing for verification of a fully integrated system on the aircraft.

Safety assessments are conducted by the applicant, and its suppliers, and are reviewed and approved by the FAA. The safety assessment process is outlined in AC 25.1309-1A and described in detail in SAE ARP4761. Although the safety assessment process outlined in the AC is not mandatory, the AC documents an established means, but not the only means, for an applicant to show compliance to the regulations. An applicant who chooses not to conduct safety assessments must demonstrate compliance in another way, which would have to be FAA-approved.

Figure 4 V-diagram for a System Development Process



## **H. Certification of the MCAS Implementation and Function:**

### **H.1 Certification Plans:**

#### **H.1.1 Certification Plan Guidance:**

When Boeing submitted its application for the 737 MAX ATC, FAA Order 8110.4C was in effect. Paragraph 2-3(d) of this order stated in part, “All TC applicants are required to submit a certification plan to the FAA and to keep it current throughout the project.” The plan should be submitted early in the project and updated throughout the project.” An NTSB review of this order found that it listed several key items that an applicant should include in its project certification plan. Some of the key items are the following:

- General information including applicant identification, application date, model designation, and so forth.
- A description of the proposed design or design change including sketches and schematics.
- The proposed certification basis including applicable regulation paragraphs and subparagraphs with amendment levels, exemptions, ELOS findings, and special conditions.
- A description of how compliance will be shown (ground test, flight test, analysis, similarity, or other acceptable means of compliance). The description of the means of compliance should be sufficient to determine that all necessary FAA data will be collected, and all findings can be made.
- A list of documentation that will be submitted to show compliance with the applicable certification basis, and how the applicant will ensure that all showings have been made. This can be accomplished using a compliance checklist addressing each section of the regulations applicable to the product.
- A project schedule including major milestones, such as preliminary hazard analysis submittal dates, substantiating data submittal dates, conformity and testing completion dates, and expected date of final certification.
- Identification of all designated manufacturing inspection representatives (DMIR), designated airworthiness representatives (DAR), and organizational designated airworthiness representatives (ODAR) intended for use, their authorized function codes, and their proposed inspection activities.
- For certification, the Certification Plan should list ARs/UMs and propose whether ODA be delegated to make compliance findings on behalf of the FAA.

#### **H.1.2 Certification Plans - MCAS:**

Two Boeing certification plans (CP) address MCAS:

1. CP13471 Flight Controls – Primary, Elevator and Stabilizer Control, and
2. CP13474 Flight Controls – Autoflight (EDFCS/FCC) & Autothrottle.

Boeing was responsible for developing and updating these certification plans, submitting the plans to the BASOO for acceptance<sup>21</sup>, and keeping the plans current throughout the design, development and certification phases of the 737 MAX project. An NTSB review of these two plans was conducted, and the findings are described below.

##### **H.1.2.1 Certification Plan 13471 - Primary, Elevator and Stabilizer Control:**

CP13471, Revision AH, dated February 16, 2017, was reviewed by the NTSB to determine the methods (i.e., design test, analysis, inspection, etc.) and approach Boeing used to demonstrate compliance to the applicable FARs. This version was the last revision before the 737 MAX 8 amended type certificate was issued.

---

<sup>21</sup> The FAA accepts certification plans; it does not approve the plans.

CP13471 detailed the activities necessary for the amended type certification of the flight controls aspects of the 737-8 Elevator and Stabilizer Control System changes. CP13471 indicated that the 737-8 will employ previously FAA-accepted methods of compliance which utilized industry standard analysis methods as well as Boeing standard analysis methods, tools and test procedures. Compliance will be demonstrated through analysis, qualification test, flight test and safety assessment using standard Boeing tools, methods and procedures. Testing to be completed under this certification plan includes Elevator Feel Computer qualification testing and Flight Testing for intended function for any new or modified systems.

The development of the Elevator and Stabilizer Trim Control system certification plan (CP13471), began with Boeing's initial submission of CP13471, labeled "NEW", to the FAA for review in March 2014. On March 29, 2016, Boeing received the FAA's acceptance of CP13471, Revision AA and the FAA indicated to Boeing that the implementation of their proposed certification activities could proceed. According to the delegation section of the plan, as of November 14, 2013, this certification plan was retained by the FAA and they would make a decision of delegation based on review of the certification plan.

According to CP13471, one of the changes to the Stabilizer Trim Control system from the baseline 737-800 (NG) was the incorporation of the MCAS. Implementation of this new function required two new analog discrete signals, generated by the FCCs, to be sent to components within the stabilizer system. One discrete will override the control column cut-out switches located in the First Officer's Column Switching Module in the "pull" direction when MCAS is operating to prevent the stabilizer command from cutting out during the pilot maneuver. The second discrete overrides the flap position input to enable the higher stabilizer trim motor (STM) operating speed with flaps retracted when MCAS is operating.

CP13471 indicated that certification of the MCAS implementation and function will be addressed in certification plan (CP13474), "737-8 Amended Type Certificate – Flight Controls – Autoflight (EDFCS/FCC)."

#### **H.1.2.1.1 Cross Reference to Certification Plans:**

The stabilizer CP contained a section titled "Cross-Referenced Certification Plans" which detailed certification plans associated with this certification plan. As previously indicated, MCAS compliance information was contained in two certification plans; the Stabilizer CP (13471) and the EDFCS CP (13474). A review of the cross-reference section contained within the Stabilizer CP confirmed that it did reference the CP titled "Flight Controls –Autoflight EDFCS/FCC"; it also indicated that the EDFCS CP proposed a means to certify the 737-8 Autoflight Changes and specifically addresses the software changes required to implement revised Yaw Damper gains.

#### **H.1.2.1.2 Functional Hazard Assessment (FHA):**

CP13471, Revision AH, contained a section titled "Functional Hazard Analysis/System Safety Assessment Summary." According to the FHA, methods for assessing Functional Hazards included Pilot Simulation, Desktop Analysis, and Engineering Judgment. A select number of failure conditions will be flown for certification based on their probabilities and airplane level effects on handling qualities. Failures that are extremely improbable or failures that were deemed Minor will not be flown. Complete system descriptions, hazard assessments and system safety analyses are referenced in deliverable #9 (Stabilizer System Safety Assessment). The functional hazard assessment identified and classified, pursuant to the guidance in AC 25.1309-1A, hazards associated with MCAS as noted below<sup>22</sup>:

---

<sup>22</sup> The FHA was included in CP13471 beginning at Rev NEW based on the revision history. There were updates made to the FHA in subsequent revisions and the final System Safety Analysis accurately reflects the FHA classifications.

- Catastrophic:  
No catastrophic hazards were identified for MCAS
- Hazardous:
  1. Uncommanded MCAS function operation until pilot recognition and reaction.
  2. Uncommanded MCAS function operation to maximum authority.
  3. Uncommanded MCAS function operation equivalent to 3 second mistrim.
- Major/Minor:  
No major or minor hazards were identified for MCAS

The NTSB notes that the FHA classification of uncommanded MCAS operation varied depending on whether the airplane was in the normal or operational flight envelope. CP 13471 lists only the most severe of the two, which in the case of the operational flight envelope is “Hazardous”.

#### **H.1.2.1.3 Delegation of Deliverables:**

CP13471 proposed delegation of all Flight Controls Primary & Secondary compliance findings. On April 14, 2015, the FAA approved the delegation of several deliverables; however, they indicated that the deliverable titled “737 Stabilizer System Description and Safety Analysis” (SSA) would be retained by the FAA and will not be proposed for delegation. In November 2016, Boeing submitted the 737 Stabilizer System Description and Safety Analysis (SSA), revision F, to the FAA for acceptance.” In December 2016, the FAA’s response to Boeing was to “accept” the submittal and with notation “delegated SSA approval to ODA.”

Retention and delegation are accomplished with respect to compliance deliverables not to specific functions i.e., MCAS itself would not be delegated to the ODA.

- Consistent with the FAA authorization, the FAA have discretionary authority as to what is reviewed, whether submitted directly to the FAA for review and approval by an applicant or submitted by a designee or ODA recommending approval.
- When delegating at the end of a program, there has been some level of FAA involvement and the delegation confirms that the designee should make the final approval.
- In all cases, delegation is not accomplished by a single individual but follows a structured review process.

#### **H.1.2.1.4 Method of Compliance (MOC):**

CP13471 indicated that a Stabilizer System Safety Analysis (SSA) will show that the Stabilizer System including both the changed and unchanged designs meet the reliability, integrity and safety requirements for the 737-8 airplane. The SSA will include a Failure Modes and Effects Analysis, Functional Hazard Assessment and Fault Tree Analysis.

#### **H.1.2.1.5 Deliverable Matrix:**

CP13471 contained a section titled “Deliverable Matrix” which provides a description of the deliverable<sup>23</sup>, the method of compliance, FAA requirements, and Approver. The NTSB’s review of CP13471 found the deliverable related to MCAS was the 737 Stabilizer System Description and Safety Analysis (SSA). This document provides the complete details of the installation, interfaces, design features, control and operation of the stabilizer control

---

<sup>23</sup> Deliverables are documents to be submitted demonstrating compliance with the applicable requirements.



system. The Stabilizer SSA also contains all top-level failure conditions or safety issues, the failure effect category according to each condition and the appropriate supporting analysis identified during the functional hazard assessment.

#### **H.1.2.2 Certification Plan – Autoflight (EDFCS/FCC) & Autothrottle:**

EDFCS consists of two Flight Control Computers (FCCs), one Mode Control Panel (MCP), and one Integrated Flight Systems Accessory Unit (IFSAU). The EDFCS provides Autopilot, Flight Director, Mach Trim, Speed Trim, Altitude Alert, and Autothrottle functions.

The development of EDFCS certification plan (CP13474) began with Boeing’s initial submission of CP13474, revision “NEW”, to the FAA for review in March 2014. On June 2, 2015, Boeing received the FAA’s acceptance of CP13474, Revision F and the FAA indicated to Boeing that the implementation of their proposed certification activities could proceed. CP13474, revision U, dated February 28, 2017, was reviewed by the NTSB to determine the methods (i.e., design test, analysis, inspection, etc.) and approach Boeing used to demonstrate compliance to the applicable FARs. This version was the last revision before the 737-8 amended type certificate was issued.

A review of CP13474 found that the changes to the EDFCS for the 737-8, as compared to the baseline 737-800, were limited to the Flight Control Computer (FCC) software only. CP13474 indicated that the FCC Operational Program Software (OPS) will be revised to add the MCAS function.

##### **H.1.2.2.1 Cross Reference to Certification Plans:**

The EDFCS CP contained a section titled “Cross-Referenced Certification Plans” which detailed certification plans associated with this certification plan. A review of the cross-reference section contained within CP13474 confirmed that it did reference the CP13471 titled “737-8 Amended Type Certificate – Flight Controls – Primary, Elevator and stabilizer Control; it also indicated that CP13471 proposed a means to certify the 737-8 Elevator and Stabilizer Control system changes, including testing and analysis for the Maneuvering Characteristics Augmentation System (MCAS).

##### **H.1.2.2.2 Compliance Matrix:**

A review of CP13474 found that it contained a compliance matrix for FAA advisory circular (AC) 25.1329 Approval of Flight Guidance Systems. The compliance matrix included a table showing the proposed compliance statement and the deliverables. According to the table, a System Safety Analysis (SSA), will provide an assessment of the EDFCS as part of an integrated system to the extent that such interactions affect the top-level hazards derived from the FHA. An airplane-level assessment of multiple system failure combinations will be address by the single and multiple failure analysis conducted by Airplane Safety Engineering Organization.

The SSA will be performed in accordance with 14 CFR 25.1309 and AC 25.1309-1A. Common mode/cause or cascading failures will be evaluated. The existing EDFCS SSA will be updated and revised as required for the 737-8.

The SSA will provide an assessment of the EDFCS hazards in the summary FHA and all possible failure modes in the EDFCS and its interfacing systems. This assessment will include consideration of interactions with other systems and the effects of failure combinations of sensors and systems on flight crew workload, airplane structural integrity, and occupant safety in accordance with AC 25.1309-1A. The SSA will be validated through analysis, lab test, simulation and flight test as appropriate. The SSA will provide documentation of the validation methods.

### **H.1.2.2.3 Functional Hazard Assessment:**

CP13474 contained a section titled “Functional Hazard Analysis/System Safety Assessment Summary.” According to this FHA, the EDFCS Functional Hazard Assessment for the 737-8 will be based on the FHA for the 737NG as documented in the document titled “Enhanced Digital Flight Control System, Autothrottle, and Yaw Damper Safety Analysis, Model 737-600/700/800/900.” CP13474 indicated that the FHA was to be updated to address any functional hazards associated with the addition of the Maneuvering Characteristics Augmentation System (MCAS), and other system changes.

### **H.1.2.2.4 Software/Airborne Electronic hardware Considerations:**

A review of CP13474 found that it contained a table describing a discussion on the software used in the FCC’s. According to the discussion, the software will be developed by Rockwell Collins in Cedar Rapids, Iowa. Rockwell Collins will create a Plan for Software Aspects of Certification (PSAC) based on the guidance of FAA Advisory Circular 20-115B, RTCA/DO-178B, the RTCA/DO-178B errata in RTCA/DO-248B and FAA Order 8110.49 Change 1. The PSAC will contain the preliminary software change impact analysis and will be available following certification plan approval. It is proposed to have a Rockwell Collins Software OBAR<sup>24</sup> to make the compliance findings

### **H.1.2.2.5 Delegation Discussion:**

CP13474 indicated that approval of the EDFCS System Safety Analysis would be retained by the FAA and would not be proposed to be delegated to the Boeing ODA. The FAA retained approval of the SSA until revision K, submitted in January 2017. At that time, the FAA stamped the revision as “rejected” due to the need to correct some information and simultaneously delegated approval of the SSA once the final edits were complete.

### **H.1.2.2.6 Method of Compliance:**

In the Method of Compliance section of the CP, Boeing proposed that the System Authorized Representative (AR) would review the applicable deliverables in this certification plan to verify the compliance and its proper documentation.

An EDFCS System Safety Analysis will show that the system design meets the reliability, integrity, and safety requirements for the 737-8 airplane. The document will include a Failure Modes and Effects Analysis, Functional Hazard Assessment, and the Fault Tree Analysis to demonstrate compliance to the applicable regulations, FAA AC 25.1309-1A, FAA Issue Paper S-1 and EASA CRI D-09.

The software will be verified by design and process reviews per the standards of DO-178B appropriate to the design assurance level. DO-178B is an FAA approved means of compliance for software per AC20-115B. The software will be developed by Rockwell Collins Inc in Iowa. The Software Accomplishment Summary (SAS) will be a summary of all design development and verification activities defined in the PSAC that provides the data to substantiate that the objectives of RTCA DO-178B for the appropriate design software level have been met. The Systems AR approval/recommend approval is limited to the integration of system requirements/functionality to the software.

---

<sup>24</sup> Outside Boeing Authorized Representative – An individual acting under the authority of the Boeing ODA who is not employed by Boeing. The name has since changed “Outside Boeing Engineering Unit Member”.

### **H.1.2.2.7 Deliverable Matrix:**

CP13474 contained a section titled “Deliverable Matrix” which provides a description of the deliverables, the method of compliance, FAA requirements, and Approver. The NTSB’s review of CP13474 found the deliverables (compliance documents) directly related to MCAS:

- Software Accomplishment Summary:  
The Software Accomplishment Summary for the Flight Control Computer (FCC-730) shows the compliance of the Flight Control Computer software development and verification to the Plan for Software Aspects of Certification for the FCC-730. Delegation of this deliverable was granted via an FAA response on 4/18/2016.
- Final Enhanced Digital Flight Control System Safety Analysis:  
This document presents the system safety assessment for the 737-8 Enhanced Digital Flight Control System.
- Final Enhanced Digital Flight Control System Description Document:  
The Enhanced Digital Flight Control System Description document provides a description of the 737-8 EDFCS, including a description of all EDFCS components, functions, maintenance and ground operations, crew interfaces, and airplane interfaces.

## **H.2 Safety Assessments:**

Safety assessments are a primary means of showing compliance for systems to FAR 25.1309. Safety assessments proceed in a stepwise, data-driven fashion, analogous to the system development process described above. Starting with airplane functions, functional hazard assessments are performed to identify the failure conditions associated with each function. Systems functional hazard analyses are performed for system level functions. Preliminary safety assessments are performed as the system is developed adding more specific design and implementation detail to address specific hazards. The bottom-up verification by safety analysis starts with an analysis of the components of a system to ensure single failures do not result in significant effects. Combinations of failures are logically combined to develop probability of a failure and checked to ensure they are commensurate with the criticality of the failure condition. Thus, the final definition and characterization of a safety-critical system is verified by the result of the analyses conducted during a safety assessment.

As previously stated, certification plans CP13471 & CP13474 each indicated that a system safety analysis (SSA) would be a method of compliance and a deliverable to their respective certification plan. An NTSB review of CP13471, revealed that a Stabilizer SSA will show that the changed and unchanged designs of the Stabilizer System meet the reliability, integrity and safety requirements for the 737-8 airplane. The review also showed that for CP13474, an EDFCS SSA will show that the system design meets the reliability, integrity, and safety requirements for the 737-8 airplane. The SSA documents will include a Failure Modes and Effects Analysis, Functional Hazard Assessment, and the Fault Tree Analysis to demonstrate compliance to the applicable regulations, FAA AC 25.1309-1A, FAA Issue Paper S-1 and EASA CRI D-09. Because the 737 MAX Air Data Inertial Reference System SSA, discussed the Angle-of-Attack (AOA) sensors and its failure modes, the NTSB also performed a review of this SSA. The following sections describe these three SSA’s in greater detail.

## H.2.1 Air Data Inertial Reference System (SSA)

Boeing’s 737 MAX Air Data Inertial Reference System SSA, dated August 12, 2016, Revision New, was a deliverable to Certification Plan CP13486 titled, “737-MAX Air Data Inertial Reference System Certification Plan.” The NTSB performed a review of this SSA and documented information that pertained to Angle-of-Attack (AOA) sensors.

A description of the Air Data Inertial Reference System (ADIRS) was provided in the SSA, it indicated that the Air Data Inertial Reference Unit (ADIRU) consisted of an Air Data Reference partition and an Inertial Reference partition packaged into a single unit. The two partitions are physically separate and operate as separate functions including independent inputs and outputs for each.

The SSA indicated that the function of the Air Data Module (ADM) is to sense the airplane’s pitot and static pressures external to the airplane and convert them to a digital electrical signal. These pressures, in conjunction with the Total Air Temperature (TAT) and the airplane’s AOA are used to calculate the basic air data information. The ADIRU then transmits the data (several parameters including indicated angle of attack), via ARINC 429 busses, to other systems for display to the flight crew, use in flight control functions (including MCAS), and other airplane system functions.

With regards to AOA, the SSA provided a description of the AOA sensor that stated the following; two independent sensors are used to provide AOA data to the air data partition of the ADIRU”. It also indicated that the two vanes are located on each side of the airplane fuselage and measure the airplane AOA relative to the local air mass. The output of the AOA internal electrical transducers (resolvers) is input directly into the ADIRU, which then outputs an indicated AOA signal to other systems.

### NTSB Note:

Each AOA sensor has two resolvers within it, one of which is connected to the associated ADIRU. The other resolver in each AOA sensor is connected to a stall management yaw damper (SMYD) computer.

The SSA indicates that the altitude and airspeed functions within the ADIRU include a correction factor for Static Source Error (SSEC<sup>25</sup>). This is a compensation for pressure errors caused by the airframe aerodynamic effects on the static port which predictably vary with AOA and Mach number.

The SSA contains a section titled “Angle of Attack Failure,” which states: “*The Angle of Attack Vane senses the alpha angle of the airplane. The Static Source Error Correction (SSEC) is calculated as a function of indicated Mach and AOA. Therefore, all parameters which are based on corrected static pressure are impacted if the AOA vane fails. Also, since the AOA vane has only two resolver output circuits, the AOA is also provided as an output to other systems. The following parameters (shown in table 4) will be output as No Computed Data (NCD)*”:

**Table 4 Air Data Parameters dependent on valid AOA**

Altitude	Altitude Rate	Static Air Temperature	Mach
Baro Corrected Altitude	Impact Pressure	True Airspeed	Corrected AOA
Computed Airspeed	Static Pressure (Corrected)	Total Air Temperature	Indicated AOA
Maximum Airspeed (Vmo)			

---

<sup>25</sup> The basic SSEC factor is a polynomial equation using a combination of airplane Mach, AOA and airframe-specific coefficients (“local measurement to aircraft true correction coefficients”) which are established during wind tunnel and flight testing.

The “Angle of Attack Failure” section of the SSA includes only AOA resolver circuit failures (open circuit, high impedance, etc.) that can be detected by the associated computer (ADIRU or SMYD). The SSA does not discuss the category of AOA sensor failures not related to the electrical circuitry that could provide misleading (erroneous) data to the ADIRU (e.g. a frozen or seized vane with limited or no motion, or a bent or broken vane resulting in angular offset). As demonstrated by the Lion Air event, erroneous input from the AOA sensor (resolver 1) affects the calculation of the SSEC and thus all parameters based on the measurement of static pressure (including airspeed and altitude). However, this failure will not result in the parameters (described in table 4) being output as No Computed Data (NCD). Instead, AOA values are transmitted as “valid” to user systems, because the ADIRU does not detect these faults.

The SSA contained a table summarizing the results of a failure analysis by functional group. The results were provided in terms of loss of function (detected failures) and misleading data (undetected failures) for each primary group. For the misleading data rates, the fault trees were reviewed to determine which components of the system could contribute to misleading information. It was determined that the ADIRU, air data module (ADM), pitot probe heat and AOA vane (and heat) have potential undetected failure modes that may result in undetected, and misleading data. An NTSB review of the functional failure rates table found the following information for AOA Sensors (reference table 5); The source of the probability numbers shown in the table were derived from fault trees. As an example, the Misleading AOA data was derived from the “Misleading Air Data from the L & R ADIRU – Airspeed / Altitude” fault tree described within this section of the report.

**Table 5 ADIRS Functional Failure Rates**

ADIRS Functional Group		Loss of function	Misleading Data
Angle of Attack	Left	<1E-3	<1E-5
	Right	<1E-3	<1E-5
	All	<1E-7	<1E-9

The SSA concludes that the ADIRS is a primary sensor on the airplane and it supports many airplane functions. By itself, the ADIRS is not required to satisfy specific functional failure rates for either independent side or as a system. However, as an input to other airplane systems, the ADIRS must provide functional failure rates to allow those systems to satisfy the airplane functional failure rate requirements.

The SSA also contained a section that summarized the functional failure conditions. This section indicated that some airplane display requirements drive the ADIRS requirements. The following failure conditions shown in table 6 are considered as the primary safety events driving the design of the system.

**Table 6 Primary Safety Events**

Misleading attitude data on one primary attitude display	Major
Loss of attitude on both primary attitude displays	Hazardous
Misleading data on both primary attitude displays	Catastrophic
Misleading data on one primary airspeed display	Major
Loss of airspeed data on both primary airspeed displays	Hazardous
Misleading data on both primary airspeed displays	Catastrophic
Misleading data on one primary altitude display	Major
Loss of altitude data on both primary altitude displays	Hazardous
Misleading data on both primary altitude displays	Catastrophic
Loss of heading data on both primary heading displays	Major

The SSA contained a section titled “Fault Tree Documentation” that developed fault trees for the events that were identified as hazardous or catastrophic. An NTSB review of these fault trees was conducted to determine if and how Boeing considered the effects of a single AOA sensor providing a “loss of data” or “misleading data (erroneous data)” to aircraft systems.

The review found that Boeing did consider the effects of a single AOA sensor providing a “loss of data” within a fault tree with the “Top Event” titled “loss of AOA data for both sides”. Or basically, there is a loss of AOA data from both the left and right side ADIRU’s. The fault tree showed that there were two failure conditions contributing to this “Top Event”: 1) Loss of number 1 AOA and 2) Loss of number 2 AOA. For each of these failure conditions, one of the contributing factors was “No AOA output to the ADIRU” which could result from either of the following basic events:

- An AOA Vane failure, or
- Loss of power

The review also found that Boeing considered the effects of a single AOA sensor providing “erroneous data” within the lower branches of a fault tree with the “Top Event” titled “Misleading Air Data from the Left and Right ADIRU – Airspeed / Altitude.” The fault tree showed there were two failure conditions that contributed to this top event:

- Misleading Air Data from the Left ADIRU, and
- Misleading Air Data from the Right ADIRU

The two failures are symmetric, the left is considered here. According to the fault tree, there are four failure conditions that contribute to the “Misleading Air Data from the Left ADIRU” hazard. One of these conditions was titled “Erroneous AOA-L data from the Captain’s side”; the other three were not related to the AOA sensor itself. The fault tree showed the following two ways (or failure conditions) that could lead to “Erroneous AOA-L data from the Captain’s side”.

- *“failure of AOA-L vane / Annunciation”*
- *“incorrect AOA output from the ADIRU-L output.”*

For the *“failure of AOA-R vane / Annunciation”*, the fault tree showed that this event could occur by the combined (ANDed) result of the following two failure conditions:

- “Loss of AOA-L Heat Annunciation”
- “Erroneous AOA-L Sensor”

In 2019, Boeing advised the NTSB of an error in this fault tree in that the above two conditions should not have been combined with an AND gate. In a June 28, 2019 revision to the SSA, “Erroneous AOA-L data from Captain’s side” is revised to show three separate conditions combined with an OR gate, meaning any one by itself could result in erroneous AOA data:

- Erroneous AOA-L Sensor
- Incorrect AOA output from ADIRU-L output
- Loss of Power to AOA-L Heater

In both the original and revised fault tree, the top event “Misleading Air Data from L & R ADIRU – Airspeed/Altitude” showed that it met the requirement to be extremely improbable.

## H.2.2 Stabilizer Trim Control System Safety Analysis (SSA):

Boeing's 737 NG/MAX Stabilizer Trim Control SSA was a deliverable to Certification Plan CP13471 titled, "Flight Controls – Primary, Elevator and Stabilizer Control." The SSA was originally developed to provide a safety analysis showing compliance with the certification agency requirements for the 737-6/7/8/900 (737 NG) family of airplanes. The safety analysis included a description of the Stabilizer Trim Control System, tables for certification and Means of Compliance, a Functional Hazard Assessment (FHA) summary, Failure modes and effects analysis, and fault tree analysis (FTA).

The NTSB performed a review of Revision H, dated November 28, 2017 of this analysis and documented information that pertained to the incorporation of MCAS in the following paragraphs. Revision F of the SSA document, dated September 7, 2016, incorporated a new Appendix G, which contained the safety analysis for the 737 MAX family of airplanes. Appendix G was added to document the safe operation of the 737 MAX stabilizer trim system and to show compliance with certification agency requirements. Included within this Appendix are sections that provide a system description of MCAS, a Functional Hazard Assessment (FHA) summary which identified the severity of potential hazards to the airplane due to the implementation of the 737 MAX stabilizer trim system changes, and fault tree analysis (FTA) documentation showing that for identified top failure scenarios, the probability of occurrence is less than extremely improbable ( $1E-9$ ). Then the summary converse statement can be made that for the 737 MAX stabilizer trim system, the airplane is capable of continued safe flight and landing without requiring exceptional pilot skill or strength, following any combination of failures not extremely improbable.

An NTSB review of Appendix "G" found that the introductory section of SSA had not been updated to reflect the March 2016 MCAS maximum authority changes. The introductory section indicated that MCAS was added on the 737 MAX to address potentially unacceptable nose-up pitching moment at high angles of attack at high airspeeds; there was no mention that MCAS had been revised to improve flaps up, low Mach stall characteristics and identification. Additionally, the functional hazard assessment summary table contained within the Appendix still reflected a pre-March 2016 MCAS maximum authority limit of 0.6 degrees.

However, an NTSB review of Boeing internal documents confirmed that the FHAs had in fact been reassessed each time that the MCAS requirements were changed, including the change in authority limit from 0.6 to 2.5 degrees. In all cases, the reassessment found that the FHA categories had not changed.

In responses to an NTSB request, the FAA provided the following response for how they became aware of the March 2016 changes to MCAS (i.e. improved flaps up, low Mach stall characteristics and identification) and if the group within the BASOO who was responsible for approving the Stabilizer system safety assessment (SSA) were aware of the change. The FAA indicated the following:

In a July 2016 briefing<sup>26</sup>, Boeing provided the FAA with a presentation on stall characteristics and configuration changes. The purpose of this briefing was to discuss company test results prior to entering into certification testing. At this briefing, Boeing discussed some of the physical aerodynamic devices (relocation of stall strip, vortex generators (VG) configurations, etc.) they used to improve the stall characteristics with only limited success. During the briefing Boeing discussed their intent to expand the MCAS function to activate at lower Mach speeds. The actual amount of authority was not defined at that time as Boeing was still conducting testing to tune and validate the system. FAA well understood that greater MCAS authority would likely be necessary to cover the lower speed region. In July 2016, Boeing

---

<sup>26</sup> According to Boeing, their records indicated that the briefing was originally scheduled for May 2016 and documents were provided to the FAA. However, their records indicated that the actual briefing was delayed and did not take place until July 2016.

provided a similar presentation to the FAA with additional company test results. Based on those results, Boeing finalized the MCAS design tables and submitted their revised certification plan in September 2016. Numerous validation meetings were held in the Fall of 2016 (CAAC, TCCA, EASA), supported primarily by FAA flight test and the policy office. In those meetings, the maximum MCAS authority of 2.5 deg in the low speed region was specifically covered. The FAA also indicated that their focus on the SSA's was mainly around other system changes and not MCAS and therefore from a flight controls / system safety perspective their team does not have recollection of specific discussions associated with Boeing regarding the MCAS changes.

### H.2.2.1 Functional Hazard Assessment

The Functional Hazard Assessment section of Appendix “G” summarized the FHA that was performed as part of the 737 MAX Stabilizer Trim Control System Safety Analysis, and addressed each system function and the result of loss of availability or loss of integrity of that function. The analysis considered all phases of flight for both the Normal and Operating flight envelopes<sup>27</sup>, interfacing systems, and established the effect category for each failure condition. Hazard assessments were determined in consideration of the impact to crew workload for the maximum flight time and longest diversion time (where a diversion is required). An NTSB review of the FHA found that it identified and classified, pursuant to the guidance in AC 25.1309-1A, the following six hazards related to MCAS:

**Table 7 Functional Hazard Assessment for MCAS**

Effect Category	Hazard Event	Flight Phase
Hazardous	Uncommanded MCAS function	All (Operating Flight Envelope)
Major <sup>28</sup>	Loss of MCAS Function	All (Operating Flight Envelope)
Major	Uncommanded MCAS function operation to maximum authority (0.6 deg)	All (Normal Flight Envelope)
Major	Uncommanded MCAS function operation equivalent to 3 second mistrim	All (Normal Flight Envelope)
Minor	Loss of MCAS Function	All (Normal Flight Envelope)
Minor	Stabilizer trim runaway with MCAS operation	Cruise (ETOPS)

### H.2.2.2 Fault Tree Analysis:

Appendix “G” contained a section titled “Fault Tree Analysis (FTA)” that presented the fault trees that were developed as part of the Stabilizer Trim Control System safety analysis. According to the analysis, FTA is a tool used to quantitatively determine the numerical probability of a certain combination of events. The failure conditions defined by the FHA provide the basis for the top-level events analyzed by the FTA to demonstrate compliance with 14 CFR 25.671(c)(2), (c)(3), and 25.1309(b)(1).

Boeing indicated that fault tree analyses were only performed on the FHA events that were determined to be either Catastrophic or Hazardous, which is consistent with the guidance in SAE ARP 4761. As described above,

<sup>27</sup> Note the two different flight envelopes designated for MCAS related hazards – “Normal Flight Envelope” and “Operating Flight Envelope”. Operating flight envelope is defined in FAA AC 25-7C Appendix 5. There is a difference between flight phase and flight envelope. Phases would be takeoff, climb, cruise, etc. Envelopes are related to altitude, weight, airspeed, AOA, maneuvering “g” loads, etc.

<sup>28</sup> The “major” classification used by Boeing indicated a remote probability of this hazard occurring and that it could result in reduced control capability, reduced system redundancy, or increased crew workload. Other classification categories include “minor,” “hazardous,” and “catastrophic.”



unintended MCAS activation was shown to be Major in the normal flight envelope and Hazardous in the operational flight envelope. FAA Advisory Circular 25-7C Appendix 5 lists the probability of being outside the normal flight envelope as 1E-3. Therefore, a condition that meets the integrity requirements for a Major within the normal flight envelope also meets the Hazardous integrity requirements for the operational flight envelope.

Therefore, unintended MCAS operational FHA events were not evaluated in the fault tree analysis as they were assessed as Major in the normal flight envelope; Boeing indicated that is consistent with FAA regulations and the Boeing process.

Although the failure conditions (such as a single AOA failure) that could result in an unintended MCAS operation were not evaluated as part of Boeing's Stabilizer System fault tree analysis, an NTSB review of their analysis found that Boeing had modified (updated) their original (737 NG) catastrophic fault trees to account for MCAS engage discrete failures which could contribute to a loss of the control column cutout function.

### **H.2.3 EDFCS Autothrottle, and Yaw Damper System Safety Analysis (SSA):**

Boeing's 737 NG/MAX Enhanced Digital Flight Control System, Autothrottle and Yaw Damper Safety Analysis (SSA) was a deliverable to Certification Plan CP13474. The NTSB performed a review of the EDFCS SSA, Revision M, dated January 24, 2018. The review found that Boeing had added an appendix (Appendix E) to the original SSA to document the information specific to the 737 MAX. Relevant to MCAS, the appendix included the following sections: compliance summary, Summary of system changes, MCAS description, and a fault tree analysis.

According to the "compliance summary" section, the EDFCS changes incorporated in the 737 MAX were evaluated for impact to the baseline safety analysis provided in the main body of the SSA (analysis for the 737-300/400/500/600/700/800/900 airplanes). The "Summary of system changes" section indicated that the EDFCS architecture in the 737 MAX is the same as in the 737 NG and the changes to the system are limited to the software resident in the FCCs. The software changes support the addition of new EDFCS functionality for the 737 MAX, including the Maneuvering Characteristics Augmentation System (MCAS) and other systems. To incorporate MCAS, the following was required: two new MCAS related FCC discrete outputs; modifications to the Column Switching Module and Stabilizer Trim Motor interface wiring.

MCAS would be active during manual flight only and would drive the stabilizer in flaps-up, high angle of attack conditions to improve pitch-up handling characteristics. The FCC software revisions include the following:

- Logic to prioritize and command the stab trim motor for MCAS operations using the active Speed Trim channel.
- Output of MCAS Engage discretely from the FCC in command, to set the high stab trim motor rate and inhibit the column cut-out function of the Column Switching Module in the aft direction.

#### **H.2.3.1 Baseline Analysis – Background:**

According to the SSA, the Digital Flight Control System (DFCS) which provided the autopilot function on 737-300/400/500 and early 737-600/700/800/900 (737NG) airplanes was replaced by an upgraded version developed by a different supplier. This upgraded version, known as the Enhanced Digital Flight Control System (EDFCS), was introduced in 2004 and used in all 737NG airplanes delivered since then as well as all 737MAX airplanes. The primary purpose of the SSA was to document the systems compliance to the safety requirements of 25.671, 25.672, and 25.1309. A Functional Hazard Assessment defines the hazards of interest. The system FMEA

ensures that no single failure will cause a Catastrophic event. The fault trees examine the probability of combinations of faults which could contribute to a hazard in manual flight, autothrottle on, single channel autopilot, and dual channel fail-passive or fail-operational autoland operation.

The general safety analysis process provided in ARP 4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems & Equipment” was used as a general guide in performing the analysis. Each system component or interfacing system was investigated to determine if any failure modes exist which could contribute to one of the functional hazards or cause a loss of fail-passive or fail-operative capability during autoland. Systems such as hydraulic power, electrical power, computers and sensors, and electrical wiring were examined to assure that adequate isolation was provided between redundant systems. System interlocks, monitoring, and warning systems were studied to ensure that these systems would protect against significant failures. Unique functions were also analyzed that could violate the brickwall architectural approach or monitoring independence if improperly implemented or applied (cross-channel communications, equalization, synchronization, initialization processes, localizer averaging, monitor testing and isolation, etc.)

The SSA included a detailed Functional Hazard Assessment, a Failure Modes and Effects Analysis (FMEA) that presented an analysis of failure modes particularly relevant to each system operation, a section that provides the results of simulated and flight test worst case failure evaluations and an assessment of the effects of potential pilot errors related to the operator interface. The system definition, functional hazard assessment, and the failure modes and effects analyses were the sources for the fault tree analyses. The analysis also included fault tree assessments for the top-level events defined by the Functional Hazard Assessment.

### **H.2.3.2 Requirements:**

The SSA contained a table describing the FAA requirements and the method of compliance. One of the requirements was 14 CFR 25.672 “Stability augmentation and automatic and power-operated systems”, which states: 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 §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.
- (b) The design of the stability augmentation system or of any other automatic or power-operated system must permit initial counteraction of failures of the type specified in §25.671(c) without requiring exceptional pilot skill or strength, by either the deactivation of the system, or a failed portion thereof, or by overriding the failure by movement of the flight controls in the normal sense.
- (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.

According to the SSA, Speed Trim, MCAS, Mach Trim and Yaw Damping are augmentation functions covered by Section 25.672. These augmentation functions comply with 25.671 and, following a system failure, can be deactivated or overridden by the pilot without exceptional skill or strength. In addition, the airplane is capable of continued safe flight and landing following any failures not extremely improbable.

A review of functional hazard assessment found that it addressed each system function and the result of loss of function or erroneous operation. The analysis considered phases of flight, flight envelope, interfacing systems, and established effect categories for the failure conditions. According to the SSA, the FHA analysis was reviewed by all affected organizations including: Flight Controls, Aero/S&C, Flight Deck, Pilots, Reliability, Safety, and Structures. Performance analysis or simulation were accomplished as needed to help define the hazards or criticality. Lab and flight test conditions for validation of the assignment of criticality of specific hazards were defined as well. Each FHA event was closed by reference to a specific analysis, design feature, or test condition. However, because MCAS only operates with the autopilot off, one hazard contained within the assessment was relevant. This hazard is: “Autoflight Malfunction at Low Altitude Which Results in Unsafe Flight Path in an A/P OFF, Single Channel, or Fail-Passive Configuration (FHA 1).

According to the fault tree analysis section of Appendix E, the original (Baseline 737 NG) fault trees contained in the EDFCS SSA document were assessed for applicability to the 737 MAX and were modified as needed to account for functional changes specific to the 737 MAX configuration.

With regards to MCAS, the SSA indicated that the inclusion of the new MCAS function creates new failure modes affecting the probability of runaway stabilizer trim which cannot be arrested by the column cutout switches. As previously described, the MCAS function normally activates only during manual flight, and operates by trimming the horizontal stabilizer in the nose-down direction while the airplane is executing a high AOA maneuver. The column cutout switch mechanism normally inhibits automatic nose-down automatic trim in the presence of aft column inputs applied by the flight crew. The MCAS implementation therefore required a new relay that provided a bypass of the column cutout switches when the MCAS Engage discrete is asserted by either FCC. Any erroneous activation of the MCAS Engage output will energize the bypass relay and prevent aft column inputs from interrupting nose-down automatic trim commands.

To account for this hazard<sup>29</sup>, Boeing modified the fault tree for the failure conditions titled “Erroneous Runaway/oscillatory stab output un-arrested by column cutout”. This failure condition was one of eight conditions that contributed to a higher-level failure condition titled “Autopilot Malfunction in the Pitch Axis at Low Altitude.” And, this failure condition is one of four conditions that contributes to the Top-Level event titled “Autoflight malfunction at low altitude which results in an unsafe flight path in an autopilot OFF, single channel or fail passive configuration,” This Top-Level event was identified as a catastrophic hazard as part of Boeing’s EDFCS functional hazard assessment.

An NTSB review of the modifications incorporated into the fault tree titled “Erroneous Runaway/oscillatory stab output un-arrested by column cutout” revealed that the following two failure conditions “AND’ed” together resulted in the hazard.

- Column Trim Cutout Fails to Interrupt Stab Motion
- Undetected stab trim runaway

For the “Column Trim Cutout Fails to Interrupt Stab Motion” hazard, the fault tree identified two potential failure conditions (OR’ed together) that could result in the hazard. One of the failure conditions “FCC-730 produces

---

<sup>29</sup> A failure condition of an erroneous MCAS activation preventing the column cutout mechanism from interrupting (as designed) an uncommanded nose-down automatic stabilizer trim command

undetected erroneous MCAS or Flaps Up/Dn discrete” is where the fault tree begins to address the erroneous activation of the MCAS Engage outputs and is also where Boeing introduced SCD requirement “3.1.1.5.3.1.1-A” which set up upper limit on “The probability of the FCC producing an erroneous flaps up/down discrete output or an erroneous MCAS Engage discrete output without detection.” For this event, the fault tree showed the requirement was satisfied.

Tracing the failure conditions that could lead to the hazard identified by the SCD led to the event titled “*input failures cause FCC to produce an undetectable erroneous MCAS engage discrete*” The probability for this event was <1E-9..”

### **H.3 Single and Multiple Failure Analysis:**

Although the single and multiple failure (S&MF) analysis was not one of the deliverables required by a certification plan, Boeing performed a S&MF analysis to help validate system functional hazard assessments (FHAs), design assurance level (DAL) assertions, and extended operations (ETOPS). For the 737 MAX, their analysis is contained within a document titled “Single and Multiple Failure Accomplishment Summary 737 MAX Program,” revision New, which was released on January 19, 2016. According to Boeing, the S&MF analysis was started internally in 2014.

The intent of this analysis was to provide a structured methodology to analyze failures of key integration components and functions to determine if airplane, flight crew, and occupant impacts are as expected and acceptable. The analysis includes intersystem failures and their cascading effects, flight deck indications, and pilot procedures. It was performed on failures originating in one or more systems with multi-system effects that are not understood without an airplane-level review.

An NTSB review of the S&MF Accomplishment Summary document revealed that the S&MF analysis process was led by a Boeing Systems Engineering team along with design engineers, system subject matter experts (SMEs), systems engineers, Safety, Crew Operations, and pilots. Other representatives also participated as appropriate (e.g., Aerodynamics, authorized representatives, etc.). Until completed, the S&MF analysis process was iterative, and the analysis was updated if significant change affected key systems. Once completed prior to flight test, there was no requirement to redo the S&MF analysis for subsequent design changes

The S&MF analysis consisted of individual cases, each of which may contain one or more failures. Analysis cases were identified by members of the team using S&MF documents from previous programs, airplane architecture descriptions and areas of change, schematics, system safety analyses and other information. The Boeing team defined each S&MF analysis case according to guidance material contained within a Boeing manual titled “Conducting Single and Multiple Failure Analyses.” This guidance was used to help the multi-discipline team to choose the S&MF cases for the MAX program. Some cases were selected based on authorized representative (AR) requirements to show cases were acceptable and for specific conditions based on common cause failures. Some candidate cases were excluded for reasons such as: duplicate and/or mirror-image candidates, worst case candidates would often replace multiple less-severe cases, etc.

The Boeing team considered including “Erroneous AOA from a single source” as a case in the S&MF, but ultimately did not, identifying other multiple failures conditions that presented a more severe hazard to the airplane. These conditions included “Erroneous L&R Air Data” and “Loss of one AOA followed by Erroneous AOA”. These multiple failure cases were rated as catastrophic because they could result in all of the air data on the primary displays being misleading. Uncommanded MCAS was documented as a potential consequence of

erroneous AOA, but was not identified as a factor contributing to the catastrophic rating in any of these. The acceptability rationale for these cases noted that these multiple failure events was beyond extremely improbable. The rationale also noted that while the failure event was catastrophic before flight crew recognition, training would support flight crew recognition and drive appropriate flight crew response to the flight deck effects (which, as noted above, included MCAS activation).

Boeing advised that after the accident, they reviewed how the case of single erroneous AOA would have been categorized if included in the original review. Boeing concluded that had the case of “Erroneous AOA from a single source” been included in the S&MF document, the same assumption about pilot response to uncommanded MCAS as used in the FHAs (which was based on regulatory guidance in AC 25-7C) would have been used, and it is unlikely that any design changes would have resulted from including this case in the S&MF analysis. As noted in section E.1, Boeing did conduct a similar, less formal analysis of the effects of erroneously high AOA on MCAS and concluded that no redesign was needed.

The S&MF Analysis was completed and published in January 2016. In March of that year, the MCAS authority was increased from 0.55 to 2.5 degrees. The NTSB notes that the S&MF analysis had been completed prior to the MCAS design change and was not re-visited as a result of the change<sup>30</sup>.

## **I. Flight Test Guidance for Certification of Transport Category Airplanes:**

FAA advisory circular (AC) 25-7C, titled, “Flight Test Guide for Certification of Transport Category Airplanes,” dated October 16, 2012, provides guidance for the flight test evaluation of transport category airplanes. AC 25-7C includes flight test methods and procedures to show compliance with the regulations contained in subpart B of Title 14, Code of Federal Regulations (14 CFR) part 25, which address airplane performance and handling characteristics. Revision C to AC 25-7, was a complete revision to reduce the number of differences from the European Aviation Safety Agency’s Flight Test Guide, provide acceptable means of compliance for the regulatory changes associated with amendments 107, 109, 113, 115, 119, and 123 to part 25, respond to National Transportation Safety Board recommendations, and to provide a general update to reflect current FAA and industry practices and policies.

### **I.1 Controllability and Maneuverability:**

Section 3, titled “Controllability and Maneuverability” of AC 25-7C provides the following information and guidance for compliance with § 25.143:

The purpose of § 25.143 is to verify that any operational maneuvers conducted within the operational envelope can be accomplished smoothly with average piloting skill and without encountering a stall warning or other characteristics that might interfere with normal maneuvering, or without exceeding any airplane structural limits. Control forces should not be so high that the pilot cannot safely maneuver the airplane. Also, the forces should not be so light that it would take exceptional skill to maneuver the airplane without over-stressing it or losing control. The airplane response to any control input should be predictable to the pilot.

The maximum forces given in the table in § 25.143(d) for pitch and roll control for short term application are applicable to maneuvers in which the control force is only needed for a short period. Where the maneuver is such

---

<sup>30</sup> According to Boeing, because the change in MCAS authority did not change the FHA category of uncommanded MCAS, there was no reason to revisit the S&MF analysis.

that the pilot will need to use one hand to operate other controls (such as during the landing flare or a go-around, or during changes of configuration or power/thrust resulting in a change of control force that needs to be trimmed out) the single-handed maximum control forces will be applicable. In other cases (such as takeoff rotation, or maneuvering during en route flight), the two-handed maximum forces will apply.

Short-term and long-term forces should be interpreted as follows:

- Short-term forces are the initial stabilized control forces that result from maintaining the intended flight path following configuration changes and normal transitions from one flight condition to another, or from regaining control following a failure. It is assumed that the pilot will take immediate action to reduce or eliminate such forces by re-trimming or changing configuration or flight conditions, and consequently short-term forces are not considered to exist for any significant duration. They do not include transient force peaks that may occur during the configuration change, change of flight conditions, or recovery of control following a failure.
- Long-term forces are those control forces that result from normal or failure conditions that cannot readily be trimmed out or eliminated.

Compliance with § 25.143 (a) through (g) is primarily a qualitative determination by the pilot during the course of the flight test program. The control forces required and airplane response should be evaluated during changes from one flight condition to another and during maneuvering flight. The forces required should be appropriate to the flight condition being evaluated. For example, during an approach for landing, the forces should be light and the airplane responsive in order that adjustments in the flight path can be accomplished with a minimum of workload. In cruise flight, forces and airplane response should be such that inadvertent control input does not result in exceeding limits or in undesirable maneuvers. Longitudinal control forces should be evaluated during accelerated flight to ensure a positive stick force with increasing normal acceleration. Forces should be heavy enough at the limit load factor to prevent inadvertent excursions beyond the design limit. Sudden engine failures should be investigated during any flight condition or in any configuration considered critical, if not covered by another section of part 25. Control forces considered excessive should be measured to verify compliance with the maximum control force limits specified in § 25.143(d). Allowance should be made for delays in the initiation of recovery action appropriate to the situation.

## **I.2 Design and Function of Artificial Stall Warning and Identification Systems:**

Chapter 8, titled “Design and Function Of Artificial Stall Warning and Identification Systems” of AC 25-7C provides the following information and guidance for compliance with Sections 25.103, 25.201, 25.203, and 25.207.

The explanation section of this chapter indicates that some airplanes require artificial stall warning systems to compensate for a lack of clearly identifiable natural aerodynamic stall warning to show compliance with the stall warning requirements of § 25.207. A stick shaker is a recommended method of providing such a warning, regardless of whether or not the natural aerodynamic stall warning is clearly identifiable. Similarly, some airplanes require a stall identification device or system (e.g., stick pusher,) to compensate for an inability to meet the stalling definitions of § 25.201 or the stall characteristics requirements of § 25.203. In addition to compliance with the flight test requirements prescribed in paragraph 29 of this AC, certain system design and function criteria should also be addressed during the certification process of these airplanes. Included are system arming and disarming, preflight checks, failure indications and warnings, and system reliability and safety. The reliability of these systems can be evaluated in terms of the probability of the system not operating when required, and the safety aspects in terms of the probability of the system operating inadvertently. The required reliability and safety of stall warning and identification systems should be defined as a function of how critical their respective functioning is to safety of flight.

The “System Reliability and Safety” section of this chapter indicates the following:

When stall warning and/or stall identification systems are installed to show compliance with the stalling requirements of §§ 25.201, 25.203, and 25.207, engineering data should be supplied to satisfy the following criteria, determined in accordance with § 25.1309.

- (1) Reliability. Probability of artificial stall warning and stall identification systems not operating when required:
  - (a) If stall warning is not clearly identifiable by natural characteristics, the loss of artificial stall warning should be improbable (not greater than 1E-5 per flight hour). This reliability requirement is normally met by using dual, independent stall warning systems.
  - (b) If the natural stall characteristics are unacceptable, the combination of failure of the stall identification system to operate and entry into a stall should be extremely improbable (not greater than 1E-9 per flight hour). A stall identification system with a failure rate not greater than 1E-4 per flight hour will satisfy this requirement.
  - (c) If the stall identification system is installed solely for the purposes of identifying the stall, and the stall characteristics would otherwise meet the requirements of Subpart B with the stall identification system disabled, a maximum failure rate of 1E-3 per flight hour will be acceptable.
  
- (2) Safety. Probability of artificial stall warning and stall identification systems operating inadvertently.
  - (a) The probability of inadvertent operation of artificial stall warning systems, during critical phases of flight, should not be greater than 1E-5 per flight hour.
  - (b) To ensure that inadvertent operation of the stall identification system does not jeopardize safe flight, and to maintain crew confidence in the system, it should be shown that:
    - 1 No single failure will result in inadvertent operation of the stall identification system; and
    - 2 The probability of inadvertent operation from all causes is improbable (not greater than 1E-5 per flight hour).
  
  - (f) System Functional Requirements.
    - (1) Operation of the stall identification system should reduce the airplane’s angle-of-attack far enough below the point for its activation that inadvertent return to the stall angle-of-attack is unlikely.
    - (2) The characteristics of stall identification systems, which by design are intended to apply an abrupt nose-down control input (e.g., a stick pusher), should make it unlikely that a flightcrew member will prevent or delay its operation. The required stick force, rate of application, and stick travel will depend on the airplane's stall and stick force characteristics, but a force of 50 to 80 pounds applied virtually instantaneously has previously been accepted as providing this characteristic.
    - (3) Normal operation of the stall identification system should not result in the total normal acceleration of the airplane becoming negative.
    - (4) The longitudinal maneuvering capability of an airplane equipped with stall identification systems, at all speeds likely to be encountered in normal operations, should be substantially the same as would be expected for an airplane with acceptable aerodynamic stall characteristics.

### **I.3 AC 25-7 History:**

On September 26, 1974, FAA Order 8110.8, titled “Engineering Flight Test Guide for Transport Category Airplanes”, was published for FAA internal use to describe acceptable means of compliance with the flight test portions of Part 25 of the Federal Aviation Regulations.

On April 9, 1986, the FAA published advisory circular (AC) 25-7, titled, “Flight Test Guide for Certification of Transport Category Airplanes.” This new AC indicates that it is an update to FAA Order 8110.8 in the areas of performance and flying qualities covered by subpart B--Flight<sup>31</sup> and the material included in this AC would be removed from Order 8110.8. This new Advisory Circular provided guidelines for the flight test evaluation of

---

<sup>31</sup> Reference item 2 of Advisory Circular 25-7, dated April 9, 1986.

transport category airplanes. According to the AC, these guidelines provide an acceptable means of demonstrating compliance with the applicable airworthiness requirements and these methods and procedures have evolved through many years of flight testing of transport category airplanes and, as such, represent current certification practices. Like all AC material, these guidelines are not mandatory and do not constitute regulations. They are derived from previous FAA experience in finding compliance with the airworthiness requirements and represent the methods and procedures found to be acceptable by that experience.

On April 22, 1994, the FAA published a Notice of Proposed Rulemaking (NPRM) 94-15 in the Federal Register (59 FR 19296). In this notice, the FAA proposed amendments to 14 CFR parts 1 and 25 to harmonize certain airworthiness standards for transport category airplanes with the European Joint Aviation Requirements 25 (JAR-25). NPRM 94-15 was developed in response to a petition for rulemaking from the Aerospace Industries Association of America, Inc. (AIA) and the Association Europeenne des Constructeurs de Materiel Aerospatial (AECMA). In their petition, AIA and AECMA requested changes to Section 25.143(c), 25.143(f), 25.149, and 25.201 to standardize certain requirements, concepts, and procedures for certification flight testing and to enhance reciprocity between the FAA and JAA. In addition, the AIA and AECMA recommended changes to FAA Advisory Circular (AC) 25-7, "Flight Test Guide for Certification of Transport Category Airplanes," to ensure that the harmonized standards would be interpreted and applied consistently. The proposals published in NPRM 94-15 were developed by the Aviation Rulemaking Advisory Committee (ARAC) and forwarded to the FAA as an ARAC recommendation. The FAA accepted the recommendation and published NPRM 94-15 for public comment in accordance with the normal rulemaking process.

On June 9, 1995, the FAA published a final rule (*72 Federal Register* Vol. 60, No. 111, Pg. 30743) titled "Revision of Certain Flight Airworthiness Standards to Harmonize with European Airworthiness Standards for Transport Category Airplanes." According to the rule, the FAA is amending part 25 of the Federal Aviation Regulations (FAR) to harmonize certain flight requirements with the European Joint Aviation Requirements 25 (JAR-25). This action responds to a petition from the Aerospace Industries Association of America, Inc. and the Association Europeenne des Constructeurs de Materiel Aerospatial. These changes are intended to benefit the public interest by standardizing certain requirements, concepts, and procedures contained in the airworthiness standards for transport category airplanes. The effective date of the rule is July 10, 1995.

On March 31, 1998, the FAA released AC 25-7A to update the original AC by incorporating the latest policy and guidance material applicable to all sections of part 25. The material related to regulations outside of subpart B supersedes that contained in Order 8110.8, which has been cancelled accordingly upon issuance of this AC (25-7A). Since AC 25-7 was released on April 9, 1986, it has been the primary source of guidance for flight test methods and procedures to show compliance with the regulations contained in subpart B of part 25, which are related to airplane performance and handling characteristics. For certification flight testing to show compliance with other part 25 regulations, Order 8110.8, "Engineering Flight Test Guide for Transport Category Airplanes," provided guidance for internal FAA use in determining acceptable means of compliance. Order 8110.8, as revised on September 26, 1974, has been subject to five "change" updates to reflect significant policy changes; the last change being the removal of the subpart B-related material concurrent with the original release of AC 25-7. Order 8110.8 reflected the policy in place when Amendment 25-29 to part 25 was adopted, and the original release of AC 25-7 reflected an Amendment 25-59 time frame. Part 25 has been amended significantly since the two referenced documents were last revised and, likewise, guidance and policy have changed in many areas as experience has been gained.

On March 29, 2011, the FAA released AC 25-7B to add an acceptable means of compliance for the regulatory changes associated with amendments 108, 109, and 115 to part 25, and a revised means of compliance for



expansion of takeoff and landing data for higher airport elevations. Means of compliance associated with flight in icing conditions was removed as this material is now contained in AC 25-25.

On October 16, 2012, the FAA released AC 25-7C, which is a significant revision to reduce the number of differences from the European Aviation Safety Agency’s Flight Test Guide, provide acceptable means of compliance for the regulatory changes associated with amendments 107, 109, 113, 115, 119, and 123 to part 25, respond to National Transportation Safety Board recommendations, and to provide a general update to reflect current FAA and industry practices and policies.

On May 4, 2018, after certification of the 737 MAX was completed, the FAA released AC 25-7D, to clarify paragraph 23.2.4, Engine Restart Capability—§ 25.903(e); adds paragraph 34.4, Circuit Protective Devices—§ 25.1357; and revises appendix B, Function and Reliability (F&R) Tests, of this AC. This AC has been re-formatted to use a new paragraph numbering system for improved usability. This AC cancels AC 25-7C, *Flight Test Guide for Certification of Transport Category Airplanes*, dated October 16, 2012.

## **J. Oversight and Delegation:**

### **J.1 Inspector General Audit Report:**

According to a 2011 Office of Inspector General audit report<sup>32</sup>, “the FAA is responsible for overseeing numerous aviation activities designed to ensure the safety of the flying public. Recognizing that it is not possible for FAA employees to personally oversee every facet of aviation, public law allows FAA to delegate certain functions, such as approving new aircraft designs, to private individuals or organizations (approved by the FAA). Designees perform a substantial amount of critical work on FAA’s behalf—for example, at one aircraft manufacturer, they made about 90 percent of the regulatory compliance determinations for a new aircraft design. FAA created the Organization Designation Authorization (ODA) program in 2005 to standardize its oversight of organizational designees.”

According to FAA Order 8100.15A, 49 CFR 44702(d) allows the FAA to delegate to a qualified private person a matter related to issuing certificates, or related to the examination, testing, and inspection necessary to issue a certificate on behalf of the FAA Administrator as authorized by statute to issue under 49 CFR 44702(a).

### **J.2 Guidance for Delegation of Compliance Findings:**

FAA Order 8110.4C, section 2.5, titled “Compliance Planning,” discusses the FAA’s involvement in a certification project, including providing guidance on oversight and delegation. According to the order, “For planning purposes, the FAA’s and the applicant’s certification teams need to know in which aspects of the project the FAA intends involvement and at what level. The heavy workloads for FAA personnel limit involvement in certification activities to a small fraction of the whole. FAA type certification team members must review the applicant’s design descriptions and project plans, determine where their attention will derive the most benefit, and coordinate their intentions with the applicant.”

Paragraph (a)(1) of section 2.5 provides guidance to the FAA and applicant on the identification of critical safety items requiring direct FAA involvement in the findings of compliance. According to the paragraph, “When a particular decision or event is critical to the safety of the product or to the determination of compliance, the FAA must be directly involved (as opposed to indirect FAA involvement by, for example, DER). Project team members

---

<sup>32</sup> Reference Office of Inspector General Audit Report, AV-2011-136, issued on June 29, 2011.

must build on their experience to identify critical issues. Some key issues that will always require direct FAA involvement include rulemaking (such as for special conditions), development of issue papers, and compliance findings considered unusual or typically reserved for the FAA. While these items establish the minimum direct FAA involvement, additional critical safety findings must also be identified based on the safety impact or the complexity of the requirement or the method of compliance. Additional factors to consider in determining the areas of direct FAA involvement include the FAA's confidence in the applicant, the applicant's experience, the applicant's internal processes, and confidence in the designees."