National Transportation Safety Board

Washington, DC 20594

Safety Recommendation Report

Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance

Accident Number:	DCA19RA017 / DCA19RA101
Operator:	PT Lion Mentari Airlines / Ethiopian Airlines
Aircraft:	Boeing 737 MAX 8 / Boeing 737 MAX 8
Location:	Java Sea, Indonesia / Ejere, Ethiopia
Date:	October 29, 2018 / March 10, 2019

The National Transportation Safety Board (NTSB) is providing the following information to urge the Federal Aviation Administration (FAA) to take action on the safety recommendations in this report. They are derived from our participation in the ongoing investigations of two fatal accidents under the provisions of Annex 13 of the International Civil Aviation Organization. As the accident investigation authority for the state of design and manufacture of the airplane in these accidents, the NTSB has been examining the US design certification process used to approve the original design of the Maneuvering Characteristics Augmentation System (MCAS) on the Boeing Company (Boeing) 737 MAX. We note that, since the PT Lion Mentari Airlines (Lion Air) accident on October 29, 2018, Boeing has developed an MCAS software update to provide additional layers of protection and is working on updated procedures and training. However, we are concerned that the process used to evaluate the original design needs improvement because that process is still in use to certify current and future aircraft and system designs.

Although the NTSB's work in this area is ongoing, based on preliminary information, we are concerned that the accident pilot responses to the unintended MCAS operation were not consistent with the underlying assumptions about pilot recognition and response that Boeing used, based on FAA guidance, for flight control system functional hazard assessments, including for MCAS, as part of the 737 MAX design.[1] We are making these recommendations to address assumptions about pilot recognition and response to failure conditions used during the design certification process as well as diagnostic tools to improve the prioritization and clarity of failure indications presented to pilots.

[1] (a) We based our preliminary findings on information from the publicly released preliminary accident reports. (b) While Boeing uses the term "uncommanded MCAS function" in its assessment documents, in this report, we are using the term "unintended MCAS operation" as it relates to our review of the accident events.

Factual Information

Accidents

On October 29, 2018, 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 crew had communicated with air traffic control and indicated that they were having flight control and altitude issues before the airplane disappeared from radar. 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.[2]

The airplane's digital flight data recorder (DFDR) recorded a difference between the left and right angle of attack (AOA) sensors that was present during the entire accident flight; the left AOA sensor was indicating about 20° higher than the right AOA sensor. During rotation, the left (captain's) stick shaker activated, and DFDR data showed that the left airspeed and altitude values disagreed with, and were lower than, the corresponding values from the right. The first officer asked a controller to confirm the altitude of the airplane and later also asked the speed as shown on the controller radar display. After the flaps were fully retracted, a 10-second automatic aircraft nose-down (AND) stabilizer trim input occurred. After the automatic AND stabilizer trim input, the flight crew used the stabilizer trim switches (located on the outboard side of each control wheel) and applied aircraft nose-up (ANU) electric trim. According to DFDR data, about 5 seconds after the completion of the pilot trim input, another automatic AND stabilizer trim input occurred. The crew applied ANU electric trim again. DFDR data then showed that the flaps were extended for almost 2 minutes. However, the flaps were then fully retracted, and automatic AND stabilizer trim inputs occurred more than 20 times over the next 6 minutes; the crew countered each input during this time using ANU electric trim. The last few automatic AND stabilizer trim inputs were not fully countered by the crew.

During the preceding Lion Air flight on the accident airplane with a different flight crew, the DFDR recorded the same difference between left and right AOA of about 20° that continued until the end of the recording. During rotation, the left control column stick shaker activated and continued for the entire flight, and DFDR data showed that the left airspeed and altitude values disagreed with, and were lower than, the corresponding values from the right. After the flaps were fully retracted, a 10-second automatic AND stabilizer trim input occurred, and the crew countered the input with an ANU electric trim input. After several automatic AND stabilizer trim inputs that were countered by pilot-commanded ANU electric trim inputs, the crew noticed that the airplane was automatically trimming AND. The captain moved the stabilizer trim cutout (STAB TRIM CUTOUT) switches to CUTOUT.[3] He then moved them back to NORMAL, and the problem almost immediately reappeared. He moved the switches back to CUTOUT. He stated that the crew

[2] Information in this section is taken from the preliminary report on this accident, which can be found at https://reports.aviation-safety.net/2018/20181029-0_B38M_PK-LQP_PRELIMINARY.pdf.

[3] Two STAB TRIM CUTOUT switches on the control stand can be used to stop the flight crew electric and autopilot trim inputs to the stabilizer trim actuator. The switches can be set to NORMAL or CUTOUT. If the switches are 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.

performed three non-normal checklists: Airspeed Unreliable, ALT DISAGREE (altitude disagree), and Runaway Stabilizer. The pilots continued the flight using manual trim until the end of the flight. Upon landing, the captain informed an engineer of IAS DISAGREE (indicated airspeed disagree) and ALT DISAGREE alerts, in addition to FEEL DIFF PRESS (feel differential pressure) light problems on the airplane.

On March 10, 2019, Ethiopian Airlines flight 302, a Boeing 737 MAX 8, Ethiopian registration ET-AVJ, crashed near Ejere, Ethiopia, shortly after takeoff from Addis Ababa Bole International Airport, Ethiopia. The flight was a scheduled international passenger flight from Addis Ababa to Jomo Kenyatta International Airport, Nairobi, Kenya. All 157 passengers and crew on board died, and the airplane was destroyed. The investigation is being led by the Ethiopia Accident Investigation Bureau.[4]

The airplane's DFDR data indicated that shortly after liftoff, the left (captain's) AOA sensor data increased rapidly to 74.5° and was 59.2° higher than the right AOA sensor; the captain's stick shaker activated. Concurrently, the airspeed and altitude values on the left side disagreed with, and were lower than, the corresponding values on the right side; in addition, DFDR data indicated a Master Caution alert. Similar to the Lion Air accident flight, a 9-second automatic AND stabilizer trim input occurred after flaps were retracted and while in manual flight (no autopilot). About 3 seconds after the AND stabilizer motion ended, using the stabilizer trim switches, the captain, who was the pilot flying, partially countered the AND stabilizer input by applying ANU electric trim. About 5 seconds after the completion of pilot trim input, another automatic AND stabilizer trim input occurred. The captain applied ANU electric trim and fully countered the second automatic AND stabilizer input; however, the airplane was not returned to a fully trimmed condition. Cockpit voice recorder data indicated that the flight crew then discussed the STAB TRIM CUTOUT switches, and shortly thereafter DFDR data were consistent with the STAB TRIM CUTOUT switches being moved to CUTOUT.

However, because the airplane remained in a nose-down out-of-trim condition, the crew was required to continue applying nose-up force to the control column to maintain level flight. About 32 seconds before impact, two momentary pilot-commanded electric ANU trim inputs and corresponding stabilizer movement were recorded, consistent with the STAB TRIM CUTOUT switches no longer being in CUTOUT. Five seconds after these short electric trim inputs, another automatic AND stabilizer trim input occurred, and the airplane began pitching nose down.

Design Certification of the 737 MAX 8 and Safety Assessment of the MCAS

The 737 MAX 8 is a derivative of the 737-800 Next Generation (NG) model and is part of the 737 MAX family (737 MAX 7, 8, and 9).[5] 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 NG family. During the preliminary design stage of the 737 MAX, Boeing testing and analysis revealed that the addition of the LEAP-1B engine and associated nacelle

[4] Information in this section is taken from the preliminary report on this accident, which can be found at http://www.ecaa.gov.et/Home/wp-content/uploads/2019/07/Preliminary-Report-B737-800MAX-ET-AVJ.pdf.

[5] The 737-600, -700, and -800 airplanes are part of the 737 NG family.

changes produced an ANU pitching moment when the airplane was operating at high AOA and mid Mach numbers. After studying various options for addressing this issue, Boeing implemented aerodynamic changes as well as a stability augmentation function, MCAS, as an extension of the existing speed trim system to improve aircraft handling characteristics and decrease pitch-up tendency at elevated AOA. As the development of the 737 MAX progressed, the MCAS function was expanded to low Mach numbers.

As originally delivered, the MCAS became active during manual flight (autopilot not engaged) when the flaps were fully retracted and the airplane's AOA value (as measured by either AOA sensor) exceeded a threshold based on Mach number. When activated, the MCAS provided automatic trim commands to move the stabilizer AND. Once the AOA fell below the threshold, the MCAS would move the stabilizer ANU to the original position. At any time, the stabilizer inputs could be stopped or reversed by the pilots using their stabilizer trim switches. If the stabilizer trim switches were used by the pilots and the elevated AOA condition persisted, the MCAS would command another stabilizer AND trim input after 5 seconds.

The FAA's procedures for aircraft type certification require an aircraft manufacturer ("applicant") to demonstrate that its design complies with all applicable FAA regulations and requirements.[6] For transport-category airplanes, as part of this process, applicants must demonstrate through analysis, test, or both that their design meets the applicable requirements under Title 14 *Code of Federal Regulations* (*CFR*) Part 25. Specifically, 14 *CFR* 25.671 and 25.672 define the requirements for control systems in general and stability augmentation and automatic and power-operated systems, respectively. Title 14 *CFR* 25.1322 addresses flight crew alerting and states, in part, that flight crew alerts must

> (1) Provide the flightcrew with the information needed to:
>
> (i) Identify non-normal operation or airplane system conditions, and
>
> (ii) Determine the appropriate actions, if any.
>
> (2) Be readily and easily detectable and intelligible by the flightcrew under all foreseeable operating conditions, including conditions where multiple alerts are provided.

Advisory Circular (AC) 25.1322-1, "Flightcrew Alerting," provides guidance for showing compliance with requirements for the design approval of flight crew alerting functions and indicates that "Appropriate flightcrew corrective actions are normally defined by airplane procedures (for example, in checklists) and are part of a flightcrew training curriculum or considered basic airmanship." Title 14 *CFR* 25.1309 relates to aircraft equipment, systems, and installations, and the primary means of compliance with this section for systems that are critical to safe flight and operations is through safety assessments or through rational analyses; AC 25.1309-1A, "System Design and Analysis," provides guidance for showing compliance with

[6] Title 14 *Code of Federal Regulations* Part 21 defines the procedures for certification.

Title 14 *CFR* 25.1309(b), (c), and (d).[7] AC 25.1309-1A explains the FAA's fail-safe design concept, which "considers the effects of failures and combinations of failures in defining a safe design." As part of demonstrating 737 MAX 8 compliance with the requirements in 14 *CFR* 25.1309, Boeing conducted a number of airplane- and system-level safety assessments, consistent with the guidance provided in AC 25.1309-1A.[8]

The NTSB reviewed sections of Boeing's system safety analysis for stabilizer trim control that pertained to MCAS on the 737 MAX. Boeing's analysis included a summary of the functional hazard assessment findings for the 737 MAX stabilizer trim control system. For the normal flight envelope, Boeing identified and classified two hazards associated with "uncommanded MCAS" activation as "major."[9] One of these hazards, applicable to the MCAS function seen in these accidents, included uncommanded MCAS operation to maximum authority.[10] Boeing indicated that, as part of the functional hazard assessment development, pilot assessments of MCAS-related hazards were conducted in an engineering flight simulator, including the uncommanded MCAS operation (stabilizer runaway) to the MCAS maximum authority.

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 in the stabilizer trim safety assessment report reviewed by the NTSB.

---

[7] Safety assessments are performed by the manufacturer and its suppliers and are reviewed and accepted by the FAA. Safety assessments proceed in a stepwise, data-driven manner to ensure that all significant single-failure conditions have been identified and all combinations of failures that could lead to hazardous or catastrophic airplane-level effects have been considered and appropriately mitigated. When a safety assessment cannot be performed on a new or complex system, a rational analysis may be performed to estimate quantitative probabilities and supplement qualitative analyses and tests. The safety assessment process outlined in AC 25.1309-1A is not mandatory, but manufacturers that do not conduct safety assessments must demonstrate compliance in another manner, such as ground or flight tests.

[8] Safety assessments can include the development of airplane- and system-level functional hazard assessments (to identify and classify potentially hazardous failure conditions), failure modes and effects analyses (a structured bottom-up analysis that evaluates the effects of each possible failure), and fault tree analyses (a structured top-down analysis to identify the conditions, failures, and events that would cause a failure condition).

[9] 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 included "minor," "hazardous," and "catastrophic."

[10] In March 2016, Boeing determined that MCAS should be revised to improve flaps up, low Mach stall characteristics and identification. The preliminary hazard assessments of MCAS were re-evaluated after this change by pilot evaluation in the motion simulator and determined to have not changed the hazard classification.

Boeing indicated to the NTSB that, based on FAA guidance, it used assumptions during its safety assessment of MCAS hazards in the engineering flight simulator. Four of these assumptions were the following:

- 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.[11]
- 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. These assumptions were consistent with requirements in 14 *CFR* 25.671 and 25.672 and guidance in AC 25-7C, "Flight Test Guide for Certification of Transport Category Airplanes."[12] AC 25-7C stated that short-term forces are the initial stabilized control forces that result from maintaining the intended flightpath after 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* [emphasis added]." In a 2019 presentation to the NTSB, Boeing indicated that the MCAS hazard classification of "major" for uncommanded MCAS function in the normal flight envelope was based on the following conclusions:

- Unintended stabilizer trim inputs are readily recognized by movement of the stabilizer trim wheel, flightpath 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 stabilizer trim or stabilizer runaway failure and the procedure for stabilizer runaway would be followed.[13]

---

[11] Title 14 *CFR* 25.672 states the following: "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."

[12] On October 16, 2012, the FAA released AC 25-7C, which revised version B 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 14 *CFR* Part 25; respond to NTSB recommendations; and provide a general update to reflect current FAA and industry practices and policies. AC 25-7C was in effect at the time of Boeing's safety assessments of the 737 MAX. On May 4, 2018, the FAA released AC 25-7D to clarify several paragraphs, revise an appendix, and improve usability with formatting changes.

[13] The runaway stabilizer procedure includes holding the control column firmly, disengaging the autopilot and autothrottles (if engaged), setting the STAB TRIM CUTOUT switches to CUTOUT, and trimming the airplane manually.

Analysis

Assumptions about Pilot Recognition and Response in the Safety Assessment

Functional hazard assessments at the aircraft and systems levels are a critical part of the design certification process because the resulting hazard classifications (severity level) drive the safety requirements for equipment design, flight crew procedures, and training to ensure the hazard effects are sufficiently mitigated. On the basis of Boeing's functional hazard assessment for the MCAS, which assumed timely pilot response to uncommanded MCAS-generated trim input, uncommanded MCAS activation was classified as "major." Boeing was then required to verify that each system that supported MCAS complied with the quantitative and qualitative safety requirements for a "major" hazard, as provided in AC 25.1309-1A, and demonstrate this to the FAA in its aircraft and system safety assessments.

On the Lion Air flight immediately before the accident flight and the Lion Air and Ethiopian Airlines accident flights, the DFDR recorded higher AOA sensor data on the left side than on the right (about 20° higher on the previous Lion Air flight and the Lion Air accident flight and about 59° higher on the Ethiopian Airlines accident flight). As previously stated, the MCAS becomes active when the airplane's AOA exceeds a certain threshold. Thus, these erroneous AOA sensor inputs resulted in the MCAS activating on the accident flights and providing the automatic AND stabilizer trim inputs. The erroneous high AOA sensor input that caused the MCAS activation also caused several other alerts and indications for the flight crews. The stick shaker activated on both accident flights and the previous Lion Air flight. In addition, IAS DISAGREE and ALT DISAGREE alerts occurred on all three flights. Also, the Ethiopian Airlines flight crew received a Master Caution alert. Further, after the flaps were fully retracted, the unintended AND stabilizer inputs required the pilots to apply additional force to the columns to maintain the airplane's climb attitude.

Multiple alerts and indications can increase pilots' workload, and the combination of the alerts and indications did not trigger the accident pilots to immediately perform the runaway stabilizer procedure during the initial automatic AND stabilizer trim input. In all three flights, the pilot responses differed and did not match the assumptions of pilot responses to unintended MCAS operation on which Boeing based its hazard classifications within the safety assessment and that the FAA approved and used to ensure the design safely accommodates failures. Although a number of factors, including system design, training, operation, and the pilots' previous experiences, can affect a human's ability to recognize and take immediate, appropriate corrective actions for failure conditions, industry experts generally recognize that an aircraft system should be designed such that the consequences of any human error are limited.[14] Further, a report on a joint FAA-industry study published in 2002, *Commercial Airplane Certification Process Study: An Evaluation of*

[14] (a) Yeh, Michelle, Cathy Swider, Young Jin Jo, and Colleen Donovan. 2016. *Human Factors Considerations in the Design and Evaluation of Flight Deck Displays and Controls*. Version 2.0, Final Report – December 2016, DOT/FAA/TC-16/56. pp. 248-249. (b) The FAA's *Pilot's Handbook of Aeronautical Knowledge*, FAA-H-8083-25B, Chapter 2, page 2-12, states, "Historically, the term 'pilot error' has been used to describe an accident in which an action or decision made by the pilot was the cause or a contributing factor that led to the accident. This definition also includes the pilot's failure to make a correct decision or take proper action."

Selected Aircraft Certification, Operations, and Maintenance Processes, noted that human performance was still the dominant factor in accidents and highlighted that the industry challenge is to develop airplanes and procedures that are less likely to result in operator error and that are more tolerant of operator errors when they do occur, in particular errors involving incorrect response after a malfunction.[15]

Consistent with this philosophy, the NTSB notes that FAA certification guidance in AC 25.1309-1A that allows manufacturers to assume pilots will respond to failure conditions appropriately is based, in part, upon the applicant showing that the systems, controls, and associated monitoring and warnings are designed to minimize crew errors, which could create additional hazards.[16] While Boeing considered the possibility of uncommanded MCAS operation as part of its functional hazard assessment, it did not evaluate all the potential alerts and indications that could accompany a failure that also resulted in uncommanded MCAS operation. Therefore, neither Boeing's system safety assessment nor its simulator tests evaluated how the combined effect of alerts and indications might impact pilots' recognition of which procedure(s) to prioritize in responding to an unintended MCAS operation caused by an erroneous AOA input.[17] The NTSB is concerned that, if manufacturers assume correct pilot response without comprehensively examining all possible flight deck alerts and indications that may occur for system and component failures that contribute to a given hazard, the hazard classification and resulting system design (including alerts and indications), procedural, and/or training mitigations may not adequately consider and account for the potential for pilots to take actions that are inconsistent with manufacturer assumptions.

Thus, the NTSB concludes that the assumptions that Boeing used in its functional hazard assessment of uncommanded MCAS function for the 737 MAX did not adequately consider and account for the impact that multiple flight deck alerts and indications could have on pilots' responses to the hazard. Therefore, the NTSB recommends that the FAA require that Boeing (1) ensure that system safety assessments for the 737 MAX in which it assumed immediate and appropriate pilot corrective actions in response to uncommanded flight control inputs, from systems such as MCAS, consider the effect of all possible flight deck alerts and indications on pilot recognition and response; and (2) incorporate design enhancements (including flight deck alerts and indications), pilot procedures, and/or training requirements, where needed, to minimize the potential for and safety impact of pilot actions that are inconsistent with manufacturer assumptions.

Further, because FAA guidance allows such assumptions to be made in transport-category airplane certification analyses without providing applicants with clear direction concerning the

---

[15] The industry study team included representatives from manufacturers, airlines, pilot labor organizations, and other aviation stakeholders. See *Commercial Airplane Certification Process Study: An Evaluation of Selected Aircraft Certification, Operations, and Maintenance Processes*. March 2002. The Report of the FAA Associate Administrator for Regulation and Certification's Study on the Commercial Airplane Certification Process.

[16] Title 14 *CFR* 25.1309(c) states, "Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards."

[17] Per Title 14 *CFR* 25.1309(d)(4), compliance demonstration as part of aircraft certification must include analysis that considers the crew warning cues, corrective action required, and the capability of detecting faults.

consideration of multiple flight deck alerts and indications in evaluating pilot recognition and response, the NTSB is concerned that similar assumptions and procedures for their validation may have also been used in the development of flight control system safety assessments for other airplanes. Therefore, the NTSB recommends that the FAA require that for all other US type-certificated transport-category airplanes, manufacturers (1) ensure that system safety assessments for which they assumed immediate and appropriate pilot corrective actions in response to uncommanded flight control inputs consider the effect of all possible flight deck alerts and indications on pilot recognition and response; and (2) incorporate design enhancements (including flight deck alerts and indications), pilot procedures, and/or training requirements, where needed, to minimize the potential for and safety impact of pilot actions that are inconsistent with manufacturer assumptions.

Because the FAA routinely harmonizes related standards and guidance with other international regulators who type certificate transport-category airplanes, the NTSB notes that those airplanes may have been designed using similar standards and therefore may also be impacted by this vulnerability. Therefore, the NTSB also recommends that the FAA notify other international regulators that certify transport-category airplane type designs (for example, the European Union Aviation Safety Agency [EASA], Transport Canada, the National Civil Aviation Agency-Brazil, the Civil Aviation Administration of China, and the Russian Federal Air Transport Agency) of Recommendation A-19-11 and encourage them to evaluate its relevance to their processes and address any changes, if applicable.

As early as 2002, the joint FAA-industry study recognized that, while excellent guidance existed for manufacturers on various topics salient to the development of system safety assessments, there were no methods available to evaluate the probability of human error in the operation of a particular system design and that existing qualitative methods for assessing human error were not "very satisfactory." The 2002 study went on to state that the processes used to determine and validate human responses to failure and methods to include human responses in safety assessments needed to be improved.[18] The NTSB notes that a number of human performance research studies have been conducted in the years since the certification guidance contained in AC 25.1309-1A was put in place (in 1988) and this study was conducted and it is likely that more rigorous, validated methodologies exist today to assess error tolerance with regard to pilot recognition and response to failure conditions. The NTSB also believes that the use of validated methods and tools to assess pilot performance in dealing with failure conditions and emergencies would result in more effective requirements for flight deck interface design, pilot procedures, and training strategies. However, we are concerned that such tools and methods are still not commonplace or required as part of the design certification process for functions such as MCAS on newly certified type designs.

Thus, the NTSB concludes that a standardized methodology and/or tools for manufacturers' use in evaluating and validating assumptions about pilot recognition and response to failure condition(s), particularly those conditions that result in multiple flight deck alerts and

[18] *Commercial Airplane Certification Process Study: An Evaluation of Selected Aircraft Certification, Operations, and Maintenance Processes*. March 2002. The Report of the FAA Associate Administrator for Regulation and Certification's Study on the Commercial Airplane Certification Process.

indications, would help ensure that system designs adequately and consistently minimize the potential for pilot actions that are inconsistent with manufacturer assumptions. Therefore, the NTSB recommends that the FAA develop robust tools and methods, with the input of industry and human factors experts, for use in validating assumptions about pilot recognition and response to safety-significant failure conditions as part of the design certification process. Further, the NTSB recommends that once the tools and methods have been developed as recommended in Recommendation A-19-13, the FAA revise existing FAA regulations and guidance to incorporate their use and documentation as part of the design certification process, including re-examining the validity of pilot recognition and response assumptions permitted in existing FAA guidance.

System Diagnostic Tools

As previously discussed, Title 14 *CFR* 25.1322 addresses flight crew alerting and states, in part, that flight crew alerts must

> (1) Provide the flightcrew with the information needed to:
> (i) Identify non-normal operation or airplane system conditions, and
> (ii) Determine the appropriate actions, if any.
> (2) Be readily and easily detectable and intelligible by the flightcrew under all foreseeable operating conditions, including conditions where multiple alerts are provided.

Multiple alerts and indications in the cockpit can increase pilots' workload and can also make it more difficult to identify which procedure the pilots should conduct. The NTSB notes that the Lion Air and Ethiopian Airlines accident pilots' responses to multiple alerts and indications are similar to the circumstances of a 2009 accident involving Air France flight 447, an Airbus A330, which was traveling from Rio de Janeiro to Paris when it crashed in the Atlantic Ocean.[19] In its accident report, the Bureau d'Enquêtes et d'Analyses Pour la Sécurité de L'aviation Civile (BEA) concluded that failure messages successively displayed on the electronic centralized aircraft monitoring system did not allow the crew to rapidly and effectively diagnose the issue (the blockage of the pitot probes) or make the connection between the messages that appeared and the procedure to use. Accordingly, the BEA recommended that EASA "study the relevance of having a dedicated warning provided to the crew when specific monitoring is triggered, in order to facilitate comprehension of the situation."[20]

Human factors research has identified that, for non-normal conditions, such as those involving a system failure with multiple alerts, where there may be multiple flight crew actions required, providing pilots with understanding as to which actions must take priority is a critical

[19] Bureau d'Enquêtes et d'Analyses Pour la Sécurité de L'aviation Civile. 2012. Final Report, *On the accident on 1st June 2009 to the Airbus A330-203, registered F-GZCP, operated by Air France, flight AF 447, Rio de Janeiro – Paris*.

[20] The response to this recommendation, FRAN-2012-049, was classified as "partially adequate," and the recommendation was closed as of February 2, 2019.

need.[21] This is particularly true in the case of functions implemented across multiple airplane systems because a failure in one system within highly integrated system architectures can present multiple alerts and indications to the flight crew as each interfacing system registers the failure. For example, the erroneous AOA output experienced during the two accident flights resulted in multiple alerts and indications to the flight crews, yet the crews lacked tools to identify the most effective response.[22] Thus, it is important that system interactions and the flight deck interface be designed to help direct pilots to the highest priority action(s).

Research demonstrates that emergency situations increase workload and require additional effort to manage effectively because of the stress involved and the lack of opportunity for pilots to practice these skills compared to those used in normal operations.[23] In addition, research into pilot responses to multiple/simultaneous anomalous situations, along with data from accidents, indicates that multiple competing alerts may exceed available mental resources and narrow attentional focus leading to delayed or inadequately prioritized responses.[24] According to FAA research, "in some airplanes, the complexity and variety of ancillary warnings and alerts associated with major system failures can make it difficult for the flightcrew to discern the primary failure."[25] The researchers noted that better system failure diagnostic tools are needed to resolve this issue.

Thus, the NTSB concludes that aircraft systems that can more clearly and concisely inform pilots of the highest priority actions when multiple flight deck alerts and indications are present would minimize confusion and help pilots respond most effectively. Therefore, the NTSB recommends that the FAA develop design standards, with the input of industry and human factors experts, for aircraft system diagnostic tools that improve the prioritization and clarity of failure indications (direct and indirect) presented to pilots to improve the timeliness and effectiveness of their response. The NTSB further recommends that once the design standards have been developed as recommended in Recommendation A-19-15, the FAA require implementation of system diagnostic tools on transport-category aircraft to improve the timeliness and effectiveness of pilots' response when multiple flight deck alerts and indications are present.

---

[21] See (a) Mumaw, Randall J. 2017. "Analysis of Alerting System Failures in Commercial Aviation Accidents." Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting; and (b) Burian, Barbara K., Immanuel Barshi, and Key Dismukes. 2005. *The Challenge of Aviation Emergency and Abnormal Situations* NASA/TM—2005–213462. NASA Scientific and Technical Information Program Office. Washington, DC.

[22] After the Lion Air accident, on November 7, 2018, the FAA issued emergency Airworthiness Directive 2018-23-51, revising the Boeing 737 MAX Airplane Flight Manual (AFM) to expand the existing runaway stabilizer procedure when erroneous AOA input is detected. This revision provided new details about the effects and indications a pilot might experience due to an erroneous AOA input, such as increasing nose-down control forces resulting from repeated AND stabilizer trim inputs. It also instructed pilots to perform the existing AFM runaway stabilizer procedure, emphasizing that the pilot set the STAB TRIM CUTOUT switches to CUTOUT and that the switches stay in the CUTOUT position for the remainder of the flight.

[23] Burian, Barbara K., Immanuel Barshi, and Key Dismukes. 2005. *The Challenge of Aviation Emergency and Abnormal Situations*. NASA/TM—2005–213462. NASA Scientific and Technical Information Program Office. Washington, DC.

[24] Burian, Barbara K., Immanuel Barshi, and Key Dismukes. 2005. *The Challenge of Aviation Emergency and Abnormal Situations*. NASA/TM—2005–213462. NASA Scientific and Technical Information Program Office. Washington, DC.

[25] Federal Aviation Administration. 1996. *Federal Aviation Administration Human Factors Team Report on: The Interfaces Between Flightcrews and Modern Flight Deck Systems*, June 18, 1996.

Recommendations

To the Federal Aviation Administration

Require that Boeing (1) ensure that system safety assessments for the 737 MAX in which it assumed immediate and appropriate pilot corrective actions in response to uncommanded flight control inputs, from systems such as the Maneuvering Characteristics Augmentation System, consider the effect of all possible flight deck alerts and indications on pilot recognition and response; and (2) incorporate design enhancements (including flight deck alerts and indications), pilot procedures, and/or training requirements, where needed, to minimize the potential for and safety impact of pilot actions that are inconsistent with manufacturer assumptions. (A-19-10)

Require that for all other US type-certificated transport-category airplanes, manufacturers (1) ensure that system safety assessments for which they assumed immediate and appropriate pilot corrective actions in response to uncommanded flight control inputs consider the effect of all possible flight deck alerts and indications on pilot recognition and response; and (2) incorporate design enhancements (including flight deck alerts and indications), pilot procedures, and/or training requirements, where needed, to minimize the potential for and safety impact of pilot actions that are inconsistent with manufacturer assumptions. (A-19-11)

Notify other international regulators that certify transport-category airplane type designs (for example, the European Union Aviation Safety Agency, Transport Canada, the National Civil Aviation Agency-Brazil, the Civil Aviation Administration of China, and the Russian Federal Air Transport Agency) of Recommendation A-19-11 and encourage them to evaluate its relevance to their processes and address any changes, if applicable. (A-19-12)

Develop robust tools and methods, with the input of industry and human factors experts, for use in validating assumptions about pilot recognition and response to safety-significant failure conditions as part of the design certification process. (A-19-13)

Once the tools and methods have been developed as recommended in Recommendation A-19-13, revise existing Federal Aviation Administration (FAA) regulations and guidance to incorporate their use and documentation as part of the design certification process, including re-examining the validity of pilot recognition and response assumptions permitted in existing FAA guidance. (A-19-14)

Develop design standards, with the input of industry and human factors experts, for aircraft system diagnostic tools that improve the prioritization and clarity of failure indications (direct and indirect) presented to pilots to improve the timeliness and effectiveness of their response. (A-19-15)

Once the design standards have been developed as recommended in Recommendation A-19-15, require implementation of system diagnostic tools on transport-category aircraft to improve the timeliness and effectiveness of pilots' response when multiple flight deck alerts and indications are present. (A-19-16)

BY THE NATIONAL TRANSPORTATION SAFETY BOARD

ROBERT L. SUMWALT, III
Chairman

JENNIFER HOMENDY
Member

BRUCE LANDSBERG
Vice Chairman

Report Date: September 19, 2019