

Statement of Michael Stumo

Before the United States Senate Committee on Commerce, Science and Transportation

Examining the Federal Aviation Administration's Oversight of Aircraft Certification June 17, 2020

Thank you Chairman Wicker, Ranking Member Cantwell and the members of the Committee on Commerce, Science and Transportation for holding this hearing and allowing me to submit this written statement.

My name is Michael Stumo and I am the father of Samya Rose Stumo who died on flight ET302 on March 10, 2019. Her 26th birthday will be in less than two weeks. I speak for my family but not for the other ET302 families.

Recent legislation introduced by Senators Wicker and Cantwell improves upon a prior version of the bill. But it is not yet supported by my family or, as many have communicated to me, the other families of Flight ET302. My testimony includes several issues that must be addressed in future improvements to this legislation.

1. The JT610 Crash

A Boeing 737 MAX 8 crashed into the Java Sea on October 29, 2018 killing all 189 passengers. The Lion Air plane was only three months old. The flight JT610 pilots fought with what we now know was the MCAS system for 13 minutes before the crash. An angle of attack (AoA) sensor had previously malfunctioned and been replaced. The replacement sensor again malfunctioned, there was no redundancy in case of failure and thus the MCAS system repeatedly pushed the nose down until it overpowered the pilots and slammed the plane into the sea.

After that crash, the JT610 pilot's mother, Sangeeta Suneja, raised the alarm about the plane and called for simulator training. But few paid attention to her. Many blamed the pilots. Boeing said the MAX 8 "is as safe as any airplane that has ever flown the skies."

It was not. My family and I now know much more than before.

2. The ET302 Crash

On March 10 last year, my daughter Samya was traveling on her first international assignment for her employer. She had recently graduated from the University of Copenhagen School of Public Health and landed her dream job at ThinkWell in January 2019 to help cause patient centered change in the global health field.

Samya flew from Dulles to Addis Ababa. After she arrived, Samya texted us, "Just landed in Addis Ababa - another 2 hours to Nairobi." She boarded a Boeing 737 MAX 8 at around 8:30a local Addis time. She sat in seat 16J, an aisle seat.

Flight ET302 was a daily flight between the two cities, often carrying US diplomats to and from Nairobi. The plane was only four months old.

As flight ET302 took off, something went wrong with the left hand angle of attack (AoA) sensor. There was another AoA sensor on the co-pilots' side. It was working properly but it was not connected to the MCAS system.

The MCAS system wrongly kicked in, repeatedly pushing the nose down soon after takeoff. Captain Sully Sullenberger said:

“the failure of an AOA sensor quickly caused multiple instrument indication anomalies and cockpit warnings. And because in this airplane type the AOA sensors provide information to airspeed and altitude displays, the failure triggered false warnings simultaneously of speed being too low and also of speed being too fast. The too slow warning was a ‘stick-shaker’ rapidly and loudly shaking the pilot’s control wheel. The too fast warning was a ‘clacker’, another loud repetitive noise signaling overspeed. These sudden loud false warnings would have created major distractions and would have made it even harder to quickly analyze the situation and take effective corrective action.”¹

For several minutes, the captain used brute physical force to pull the control yoke back up. He became exhausted and asked for the first officer’s help. During the six minute flight, my daughter was terrified riding this roller coaster. At 8:43 am local time, the plane plowed into the ground, in an Ethiopian farm field, and buried itself dozens of feet below the surface.

The plane and the passengers disintegrated into pieces. Their parts were mixed up with the jet fuel. I was there. My family and I were at the crash site. We saw the wreckage. My wife and son saw body parts exposed to the elements.

3. The Boeing 737 MAX 8 Development and Concealment

The MAX is an Obama era plane that was certified to fly in March 2017, the third month of the Trump administration.

It is a deadly aircraft with ill-fitting engines bolted onto a 50 year old aircraft design. Rather than physically fixing the aerodynamic design of the aircraft, Boeing took the cheap route. It used glitchy software that relied upon input from a single sensor to push the nose of the plane towards the ground in certain conditions.

Even today, the FAA still has not resolved the issue of whether MCAS exists to make the MAX handle like prior planes or to resolve aerodynamic instability. Until FAA can answer that question, the MAX should not fly again. It may be that the aircraft is so flawed that physical changes, rather than software fixes, are required.

¹ Attachment 3: Testimony of Sully Sullenberger, US House of Representatives, Committee on Transportation and Infrastructure, June 19, 2019 (attached)

Boeing hid MCAS for many years. In June 2013 the company first devised a plan to conceal MCAS from the public and to minimize its existence for the FAA. It was described as merely “an addition to [the existing] speed trim [system]”.²

In 2016, Boeing drastically strengthened MCAS’ ability to push the MAX’s nose down. It never informed the FAA or anyone else of this change. Neither Boeing nor FAA performed a safety assessment which was necessary for critical safety systems. In May 2019, then-Acting FAA Administrator Dan Elwell admitted that Boeing and the FAA failed to designate MCAS as a safety critical system.³

The MCAS violated Boeing’s internal requirements requiring that the systems should “not interfere with dive recovery” and “not have any objectionable interaction with the piloting of the airplane.”⁴

The effort to hide MCAS continued throughout 2016 as the FAA allowed Boeing to remove references to MCAS from Boeing’s Flight Crew Operations Manual.⁵ The company wanted to avoid simulator training. In November 2016, Boeing chief technical pilot Mark Forkner wrote to a colleague that he was “jedi-mind tricking regulators into accepting” lesser pilot training.

One Boeing employee rejoiced when the FAA said there should only be computer-based training, without a simulator. “You can be away from an NG for 30 years and still be able to jump into a MAX? LOVE IT!!... This is a big part of the operating cost structure in our marketing decks.”

In 2017, a Boeing employee wrote, about the MAX, “This airplane is designed by clowns, who are in turn supervised by monkeys.” In 2018, another employee wrote “I still haven’t been forgiven by God for the covering up I did last year.”

The FAA’s years long drive to delegate everything and relegate staff to paper pushers and presentation watchers resulted in Boeing employees mocking them as “dogs watching TV.” The FAA remains happy to be sidelined, rather than have direct involvement in certification.

4. Between the Crashes: What were they doing?

After the Lion Air crash, FAA knew that MCAS was a problem, but failed to ground the plane. They blamed the pilots for not winning the fight with the then-secret MCAS system.

One can argue whether the FAA and Boeing should have known about the aerodynamics issues, the AoA sensor and MCAS’s catastrophic risks before JT610. But after JT610, there is no excuse.

² “The Boeing 737 MAX Aircraft: Costs, Consequences, and Lessons from its Design, Development and Certification,” The House Committee on Transportation & Infrastructure, p7, March 2020.

³ Id.

⁴ Id.

⁵ Id.

On December 3, 2018, the FAA's internal risk assessment projected that there would be at least 15 more MAX crashes without a fix.⁶ The agency did not require Boeing to fix the problem but instead issued an Airworthiness Directive that still did not disclose the MCAS. Rather it reiterated the procedure for handling runaway trim, which Captain Sullenberger said was very different. American Airlines pilots, in a meeting with Boeing, complained that the company hid MCAS from them.

But secretly the FAA asked Boeing for a software fix within 10 months. My daughter died in the ET302 crash before the 10 months were up. They gambled with her life, and we lost. As did 156 others on the plane.

Even in December 2018, Boeing was falsely reassuring the FAA that pilots could handle MCAS failures. In a slide deck obtained by the House Transportation and Infrastructure Committee, Boeing told FAA that:

- repeated MCAS activation were readily recognizable and able to be counteracted;
- the action to counter the failure should not require exceptional piloting skill or strength;
- the pilot will take immediate action to counter; and
- trained flight crew memory procedures shall be followed.

(See attached Boeing slide deck from December 18, 2018, page 11).

There was no evidence that pilots could react immediately. In fact, Boeing own analysis revealed that if pilots took more than 10 seconds to react, the result would be catastrophic.⁷

5. FAA Resistance and Denial Continues

To this day, the FAA has not admitted any mistakes. Instead, it strategically shifts the focus to its US-centric history of no recent crashes despite the international reach of America's aviation system. My family hoped that new Administrator Steve Dickson would show leadership and clean up the agency. But he has not. No new management team has been chosen. Nobody who made mistakes has been disciplined. Transparency is proclaimed in words but not by deeds.

Administrator Dickson, Deputy Administrator Dan Elwell and others promised that families would receive answers to our questions and be informed of the agency's actions as it determines whether and when to unground the MAX. We received no documents when we asked for them.

We were then told to submit a Freedom of Information Act (FOIA) request. We did so on October 28 2019. But the FAA has still refused to provide us with any documents in response to that request.

A passenger advocacy group, Flyers Rights, requested information, pursuant to FOIA, about the data and analysis surrounding whether and when to return the MAX to service. FAA refused to provide the information. Flyers Rights went to court seeking an order requiring the FAA to

⁶ Attachment 4: Boeing slides prepared for FAA, December 18, 2020, obtained and publicly disclosed by US House of Representatives, Committee on Transportation and Infrastructure.

⁷ The Boeing 737 MAX Aircraft, supra at 9.

provide the information. The FAA has used every legal tool in its arsenal to prevent disclosure of the documents requested.

On August 1, 2019, my wife Nadia and son Tor met with FAA Safety Director Ali Bahrami who previously worked for an aviation industry lobby group. He was a substantial part of the FAA's "blame the pilots and leave Boeing alone" approach. Bahrami never admitted to my family that the FAA made a mistake by not classifying the MCAS as a critical safety system. When my son asked if there was anything he would do differently, he said "no, they did everything right."

Having been denied information and assistance from the FAA, we searched for answers on our own. We learned from Boeing engineers that the change from Designated Engineering Representative (DER) to Organization Designation Authorization (ODA) was a clever and opaque bureaucratic alphabet soup method to hamstring the safety culture at Boeing.

Under DER, the FAA appointed, supervised and removed the Boeing engineers that were designated with certification authority. Boeing paid the engineers, but the DER reported both to FAA and Boeing. That dual chain of command prevented the profit and timeline pressures of Boeing managers from overruling safety concerns.

That safety culture changed when FAA changed to ODA and Boeing was designated as an organization with certification authority. The Boeing engineers, now called ARs, were isolated from their FAA counterparts, reporting only to Boeing managers. Boeing engineers with safety concerns could be shut down and reassigned if company profit or timeline goals were threatened.

While it is easy to lose the thread among the acronyms, this organizational culture and chain of command dynamic must be grasped and fixed. Boeing engineers told me that the DER system resisted undue influence while the ODA system invited undue influence.

The Joint Authority Technical Review, composed of international aviation agency experts, found that "there are signs of undue pressure on [Boeing engineers] performing delegated functions".⁸ Congress needs to re-establish the direct communication between FAA and Boeing engineers at the ground level. FAA also needs to be able to appoint, supervise and remove those Boeing engineers so they cannot be subject to undue influence from Boeing managers to compromise safety.

The Joint Authorities Technical Review report also found dozens of faults with FAA's certification process. It found, for example, that the FAA's Boeing Aviation Safety Oversight Office (BASOO) office is simply not equipped with the quantity and quality of personnel that can oversee Boeing. FAA has not responded to that report.

The FAA will continue delegating to Boeing unless Congress stops it from doing so.

In March 2017, the FAA released a report called "[A Blueprint for AIR Transformation](#)". Dorenda Baker, Executive Director of the Aircraft Certification Service, signed the document.

⁸ "Joint Authorities Technical Review (JATR), "Boeing 737 MAX Flight Control System: Observations, Findings, and Recommendations," pg 28, October 11, 2019.

The AIR Transformation report is a blizzard of management consulting words conveying aspirations towards communications with stakeholders, innovation and strategic vision. But the core of that report was intended to continue getting FAA out of the business of direct involvement in critical paths of the certification process. Three unions - PASS, NATCA and AFSCME - wrote a dissenting report showing how the FAA's paper-pushing, management consulting approach compromises the safety of aircraft passengers.⁹

The FAA's core vision is apparently to push paper and watch power point presentations compiled by Boeing. The public expects FAA to engage in direct involvement, acting as the check on an aircraft manufacturer's urge to cut corners to save a buck.

The FAA currently shows no intention of freeing itself from capture and directly engaging in certification functions rather than merely pushing paper. A recent Special Committee report of hand-picked industry insiders issued a January 16, 2020 document that copied and pasted past FAA talking points about delegation and its long and safe history.¹⁰ Unsurprisingly, FAA agreed saying that "the delegation system allows U.S. industry and innovation to thrive".¹¹ Nobody - except FAA and its handpicked insider committee - believes that this version of delegation is fine. Congress must be very specific in demanding more direct involvement by FAA in the certification process because FAA will not otherwise do it.

The October 2019 JATR report, appointed by FAA, found dozens of problems with FAA's delegation process and the certification of the MAX. FAA has not responded to the JATR report, apparently choosing only to respond to more friendly reports.

I have also been told by inside whistleblowers that Boeing did not engage in safety assessments of critical systems beyond MCAS in the MAX. Safety assessment is an analysis of the identified hazards for a system and demonstrates compliance with airworthiness regulations. Congress should require FAA to disclose the safety assessments for all critical systems in the MAX before it is allowed to fly again.

6. Legislation needed

ET302 victims families were very disappointed at the lack of substance in the first draft of legislation filed in the Senate this month. The second draft filed recently is improved in that it obligates FAA to appoint, remove and communicate with Boeing engineers performing certification work. It also protects whistleblowers throughout the supply chain.

While the recent legislation filed by the Chairman and Ranking Member improves on a prior version of the bill, this second draft is not yet supported by my family. We believe that other

⁹ "Aircraft Certification 'Transformation' Pre-Decisional Involvement Report, Union Recommendations and Dissenting Opinion, February 6, 2017.

¹⁰ "Official Report of the Special Committee to review the Federal Aviation Administration's Aircraft Certification Process," Chaired by Lee Moak and Darren W. McDew, January 16, 2020.

¹¹ "Response to Official Report of the Special Committee on the Federal Aviation Administration's Aircraft Certification Process," Federal Aviation Administration, April 2020.

ET302 families also oppose it without many more improvements. The legislation must also include:

1. Rebalance of delegation. It is absolutely critical that excessive delegation is fixed. FAA must not be allowed to slump further into paper-pusher status, distant from Boeing engineering and the plant production floor.

FAA must retain direct involvement in critical safety systems - as well as novel and new systems - and not delegate its functions to Boeing. Critical safety systems are those deemed major, hazardous or catastrophic. FAA must verify that the fault tree analysis and other analysis are performed to guarantee redundancies and fail safes to prevent failure. New and novel systems are, like MCAS, those not included on aircraft and not fully tested in the past.

2. Lifetime limit for type certificates. The Boeing board, including current CEO David Calhoun, rejected the option to develop a new aircraft to compete with Airbus, opting to amend the old 737 model. They did so to cut corners, save money, extract profit from legacy product, and avoid many current FAA safety rules. The original 737 was certified in 1967. Fifty three years later, it is clear that it should no longer have modern engines and software bolted on to its old fuselage. Boeing should have chosen innovation rather than profitable but unsafe stagnation. A lifetime limit on type certificates should be mandated, and no more future aircraft designs should be based on the 737.

3. FAA certification should not equal immunity for Boeing. Boeing management may bow their heads and express sorrow for the crash. But in private they are doing everything possible to prevent families from holding Boeing accountable. Boeing is asserting, in court, that the fact of FAA certification pre-empts families from making claims for the loss of our loved ones. Boeing's conduct should not be awarded with immunity. This bill should make clear that FAA certification is the bare minimum that manufacturers like Boeing should meet. While I hope no family has to experience the loss of a loved one in a plane crash, legislation should preserve the right to hold all responsible parties accountable.

4. End the secrecy. The National Transportation Safety Board (NTSB) and the FAA have invoked every possible law to prevent families, Congress and the public from receiving information about the causes of the crash and the future ungrounding analysis. The NTSB has prevented the release of many documents held by Boeing. The FAA has refused to comply with families FOIA requests citing expansive caselaw protecting company claims of confidentiality despite the public safety concerns. The result is zero production of documents to the public. This Committee should substantially narrow the scope of legal provisions that hide documents, data and analysis relating to a crash from the public.

5. Penalties must apply or new law does not matter: Boeing has paid civil penalties in the past, but that has not stopped the company from misleading the FAA, pilots and the public. The company pays the penalty from general funds and goes about generating more profit. Criminal penalties with the threat of jail time have the needed deterrent effect for individuals who must then invoke their personal morality rather than company goals.

6. Implement the JATR recommendations. The FAA refused to respond to the Joint Authorities Technical Review report which it commissioned. The international participants in the report were not cozy industry insiders and therefore produced a solid set of findings and recommendations. FAA can congratulate itself for safety. But the public does not trust it and foreign aviation agencies are not deferring to it any longer. This committee's bill should require the FAA to implement the recommendations in the JATR report.

Thank you.

Attachments

1. FOIA letter, Michael Stumo and Nadia Milleron to FAA, October 28, 2019 (pg 10).
2. Joint Authorities Technical Review report, October 11, 2019 (pp 11-81).
3. Testimony of Sully Sullenberger, US House of Representatives, Committee on Transportation and Infrastructure, June 19, 2019 (pp 82-86).
4. Boeing slides prepared for FAA, December 18, 2019, obtained and publicly disclosed by US House of Representatives, Committee on Transportation and Infrastructure (pp 89-131).
5. FAA Quantitative Risk Assessment, December 3, 2018, obtained and publicly disclosed by US House of Representatives, Committee on Transportation and Infrastructure (pg 132).
6. Letter from Mattieu Willm, a French aeronautical engineer who lost his sister, Clemence-Isaure Boutan-Willm in the ET302 crash, dated June 15, 2020 (pp 133-135).

October 28, 2019

FOIA Coordinator
Federal Aviation Administration
National FOIA Staff (AFN-400)
800 Independence Avenue, SW
Washington, DC 20591

Re: Freedom of Information Act Expedited Request

Dear FOIA Officer:

This is an expedited request under the Freedom of Information Act. We hereby request copies of the following records:

1. Any and all documentation Boeing has submitted to the FAA in the last three months for the Boeing 737 MAX return to service, including but not limited to the final software load and the complete system description.
2. Any and all documents showing changes to the Boeing 737 MAX, including but not limited to its Maneuvering Characteristics Augmentation Software (MCAS), that were requested by the FAA or the Technical Advisory Board since March 10, 2019.
3. Any and all documents showing the Transport Airplane Risk Assessment Methodology (TARAM) process conducted by FAA and/or related parties following the Lion Air JT610 crash on October 29, 2018.

We were told by Administrator Steve Dickson that FAA would be fully forthcoming and transparent to the families of the ET302 crash. We were later told that our requests must be in the form of a FOIA request. This is that request.

We request that this information be delivered on an expedited basis well before the Boeing 737 MAX is returned to service. There is an imminent threat to the lives and physical safety of the flying public regarding the potential return to service of this aircraft which has already killed 346 persons.

It may be delivered via email to michaelstumo@gmail.com. We can pick it up at the FAA headquarters in Washington. Our mailing address is 615 Boardman St, Sheffield MA 01257. Michael Stumo's telephone number is 413.717.0184.

We ask for a waiver of fees because we are requesting this information on behalf of ET302 crash victims' families for personal, public safety and not for profit use. The disclosure of this information will contribute to the understanding of the public at large and the public understanding of the federal government operations will be significant as the media attention and scrutiny of the 737 MAX has been significant, and public confidence must be restored. We will pay up to \$750 if required to do so. If the required fees will exceed \$750, please notify us immediately by telephone.

Thank you.



Michael Stumo and Nadia Milleron
(parents of ET302 victim Samya Rose Stumo)

cc: Steve Dickson, Dan Elwell, Michael O'Donnell

Boeing 737 MAX Flight Control System



Observations, Findings, and Recommendations

Submitted to the Associate Administrator for Aviation Safety,
U.S. Federal Aviation Administration

October 11, 2019

Page intentionally left blank

HART SOLUTIONS LLC

HELPING YOU DO IT BETTER
CHRIS@HARTSOLUTIONSLLC.COM

October 11, 2019

Mr. Ali Bahrami
Associate Administrator for Aviation Safety
Federal Aviation Administration
800 Independence Avenue SW
Washington, DC 20591

Dear Mr. Bahrami,

On June 1, 2019, you chartered the Boeing 737 MAX Flight Control System Joint Authorities Technical Review (JATR), consisting of technical representatives from the FAA, National Aeronautics and Space Administration (NASA), and civil aviation authorities from Australia, Brazil, Canada, China, Europe, Indonesia, Japan, Singapore, and the United Arab Emirates. The members of the JATR team wish to thank you for the opportunity to conduct this review and to share our observations and findings. You also invited JATR members to submit recommendations whether or not they represented a consensus. Per your guidance, a compilation of those recommendations from JATR members is attached. It has been a privilege for us to work collaboratively on this multi-national team.

In addition, our review of work conducted during the certification process would not have been possible without the notable support of a number of FAA aircraft certification, evaluation, and oversight personnel. Last but not least, we would like to thank Boeing for its cooperation in our review, including diverting people and other resources from their intense effort to return the airplane to service in order to respond to many of the issues that the JATR team raised.

Overview. The FAA's aircraft certification process has played a major role in producing airliners with an exemplary safety record consisting of a five-year worldwide average of only one fatal airliner crash for every 2 ½ to 3 million flights, and a U.S. record of only one airline passenger fatality in more than 10 years. Nonetheless, as with any system that is designed and operated by humans, the certification process can never be perfect, and the two tragic crashes that resulted in the creation of the JATR reveal a critical need to review the process to determine whether improvement and modernization are warranted.

After extensive effort, the JATR members have made many recommendations regarding modernization and improvement of the certification process. Some of the recommendations are very broad in their application and others are more specific.

Broad Recommendations. Some of the broader recommendations derive from the increasing complexity of aircraft systems, particularly automated systems and the interaction and the interrelationship between systems. As aircraft systems become more complex, ensuring that the certification process adequately addresses potential operational and safety ramifications for the entire aircraft that may be caused by the failure or inappropriate operation of any system on the aircraft becomes not only far more important, but also far more difficult.

Other broader recommendations raise the foundational issue of whether a process that has historically served the industry well for decades based largely upon compliance needs to be revisited to address not only compliance but also safety. As systems become more complex and may interact in unforeseeable ways, the likelihood increases that regulations and standards will not address every conceivable scenario. To the extent they do not address every scenario, compliance with every applicable regulation and standard does not necessarily ensure safety. Moreover, as systems become more complex, the certification process should ensure that aircraft incorporate fail-safe design principles. These principles prioritize the elimination or mitigation of hazards through design, minimizing reliance on pilot action as primary means of risk mitigation.

Specific Recommendations. The specific recommendations include reviewing whether the ODA process can be made less cumbersome and bureaucratic to avoid stifling needed communications. The recommendations do not address the desirability of the ODA concept in general, but they do recommend examining how to help ensure adequate communications in future certification processes about important characteristics of what is being certificated.


Query, for example, whether inadequate communications were partly responsible for the failure to address potential unintended consequences from the evolution of MCAS from a relatively benign system to a much more aggressive system; and query whether inadequate communications played a role in the failure to address potential unintended consequences that can result from designing software for one scenario – in this case, high-speed windup turns – and then modifying the software for a different scenario – in this case reducing the pitch-up tendency at higher angles of attack at low speeds.

Other specific recommendations relate to revisiting the FAA's standards regarding the time needed by pilots to identify and respond to problems that arise. Although existing standards have served the industry well for decades, the JATR members recommend an examination of whether those standards are as appropriate for the complex integrated systems in today's airplanes. For example, when the failure or inappropriate operation of a system results in cascading failures and multiple alarms, query how adequately the certification process considers the impact of multiple alarms, along with possible startle effect, on the ability of pilots to respond appropriately. Inherent in this issue is the adequacy of training to help pilots be able to respond effectively to failures that they may never have encountered before, not even in training.

Post-Certification. The initial scope of the JATR process was limited to the certification process itself, but the charter enabled the co-chairs, in their discretion, to expand the scope if warranted. Hence, some of the recommendations pertain to post-certification activities because of their potential to help improve the safety of future certification processes.

Conclusion. The JATR members look forward to the FAA's actions in response to these recommendations, and we hope they will help improve the certification process in ways that will continue to improve safety.

Respectfully on behalf of the JATR Team,


Christopher A. Hart, Team Chair

Contents

Executive Summary	I
Background	I
Summary of JATR Team Members' Recommendations	III
The Certification Process	III
Integrated Approach to Development and Certification	VIII
Impact of Design Changes on Operations and Training	XI
Post-Certification Activities.....	XIII
JATR Team Observations and Findings; Member Recommendations	1
Terminology.....	1
Acronyms	1
FAA Guidance, Directives, and Regulations	3
Observations, Findings, and Recommendations.....	5
The Certification Process	6
Integrated Approach to Development and Certification	30
Impact of Design Changes on Operations and Training	43
Post-Certification Activities.....	49

Page intentionally left blank

Executive Summary

Background

In March 2017, the Federal Aviation Administration (FAA) issued an amended type certificate to The Boeing Company (Boeing) for the Boeing 737-8 MAX (B737-8 MAX), which was based on the type certificate for the Boeing 737 Next Generation (B737 NG).¹ In February 2018, the FAA approved the Boeing 737-9 MAX (B737-9 MAX). The B737-8 MAX and B737-9 MAX are hereinafter collectively referred to as the B737 MAX.

The B737 MAX incorporated a number of design changes from the B737 NG. These changes included, but were not limited to, the incorporation of CFM LEAP-1B Series turbofan engines, structural changes to accommodate the new engines, advanced technology winglets, aft body aerodynamic improvements, fly-by-wire spoilers, and a Maneuvering Characteristics Augmentation System (MCAS) function. Collectively, the changes incorporated into the B737 MAX design resulted in increased fuel efficiency, increased range, and a reduced noise profile compared to its predecessor, the B737 NG.

On October 29, 2018, Lion AIR Flight JT610 (JT610), a B737-8 MAX, crashed shortly after takeoff in Jakarta, Indonesia. On November 7, 2018, the FAA issued Emergency Airworthiness Directive (AD) 2018-23-51 to require revising certificate limitations and operating procedures of the Airplane Flight Manual (AFM) for the B737 MAX to provide the flight crew with runaway horizontal stabilizer trim procedures to follow under certain conditions.

On March 10, 2019, Ethiopian Airlines Flight 302 (ET302), also a B737-8 MAX, crashed shortly after takeoff in Addis Ababa, Ethiopia. On March 13, 2019, the FAA issued an emergency order prohibiting operation of the B737 MAX in the United States.

Because of apparent similarities in factors that may have contributed to these accidents, the FAA Associate Administrator for Aviation Safety established a Joint Authorities Technical Review (JATR) to review the type certification of the flight control system on the B737 MAX.

The JATR was chaired by Mr. Christopher Hart, an independent aviation safety professional and former Chairman of the National Transportation Safety Board (NTSB). The remainder of the JATR team was comprised of 28 members from the FAA,² the National Aeronautics and Space Administration (NASA), and nine civil aviation authorities (CAAs) representing:

- Australia
- Brazil

¹ The B737 MAX aircraft series is the fourth generation of the B737 (i.e., a “derivative” or “related” aircraft), succeeding the B737 NG. Boeing applied for certification of the B737-8 MAX (the first in the series) on June 30, 2012, and the FAA certified the aircraft on March 8, 2017. *See* Type Certificate Data Sheet No. A16WE.

² The FAA participants selected for the JATR team did not participate in certification of the B737 MAX.

- Canada
- China
- European Union
- Indonesia
- Japan
- Singapore
- United Arab Emirates

The FAA chartered the JATR to review the work conducted during the B737 MAX certification program, to assess whether compliance was shown with the required applicable airworthiness standards related to the flight control system and its interfaces, and to recommend improvements to the certification process if warranted. Of particular concern to the FAA in chartering the JATR was the function, evaluation, and certification of the MCAS function on the B737 MAX.³ The JATR team's review also focused on flight crew training and operational suitability of the design. The JATR team considered whether the appropriate regulations and policy were applied, as well as how applicable regulations and policy material could be improved to enhance safety.

The FAA did not charter the JATR to review the entire certification process for all aspects of the aircraft, nor did it task the team to review details related to returning the B737 MAX to service. The FAA made clear that it did not create the JATR to inform its decision on returning the B737 MAX to service.

The JATR team conducted its review from approximately May through September 2019. The team met in person three times during this period for a total of four weeks and exchanged information electronically between meetings. The team received briefings from FAA and Boeing personnel knowledgeable of the B737 MAX program, and the team conducted an intensive two-week review of certification compliance documentation and related data held by Boeing. The JATR team also reviewed applicable FAA regulations and guidance. The team's findings and compilation of members' recommendations are commensurate with the information made available to the team and with the time constraints inherent in such a review.

The charter did not require consensus recommendations; the recommendations provided in this submittal are a compilation of team members' recommendations. Also in accordance with the charter, the JATR team produced observations and findings but did not prepare a report. The team endeavored to provide sufficient context through the background information included with each of the 12 main recommendations below and through the detailed supporting observations, findings, and recommendations that follow this Executive Summary.

³ The MCAS function resides in the aircraft's flight control computer.

Summary of JATR Team Members' Recommendations

The Certification Process

1. Changed Product Rule

The FAA continually amends aircraft design regulations to improve safety. New aircraft designs are required to meet the latest amendments to the regulations, but in some circumstances, changes to previously approved designs can be certified under previous regulatory amendments. The process for determining the applicable amendments is governed by Section 21.101 of Title 14 of the Code of Federal Regulations (CFR), known as the Changed Product Rule.⁴ The design regulations for the B737 MAX included a combination of the following:

- Regulatory amendments in effect when the B737 was originally certified in 1967.
- Regulatory amendments in effect when Boeing applied for certification of the B737 MAX project.
- Regulatory amendments in effect during the time between original certification in 1967 and application for certification of the B737 MAX.
- Certain regulatory amendments that became effective after Boeing's application date that the company elected to comply with.⁵
- Special conditions, exemptions, and equivalent level of safety findings (typical of similar certification projects).
- Additional design requirements and conditions (ADRCs).

⁴ The certification procedures for aircraft are in 14 CFR part 21. Subparts A through E specify certain regulations and the applicable airworthiness standards for type certification of new and changed products. Airworthiness standards for transport category aircraft are in 14 CFR parts 25 and 26. The term "changed product" includes changes that are made through an amended type certificate (ATC), a supplemental type certificate (STC), or an amended STC. Guidance for complying with the Changed Product Rule (14 CFR 21.101) is found in Advisory Circular 21.101-1B, *Establishing the Certification Basis of Changed Aeronautical Products*, and FAA Order 8110.48A, *How to Establish the Certification Basis for Changed Aeronautical Products*.

⁵ An applicant for a change to a type certificate must show that the change and areas affected by the change comply with the applicable airworthiness requirements in effect on the date of the application for the change (i.e., the latest amendment of the regulation), unless the applicant shows that the change meets the criteria for an exception set out in § 21.101(b) or (c). Under § 21.101(b), an applicant may propose a certification basis using an airworthiness requirement in effect before the date of application (but not earlier than the existing certification basis) if the earlier amendment is considered adequate and meets one of the criteria in § 21.101(b) – i.e., the change is not significant (§ 21.101(b)(1)); the area, system, component, equipment, or appliance is not affected by the change (§ 21.101(b)(2)); or compliance with latest amendment would not contribute materially to the level of safety of the product or would be impractical (§ 21.101(b)(3)). Even if an exception is available under § 21.101(b), an applicant may still elect to comply with the latest amendment.

The Changed Product Rule requires changed areas of the design and areas affected by the change to be assessed for compliance, but allows unaffected areas of the aircraft not to be reassessed.

The JATR team reviewed how the Changed Product Rule process was applied to the certification of the flight control system of the B737 MAX. The JATR team determined that the Changed Product Rule process was followed and that the process was effective for addressing discrete changes. However, the team determined that the process did not adequately address cumulative effects, system integration, and human factors issues. The Changed Product Rule process allows the applicant⁶ to only address in a limited way changed aspects (and areas affected by the change) and does not require analysis of all interactions at the aircraft level.

The current Changed Product Rule process lacks an adequate assessment of how proposed design changes integrate with existing systems and the associated impact of this interaction at the aircraft level. A more fulsome assessment process would apply to establishing the certification basis as well as to finding compliance throughout the certification process.

Recommendation R1

Based on the JATR team’s observations and findings related to the application of the Changed Product Rule to the certification of the flight control system of the B737 MAX, JATR team members recommend that the FAA work with other civil aviation authorities to revise the harmonized approach to the certification of changed products. Changed Product Rules (e.g., 14 CFR §§ 21.19 & 21.101) and associated guidance (e.g., Advisory Circular 21.101-1B and FAA Orders 8110.4C and 8110.48A) should be revised to require a top-down approach whereby every change is evaluated from an integrated whole aircraft system perspective. These revisions should include criteria for determining when core attributes of an existing transport category aircraft design make it incapable of supporting the safety advancements introduced by the latest regulations and should drive a design change or a need for a new type certificate. The aircraft system includes the aircraft itself with all its subsystems, the flight crew, and the maintenance crew.

These Changed Product Rule revisions should take into consideration the following key principles:

- ***A comprehensive integrated system-level analysis recognizing that in this complex interactive system, every change could interact with other parts of the system.***
- ***The assessment of proposed design changes on existing systems at the aircraft level includes using development assurance principles, system safety principles, and***

⁶ The term “applicants” as used in this document refers to persons applying for a type certificate (TC), a supplemental type certificate (STC), or an amendment to either a TC or STC. This includes both aircraft manufacturers (often referred to as original equipment manufacturers) and, in the case of STCs and amended STCs, aircraft modifiers as well.

validation & verification techniques. The level of assessment should be proportional to the impact of the change at the aircraft level.

- *The consideration of training and qualification of flight and maintenance personnel, as well as detailed explicit procedures for the safe operation of the aircraft.*

2. Development and use of up-to-date requirements and practices

The JATR team reviewed the regulations, policy, and compliance methods applied to the B737 MAX. The JATR team determined that some regulations, policies, and compliance methods that address safety issues related to system integration and human factors and that were available at the time of the B737 MAX certification process were not applied to the B737 MAX or were only partially applied in a way that failed to achieve the full safety benefit. In some cases, this failure to achieve the full safety benefit associated with the application of the latest compliance methods was because the FAA regulations and guidance were out of date. Another area the JATR team determined is in need of an update is the guidance concerning pilot recognition time and pilot reaction time to failures. Additionally, the JATR team determined that new and novel application of specific design features was not adequately considered.

Recommendation R2

Based on the JATR team's observations and findings related to the regulations, policy, and compliance methods applied to the B737 MAX, JATR team members recommend that the FAA update regulations and guidance that are out of date and update certification procedures to ensure that the applied requirements, issue papers, means of compliance, and policies fully address the safety issues related to state-of-the-art designs employed on new projects. JATR team members also recommend that the FAA review its processes to ensure that regulations and guidance materials are kept up to date.

3. Consistent interpretation and application of requirements

The JATR team reviewed the certification of the Boeing B737 MAX flight control system and related interfaces to assess whether compliance was shown to the applicable design standards and requirements. The JATR team identified concerns with the consistent application and interpretation of regulatory guidance pertaining to the system safety assessment (SSA), handling qualities rating method (HQRM), and conformity requirements for engineering simulators and devices. The application of 14 CFR § 25.1329 (Flight Guidance System) and § 25.1581 (Airplane Flight Manual - General) and the supporting data and techniques used for § 25.201 (Stall Demonstration) were questioned.

Recommendation R3

Based on the JATR team's observations and findings related to the certification of the B737 MAX flight control system and related interfaces, JATR team members recommend that the FAA review the B737 MAX compliance to 14 CFR §§ 25.1329 (Flight Guidance System), 25.1581 (Airplane Flight Manual – General), and 25.201 (Stall Demonstration) and ensure the consistent application and interpretation of regulatory guidance material for the system safety assessment, handling qualities rating method, and conformity requirements for engineering simulators and devices. Should there be a non-compliance, the root cause should be identified and measures implemented to prevent recurrence.

4. Changes during the certification process

The JATR team reviewed the type certification process (per FAA Order 8110.4C, *Type Certification*, and related guidance) to determine whether the process includes sufficient feedback paths to accommodate changes in aircraft design and methods of compliance during the lengthy span (e.g., five years) of a typical major aircraft certification program such as the B737 MAX. The JATR team identified specific areas related to the evolution of the design of the MCAS where the certification deliverables were not updated during the certification program to reflect the changes to this function within the flight control system. In addition, the design assumptions were not adequately reviewed, updated, or validated; possible flight deck effects were not evaluated; the SSA and functional hazard assessment (FHA) were not consistently updated; and potential crew workload effects resulting from MCAS design changes were not identified.

Recommendation R4

Based on the JATR team's observations and findings related to the FAA type certification process, JATR team members recommend that the FAA review and update the regulatory guidance pertaining to the type certification process with particular emphasis on early FAA involvement to ensure the FAA is aware of all design assumptions, the aircraft design, and all changes to the design in cases where a changed product process is used. The FAA should consider adding feedback paths in the process to ensure that compliance, system safety, and flight deck/human factors aspects are considered for the aircraft design throughout its development and certification.

5. Delegation of certification authority

Under the FAA's Organization Designation Authorization (ODA) program, the FAA granted Boeing designee authority over parts of the certification project.⁷ FAA oversight of the certification process was performed by the FAA's Boeing Aviation Safety Oversight Office (BASOO).⁸

The act of delegating, i.e., designating industry as representatives of a CAA, is well established and is common practice by the majority of CAAs around the world. Delegation provides CAAs with a pool of expertise to exercise approvals and findings of compliance within the scope of delegated authority. However, the ongoing oversight of designees and ODAs by the CAA is critically important to provide assurance to the CAA that safety and certification work is being carried out satisfactorily.

The BASOO is required to perform a certification function, including making findings of compliance of retained (non-delegated) requirements, while also performing the oversight function of the Boeing ODA. The BASOO must have the resources to carry out these two primary functions without compromise. The JATR team concluded that FAA resource shortfalls in the BASOO (and other allocated resources) may have contributed to an inadequate number of FAA specialists being involved in the B737 MAX certification program. In some cases, BASOO engineers had limited experience and knowledge of key technical aspects of the B737 MAX program.

The BASOO delegated a high percentage of approvals and findings of compliance to the Boeing ODA for the B737 MAX program. With adequate FAA engagement and oversight, the extent of delegation does not in itself compromise safety. However, in the B737 MAX program, the FAA had inadequate awareness of the MCAS function which, coupled with limited involvement, resulted in an inability of the FAA to provide an independent assessment of the adequacy of the Boeing proposed certification activities associated with MCAS. In addition, signs were reported of undue pressures on Boeing ODA engineering unit members (E-UMs) performing certification activities on the B737 MAX program, which further erodes the level of assurance in this system of delegation.

⁷ Under 49 U.S.C. 44702(d), the FAA may 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.

⁸ FAA's Transport Aircraft Seattle Aircraft Evaluation Group coordinated and assisted in the certification process. FAA also formed a Flight Standardization Board to evaluate and validate Boeing's (as the applicant) proposed training program for the B737 MAX.

Recommendation R5

Based on the JATR team’s observations and findings related to FAA’s oversight by the Boeing Aviation Safety Oversight Office (BASOO), JATR team members recommend that the FAA conduct a workforce review of the BASOO engineer staffing level to ensure there is a sufficient number of experienced specialists to adequately perform certification and oversight duties, commensurate with the extent of work being performed by Boeing. The workforce levels should be such that decisions to retain responsibility for finding compliance are not constrained by a lack of experienced engineers.

The FAA should review the Boeing Organization Designation Authorization (ODA) work environment and ODA manual to ensure the Boeing ODA engineering unit members (E-UMs) are working without any undue pressure when they are making decisions on behalf of the FAA. This review should include ensuring the E-UMs have open lines of communication to FAA certification engineers without fear of punitive action or process violation.

Integrated Approach to Development and Certification

6. Holistic, integrated aircraft-level approach

The JATR team reviewed the design process of the flight control system and the related SSAs for the B737 MAX to assess whether the flight control system complies with applicable system design and safety requirements and standards. The JATR team found that the MCAS was not evaluated as a complete and integrated function in the certification documents that were submitted to the FAA. The lack of a unified top-down development and evaluation of the system function and its safety analyses, combined with the extensive and fragmented documentation, made it difficult to assess whether compliance was fully demonstrated. The MCAS design was based on data, architecture, and assumptions that were reused from a previous aircraft configuration without sufficient detailed aircraft-level evaluation of the appropriateness of such reuse, and without additional safety margins and features to address conditions, omissions, or errors not foreseen in the analyses.

Recommendation R6

Based on the JATR team’s observations and findings related to the design process of the flight control system and the related system safety assessments for the B737 MAX, JATR team members recommend that the FAA promote a safety culture that drives a primary focus on the creation of safe products, which in turn comply with certification requirements. Aircraft functions should be assessed, not in an incremental and fragmented manner, but holistically at the aircraft level. System function and performance, including the effects of failures, should be demonstrated and associated assumptions should be challenged to

ensure robust designs are realized. The safety analysis process should be integrated with the aircraft development assurance process to ensure all safety requirements and associated assumptions are correct, complete, and verified. The FAA should encourage applicants to have a system safety function that is independent from the design organization, with the authority to impartially assess aircraft safety and influence the aircraft/system design details. Adoption of a safety management system is one way this can be achieved.

7. Human factors

Humans design, build, maintain, and operate every part of the global aviation system. The enviable safety record of the aviation system is a direct result of human capabilities. At the same time, all aviation accidents are the result of human limitations. This is not to say that all accidents are the result of human error, but of human limitations, such as limitations to people's imagination and their ability to foresee, predict, and anticipate possible situations. As the technology becomes more advanced, and as the operational environment becomes more complex, understanding the scope and nature of the interactions between the technology, the human, and the environment becomes more critical to aviation safety. This criticality of human factors to aviation safety has been recognized and has been codified in various rules such as 14 CFR §§ 25.1302 (Installed Systems and Equipment for Use by the Flightcrew), 25.1309 (Equipment, Systems, and Installations), and 25.1322 (Flightcrew Alerting). While issues in human-machine interaction are at the core of all recent aviation accidents and are implicated in the two B737 MAX accidents, the FAA has very few human factors and human system integration experts on its certification staff. The JATR team identified multiple human factors-related issues in the certification process. Because human factors is a cross-cutting aspect, related recommendations are made under several of the different areas identified in this summary.

Recommendation R7

Based on the JATR team's observations and findings related to human factors-related issues in the certification process, JATR team members recommend that the FAA integrate and emphasize human factors and human system integration throughout its certification process. Human factors-relevant policies and guidance should be expanded and clarified, and compliance with such regulatory requirements as 14 CFR §§ 25.1302 (Installed Systems and Equipment for Use by the Flightcrew), 25.1309 (Equipment, Systems, and Installations), and 25.1322 (Flightcrew Alerting) should be thoroughly verified and documented. To enable the thorough analysis and verification of compliance, the FAA should expand its aircraft certification resources in human factors and in human system integration.

8. Development assurance

Development assurance is a methodology applied to aircraft and aircraft systems to ensure safe and compliant designs in increasingly complex and integrated aircraft systems. Design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for complex systems. As evidenced in the B737 MAX, integrated aircraft-level functions, such as the MCAS, present a risk of development error (requirements determination and design errors) and undesirable, unintended effects.

The systematic use of development assurance techniques increases confidence that errors in requirements or design, and integration or interaction effects, have been adequately identified and corrected by the applicant.

Boeing elected to meet the objectives of SAE International's Aerospace Recommended Practice 4754A, *Guidelines for Development of Civil Aircraft and Systems*, (ARP4754A) for development assurance of the B737 MAX. Issue Paper SA-1 documented the methods and means that Boeing used to show that the processes used for B737 MAX systems development were, when appropriate, in accordance with the objectives of ARP4754A and were an acceptable means of addressing requirement, design, and implementation errors. The use of ARP4754A is consistent with the guidance contained in FAA Advisory Circular (AC) 20-174, *Development of Civil Aircraft and Systems*. The JATR team identified areas where the Boeing processes can be improved to more robustly meet the development assurance objectives of ARP4754A.

Recommendation R8

Based on the JATR team's observations and findings related to the development assurance process applied to the design of the flight control system of the B737 MAX, JATR team members recommend that the FAA ensure applicants apply industry best practice for development assurance, including requirements management, visibility of assumptions, process assurance activities, and configuration management. The FAA should ensure achievement of the close coupling that is required between the applicant safety analysis process and the development assurance process to classify failure conditions and derive the level of rigor of design development and verification. A current example of industry best practice is SAE International's Aerospace Recommended Practice 4754A (ARP4754A).

The FAA should review and amend Advisory Circular 20-174 to clearly articulate the principles of ARP4754A, promoting industry best practice for development assurance of aircraft and aircraft systems to address applicants' design trend of increasing integration between aircraft functions and systems.

Impact of Design Changes on Operations and Training

9. Impact of product design changes on operations

A review of preliminary accident reports KNKT.18.10.35.04 (for Lion AIR Flight JT610) and AI-0/19 (for Ethiopian Airlines Flight 302) indicates that the complex operational environment that faced the flight crews during the events leading up to the accidents and the associated flight crew workload may not have been anticipated in the certification process. Applicants make various assumptions during the requirements definition phase which can influence the design and how that design is certified. Boeing made several assumptions for the B737 MAX which directly influenced the design and certification of MCAS. The evaluation of an applicant's operational design assumptions concerning crew response is under the purview of the FAA Aircraft Evaluation Group (AEG).

FAA Order 8110.4C articulates the need for AEG's early involvement in the certification process, starting at the requirements definition phase. Test pilots working in the certification process may not have complete knowledge of operational issues, while pilots working in the operational evaluation process may not have complete knowledge of certification issues. This gap may contribute to limited communication between the two processes, creating the potential for a lack of operational insight into the certification process.

Recommendation R9

Based on the JATR team's findings and observations related to the operational design assumptions of crew response applied during the certification process for the flight control system of the B737 MAX, JATR team members recommend that the FAA require the integration of certification and operational functions during the certification process. The FAA should be provided all system differences between related aircraft in order to adequately evaluate operational impact, systems integration, and human performance.

10. Impact of product design changes on flight crew training

A review of preliminary accident reports KNKT.18.10.35.04 and AI-0/19 indicates that both flights suffered an extreme mis-trim event which involved the activation of the MCAS function. During the certification process, a decision was made to remove information relating to MCAS functionality from the draft Flight Crew Operating Manual (FCOM). This decision meant that the FAA Flight Standardization Board (FSB) was not fully aware of the MCAS function and was not in a position to adequately assess training needs.

The Boeing AFM does not include all the normal, non-normal, and emergency operating procedures as required by regulations. Boeing has included most of the operating procedures in the FCOM in accordance with FAA guidance (AC 25.1581-1, *Airplane Flight Manual*). This

difference between the rule and the guidance enabled Boeing to make changes to aircraft operating procedures (via the FCOM) without requiring FAA approval for such changes. This can result in situations where the FAA is unaware of changes to normal, non-normal, and emergency operating procedures. Systems information is often included in the FCOM and may not be required to be included in the FAA-approved AFM. However, technology, even if it functions without pilot involvement, may be integrated with other aircraft systems, such that one system or functional failure could impact other systems and require pilot intervention. When such technologies, systems, or possible malfunctions are not included in the FCOM or in the Flight Crew Training Manual (FCTM), the pilot is unlikely to be aware of them and may fail to recognize a malfunction when it occurs or may not know how to respond appropriately.

To be compliant with FAA regulations and guidance material, Boeing utilized four fundamental assumptions on crew actions in the flight control functional hazard assessment (FHA) for the B737 MAX and other Boeing models. The third assumption, taken from AC 25-7C, stated: “The pilot will take immediate action to reduce or eliminate high control forces by re-trimming or changing configuration or flight conditions.”⁹ It is evident from the accident flights that the flight crews’ actions were not consistent with Boeing’s third operational design assumption.

Recommendation R10

Based on the JATR team’s findings and observations related to flight crew training, JATR team members recommend that the FAA require a documented process to determine what information will be included in the Airplane Flight Manual, the Flight Crew Operating Manual, and the Flight Crew Training Manual. The FAA should review training programs to ensure flight crews are competent in the handling of mis-trim events.

11. Impact of product design changes on maintenance training

The JATR team was tasked to consider maintenance suitability of the design. Due to lack of maintenance expertise on the JATR, the team was unable to make a determination of such adequacy.

⁹ Some of the FAA advisory circulars (ACs) referenced in this document are referred to at different revision levels depending on the context. Where the JATR team made an observation or finding about an AC as applied to the certification of the B737 MAX, the revision of the AC in effect at the time of certification was the version reviewed by the JATR team and is referenced accordingly. If such an AC has since been revised, the later revision of the AC is referred to in observations or findings about current content and in recommendations for improvements to FAA guidance. For example, several references are made to AC 25-7C, which was current at the time of the B737 MAX certification program and was used as compliance guidance. Other references are made to AC 25-7D, which is the current version of the AC and is therefore referred to in observations and findings about current content and in the JATR team’s recommendations for future enhancements to the AC.

Recommendation R11

JATR team members recommend that the FAA conduct a study to determine the adequacy of policy, guidance, and assumptions related to maintenance and ground handling training requirements.

Post-Certification Activities

12. Post-certification corrective actions and data sharing

In accordance with its charter, the JATR team focused on reviewing the flight controls work conducted by Boeing and the FAA leading up to certification of the B737 MAX. The team did not conduct an in-depth review of post-certification activities, as this was beyond the initial scope of the JATR. However, during the course of its review, the team became aware of some aspects of post-certification activities. As a result, the team took advantage of the provision in the charter for expanding the JATR's scope at the discretion of the Chair and Co-chair in order to identify additional observations and recommendations that have the potential for further enhancing aviation safety.

Recommendation R12

JATR team members recommend that the FAA review its policies for analyzing safety risk and implementing interim airworthiness directive action following a fatal transport aircraft accident. The FAA should ensure that it shares post-accident safety information with the international community to the maximum extent possible.

Page intentionally left blank

JATR Team Observations and Findings; Member Recommendations

Terminology

This submittal consists of observations and findings developed by the JATR team, as well as a compilation of team members' recommendations, as follows:

Observation

An *observation* is a noteworthy fact or issue gained from the JATR team's review of the FAA's certification of the B737 MAX flight control system and its related interfaces.

Finding

A *finding* is a conclusion drawn by the JATR team based on review of design details, analyses, reports, or other factual evidence.

Recommendation

A *recommendation* is a proposed action for the FAA to consider and is intended to identify "what" is to be done, as opposed to "how" actions are to be accomplished. Recommendations are based on the JATR team's findings and observations. Note that not all findings or observations necessarily resulted in a recommendation.

Acronyms

The JATR uses the following acronyms in this submittal.

AC – Advisory Circular

AD – Airworthiness Directive

ADRC – Additional design requirements and conditions

AEG – Aircraft Evaluation Group (FAA)

AFM – Airplane Flight Manual

AMC – Acceptable means of compliance

AOA – Angle of attack

ARAC – Aviation Rulemaking Advisory Committee

ATC – Amended type certificate

BASOO – Boeing Aviation Safety Oversight Office (FAA)

CAA – Civil Aviation Authority

CFR – Code of Federal Regulations

DOORS – Dynamic Object-Oriented Requirements System

EASA – European Aviation Safety Agency

EFS – Elevator feel shift

E-UM – Engineering unit member

FAA – Federal Aviation Administration

FCC – Flight control computer

FCOM – Flight Crew Operating Manual

FCTM – Flight Crew Training Manual

FHA – Functional hazard assessment

FSB – Flight Standardization Board (FAA)

HQRM – Handling qualities rating method

HUD – Head-up display

ICAO – International Civil Aviation Organization

JATR – Joint Authorities Technical Review

MCAS – Maneuvering Characteristics Augmentation System

MMEL – Master minimum equipment list

MSAD – Monitor Safety/Analyze Data

NASA – National Aeronautics and Space Administration

NTSB – National Transportation Safety Board

ODA – Organization Designation Authorization

OFE – Operational flight envelope

PSSA – Preliminary system safety assessment

SDAHWG – Systems Design and Analysis Harmonization Working Group

SACO – Seattle Aircraft Certification Office

S&MF – Single & multiple failure

SSA – System safety assessment

STC – Supplemental type certificate

STS – Speed trim system

TC – Type certificate

TCDS –Type certificate data sheet

FAA Guidance, Directives, and Regulations

The JATR team also addresses the following FAA advisory circulars (ACs), FAA orders, and sections of Title 14 of the Code of Federal Regulations in this submittal.

Note: Latest revisions of relevant FAA ACs and orders are listed below for reference in the context of recommended improvements that follow. However, the JATR team generally considered the revision of an FAA AC or order that was applicable during the certification of the B737 MAX, which in some cases was an earlier revision than listed below.

FAA Advisory Circulars

AC 20-174, *Development of Civil Aircraft and Systems*

AC 21.101-1B, *Establishing the Certification Basis of Changed Aeronautical Products*

AC 25-7D, *Flight Test Guide for Certification of Transport Category Airplanes*

AC 25-11B, *Electronic Flight Displays*

AC 25.1302-1, *Installed Systems and Equipment for Use by the Flightcrew*

AC 25.1309-1A, *System Design and Analysis*

AC 25.1329-1C, *Approval of Flight Guidance Systems*

AC 25.1581-1, *Airplane Flight Manual*

AC 120-53B, *Guidance for Conducting and Use of Flight Standardization Board Evaluations*

FAA Orders

FAA Order 8100.15B, *Organization Designation Authorization Procedures*

FAA Order 8110.4C, *Type Certification*

FAA Order 8110.48A, *How to Establish the Certification Basis for Changed Aeronautical Products*

FAA Order 8110.107A, *Monitor Safety/Analyze Data*

Sections of Title 14 of the Code of Federal Regulations (CFR)

PART 21 – CERTIFICATION PROCEDURES FOR PRODUCTS AND ARTICLES

Subpart B – Type Certificates

§ 21.19 Changes requiring a new type certificate

Subpart D – Changes to Type Certificates

§ 21.101 (Designation of applicable regulations)

PART 25 – AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES

Subpart B - Flight

STALLS

§ 25.201 Stall demonstration

MISCELLANEOUS FLIGHT REQUIREMENTS

§ 25.255 Out-of-trim characteristics

Subpart D – Design and Construction

CONTROL SYSTEMS

§ 25.671 General

§ 25.672 Stability augmentation and automatic and power-operated systems

Subpart F – Equipment

GENERAL

§ 25.1302 Installed systems and equipment for use by the flightcrew

§ 25.1309 Equipment, systems, and installations

INSTRUMENTS: INSTALLATION

§ 25.1322 Flightcrew alerting

§ 25.1329 Flight guidance system

Subpart G – Operating Limitations and Information

AIRPLANE FLIGHT MANUAL

§ 25.1581 General

§ 25.1583 Operating limitations

§ 25.1585 Operating procedures

§ 25.1587 Performance information

Observations, Findings, and Recommendations

The following observations, findings, and recommendations are based on the data and information that was made accessible to the JATR team. The team's access to some information was limited by factors such as U.S. export controls and the obligations that participants in accident investigations conducted by another State have under International Civil Aviation Organization (ICAO) Annex 13 not to divulge certain information.

Some of the JATR team members' recommendations for the FAA are specifically related to Boeing and/or the B737 MAX, and these recommendations are clearly stated as such. Because the JATR team was also chartered to identify potential enhancements to the certification process, many of the team members' recommendations are general in nature. These general recommendations should not necessarily be construed as a reflection on Boeing or the B737 MAX specifically, but rather as opportunities identified by the JATR team members for the FAA to improve the certification process.

The FAA, European Aviation Safety Agency (EASA), and Transport Canada Civil Aviation previously conducted B737 MAX development assurance certification/validation reviews. The

JATR team’s findings below are not intended to invalidate the results of those reviews but rather to supplement them with a more focused, event-driven review.

The order of the observations, findings, and recommendations does not imply any level of importance or priority.

The Certification Process

1. Changed Product Rule

Recommendation R1

Based on the JATR team’s observations and findings related to the application of the Changed Product Rule to the certification of the flight control system of the B737 MAX, JATR team members recommend that the FAA work with other civil aviation authorities to revise the harmonized approach to the certification of changed products. Changed Product Rules (e.g., 14 CFR §§ 21.19 & 21.101) and associated guidance (e.g., Advisory Circular 21.101-1B and FAA Orders 8110.4C and 8110.48A) should be revised to require a top-down approach whereby every change is evaluated from an integrated whole aircraft system perspective. These revisions should include criteria for determining when core attributes of an existing transport category aircraft design make it incapable of supporting the safety advancements introduced by the latest regulations and should drive a design change or a need for a new type certificate. The aircraft system includes the aircraft itself with all its subsystems, the flight crew, and the maintenance crew.

These Changed Product Rule revisions should take into consideration the following key principles:

- ***A comprehensive integrated system-level analysis recognizing that in this complex interactive system, every change could interact with other parts of the system.***
- ***The assessment of proposed design changes on existing systems at the aircraft level includes using development assurance principles, system safety principles, and validation & verification techniques. The level of assessment should be proportional to the impact of the change at the aircraft level.***
- ***The consideration of training and qualification of flight and maintenance personnel, as well as detailed explicit procedures for the safe operation of the aircraft.***

Recommendation R1 is based on the following observations, findings, and supporting recommendations related to the JATR team’s review of how the Changed Product Rule process was applied to the certification of the B737 MAX. In achieving R1, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R1.1: The FAA, in collaboration with other CAAs, should:
 - (a) Revise the harmonized approach to certifying changed products to achieve the expectations of a top-down approach intended by 14 CFR 21.101, where every change is evaluated from an integrated, whole aircraft/human system engineering perspective and where the whole aircraft is assumed affected by the change(s) until substantiated otherwise. This approach should focus on a safe design that as a by-product leads to compliance with regulatory requirements.
 - (b) Develop criteria for determining when core attributes of an existing design make it incapable of supporting the safety advancements introduced by the latest regulations and therefore warrant consideration of a design change and/or certification under a new type certificate.
 - (c) Expand the guidance as to what constitutes a substantial change and what can be considered as only a significant change to address such aspects as changes in software, changes in the roles and responsibilities of the flight crew, and changes to maintenance practices.
 - Finding F1.1-A: Although many aspects of the B737 design have been required to meet updated certification requirements each time the type certificate has been amended over the years, some elements of the design and certification remain rooted in the original 1967 certification of the B737-100. The basic federated architecture of the B737 has remained largely unchanged from its original conception and drove many design decisions more than 50 years after it was originally designed.¹⁰ In the intervening 50 years, significant advancements have been made in design methodologies and tools and in analysis and analytical tools, which have led to significant improvements in the safety of air transportation. While some of these advancements and associated design concepts have been incorporated into the B737 MAX, others have been determined to be impractical for incorporation into the B737 MAX design or certification requirements using current regulations and policies.
 - Observation O1.1-A: There are no criteria for determining when the core attributes of an existing design make it fundamentally incapable of supporting the safety advancements introduced by the latest amendments to airworthiness standards.

¹⁰ “Federated architecture” refers to a style of avionics architecture in which each digital flight control function (e.g., autopilot, autothrottle, flight management) has its own fault-tolerant computer system, which is only loosely coupled to the computer systems of other functions.

- Finding F1.1-B: The guidance given in AC 21.101-1B, *Establishing the Certification Basis of Changed Aeronautical Products*, as to what constitutes a substantial change that requires a new type certificate is insufficient. This guidance is focused on large-scale structural changes and does not consider changes in software or changes in the roles of either the flight crew or the maintenance crew to be “substantial changes.”
- Observation O1.1-B: Section 21.101 was designed to lead to a top-down approach to the certification of changed products whereby the whole aircraft is assumed to be affected by changes, and compliance with current amendments must be found at the level of the aircraft, unless otherwise noted.
- Finding F1.1-C: Boeing’s compliance submissions to the FAA followed a bottom-up approach whereby each change and areas affected by a change were presented separately, showing compliance at the level of the specific regulation and its application to a given change.
- Finding F1.1-D: Several risk and failure analyses were mostly done at the level of the change and subsystem and not at an integrated aircraft level.
- Finding F1.1-E: Some of the Boeing engineers the JATR team spoke with described the Boeing process in a manner that reflected an emphasis on meeting individual certification requirements, without necessarily having an appreciation for the overall safety-based reasons for those requirements.
- Recommendation R1.2: The FAA, in collaboration with other CAAs, should expand the certification process to include “change, areas affected by the change, and ***areas affecting a change***.” This expansion should allow for the identification of interactions such as the one between the angle of attack (AOA) system and MCAS in the case of the B737 MAX.
 - Observation O1.2-A: The certification process of a derivative aircraft is focused on “change and areas affected by the change.” The AOA sensing system of the B737 MAX was not changed from the B737 NG and was not affected by any of the changes, including the MCAS.
 - Observation O1.2-B: Based on preliminary accident information, both B737-8 MAX accidents appear to have involved an interaction between the AOA system and MCAS.
- Recommendation R1.3: The FAA should implement mandatory aircraft-level reviews along the certification process. These reviews should require risk and failure analyses at the integrated aircraft system-level including the flight crew.

- Finding F1.3-A: The certification process is focused on a large number of small details which may minimize the opportunity for a “big picture” view.
- Recommendation R1.4: The FAA should provide clear definitions of key terms in its guidance for 14 CFR §§ 21.19 and 21.101.
 - Finding F1.4-A: The FAA and Boeing adhered to the applicable regulations, policy, and guidance that existed at the time of application for determining whether a new type certificate (versus amended type certificate) would be required, and for determining the certification basis for the B737 MAX.
 - Finding F1.4-B: During the certification process of the B737 MAX, FAA personnel had no doubt about its suitability to qualify as a derivative aircraft which does not require a new type certificate.
 - Finding F1.4-C: The existing rules and guidance governing the certification process leave much room for interpretation. Key terms such as “substantial” as in “substantially complete investigation” in § 21.19, as well as “affect” as in “areas affected by the change” and “material” as in “contribute materially to the level of safety” in § 21.101, are not clearly defined.
- Recommendation R1.5: The FAA should define and clearly describe the intent and expected use of an ADRC in available guidance. In addition, the FAA should elaborate on the application of ADRCs in future developments (e.g., future applicant modification and supplemental type certificates (STCs)). The FAA should identify the legal standing that ensures the adherence to ADRCs for future changes.
 - Observation O1.5-A: ADRCs are identified in the certification basis for the B737 MAX, but the term is not defined in FAA directives or guidance. The term also appears in other aircraft type certificate data sheets (TCDSs).
- Recommendation R1.6: The FAA should develop processes for identifying perceptions of vagueness and ambiguity in its guidance and strive to clarify all certification guidance that is deemed vague or incomplete.
 - Observation O1.6-A: Different FAA officials the JATR team spoke with demonstrated differences in opinions about how to apply the Changed Product Rule.
 - Observation O1.6-B: Some FAA officials the JATR team spoke with complained about vague and partial guidance for the implementation of the Changed Product Rule.

- Recommendation R1.7: The FAA and applicants should develop, validate, and implement analytical tools appropriate for the analysis of complex systems.
 - Finding F1.7-A: The requirements of an amended type certificate certification process to focus only on “change and areas affected by the change” may fail to recognize that the whole aircraft system (including the flight crew) could be affected by seemingly small changes.
 - Observation O1.7-A: A complicated system is characterized by a linear relationship between cause and effect, whereas a complex system is characterized by a non-linear relationship between cause and effect, such that small causes could lead to very large effects.
 - Finding F1.7-B: Although the aircraft itself may only be a complicated system, the aircraft system including the flight crew is a complex system.
 - Finding F1.7-C: Analytical tools designed for complicated systems may not be sufficient for the analysis of complex systems.
- Recommendation R1.8: The FAA should ensure that the TCDS for the B737 MAX (TCDS No. A16WE) clearly states which part of 14 CFR 25.1322 (Flightcrew Alerting), and at which amendment level, the B737 MAX complies to.
 - F1.8-A: The A16WE TCDS does not clearly state the applicable amendment level that the B737 MAX complies with for § 25.1322. Significant review and background knowledge is required to determine that the B737 MAX is compliant with the following:
 - Amdt 131: (a), (b)(1), (c)(1), (e), and (f).
 - Amdt 38: none, even though this is the certification basis of the B737 NG.
 - Amdt NA: none, § 25.1322 not present in initial part 25 regulation.
 - ADRC: (b)(2), which is technically equivalent to Amdt 38 para (b), and (c)(3).
- Recommendation R1.9: The FAA should ensure that TCDSs accurately reflect when compliance is found at the stated amendment level and when compliance is limited to a subset of the aircraft (such as a change).
 - Finding F1.9-A: Compliance with regulatory requirements and the certification process as a whole are the results of a negotiation process between the applicant and the FAA. The TCDS contains the certification basis for the aircraft, which is the output of the Changed Product Rule process. In some cases, for example where compliance is limited to a change rather than to the whole aircraft, this

negotiated agreement between the applicant and the FAA is not consistently documented. For example, the certification basis for the B737 MAX documented exceptions to the application of some amendments, but not others. Exceptions are listed for 14 CFR 25.607 (typical of about 40 regulations that had exceptions), and not for 14 CFR 25.1302. This indicates that § 25.1302 applies to the entire aircraft; yet, § 25.1302 was only partially applied on the B737 MAX.

- Finding F1.9-B: Because the aircraft alerting system is not designed to comply with all aspects of the latest amendment of § 25.1322 (Amendment 131), § 25.1302 cannot be fully applicable. These rules depend on each other, and this is further indication that § 25.1302 was not applied to the entire aircraft despite the TCDS indicating that it was.

2. **Development and use of up-to-date requirements and practices**

Recommendation R2

Based on the JATR team’s observations and findings related to the regulations, policy, and compliance methods applied to the B737 MAX, JATR team members recommend that the FAA update regulations and guidance that are out of date and update certification procedures to ensure that the applied requirements, issue papers, means of compliance, and policies fully address the safety issues related to state-of-the-art designs employed on new projects. JATR team members also recommend that the FAA review its processes to ensure that regulations and guidance materials are kept up to date.

Recommendation R2 is based on the following observations, findings, and supporting recommendations related to the JATR team’s review of the regulations, policy, and compliance methods applied to the certification of the B737 MAX. In achieving R2, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R2.1: The FAA should review the scope of 14 CFR 25.1302 (Installed Systems and Equipment for Use by the Flightcrew) applicability and clearly define in the TCDS the approach taken for certification.
 - Observation O2.1-A: MCAS, although a significant functional change, was never highlighted as an area requiring additional scrutiny from a human factors perspective. As a result, no human factors test cases were designed to investigate the adequacy of the design.

- Recommendation R2.2: The FAA should update AC 25.1302-1, *Installed Systems and Equipment for Use by the Flightcrew*, to clarify the acceptability (or not) of using 14 CFR 25.1302 in changed areas.
 - Observation O2.2-A: The application of § 25.1302 to areas of change is not explicitly described in its associated guidance material, AC 25.1302-1. The intent of § 25.1302 is stated as follows in its introductory paragraph:

This section applies to installed systems and equipment intended for flightcrew members' use in operating the airplane from their normally seated positions on the flight deck. The applicant must show that these systems and installed equipment, individually and in combination with other such systems and equipment, are designed so that qualified flightcrew members trained in their use can safely perform all of the tasks associated with the systems' and equipment's intended functions.
 - Finding F2.2-A: The JATR team's assessment is that the design and evaluation aspects should be considered for the whole of the cockpit environment, and not to components in isolation.
- Recommendation R2.3: The FAA should expedite a rule change to 14 CFR 25.1309 (Equipment, Systems, and Installations) and its associated means of compliance in order to implement the recommendations stemming from the Aviation Rulemaking Advisory Committee (ARAC) Systems Design and Analysis Harmonization Working Group (SDAHWG) (2001). This action is necessary to minimize the possibility of applicants using old guidance that is not fully effective for the system development and for conducting SSA in the context of increased system complexity and interactions.
 - Finding F2.3-A: Although the certification basis for § 25.1309 was updated for the latest amendment per Changed Product Rule analysis, delayed FAA rulemaking for updating § 25.1309 and related guidance according to the recommendations of the ARAC SDAHWG allows applicants to use geriatric guidance for safety assessment demonstration.
- Recommendation R2.4: The FAA should evaluate applicants' procedures for determining the need of any subsystem and any change to show compliance with a regulatory requirement. Special attention should be paid to compliance with new requirements.
 - Observation O2.4-A: Boeing did not identify MCAS as requiring compliance with § 25.1302, and MCAS was not assessed for such compliance.

- Recommendation R2.5: Sufficient time and resources should be allocated for the proper treatment of issue papers to avoid inconsistencies and errors.
 - Observation O2.5-A: Issue papers document the negotiation process between the applicant and the FAA to determine the certification basis of a product, establish means of compliance, and resolve other issues.
 - Observation O2.5-B: All issue papers must be closed prior to granting certification.
 - Finding F2.5-A: Some closed B737-8 MAX issue papers contain inconsistencies. For instance, in Issue Paper O-1, MDR and ODR stand for different definitions between Boeing's position and the FAA's response.
 - Finding F2.5-B: Some B737-8 MAX issue papers contain typographical and grammatical errors which could indicate a hurried process.
- Recommendation R2.6: The FAA should review its internal procedures to emphasize the need for issue papers when the applicant proposes means of compliance that deviates from advisory circulars.
 - Observation O2.6-A: A combination of ACs was used for demonstrating compliance with system safety requirements; no AC/acceptable means of compliance (AMC) was followed in its entirety. The detailed use of the referenced ACs and an indication of which sections are applicable was not formally recorded in any certification document that the JATR team reviewed.
 - Finding F2.6-A: The use of a combination of partial ACs as means of compliance should have led the FAA to formalize the agreement with this strategy, possibly by means of an AMC issue paper.
- Recommendation R2.7: If any flight control surface is used in a novel manner, the FAA should be directly involved. The FAA should assess the need for an issue paper for development of acceptable means of compliance with existing regulations, or develop special conditions if the regulations do not contain adequate or appropriate safety standards.
 - Finding F2.7-A: The FAA was not completely unaware of MCAS; however, because the information and discussions about MCAS were so fragmented and were delivered to disconnected groups within the process, it was difficult to recognize the impacts and implications of this system. If the FAA technical staff had been fully aware of the details of the MCAS function, the JATR team believes the agency likely would have required an issue paper for using the

stabilizer in a way that it had not previously been used. MCAS used the stabilizer to change the column force feel, not trim the aircraft. This is a case of using the control surface in a new way that the regulations never accounted for and should have required an issue paper for further analysis by the FAA. If an issue paper had been required, the JATR team believes it likely would have identified the potential for the stabilizer to overpower the elevator.

- Recommendation R2.8: The FAA should establish appropriate pilot recognition times and reaction times, based on substantive scientific studies which take into account the operational environment, the circumstances under which malfunctions may occur, and the effect of surprise.
 - Observation O2.8-A: FAA guidance for test flights in AC 25-7D, *Flight Test Guide for Certification of Transport Category Airplanes*, and AC 25.1329-1C, *Approval of Flight Guidance Systems*, require test pilots to delay initiation of response to flight control or flight guidance malfunctions to account for pilot recognition time and pilot reaction time. Often, recognition time is assumed to be 1 second, and reaction time is assumed to be 3 seconds. Thus, test pilots are told that “Recovery action should not be initiated until 3 seconds after the recognition point” (AC 25.1329-1C).
 - Observation O2.8-B: The current guidance recognizes that pilot recognition time may depend on various factors including the nature of the failure, but applicants are only required to prepare specific justification of their assumed recognition time if it is less than 1 second.
 - Observation O2.8-C: Although the above guidance is aimed at test pilots conducting test flights, applicants seem to use this guidance as a design assumption that the pilot will be able to respond correctly within 4 seconds of the occurrence of a malfunction. For example, in the case of the B737 MAX, it was assumed that, since MCAS activation rate is 0.27 degrees of horizontal stabilizer movement per second, during the 4 seconds that it would take a pilot to respond to an erroneous activation, the stabilizer will only move a little over 1 degree, which should not create a problem for the pilot to overcome.
 - Observation O2.8-D: No studies were found that substantiate the FAA guidance concerning pilot recognition time and pilot reaction time.
 - Observation O2.8-E: Several FAA studies with general aviation pilots demonstrate that these general aviation pilots may take many seconds, and in

some cases many minutes, to recognize and respond to malfunctions (e.g., DOT/FAA/AM-97/24; DOT/FAA/AM-02/19; DOT/FAA/AM-05/23).

- Observation O2.8-F: A NASA study of abnormal flight events with qualified, current, and active airline pilots also found substantially longer recognition times and reactions times, even in the case of expected events, than the times given in AC 25-7D and AC 25.1329-1C.¹¹
- Observation O2.8-G: Analysis of aviation accidents demonstrates that pilots may take a significantly longer time to recognize a malfunction and respond to it than the test flight guidance suggests. For example, the NTSB states: “When a flight crew is confronted with a sudden, abnormal event, responses are more likely to be delayed or inappropriate.” (NTSB/AAR-14/01)
- Observation O2.8-H: Modern aircraft can have subtle failure modes that may take substantial amounts of time to be recognized. Furthermore, automation can mask some failures and significantly delay the possibility for the pilot to recognize the malfunction.
- Finding F2.8-A: It is not clear on what the FAA guidance concerning pilot recognition time and pilot reaction time is based.
- Finding F2.8-B: Pilot recognition time and reaction time to a malfunction may depend on the particular nature of the malfunction, the circumstances under which it occurs, the corrective action required, and the individual pilot.
- Finding F2.8-C: There is a substantial difference between the situation of a test pilot who is testing a particular malfunction with precise foreknowledge of the malfunction to be tested and the proper response to be initiated, and the situation of a line pilot on a routine revenue flight who is not expecting any malfunction. Thus, guidance that is relevant to test flights may not be appropriate for routine revenue flights.
- Finding F2.8-D: The 3-second reaction time assumption dates back decades, to where the performance of the autopilot was constantly monitored by the crew in flight (e.g., guidance given in AC 25.1329-1A, *Automatic Pilot Systems Approval*, dated July 8, 1968). However, with increasing reliability and advances in flight

¹¹ Casner, S.M., R.W. Geven, and K.T. Williams (2013). The Effectiveness of Airline Pilot Training for Abnormal Events, *Human Factors*, 55, 477-485.

deck alerting and displays, it may no longer be appropriate to assume that the pilot flying will be monitoring the automation as closely as in the past.

- Finding F2.8-E: The FAA’s guidance concerning pilot reaction time of 3 seconds may not be appropriate given current aircraft technology and the current operational environment.
- Finding F2.8-F: Although current guidance seems to recognize potential variability in pilot recognition time, it is not clear that applicants are following the spirit of that guidance, because only recognition times of less than 1 second must be formally justified.
- Recommendation R2.9: The FAA should require applicants to provide validated and justified pilot recognition and reaction times for any given failure, with consideration of all associated flight deck effects within the expected operational environment.
 - This recommendation is based on Observations O2.8-A through O2.8-H and Findings F2.8-A through F2.8-F, above.
- Recommendation R2.10: The FAA should provide guidance to test pilots to initiate recovery action only once the combined recognition time and reaction time validated for the given failure being tested have elapsed.
 - This recommendation is based on Observations O2.8-A through O2.8-H and Findings F2.8-A through F2.8-F, above.

3. Consistent interpretation and application of requirements

Recommendation R3

Based on the JATR team’s observations and findings related to the certification of the B737 MAX flight control system and related interfaces, JATR team members recommend that the FAA review the B737 MAX compliance to 14 CFR §§ 25.1329 (Flight Guidance System), 25.1581 (Airplane Flight Manual – General), and 25.201 (Stall Demonstration) and ensure the consistent application and interpretation of regulatory guidance material for the system safety assessment, handling qualities rating method, and conformity requirements for engineering simulators and devices. Should there be a non-compliance, the root cause should be identified and measures implemented to prevent recurrence.

Recommendation R3 is based on the following observations, findings, and supporting recommendations related to the JATR team’s review of the certification of the B737 MAX flight control system and related interfaces. In achieving R3, JATR team members advise the FAA to

take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R3.1: The FAA should ensure early involvement by applicants and the FAA in the establishment of the detailed means of compliance for SSA demonstration (e.g., 14 CFR §§ 25.1309 (Equipment, Systems, and Installations) and 25.671 (Control Systems – General)), especially in case any deviations from standard guidance are planned, or if additional guidance not originally intended for §§ 25.1309 and 25.671 is expected to be part of the compliance demonstration.
 - This recommendation is based on Observation O2.6-A and Finding F2.6-A, above.
- Recommendation R3.2: The FAA should issue a policy statement on the need for caution and early negotiation with the certification authority when an applicant proposes using additional guidance not originally intended for showing compliance to system safety requirements.
 - Observation O3.2-A: The JATR team observed that the SSA takes credit for the probability that the aircraft will be flying in certain portions of the flight envelope, as documented in AC 25-7C. A probability of 1E-3 for the aircraft in the operational flight envelope (OFE) was used in combination with the probability of the system failure to achieve the 1E-7 minimum probability required for the “hazardous” MCAS failure condition. Use of AC 25-7C is not a standard industry approach for § 25.1309 compliance. The JATR team’s view of the intent of the probability of 1E-3 for the OFE in the HQRM is to select flight test cases for handling qualities evaluation, not to support the quantitative aspects of §§ 25.1309 or 25.672(c) compliance.
- Recommendation R3.3: The FAA should implement policy that emphasizes compliance with “safe and reliable” guidance (e.g., AC 25-22, *Certification of Transport Airplane Mechanical Systems*) for establishing minimum reliability requirements for system functions used for flight requirements demonstration in addition to the minimum reliability safety requirements defined by the FHA process.
 - Observation O3.3-A: The JATR team observed that the minimum required probability for the loss of MCAS is 1E-3 as recorded in the internal safety requirements, i.e., consistent with the “minor” classification in the FHA. “Safe and reliable” guidance for system functions used for compliance with 14 CFR part 25, subpart B requirements was not considered during development, nor required by the FAA. Because quantitative analysis for “minor” failure conditions is not required, it is unclear if the MCAS design would be considered safe and reliable

to be used as an augmentation function for compliance with flight requirements under 14 CFR part 25, subpart B.

- Recommendation R3.4: The FAA should review the natural (bare airframe) stalling characteristics of the B737 MAX to determine if unsafe characteristics exist. If unsafe characteristics exist, the design of the speed trim system (STS)/MCAS/elevator feel shift (EFS) should be reviewed for acceptability.
 - Observation O3.4-A: The original implementation of MCAS was driven primarily by its ability to provide the B737 MAX with FAA-compliant flight characteristics at high speed. An unaugmented design would have been at risk of not meeting 14 CFR part 25 maneuvering characteristics requirements due to aerodynamics.
 - Observation O3.4-B: Extension of MCAS to the low-speed and 1g environment during the flight program was due to unacceptable stall characteristics with STS only. The possibility of a pitch-up tendency during approach to stall was identified for the flaps-up configuration prior to the implementation of MCAS.
 - Finding F3.4-A: The acceptability of the natural stalling characteristics of the aircraft should form the basis for the design and certification of augmentation functions such as EFS and STS (including MCAS) that are used in support of meeting 14 CFR part 25, subpart B requirements.
- Recommendation R3.5: The FAA should review 14 CFR 25.201 (Stall Demonstration) compliance for the B737 MAX and determine if the flight control augmentation functions provided by STS/MCAS/EFS constitute a stall identification system.
 - Finding F3.5-A: The nose-down pitch identified during Boeing flight tests for stall appears to the JATR team to be the product of system augmentation with flaps and gear up, and is likely due to stabilizer motion from the MCAS function.
 - Finding F3.5-B: The FAA-accepted Boeing flight test technique of freezing column deflection at the onset of EFS was perceived by the JATR team as possibly not meeting the requirements of § 25.201 for natural stall identification from nose-down pitch, not readily arrested. Column/elevator deflection data indicates that there may be an insufficient column input to attempt to arrest the nose-down pitch created by system augmentation.
 - Finding F3.5-C: The JATR team considers that the STS/MCAS and EFS functions could be considered as stall identification systems or stall protection systems, depending on the natural (unaugmented) stall characteristics of the aircraft. From its data review, the JATR team was unable to completely rule out

the possibility that these augmentation systems function as a stall protection system.

- Recommendation R3.6: The FAA should review the use of non-standard flight test techniques, such as freezing column position at EFS actuation, when showing compliance with 14 CFR 25.201 (Stall Demonstration). The use of non-standard flight test techniques may not meet the associated regulatory requirements.
 - This recommendation is based on Findings F3.5-A, F3.5-B, and F3.5-C, above.
- Recommendation R3.7: The FAA should review how compliance was shown for the stall identification system on the B737 MAX with respect to inadvertent operation due to single failures.
 - Finding F3.7-A: The JATR team considers that system features on the B737 MAX might constitute a stall identification system. This system is vulnerable to inadvertent actuation due to a single failure, which would not meet the accepted guidance contained within AC 25-7C, Chapter 8, Section 228.
- Recommendation R3.8: The FAA should review the prescriptive use of 3 seconds under 14 CFR 25.255 (Out-of-Trim Characteristics) for the evaluation of mis-trim conditions, especially for automatic trim systems where pilot recognition is relied upon to detect and arrest runaway failures. The rate of trim used by these automatic systems should also be considered in showing compliance to § 25.255.
 - Observation O3.8-A: Out-of-trim characteristics, per the requirements of § 25.255, were found acceptable for a 0.6 unit nose-down out-of-trim condition. This out-of-trim value was determined by 3 seconds of trim input at the flaps-up main electric stabilizer trim rate of 0.2 degrees per second, which is greater than the autopilot trim rate.
 - Observation O3.8-B: The higher MCAS trim rate of 0.27 degrees per second was not selected for the demonstration of compliance with § 25.255, even though failures could result in un-commanded stabilizer trim movement at this rate.
 - Finding F3.8-A: Section 25.255 applies to jet upset events and uses a prescriptive 3 seconds as the amount of out-of-trim that could occur before pilot reaction. For automatic trim systems, the 3-second reaction time may not be appropriate, depending on the cockpit alerting philosophy and trim system architecture and controls.
- Recommendation R3.9: The FAA should review the AFM procedure for stabilizer runaway and ensure that adequate emphasis is placed on the importance of using main

electric stabilizer trim to return to a trimmed state. Crew error should be considered in the event that aisle stand stabilizer cutout switches are used before returning to trim conditions.

- Finding F3.9-A: Certain stabilizer runaway failures may generate significant out-of-trim conditions. Main electric stabilizer trim is considered the primary means to stop runaway stabilizer in Boeing's assumptions and validation tests. The degree of stabilizer mis-trim and resulting transient from steady-state flight may result in hazardous or even catastrophic failure conditions.
- Recommendation R3.10: The FAA should review the Boeing assumption of a 4-second pilot reaction time to stabilizer runaway failures to ensure that a conservative value is used, since pilot action is required to counter these failures.
 - Finding F3.10-A: Manual stabilizer trim wheel forces increase with increased speed and degree of out-of-trim condition. The degree of out-of-trim condition is dependent on pilot recognition and reaction technique and time. Manual stabilizer trim wheel forces could become significant when assumed pilot reaction times are reasonably exceeded, especially for high-speed conditions. During stabilizer runaway conditions where main electric stabilizer trim is not available, either due to system failures or the erroneous selection of stabilizer cutout switches prior to returning to trim, the crew must use the manual stabilizer trim wheel to return to a trimmed condition.
- Recommendation R3.11: For failure of the STS, the FAA should consider the requirement to alert flight crews to the reduction in safety margins due to the absence of the stability augmentation function provided by the system. Consideration should be given to AFM flight envelope limitations or warning/caution statements, if required.
 - Observation O3.11-A: STS inoperative wind-up turns were completed to 1.6g as part of the B737 MAX certification. STS inoperative stalls were completed to stick shaker + 1 second (approach to stall). The JATR team's assessment is that the limited envelope for evaluation of characteristics for this failure condition does not support the absence of an envelope limitation in the associated non-normal procedure.
 - Observation O3.11-B: STS inoperative wind-up turns, flown by Boeing during the course of the JATR, did not show any unsafe characteristics to approximately 2g.
 - Finding F3.11-A: HQRM guidance from AC 25-7C was applied for the evaluation of control systems malfunctions. The application of the probabilistic aspects of this guidance was appropriate to the determination of the required handling

qualities, but may not be suitable for evaluation of the failure condition per AC 25.1309-1A, *System Design and Analysis*, and AC 25-7C.

- Finding F3.11-B: For § 25.1309 compliance, the criticality of the failure condition should account for intensifying conditions, such as crew workload or multiple cockpit indications, and effects and interrelationship of failures with the flight envelopes.
- Finding F3.11-C: Boeing's application of HQRM allowed for a reduced envelope in the evaluation of SPEED TRIM FAIL, which may not meet the intent of guidance within AC 25-7C and AC 25-1309-1A.
- Recommendation R3.12: Because the guidance provided by the HQRM in AC 25-7D is not harmonized, the FAA should determine if continued application of HQRM is appropriate for the evaluation of failure conditions and revise the AC accordingly.
 - This recommendation is based on Observations O3.11-A and O3.11-B and Findings F3.11-A, F3.11-B, and F3.11-C, above.
- Recommendation R3.13: The FAA should ensure that simulation devices that are used for certification credit have the required level of fidelity for the associated test.
 - Observation O3.13-A: During evaluation in the Boeing engineering simulator (E-Cab), the JATR team observed that the device does not incorporate control loading on the manual stabilizer trim wheel. As a result, control forces on the manual stabilizer trim wheel are not representative of the aircraft.
- Recommendation R3.14: The FAA should review the B737 MAX's compliance to 14 CFR 25.1581 (Airplane Flight Manual – General) and address the inconsistency between AC 25.1581-1 and 14 CFR §§ 25.1581 thru 25.1587, which outline the required information to be included in the AFM and approved under § 25.1581.
 - Finding F3.14-A: Part 25 regulations require that the AFM be approved by the FAA and contain information necessary to safely operate the aircraft, including all the normal, non-normal, and emergency operating procedures. Contradictory guidance in AC 25.1581-1 has allowed Boeing AFMs to minimize the content of operating procedures that are subject to FAA scrutiny and approval. The result is that the FCOM/Quick Reference Handbook includes most of the operating procedures, in accordance with FAA guidance (AC 25.1581-1), and has become the master document for procedures to ensure safe operation. The FCOM, which is not approved by the FAA, includes systems information that is not included in the AFM. Subsequent changes to these procedures can therefore occur without

certification oversight. As a result, there is a question about whether compliance to § 25.1581 in accordance with AC 25.1581-1 for the B737 MAX meets the intent of § 25.1581.

- Recommendation R3.15: The FAA should exercise careful oversight and scrutiny of AFM procedures for Boeing aircraft.
 - This recommendation is based on Finding F3.14-A, above.
- Recommendation R3.16: The FAA should review the certification of the B737 MAX to Amendment 119 for 14 CFR 25.1329 (Flight Guidance System). If necessary, system changes should be introduced to ensure compliance and safe operations.
 - Observation O3.16-A: The B737 MAX TCDS shows that the B737 MAX complies with Amendment 119 for § 25.1329 at the whole aircraft level with no exceptions.
 - Observation O3.16-B: The B737 MAX autopilot does not automatically disconnect upon stick shaker activation. The JATR team was unable to determine how compliance was shown to Amendment 119 for § 25.1329.
- Recommendation R3.17: The FAA should review the compliance details of the optional head-up display (HUD) approved under STC on the B737 MAX and determine if its alerting meets regulatory requirements.
 - Finding F3.17-A: The JATR team was unable to determine that the third-party HUD installed at the factory follows FAA guidance in AC 25-11B, *Electronic Flight Displays*, because the team could not conclusively determine whether the HUD includes the IAS DISAGREE, ALT DISAGREE, and AOA DISAGREE alerts. Further, the HUD displays an AOA gauge but the head-down display does not display an AOA gauge unless the customer requested this option to be enabled. The alerting presented to the pilot who is using the HUD will be different from the alerting presented to the pilot who is using the head-down display.

Additional Observations

The JATR team makes the following additional observations:

- Observation O3.18-A: The high-speed MCAS function was reviewed, and for normal operation (not considering failure cases) no concerns were noted.

- Observation O3.18-B: Within the limited scope of the E-Cab session conducted by the JATR team, no unsafe conditions were noted with MCAS inoperative for high-speed wind-up turns.
- Observation O3.18-C: The certification of the fly-by-wire spoiler system, from a 14 CFR part 25, subpart B perspective, appeared to meet all related requirements.
- Observation O3.18-D: The certification of the B737 MAX for flight in icing was reviewed and judged acceptable with respect to 14 CFR part 25, subpart B requirements.

4. **Changes during the certification process**

Recommendation R4

Based on the JATR team’s observations and findings related to the FAA type certification process, JATR team members recommend that the FAA review and update the regulatory guidance pertaining to the type certification process with particular emphasis on early FAA involvement to ensure the FAA is aware of all design assumptions, the aircraft design, and all changes to the design in cases where a changed product process is used. The FAA should consider adding feedback paths in the process to ensure that compliance, system safety, and flight deck/human factors aspects are considered for the aircraft design throughout its development and certification.

Recommendation R4 is based on the following observations, findings, and supporting recommendations related to the JATR team’s review of the FAA type certification process. In achieving R4, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R4.1: The FAA should consider defining objective criteria for FAA familiarization with design details and FAA involvement in compliance findings, to be applied initially and all along the certification process, when development and certification prompt design or compliance method revision.
 - Finding F4.1-A: The JATR team finds it unclear how items to be presented to the FAA BASOO staff are selected. Other authorities have published guidelines in the matter, which typically require items to be presented to the authority based upon critically, novelty, or past experience. [Note: In the context of the B737 MAX, the JATR team’s assessment is that MCAS should have been considered a novelty (and therefore clearly highlighted to the FAA technical staff) owing to the important differences in function and implementation it has on the B737 MAX compared with the previous MCAS installed on the B767-C2 (tanker).]

- Finding F4.1-B: Although some FAA personnel may have been briefed on the MCAS function, the JATR team did not have access to the contents of such briefings to evaluate the level of information provided to the FAA. In addition, based on its review, the JATR team concluded that the content of certification deliverables would not have provided FAA technical staff with awareness of key details of the MCAS function on the B737 MAX, including architecture, signal inputs, and limits of authority.
- Finding F4.1-C: The JATR team found that the certification plans and some certification deliverables (e.g., the preliminary system safety assessment (PSSA)) were not updated to describe the expansion of the MCAS function for the low Mach portion of the flight envelope and for compliance with stall-related requirements.
- Recommendation R4.2: The FAA should consider developing policy or standards to be followed by applicants on proper visibility, clarity, and consistency of key design and compliance information that is submitted for certification, particularly with new design features.
 - Finding F4.2-A: As an amended type certificate under the Changed Product Rule (§ 21.101), many B737 MAX certification deliverables consisted of revisions to B737 NG certification documents. As a result, the MCAS description, including architecture, interfaces, logics, etc., is fragmented among several documents.
 - Finding F4.2-B: Although MCAS may have been briefed to some FAA personnel, key aspects of the MCAS function such as intended function description, its interfaces, and architecture, were not directly visible to the FAA in a straightforward manner through the certification deliverable documents.
- Recommendation R4.3: The FAA should implement policy or further guidance that emphasizes the need for early coordination with the certification authority for the FHA validation and PSSA review to ensure the proposed system architecture can reasonably meet the FHA safety requirements. In addition, the FAA should emphasize that early involvement with the certification authority is recommended for design changes.
 - Finding F4.3-A: The FAA certification process resulted in FHA/ PSSA information being submitted much too late (at type inspection authorization) for the FAA to have any influence on the proposed MCAS design for the purpose of demonstrating compliance. The FHA information that is delivered to the FAA is the FHA summary. Therefore, the FAA does not have the details of the analysis, which are documented in Boeing's internal coordination sheets (including

important FHA assumptions). FAA's visibility into important system safety information was therefore incomplete and fragmented.

- Recommendation R4.4: The FAA should refuse to accept function descriptions that are fragmented among several documents.
 - This recommendation is based on Finding F4.2-A, above.
- Recommendation R4.5: The FAA should require applicants to highlight and properly describe any functional change at the earliest stage possible in the certification process regardless of the preliminary functional hazard classification.
 - This recommendation is based on Findings F4.1-A, F4.1-B, and F4.1-C, above.
- Recommendation R4.6: The FAA should ensure applicants maintain records of interactions with certification authorities, especially if those interactions lead to agreements affecting documentation and certification deliverables.
 - Observation O4.6-A: Regarding aircraft-level safety analyses, the aircraft functional hazard assessment was included as a certification deliverable to the FAA in the "Airplane Level FHA and Development Assurance process Certification Plan" (13449 Revision F), but the aircraft safety assessment was not. The JATR team was informed that there was an agreement with the certification authorities not to include the aircraft safety assessment in the certification plan, but the team could not find the recording of such agreement outside of the agreement inherent in the acceptance of the certification plan.

5. Delegation of certification authority

Recommendation R5

Based on the JATR team's observations and findings related to FAA's oversight by the Boeing Aviation Safety Oversight Office (BASOO), JATR team members recommend that the FAA conduct a workforce review of the BASOO engineer staffing level to ensure there is a sufficient number of experienced specialists to adequately perform certification and oversight duties, commensurate with the extent of work being performed by Boeing. The workforce levels should be such that decisions to retain responsibility for finding compliance are not constrained by a lack of experienced engineers.

The FAA should review the Boeing Organization Designation Authorization (ODA) work environment and ODA manual to ensure the Boeing ODA engineering unit members (E-UMs) are working without any undue pressure when they are making decisions on behalf of the FAA. This review should include ensuring the E-UMs have open lines of communication to FAA certification engineers without fear of punitive action or process violation.

Recommendation R5 is based on the following observations, findings, and supporting recommendations related to the JATR team's review of the FAA's oversight of the Boeing ODA. In achieving R5, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R5.1: The FAA should identify and implement procedures for increased direct FAA involvement in safety critical areas of ODA certification projects. Safety critical areas may include certain regulations, reports, inspections, tests, or other critical items. Direct involvement may include the FAA retaining approvals, conducting real-time oversight, or implementing other procedures.
 - Observation O5.1-A: The FAA initially delegated acceptance of approximately 40% of the B737 MAX project's certification plans to the Boeing ODA. Additional certification plans that were originally retained for acceptance by the FAA were later delegated to the Boeing ODA as the certification project progressed. While the JATR team did not conduct an exhaustive review of other ODAs, the team observed that delegating the acceptance of certification plans does not appear to be a widespread practice for the FAA.
 - Finding F5.1-A: The FAA extensively delegated compliance findings on the B737-8 MAX project to the Boeing ODA. Safety critical areas, including system safety documents related to MCAS, were initially retained by the FAA and then delegated to the Boeing ODA. (See also Findings F4.1-A, F4.1-B, and F4.1-C.)

- Finding F5.1-B: The JATR team’s belief is that FAA involvement in the certification of MCAS would likely have resulted in design changes that would have improved safety.
- Recommendation R5.2: The FAA should conduct a workforce review of the BASOO engineer staffing level to ensure sufficient personnel to adequately perform all assigned duties (including but not limited to: certification document approval, findings of compliance, and ODA oversight).
 - Observation O5.2-A: The certification process of the B737-8 MAX was extensive and produced a large number of large documents.
 - Observation O5.2-B: The Boeing ODA organization is staffed by approximately 1,500 people, whereas the FAA’s BASOO is staffed by 45 people.
 - Finding F5.2-A: There may be a lack of capacity and depth of experience of BASOO engineering members to approve and make findings of compliance for retained items.
 - a) Out of 45 BASOO personnel, there are 18 working-level engineers and 6 senior engineers (24 engineers total). The JATR team was unable to conclusively determine the levels of experience of the working-level engineers and understands at least some of them may be entry-level engineers. Depending on the number of entry-level engineers in the BASOO, there could be an imbalance of working-level engineers in relation to the number of senior engineers reasonably expected to be required given the complexity of work by Boeing.
 - b) Depending on the number of working-level engineers who are entry-level, there could be a training burden that may further impact the capacity of senior engineers and program managers.
 - Finding F5.2-B: The allocated staffing levels of 24 BASOO engineers may not be sufficient to carry out the work associated with retained items and with the conduct of oversight duties.
 - a) BASOO engineers are required to review and find compliance for retained items as well as conduct on-site and desk audits of the Boeing ODA.
 - b) The BASOO may not be sufficiently staffed to review all the Boeing programs (737, 747, 767, 777, and 787). There are two technical staff assigned per Boeing program. Some of the technical staff are new engineers with limited airworthiness experience.

- Finding F5.2-C: BASOO engineers may not have had the technical insight, due to lack of involvement, to assess compliance.
- Recommendation R5.3: The FAA should review the Boeing work environment for E-UMs to ensure the FAA requirements for undue pressure are being complied with such that E-UMs have an acceptable environment to perform certification work on behalf of the FAA.
 - Observation O5.3-A: FAA Order 8100.15B, *Organization Designation Authorization Procedures*, paragraph 3-6, calls on ODAs to administer duties for the FAA without undue pressure or influences from other organizational segments or individuals.
 - Finding F5.3-A: There are signs of undue pressure on E-UMs performing delegated functions, which may be attributed to conflicting priorities and an environment that does not support FAA requirements.
 - Observation O5.3-B: The BASOO conducted oversight interviews of the E-UMs, resulting in a finding and associated corrective action pertaining to undue pressure.
- Recommendation R5.4: The FAA should review ODA procedures in order to remove undue burdens and barriers between the Boeing ODA and the FAA and promote cultural changes at both organizations.
 - Observation O5.4-A: The FAA is responsible for establishing the certification basis for new and changed products, including guidance to be followed. Boeing, as the applicant, was ultimately responsible for the design, compliance with the defined certification basis, and delivery of a safe product. The FAA is not able to properly perform its reviews if the technical staff is missing an adequate level of information on the proposed change.
 - Observation O5.4-B: In its review of Boeing's ODA manual and related Boeing Process Instructions, the JATR team observed that Boeing's procedures could be improved to facilitate a culture where Boeing and the FAA work together toward the common goal of safety and certification.
- Recommendation R5.5: The FAA should emphasize that the ODA system should allow for direct contact between the E-UMs and the FAA technical experts without fear of reprisal for the ODA E-UMs. The FAA should also reinforce the need for the ODA to protect the E-UMs from reprisal so that the communication is as direct and as open as possible with the FAA technical staff.
 - Finding F5.5-A: There are a number of Boeing internal procedural layers that hinder the E-UMs from directly communicating with the BASOO/FAA engineers.

If an E-UM has questions or has difficulties with a subject, the E-UM is required to first try to solve the issue within the ODA instead of directly involving the BASOO experts. Although Boeing's internal guidelines documented in D6-85963, *Guidelines for Communicating Certification Related Issues*, allow E-UMs to directly contact the FAA, this contact is for technical-only communication and only to better understand a documented FAA method of compliance. Even though the communication is allowed between the E-UM and FAA, the E-UM would have to submit a summary of the conversation to the ODA. These procedural layers may prevent "free" communication of issues/concerns to the FAA.

- Recommendation R5.6: The FAA should review all oversight corrective actions and survey results (open and closed) raised by the BASOO to identify any systemic trends in non-compliances and ensure all open findings are being actioned in the appropriate timeframe.
 - Observation O5.6-A: There have been many Boeing ODA corrective actions initiated and verified by the BASOO since 2009. These corrective actions provide 10 years of oversight findings on the Boeing ODA and are a valuable source of data to analyze and review the performance of the Boeing ODA, including any themes of recurring findings or longstanding open corrective actions.
- Recommendation R5.7: The FAA should require Boeing to submit compliance data recommending FAA approval for FAA flight test activities. Compliance data submissions should include FAA Form 8100-9, *Statement of Compliance with Airworthiness Standards*, signed by the appropriate E-UM recommending approval of the data.
 - Observation O5.7-A: For FAA flight test activities, the Boeing ODA manual specifically excludes E-UMs' use of "Recommend Approval" using FAA Form 8100-9 for FAA-retained flight test reports. This practice of the Boeing ODA not recommending approval of flight test data is inconsistent with other ODAs. The Boeing ODA manual states that Boeing will assist and submit the compliance data for approval; however, compliance data submitted by Boeing should be accompanied by FAA Form 8100-9(s) signed by the appropriate E-UM(s) recommending approval of these data.
 - Finding F5.7-A: The Boeing ODA manual refers to internal procedures documents, which the JATR team believes creates an additional and unnecessary level of complexity. This practice of referring to internal procedures is inconsistent with other ODAs, which have a single manual (standalone document) that contains all necessary information.

Integrated Approach to Development and Certification

6. *Holistic, integrated aircraft-level approach*

Recommendation R6

Based on the JATR team’s observations and findings related to the design process of the flight control system and the related system safety assessments for the B737 MAX, JATR team members recommend that the FAA promote a safety culture that drives a primary focus on the creation of safe products, which in turn comply with certification requirements. Aircraft functions should be assessed, not in an incremental and fragmented manner, but holistically at the aircraft level. System function and performance, including the effects of failures, should be demonstrated and associated assumptions should be challenged to ensure robust designs are realized. The safety analysis process should be integrated with the aircraft development assurance process to ensure all safety requirements and associated assumptions are correct, complete, and verified. The FAA should encourage applicants to have a system safety function that is independent from the design organization, with the authority to impartially assess aircraft safety and influence the aircraft/system design details. Adoption of a safety management system is one way this can be achieved.

Recommendation R6 is based on the following observations, findings, and supporting recommendations related to the JATR team’s review of the design process of the flight control system and the related SSAs for the B737 MAX. In achieving R6, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R6.1: The FAA should ensure applicants improve adherence to fail-safe design concept principles when designing or modifying systems. The FAA should encourage applicants not to design only for compliance, but also to follow basic principles to design for safety when developing or changing system functions. This should include elimination of hazards and use of design features, warnings, and procedures.
 - Observation O6.1-A: Proper flight crew action was considered an adequate mitigation to risks such as erroneous activation of MCAS.
 - Finding F6.1-A: The JATR team identified that the design process was not sufficient to identify all the potential MCAS hazards. As part of the single-channel speed trim system, the MCAS function did not include fault tolerant features, such as sensors voting or limits of authority, to limit failure effects consistent with the hazard classification.

- Finding F6.1-B: The use of pilot action as a primary mitigation means for MCAS hazards, before considering eliminating such hazards or providing design features or warnings to mitigate them, is not in accordance with Boeing’s process instructions for safe design in the conception of MCAS for the B737 MAX.
- Finding F6.1-C: The JATR team found that there was a missed opportunity to further improve the system design through the use of available fail-safe design principles and techniques presented in AC 25.1309-1A and in EASA AMC 25.1309 in the MCAS design.
- Recommendation R6.2: As part of the certification process for transport category airplanes, the FAA should examine all “major hazards” where a key mitigation is flight crew action to see if they are potentially catastrophic. The FAA should evaluate the impact of the hazard and its mitigations at the aircraft level, including the impact on the crew and cockpit environment, to determine if additional mitigating design features are required.
 - This recommendation is based on Findings F6.1-A, F6.1-B, and F6.1-C, above.
- Recommendation R6.3: The FAA should implement policies and further guidance to reinforce that all system functions that are used in flight critical functions should implement means for increased fault tolerance, such as signal health monitoring, voting means, and failure annunciation. Increased system fault tolerance should be sought to the extent practicable to accommodate unforeseen scenarios or unconfirmed assumptions during system operation.
 - This recommendation is based on Findings F6.1-A, F6.1-B, and F6.1-C, above.
- Recommendation R6.4: The FAA should implement policies and further guidance to reinforce that workload evaluations should not be limited to the areas affected by the design changes alone. Workload evaluation should be performed with the complete flight deck effects of the failure conditions, including associated procedures.
 - Finding F6.4-A: When all flight deck effects are considered, the introduction of the MCAS function invalidated aircraft-level assumptions for flight crew responses related to erroneous AOA failures under certain conditions. A complete workload assessment was not performed for validation of the erroneous AOA effects with the added MCAS functionality. The same assumptions for flight crew responses to erroneous AOA were carried over from previous programs without formal validation.

- Recommendation R6.5: The FAA should emphasize the need to perform a functional SSA. The complete system function, including interfaces and unchanged parts of the implementation, should be assessed. When adding new functions, a complete top-down safety assessment process from the aircraft level should be performed. Special emphasis should be given on exercising care for reuse of safety assessment analysis information.
 - Finding F6.5-A: An integrated SSA to investigate the MCAS as a complete function was not performed. The safety analyses were fragmented among several documents, and parts of the SSA from the B737 NG were reused in the B737 MAX without sufficient evaluation. ARP4754A section 6, for example, has guidance that should have been used, given Boeing's election to follow ARP4754A as means of compliance.
 - Observation O6.5-A: While the JATR team would not expect applicants to prepare a specific SSA for a flight control law, safety analyses should be conducted from a functional perspective. Applicants may document the safety analyses in multiple documents provided the documents are well organized and clearly record the results of the safety analyses conducted from a functional perspective.
- Recommendation R6.6: The FAA should ensure that when new functions are introduced, the applicants develop a new FHA specific to that function that is used to develop design mitigations for identified hazards.
 - Finding F6.6-A: There is a perception that the FHA reports are not used to drive the design; rather, they are used to document the design as already defined. The STS and flight control computer (FCC) FHAs were updated reports from the B737 NG, and in the JATR team's assessment, they did not appear to be used as tools to identify new hazards related to MCAS and drive design mitigations. As an example, in the hierarchy of safety solutions, mitigation by design should be prioritized over warnings and training/procedures. By documenting the as-is configuration, Boeing concluded that pilot training and procedures were sufficient to ensure safety.
- Recommendation R6.7: The FAA should encourage applicants to have a system safety function that is independent from the design organization in order to independently assess aircraft safety, and that has the authority to influence the aircraft/system design details. Such system safety function should ensure that comprehensive and integrated risk, failure, and safety analyses are performed any time a design change is made that could affect the safe operation of the aircraft. Adoption of a safety management system is one way this can be achieved.

- Observation O6.7-A: The JATR team could not identify whether Boeing has an independent safety group coordinating the systems safety analysis and their role within a development program. Each system team conducts both the design and related safety assessments. It was also noted that flight test pilots, including the chief pilot, are often used to validate key design decisions. This is not a problem, as long as the engineers have robust information, which might be an issue, considering that the system description and SSA documentation are fragmented.
- Finding F6.7-A: The Boeing analysis of erroneous MCAS activation did not adequately take into account what else might be happening at the same time, such as the possibility of an AOA failure with all its associated flight deck effects potentially distracting the crew from recognizing the trim action.
- Recommendation R6.8: Given the importance of the single & multiple failure (S&MF) analysis or equivalent in the development assurance process, the FAA should require the S&MF analysis or equivalent as a certification deliverable to demonstrate system-level integration and the effects of cascading hazards at the aircraft level.
 - Observation O6.8-A: The aircraft-level S&MF analysis was developed and used by Boeing as an internal document and not as a certification deliverable. The JATR team expects the S&MF analysis to have been a compliance artifact and provided to the FAA to demonstrate system-level integration. This was already an EASA recommendation in its certification review item CRI-F6 for the B737-8 MAX.
- Recommendation R6.9: The FAA should not accept analysis of a single “worst-case scenario” as covering all possible failure modes of the related systems. The FAA should require applicants to analyze each function to identify failure modes for each signal input considering all foreseeable scenarios and the multiple possible outcomes for each flight phase in their cascading effects analysis.
 - Observation O6.9-A: As far as AOA failures are concerned, the JATR team observed that the S&MF analysis was limited to a single worst-case scenario: loss of AOA on one side plus erroneous AOA on the other side. Other AOA failures were not evaluated because the worst-case failure modes were analyzed and the hazard analyses in the S&MF was limited to only those combined worst-case failures. Because this worst-case scenario was already considered catastrophic, the S&MF analysis was not updated after introduction of MCAS.
 - Finding F6.9-A: Evaluating worst-case scenario for the AOA failures was not adequate to identify the hazardous effects (including complete flight deck effects) of the single AOA failures.

- Observation O6.9-B: Boeing engineers did not see MCAS as “new or novel,” partly because it was already operational on the military tanker version of the B767.
- Observation O6.9-C: Boeing conducted an S&MF analysis on Revision C of the STS requirements for MCAS software, which only included high-speed values in its lookup table (as was used in the military tanker version of the B767).
- Observation O6.9-D: During Boeing flight tests, the company added low-speed values to the MCAS lookup table in its Revision D of the STS requirements for MCAS.
- Observation O6.9-E: The B737-8 MAX was certified with Revision E of the STS requirements for MCAS software.
- Observation O6.9-F: The SSA was not updated beyond Revision C of the STS requirements for MCAS. The JATR team observed no documented risk, failure, or safety analyses conducted on the MCAS software beyond Revision C.
- Observation O6.9-G: Boeing determined the high-speed regime to be the critical aspect of MCAS, and thus no revision to the SSA was necessary when the low speeds were added to the software’s lookup table.
- Observation O6.9-H: Boeing concluded that multiple erroneous MCAS activations were not worse than a single erroneous activation, based on the assumption that the crew would return the aircraft to a trimmed state (consistent with AC 25-7C guidance) following each activation.
- Recommendation R6.10: The FAA should not accept a mitigation for the single “worst-case scenario” as mitigating all possible scenarios. The FAA should ensure that mitigations are developed as appropriate for the multiple outcomes identified in the cascading effects analysis.
 - This recommendation is based on Observation O6.9-A and Finding F6.9-A, above.
- Recommendation R6.11: The FAA should require applicants to develop an SSA process description to be followed by each system for consistency of methodology, use of guidance, and assumptions.
 - Observation O6.11-A: The JATR team was unable to identify a Boeing document that provides a consistent process and methodology for the SSA process to be

followed across each system. Report templates are provided, but templates are not sufficient to ensure uniformity of analysis.

- Recommendation R6.12: The FAA should develop a practice of questioning the validity of assumptions made by the applicant and require substantive support for all such assumptions.
 - Finding F6.12-A: The JATR observed in Issue Paper G-1 that Boeing’s rationale for exceptions from current amendments for the B737 MAX was focused on similarity with the B737 NG model and the risk of confusing the pilots by introducing differences between the two models (e.g., exceptions for § 25.1322). These approaches were driven by Boeing’s assumptions that the MAX is a replacement for the NG and that MAX pilots will be experienced NG pilots. These assumptions were not warranted, as demonstrated by airlines for which the MAX was the first B737 model to be purchased (e.g., Air Canada), and by new pilots entering service directly to the MAX (e.g., the First Officer on ET302).
 - Finding F6.12-B: Basic assumptions about trained and qualified flight crew response to malfunctions used in the design and certification of the B737-8 MAX did not appear to hold in the two accident cases, based on preliminary information.

7. Human Factors

Recommendation R7

Based on the JATR team’s observations and findings related to human factors-related issues in the certification process, JATR team members recommend that the FAA integrate and emphasize human factors and human system integration throughout its certification process. Human factors-relevant policies and guidance should be expanded and clarified, and compliance with such regulatory requirements as 14 CFR §§ 25.1302 (Installed Systems and Equipment for Use by the Flightcrew), 25.1309 (Equipment, Systems, and Installations), and 25.1322 (Flightcrew Alerting) should be thoroughly verified and documented. To enable the thorough analysis and verification of compliance, the FAA should expand its aircraft certification resources in human factors and in human system integration.

Recommendation R7 is based on the JATR team’s identification of human factors-related issues in the certification process. These issues are reflected in multiple recommendations throughout the JATR’s submittal, including but not limited to Recommendations R1.3, R1.9, R2.1, R2.2, R2.4, R2.8, R2.9, R2.10, R3.8, R3.9, R3.10, R3.11, R3.13, R3.14, R3.15, R3.17, R6.2, R6.4,

R9.1, R9.6, R9.7, and R11.2. In achieving R7, JATR team members advise the FAA to also take actions that include, but are not necessarily limited to, the additional supporting recommendation below.

- Recommendation R7.1: The FAA should expand its aircraft certification resources in human factors and in human system integration to enable the thorough analysis and verification of compliance with such regulatory requirements as 14 CFR §§ 25.1302 (Installed Systems and Equipment for Use by the Flightcrew) and 25.1322 (Flightcrew Alerting).
 - Observation O7.1-A: There are very few human factors specialists in the FAA’s nationwide Aircraft Certification Organization.
 - Observation O7.1-B: The FAA has extremely limited human factors and human system integration resources in an era where most safety failures are linked to human-machine interaction.
- Recommendation R7.2: The FAA should review existing guidance material and update as necessary to emphasize the importance of human factors and human system integration throughout the certification process.
 - Observation O7.2-A: Existing human factors guidance material (e.g., AC 25-1302-1) may be insufficient to emphasize the importance of human factors and human system integration throughout the certification process. (See also Observations O2.1-A and O2.2-A and Findings F2.2-A and F6.4-A)

8. Development assurance

Recommendation R8

Based on the JATR team’s observations and findings related to the development assurance process applied to the design of the flight control system of the B737 MAX, JATR team members recommend that the FAA ensure applicants apply industry best practice for development assurance, including requirements management, visibility of assumptions, process assurance activities, and configuration management. The FAA should ensure achievement of the close coupling that is required between the applicant safety analysis process and the development assurance process to classify failure conditions and derive the level of rigor of design development and verification. A current example of industry best practice is SAE International’s Aerospace Recommended Practice 4754 (ARP4754).

The FAA should review and amend Advisory Circular 20-174 to clearly articulate the principles of ARP4754, promoting industry best practice for development assurance of

aircraft and aircraft systems to address applicants' design trend of increasing integration between aircraft functions and systems.

Recommendation R8 is based on the following observations, findings, and supporting recommendations related to the JATR team's review of the Boeing development assurance process applied to the design of the flight control system of the B737 MAX. In achieving R8, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R8.1: The FAA, as part of the BASOO oversight activities, should review the Boeing development assurance process to ensure industry best practice for development assurance is being followed for an integrated approach to design changes at the aircraft, system, subsystem and item levels. Developing internal procedures to more robustly meet the objectives of ARP4754A and the adoption of Dynamic Object-Oriented Requirements System (DOORS) to manage all requirements is one way to achieve this integrated approach.
 - Observation O8.1-A: The Boeing development assurance process was agreed to by the FAA via Issue Paper SA-1; however, the process was not aligned to industry best practice for integrated systems.
 - a) Section 3 of the B737 MAX Development Assurance Compliance Plan D925A003-01 states that the development assurance process meets the objectives of ARP4754A; however, the JATR found numerous instances where the development assurance process does not satisfy the objectives of ARP4754A for an integrated approach to design.
 - b) Not all requirements are traceable, and assumptions are managed independent of requirements.
 - c) Boeing attempted to apply ARP4754A methodology to the B737 MAX, however the benefits could not be fully realized as the application was limited to changed areas. The retirement of older design provides opportunities to use more fulsome assurance methods.
 - Observation O8.1-B: The JATR team's assessment is that Boeing's integration of the design and safety analysis is heavily reliant on the use of the chief pilot or test pilot to perform development assurance integration functions at the aircraft level.
 - a) It is not clear to the JATR team how pilot verification and validation activities are captured within an integrated approach to design development.

- b) It is not clear to the JATR team how discipline specialists are identified for assessment of a design change after regression testing has been completed, or how these specialists provide assistance to an aircraft-level integrated assessment.
 - Finding F8.1-A: The Boeing development assurance process, as applied to the B737 MAX, can be improved to more robustly meet the objectives of ARP4754A for an integrated approach to design – specifically, the integration of more complex systems and software into legacy aircraft.
 - Recommendation R8.2: The FAA, as part of the BASOO oversight activities, should review the Boeing safety analysis process, including how candidate items are identified for the S&MF analysis, to ensure hazards are assessed in an integrated manner across systems and subsystems, and all credible hazards are identified for assessment at the aircraft level.
 - Observation O8.2-A: The Boeing safety analysis process is not fully aligned with the development assurance process.
 - a) Documenting identified risks and mitigating only the “worst-case scenario” does not necessarily identify all critical failure modes, particularly when the interaction between related systems is not considered.
 - b) Requirements-based testing and intended-function testing may not adequately capture cascading failure conditions if the S&MF candidate item list does not adequately document a complete set of hazards.
 - Finding F8.2-A: The Boeing safety analysis process, as applied to the B737 MAX, can be improved to be more integrated with the development assurance process at the aircraft, system, subsystem, and item levels.
 - Recommendation R8.3: The FAA, as part of the BASOO oversight activities, should review the Boeing safety analysis process and ensure it is aligned with the Boeing development assurance process to meet the objectives of ARP4754A. A more robust alignment between these two processes will ensure completeness of hazard identification in the S&MF candidate list, identification of all critical failure modes, and incorporation of the mitigations into the design.
 - This recommendation is based on Observation O8.2-A and Finding F8.2-A, above.
 - Recommendation R8.4: The FAA, as part of the BASOO oversight activities, should review the Boeing process for managing assumptions to ensure assumptions are visible

throughout the development assurance and safety analysis processes. Increased visibility includes the integrated reassessment of assumptions to ensure that associated hazards are appropriately identified and remain valid and that the design complies with functional and safety requirements derived from assumptions.

- Observation O8.4-A: The JATR team’s assessment is that the approach taken to record assumptions in coordination sheets (and not DOORS) results in a loss of visibility of assumptions through the development assurance process. The assumptions listed in the coordination sheet are not directly visible to system-level requirements, and there is no obvious feedback loop to ensure these assumptions remain valid throughout the development process.
- Recommendation R8.5: The FAA, as part of the BASOO oversight activities, should ensure Boeing implements a more iterative approach to verify and validate requirement functional dependencies and assess the interaction between hazards identified at the system level and the aircraft level. Such an approach would increase the involvement of system safety specialists, human factors specialists, and pilots to perform independent reviews of potential hazard impacts at the aircraft level. This independent review would supplement and inform the aircraft-level development assurance integration activities carried out by the Boeing chief pilot/test pilot.
 - Finding F8.5-A: An opportunity exists for Boeing to adopt an integrated approach for requirements management through use of requirements management tools like DOORS for all requirements. This will improve the robustness of requirements management and verification and validation activities.
 - a) While the JATR team observed that Boeing had managed requirements through a number of different processes, this does not meet the objectives of ARP4754A for an integrated approach to requirements management.
 - b) The process assurance checklist for requirements identified as “Alternate MoC” and “Alternate MoC Plus” may not be sufficient to address the integration effects of the design change.
 - c) Adopting an integrated approach using a requirements management tool like DOORS will allow airworthiness authorities and delegated persons/designees to easily and independently review findings of compliance and understand the interrelationships between systems to ensure completeness of certification activities.

- Finding F8.5-B: Establishing requirements baselines at system and subsystem levels will assist configuration management of requirements throughout the development assurance process.
 - a) The process to establish a requirements baseline should be aligned to the configuration management process.
 - b) At a minimum, the establishment of baselines for requirements identified as “safety” will facilitate increased control of these requirements throughout the development assurance process.
- Observation O8.5-A: DOORS information notes observed by the JATR team read like requirements and were reportedly identified in the coordination sheet but were not identified in DOORS as a requirement to be verified.
- Recommendation R8.6: The FAA, as part of the BASOO oversight activities, should ensure Boeing improves the system architecture used for requirements management. This includes expanding the use of a requirements management tool, such as DOORS, to manage all requirements to improve the integration of system- and item- level requirements to other systems and items and also to parent aircraft-level requirements.
 - This recommendation is based on Observation O8.5-A and Findings F8.5-A and F8.5-B, above.
- Recommendation R8.7: To the extent applicants rely on original aircraft- and system-level assumptions, the FAA should ensure the applicants perform a thorough review of system design changes to ensure they are not inconsistent with those assumptions.
 - This recommendation is based on Finding F6.4-A, above.
- Recommendation R8.8: The FAA should emphasize in guidance that, besides requirements-based testing, the applicant should perform robustness test cases for identifying and investigating unexpected system effects and flight crew responses. For example, the process should account for evaluation of cases where pilots do not follow the assumptions (e.g., not trimming out the failure).
 - This recommendation is based on Finding F6.4-A, above.
- Recommendation R8.9: The FAA should develop, validate, and implement design and analysis models, methodologies, and approaches capable of identifying interactions among systems such as the catastrophic interaction between the AOA system and MCAS.
 - Observation O8.9-A: FAA Order 8110.48A, *How to Establish the Certification Basis for Changed Aeronautical Products*, provides the following guidance in

paragraph 2-1: “Essentially, a substantial design change is an alteration to a product that is so extensive that the design models, methodologies, and approaches used to demonstrate a previous compliance finding cannot be used.”

- Finding F8.9-A: The B737-8 MAX accident scenarios were not identified during the testing and certification process. This is an indication that the “design models, methodologies, and approaches” used to demonstrate compliance need improvement to identify interactions among systems.
- Recommendation R8.10: The FAA should review AC 20-174 to ensure that expectations for a holistic aircraft-level design assurance practice for transport category aircraft is achieved which includes consideration of all systems (including safety) requirements and assumptions. In particular, the AC should address how credit can be given for traditional techniques for simple deterministic systems within a structured methodology.
 - Finding F8.10-A: AC 20-174 does not provide clear and unambiguous guidance for the application of ARP4754A to Part 25 Aircraft.
 - Observation O8.10-A: AC 20-174 provides for limited application of the development assurance process “where traditional techniques have been shown to be acceptable for more traditional systems designs.”
 - a) Not requiring the more structured techniques be applied as indicated in AC 20-174 may result in misinterpretation that the structured methodology would not be required. This is not the expectation of the ARP4754A.
 - b) There is no definition provided within AC 20-174 to identify what constitutes a “traditional systems design” or “traditional techniques.”
 - c) Previous design practice considered as “traditional” did not include the design assurance processes rigor provided by ARP4754A. The process is expected to identify, validate, and verify all system requirements including safety requirements and would include identification and disposition of all assumptions.
- Recommendation R8.11: The FAA should ensure applicants provide a full list of all aircraft proposed changes (no matter how trivial), complete with a system description and all interfaces associated with each proposed change, such that an informed assessment can be made using established criteria prior to agreeing on the systems which will be subject to limited application of a development assurance process.
 - Finding F8.11-A: The practice of applying a limited application of a development assurance process for modifications to aircraft or systems can be improved –

specifically, the criteria used to assess each proposed modification and the requirement to satisfy safety assessment objectives.

- Observation O8.11-A: The limited application of a development assurance process agreed between the FAA and Boeing did not adequately establish the criteria for determining which new or modified systems require certification compliance findings relative to development assurance.
 - a) Each candidate system should be critically assessed against a robust set of criteria.
 - b) Criteria should be informed by the objectives and requirements of ARP4754A.
 - c) The FAA should be provided with sufficient insight into the modifications to make an informed assessment of each proposed modification against the established criteria.
 - d) The rationale and decisions resulting from this assessment should be documented.
- Recommendation R8.12: The FAA should ensure that agreement of any limited application of a development assurance process includes the requirement for the applicant's safety analysis processes to satisfy the ARP 4754A safety assessment objectives.
 - Observation O8.12-A: The limited application of a development assurance process agreed between the FAA and Boeing did not adequately consider the applicant's safety analysis process and how that integrates with the tailored development assurance process for complex and integrated systems.
 - a) The FAA's participation in system reviews did not result in ensuring Boeing's process was equivalent to ARP4754A.
 - b) The expectation that safety requirements be considered within the design assurance process was not realized.
 - c) ARP4754A Section 6 provides the necessary guidance for modifications to aircraft or systems.
 - d) ARP4754A Section 5.1 details the objectives of the safety assessment process regarding analysis of functional interactions and interdependencies.

Impact of Design Changes on Operations and Training

9. Impact of Product Design Changes on Operations

Recommendation R9

Based on the JATR team's findings and observations related to the operational design assumptions of crew response applied during the certification process for the flight control system of the B737 MAX, JATR team members recommend that the FAA require the integration of certification and operational functions during the certification process. The FAA should be provided all system differences between related aircraft in order to adequately evaluate operational impact, systems integration, and human performance.

Recommendation R9 is based on the following observations, findings, and supporting recommendations related to the JATR team's review of the operational design assumptions of crew response that Boeing applied during the certification process for the B737 MAX. In achieving R9, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R9.1: The FAA should revise AC 120-53B and FAA Order 8900.1 Volume 8, Chapter 2 to include an assessment of the cumulative effects of changed products, such as differences in aircraft systems, displays, flight characteristics, and procedures.
 - Observation O9.1-A: AC 120-53B does not require the cumulative effects on system changes to be considered.
 - Observation O9.1-B: Boeing submitted to the FAA's AEG a list of features of the B737 MAX cockpit which were changed from the base model B737-800. In Issue Paper O-1, *Type Rating Determination and 14 CFR Training Requirements*, the FAA raised concerns about cumulative effects of system changes from the B737 NG to the B737 MAX that may cause greater than level B differences training. Boeing's response to this concern was that there was no precedent in prior Boeing amended type certification projects and that AC 120-53B did not require the cumulative effects on system changes to be considered. The FAA accepted Boeing's response on 26 January 2016.
- Recommendation R9.2: The FAA should review and if necessary revise AC 120-53B to ensure that the AEG and FSB are provided with all the system differences between related aircraft irrespective of engineering determination of the safety significance.

- Observation O9.2-A: Issue Paper O-6 and FAA Order 8110.4C articulate AEG’s responsibility, among other things, to address Flight Standards considerations such as contribution of operational perspective to engineering activities during the type certification process. The Order specifically requires AEG’s early involvement in the certification process starting at the requirements definition phase of the system’s life-cycle.
- Finding F9.2-A: The limited information provided to the FSB limited their ability to assess the operational impacts of failures of systems associated with MCAS and the subsequent requirements for flight crew training. With the information AEG was provided, it is reasonable to conclude that the FSB would not know the full impact of the changed design and thus would be unaware that they had been provided insufficient information to adequately comply with the requirements in FAA Order 8110.4C.
- Recommendation R9.3: Where the assessment of the effectiveness of differences training is not conducted in an aircraft, the FAA should require the AEG to use operational flight crew complements (e.g., line captains and line first officers), with a range of flight experience, as part of the assessment.
 - Observation O9.3-A: To be consistent with §§ 25.671 and 25.672, and to comply with the guidance in AC 25-7C, Boeing utilized four fundamental assumptions on crew actions in the flight control FHA for the B737 MAX and other Boeing models. The third assumption, taken from AC 25-7C, stated: “The pilot will take immediate action to reduce or eliminate high control forces by re-trimming or changing configuration or flight conditions.”
 - Finding F9.3-A: Based on the JATR team’s review of preliminary accident information, in both aircraft accidents the flight crew did not appear to meet the “immediate action” assumption. This assumption makes no allowance for differing training and certification requirements for flight crew operating under other CAAs. The FAA requires an air transport license with 1,500 hours experience before being employed by a Part 121 operator. Other CAAs have no such requirement, with co-pilots required only to have a commercial pilot’s license.
- Recommendation R9.4: The AEG should have deeper involvement during the certification process and collaborate closely with FAA’s Aircraft Certification Service (AIR) to ensure they have the proper knowledge to make informed decisions about operational suitability issues that may be affected by certification details.

- Observation O9.4-A: Pilots working in the certification process may not have complete knowledge of operational issues, while pilots working in the operational evaluation process may not have complete knowledge of certification issues. This may contribute to a lack of communication between the two processes.
- Finding F9.4-A: Communication of MCAS functionality between certification and AEG was not sufficiently robust for AEG to fully understand MCAS implications in an operational environment.
- Recommendation R9.5: The FAA should conduct a study to determine the value of AEG pilots receiving familiarization training to enhance their understanding of certification flight tests.
 - This recommendation is based on Observation O9.4-A and Finding F9.4-A, above.
- Recommendation R9.6: The FAA should review and if necessary revise AC 25.1302-1, *Installed Systems and Equipment for Use by the Flightcrew*, to ensure that failures of related systems are assessed taking into account human performance and the operational environment utilizing an AEG operational specialist.
 - Observation O9.6-A: A review of preliminary accident reports KNKT.18.10.35.04 and AI-0/19 indicates that the complex operational environment that faced the flight crews and the associated workload may not have been anticipated in the certification process.
 - Finding F9.6-A: AC 25.1302-1 does not adequately address the operational aspect of an aircraft's design.
 - Finding F9.6-B: AC 25.1302-1, paragraph 1-2(a), Applicability, lists a number of certification roles that the guidance is directed toward, and the list does not include an operational pilot specialist such as an aviation safety inspector from the AEG.
- Recommendation R9.7: The FAA should review and if necessary revise guidance material to ensure that operational considerations associated with the design change are adequately risk-assessed to minimise the potential for flight crew error.
 - This recommendation is based on Observation O9.6-A and Findings F9.6-A and F9.6-B, above.

10. Impact of product design changes on flight crew training

Recommendation R10

Based on the JATR team's findings and observations related to flight crew training, JATR team members recommend that the FAA require a documented process to determine what information will be included in the Airplane Flight Manual, the Flight Crew Operating Manual, and the Flight Crew Training Manual. The FAA should review training programs to ensure flight crews are competent in the handling of mis-trim events.

Recommendation R10 is based on the following observations, findings, and supporting recommendations related to the JATR team's review of the FCOM, FCTM, and AFM developed during the certification process for the B737 MAX. In achieving R10, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R10.1: The FAA should include in the FSB report the flight experience level and qualification of the flight crew used to assess the effectiveness of the differences training.
 - Finding F10.1-A: Boeing's test pilots are not a representative sample of the operators' pilot population.
 - Finding F10.1-B: The AEG pilots are not a representative sample of the operators' pilot population.
 - Finding F10.1-C: A validation flight conducted under AC 120.53B is conducted with an experienced line captain in the left seat, and includes an experienced flight test pilot in the right seat as a safety pilot.
 - Finding F10.1-D: The AEG's evaluation flights do not evaluate crew performance and do not represent operators' pilots' experience level or operation.
 - This recommendation is also based on Observation O9.3-A and Finding F9.3-A, above.
- Recommendation R10.2: The FAA should review the B737 MAX type rating training program to include training in the operation of the manual stabilizer trim wheel throughout the speed range.

- Observation O10.2-A: A review of preliminary accident reports KNKT.18.10.35.04 and AI-0/19 indicates both flights suffered an extreme mis-trim event which involved the activation of the MCAS function.
- Finding F10.2-A: A review of the B737 MAX type rating training syllabus indicates that, although exercises are conducted in the flight simulator to address a STAB TRIM runaway, the syllabus does not specifically address awareness of airspeed versus the forces required to manually trim the aircraft and to recognize and correct a mis-trim state.
- Recommendation R10.3: The FAA should require operators of the B737 to include operation of the manual stabilizer trim wheel throughout the speed range in their recurrent training programs.
 - This recommendation is based on Observation O10.2-A and Finding F10.2-A, above.
- Recommendation R10.4: The FAA should add a special emphasis training item to the B737 FSB Report to include training in the operation of the main electric stabilizer trim and the manual stabilizer trim wheel and recovery from a mis-trim state throughout the speed range.
 - This recommendation is based on Observation O10.2-A and Finding F10.2-A, above.
- Recommendation R10.5: The FAA should develop a documented process to determine what information will be included in the AFM, FCOM, and FCTM. The process must include agreement from all disciplines (e.g., certification, operations, maintenance, human factors) for the system or function descriptions to be removed.
 - Observation O10.5-A: Information related to the MCAS functionality within the FCC originally was in the draft FCOM and was subsequently removed (around the time of MCAS Revision D, in early 2016), but without a formal process in place to ensure agreement from all disciplines on the removal of that information. Technology, even if it functions without pilot involvement, may be integrated with other aircraft systems. One system or functional failure could impact other systems requiring pilot involvement.
 - Finding F10.5-A: Information related to MCAS functionality and failure scenarios is critical for pilot knowledge and understanding of the system as it interfaces with the aircraft's trim system and AOA inputs.

- R10 is also supported by Recommendation R3.14 and accompanying Finding F3.14-A, and by Recommendation R9.2 and accompanying Observation O9.2-A and Finding F9.2-A, above.

11. Impact of product design changes on maintenance training

Recommendation R11

JATR team members recommend that the FAA conduct a study to determine the adequacy of policy, guidance, and assumptions related to maintenance and ground handling training requirements.

In furtherance of R11, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R11.1: The FAA should conduct a study to focus on adequacy of maintenance and ground handling differences training requirements for transport category aircraft.
 - Observation O11.1-A: JATR tasking included assessing the adequacy of policy/guidance and assumptions related to training of mechanics and ground handlers for new and related aircraft. The B737 MAX Maintenance Review Board Chairman briefed the JATR team. The JATR team solicited an AEG maintenance specialist that was not associated with the B737 MAX certification activities for discussion.
 - Finding F11.1-A: The JATR team was unable to make a determination of the adequacy of policy/guidance and assumptions related to training of mechanics and ground handlers for new/related aircraft.
- Recommendation R11.2: The FAA should develop regulatory requirements to consider and mitigate potential errors by maintenance technicians and by ground handling personnel as part of the certification process of a product.
 - Observation O11.2-A: Section 25.1302 requires applicants to consider and mitigate potential flight crew errors.
 - Observation O11.2-B: There are no aircraft-level regulatory requirements, equivalent to § 25.1302, to consider and mitigate potential errors by maintenance technicians or by ground handling personnel.

- Observation O11.2-C: Maintenance and ground handling errors have contributed to several accidents and multiple incidents, and maintenance issues might also be relevant to the Lion Air B737 MAX accident based on the preliminary report.

Post-Certification Activities

12. Post-Certification Corrective Actions and Data Sharing

Recommendation R12

JATR team members recommend that the FAA review its policies for analyzing safety risk and implementing interim airworthiness directive action following a fatal transport aircraft accident. The FAA should ensure that it shares post-accident safety information with the international community to the maximum extent possible.

Recommendation R12 is based on the following observations, findings, and supporting recommendations. In achieving R12, JATR team members advise the FAA to take actions that include, but are not necessarily limited to, the supporting recommendations below.

- Recommendation R12.1: The FAA should review FAA Order 8110.107A, *Monitor Safety/Analyze Data*, and consider reducing the control program risk guideline for post-accident corrective action if a catastrophic fatal accident of a transport category aircraft has occurred. For example, the allowable FAA Monitor Safety/Analyze Data (MSAD) guidelines for control program fleet risk for the related corrective action could be reduced to between 10% and 25% of their normal values.
 - Observation O12.1-A: The FAA uses the MSAD process, Order 8110.107A, to manage potential safety issues. If an unsafe condition is discovered, the FAA uses the MSAD process to assess the adequacy of the timeline to implement a corrective action (the airworthiness directive (AD) compliance time) using quantitative risk analysis. The FAA compares the calculated control program fleet and individual risk to an allowable risk guideline.
 - Observation O12.1-B: Most of the safety issues assessed and managed using the MSAD process are triggered by in-service data, production escapes, or engineering discoveries. Actions taken in response to these precursors, through use of the MSAD process, generally proactively prevent a fatal accident from occurring.
 - Finding F12.1-A: It is evident that the impact of a second fatal transport aircraft accident due to the same cause far exceeds the impact of the first. When the MSAD process is initiated due to a fatal transport accident, there should be lower

risk tolerance for a second accident and the control program fleet risk guideline should be reduced.

- Recommendation R12.2: The FAA, in harmonization with other CAAs, should review the airworthiness directive processes to determine the need and proper intervals for a flight crew pre-flight briefing when an interim action AD mandates an existing AFM procedure or mandates a revision to the AFM to address a major contributing factor to a catastrophic fatal accident of a transport category aircraft.
 - Observation O12.2-A: After a catastrophic fatal accident, an interim corrective action is often issued to prevent a second accident. Sometimes flight crew procedural changes are used, and the interim action AD requires a revision to the AFM.
 - Finding F12.2-A: Flight crew procedural changes can be ineffective. After the Helios Airways Flight 522 accident in 2005, the FAA issued AD 2006-13-13 that required a flight crew recall item: if the altitude warning horn sounds, don the oxygen masks. After issuance of the AD, an FAA inspector was performing an enroute inspection of a major U.S. airline B737 flight crew when the altitude warning horn sounded. Despite the AFM revision, the crew did not don their masks as required.¹²
 - Finding F12.2-B: A method to increase the effectiveness of a flight crew procedural change is to require that the AFM revision be part of a pre-flight briefing. Having briefed a procedure, the crew is more likely to remember and perform the procedure correctly if the need arises during flight. This briefing could be performed less frequently than every flight, for example before the first flight of the day or other suitable interval.
- Recommendation R12.3: Where the FAA assigns responsibility for continued operational safety oversight of a product to a different FAA office than the one that conducted oversight of the type certification, the agency should ensure that it has sufficient mechanisms in place for the transfer of requisite technical knowledge about the design to the responsible office.
 - Observation O12.3-A: The FAA BASOO is responsible for overseeing the Boeing ODA and certification of Boeing products, while the Seattle Aircraft Certification Office (SACO) is responsible for overseeing continued operational safety management of Boeing products once they are certificated. This transfer of

¹² After the FAA issued AD 2006-13-13, it received continuing reports of in-service events involving failure of the flight crew to recognize and react properly to valid cabin altitude warning horns. Therefore, the FAA issued AD 2008-23-07 that required a new flight crew briefing before the first flight of the day and following any change in flight crewmembers, in addition to the existing AFM procedures.

responsibility after the product is certificated was not a review area of the JATR team, but the team assumes the transfer may involve familiarizing and/or briefing SACO staff on design details.

- Observation O12.3-B: Some details, such as the system safety analyses related to the MCAS function, were fragmented among several documents for the B737 MAX. This could hinder the successful transfer of information to the SACO for the purpose of overseeing the continued operational safety management of the product.
- Recommendation R12.4: The FAA should review its safety information sharing policy to ensure that it shares technical safety information with other CAAs to the maximum extent possible. Maximum sharing of such information would enhance safety and minimize incorrect speculation by parties that are not participants in an ongoing accident investigation.
 - Observation O12.4-A: As a participant in an accident investigation conducted by another State, the FAA is obligated under International Civil Aviation Organization (ICAO) Annex 13, *Aircraft Accident and Incident Investigation*, not to divulge information on the progress and the findings of the investigation without the express consent of the State conducting the investigation.
 - Observation O12.4-B: A benefit of participating in an accident investigation as the State of Design is that it allows risks to be addressed by the State of Design as quickly as possible.¹³ Unfortunately, due to constraints on the flow of information from the design state and other CAAs, the third-party CAAs are reliant on the State of Design to act in their interest. The State of Design will apply their own risk processes as influenced by their regulatory and cultural environment. Delays or absence of authoritative and consistent communication results in the outside party's speculation.
 - Observation O12.4-C: ICAO Annex 13 also recommends that, "States should promote the establishment of safety information sharing networks among all users of the aviation system and should facilitate the free exchange of information on actual and potential safety deficiencies."
 - Finding F12.4-A: Restrictions on the flow of safety information impacted the capacity and efficiency of the JATR under the umbrella of, "the accidents are still under investigation."

¹³ Part 21 defines "State of Design" as "the country or jurisdiction having regulatory authority over the organization responsible for the design and continued airworthiness of a civil aeronautical product or article." 14 CFR 21.1(b)(8).

STATEMENT OF CHESLEY B. “SULLY” SULLENBERGER III

Subcommittee on Aviation of the The United States House Committee on Transportation and Infrastructure

June 19, 2019

Thank you, Chairman Larsen, Ranking Member Graves, Chairman DeFazio, Ranking Member Graves, and other members of the committee. It is my honor to appear today before the Subcommittee on Aviation.

We are here because of the tragic crashes within five months of Lion Air 610 and Ethiopian 302, two fatal accidents with no survivors on a new aircraft type, something that is unprecedented in modern aviation history.

Like most Americans and many others around the world I'm shocked and saddened by these two awful tragedies and the terrible loss of life. Now we have an obligation to find out why these tragic crashes happened, and keep them from ever happening again.

These crashes are demonstrable evidence that our current system of aircraft design and certification has failed us.

We don't yet know in every way how it has failed us. Multiple investigations are ongoing. We owe it to everyone who flies to find out where and how the failures occurred, and what changes must be made to prevent them from happening in the future.

It is obvious that grave errors were made that have had grave consequences, claiming 346 lives.

The accident investigations of these crashes will not be completed for many months, but some things are already clear.

Accidents are the end result of a causal chain of events, and in the case of the Boeing 737 MAX, the chain began with decisions that had been made years before, to update a half-century-old design.

Late in the flight testing of the 737 MAX, Boeing discovered an aircraft handling issue. Because the 737 MAX engines were larger than the engines on previous 737 models they had to be mounted higher and farther forward for ground clearance, which reduced the aircraft's natural aerodynamic stability in certain conditions. Boeing decided to address the handling issue by adding a software feature, Maneuvering Characteristics Augmentation System (MCAS), to the 737 MAX. MCAS was made autonomous, able in certain conditions to move a secondary flight control by itself to push the nose down without pilot input.

In adding MCAS, Boeing added a computer-controlled feature to a human-controlled airplane but without also adding to it the integrity, reliability and redundancy that a computer-controlled system requires.

Boeing also designed MCAS to look at data from only one Angle of Attack (AOA) sensor, not two. One result of this decision was that it allowed false data from a single sensor to wrongly trigger the activation of MCAS, thus creating a single point of failure. A single point of failure in an aircraft goes against widely held aircraft design principles.

On both accident flights, the triggering event was a failure of an AOA sensor. We do not yet know why the AOA sensors on these flights generated erroneous information, triggering MCAS, whether they were damaged, sheared off after being struck, were improperly maintained or repaired, or for some other reason.

Boeing designers also gave MCAS too much authority, meaning that they allowed it to autonomously move the horizontal stabilizer to the full nose-down limit.

And MCAS was allowed to move the stabilizer in large increments, rapidly and repeatedly until the limit was reached. Because it moved stabilizer trim intermittently, it was more difficult to recognize it as a runaway trim situation (an uncommanded and uncontrolled trim movement emergency), as appears to have happened in the first crash.

Though MCAS was intended to enhance aircraft handling, it had the potential to have the opposite effect; being able to move the stabilizer to its limit could allow the stabilizer to overpower the pilots' ability to raise the nose and stop a dive toward the ground. Thus it was a trap that was set inadvertently during the aircraft design phase that would turn out to have deadly consequences.

Obviously Boeing did not intend for this to happen. But to make matters worse, even the existence of MCAS, much less its operation, was not communicated to the pilots who were responsible for safely operating the aircraft until after the first crash.

Also with the MAX, Boeing changed the way pilots can stop stabilizer trim from running when it shouldn't. In every previous version of the 737, pilots could simply move the control wheel to stop the trim from moving, but in the MAX, with MCAS activated, that method of stopping trim no longer worked. The logic was that if MCAS activated, it had to be because it was needed, and pulling back on the control wheel shouldn't stop it.

It is clear that the original version of MCAS was fatally flawed and should never have been approved.

It has been suggested that even if the MCAS software had flaws, the pilots on these flights should have performed better and been able to solve the sudden unanticipated crises they faced. Boeing has even said

that in designing MCAS they did not categorize a failure of MCAS as critical because they assumed that pilot action would be the ultimate safeguard.

We owe it to everyone who flies, passengers and crews alike, to do much better than to design aircraft with inherent flaws that we intend pilots will have to compensate for and overcome.

Pilots must be able to handle an unexpected emergency and still keep their passengers and crew safe, but we should first design aircraft for them to fly that do not have inadvertent traps set for them.

We must also consider the human factors of these accidents.

From my 52 years of flying experience, and my many decades of safety work – I know that nothing happens in a vacuum, and we must find out how design issues, training, policies, procedures, safety culture, pilot experience and other factors affected the pilots' ability to handle these sudden emergencies, especially in this global aviation industry.

Dr. Nancy Leveson, of the Massachusetts Institute of Technology, has a quote that succinctly encapsulates much of what I have learned over many years: "Human error is a symptom of a system that needs to be redesigned."

These two recent crashes happened in foreign countries, but if we do not address all the important issues and factors, they can and will happen here. To suggest otherwise is not only wrong, it's hubris.

As one of our preeminent human factors scientists, Dr. Key Dismukes, now retired as Chief Scientist for Human Factors at the NASA Ames Research Center, has said, "Human performance is variable and it is situation-dependent."

I'm one of the relatively small group of people who have experienced such a sudden crisis – and lived to share what we learned about it. I can tell you firsthand that the startle factor is real and it is huge – it interferes with one's ability to quickly analyze the crisis and take effective action.

Within seconds, these crews would have been fighting for their lives in the fight of their lives.

These two accidents, as well as Air France 447 which crashed in the South Atlantic in June 2009, are also vivid illustrations of the growing level of interconnectedness of devices in aircraft. Previously, with older aircraft designs, there were mostly stand-alone devices, in which a fault or failure was limited to a single device that could quickly be determined to be faulty and the fault remain isolated. But with integrated cockpits and data being shared and used by many devices, a single fault or failure can now have rapidly cascading effects through multiple systems, causing multiple cockpit alarms, cautions and warnings, which can cause distraction and increase workload, creating a situation that can quickly become ambiguous, confusing and overwhelming, making it much harder to analyze and solve the problem.

In both 737 MAX accidents, the failure of an AOA sensor quickly caused multiple instrument indication anomalies and cockpit warnings. And because in this airplane type the AOA sensors provide information to airspeed and altitude displays, the failure triggered false warnings simultaneously of speed being too low and also of speed being too fast. The too slow warning was a 'stick-shaker' rapidly and loudly shaking the pilot's control wheel. The too fast warning was a 'clacker', another loud repetitive noise signaling overspeed. These sudden loud false warnings would have created major distractions and would have made it even harder to quickly analyze the situation and take effective corrective action.

I recently experienced all these warnings in a 737 MAX flight simulator during recreations of the accident flights. Even knowing what was going to happen, I could see how crews could have run out of time and altitude before they could have solved the problems.

Prior to these accidents, I doubt if any U.S. airline pilots were confronted with this scenario in simulator training.

We must make sure that everyone who occupies a pilot seat is fully armed with the information, knowledge, training, skill, experience and judgment they need to be able to be the absolute master of the aircraft and all its component systems, and of the situation, simultaneously and continuously throughout a flight.

As aviation has become safer, it has become harder to avoid complacency. We have made air travel so safe and routine, some have assumed that because we haven't had a lot of accidents in recent years we must be doing everything right.

But we can no longer define safety solely as the absence of accidents. We must do much more than that; we must be much more proactive than that.

We need to proactively find flaws and risks and mitigate them before they lead to harm.

We must investigate accidents before they happen.

Each aircraft manufacturer must have a comprehensive safety risk assessment system that can review an entire aircraft design holistically, looking for risks, not only singly, but in combination.

We must also look at the human factors and assumptions made about human performance in aircraft design and certification, and pilot procedure design.

In addition to fixing MCAS in a way that resolves all the many issues with it, including that the AOA Disagree light be made operative on all Max aircraft, we must greatly improve the procedures to deal with uncommanded trim movement, provide detailed system information to pilots that is more complete, give pilots who fly the 737 MAX additional Level D full flight simulator training so that they will see, hear, feel, experience and understand the challenges associated with MCAS, such as Unreliable Airspeed, AOA Disagree, Runaway Stabilizer and Manual Trim. They must have the training opportunity to understand how higher airspeeds greatly increase the airloads on the stabilizer, making it much more difficult to move manually, often requiring a pilot to use two hands, or even the efforts of both pilots to move it. And in some cases, how it cannot be moved at all unless the pilot flying temporarily stops trying to raise the nose and relieves some of the airloads by moving the control wheel forward.

Pilots must develop the muscle memory to be able to quickly and effectively respond to a sudden emergency. Reading about it on an iPad is not even close to sufficient; pilots must experience it physically, firsthand.

We should all want pilots to experience these challenging situations for the first time in a simulator, not in flight with passengers and crew on board.

We must look closely at the certification process. There have been concerns about the aircraft certification process for decades. Just a brief search revealed 18 reports produced by GAO, DOT OIG, and Congressional committees since 1992.

Many questions remain to be and must be answered:

Has the Federal Aviation Administration (FAA) outsourced too much certification work?

Should FAA be selecting the manufacturer employees who do certification work on behalf of FAA, instead of the employer, as is currently the case?

Did oversight fail to result in accountability?

Do the Federal Aviation Administration (FAA) employees and Boeing employees doing certification work have the independence they need to ensure safe designs?

Was there a failure to identify risks and their implications?

Was the analysis of failure modes and effects inadequate?

How was it that critically important information was not effectively communicated and shared with airlines and pilots?

Many other questions must be asked about the role Boeing played in these accidents:

Was there a leadership failure?

A governance failure?

An engineering failure?

A risk analysis failure?

A safety culture failure?

Whistle-blower protection must be strong and effective, and if it is not strong enough, we must strengthen it.

Key leaders and members of each safety-critical aviation organization must have subject matter expertise; in other words, they must be pilots who understand the science of safety. There should be at least one person so qualified on each corporate board of directors of each aviation company. Top project engineers of aircraft manufacturers must also be pilots.

Airlines worldwide must adhere to the highest standards of aircraft maintenance and crew training.

All the layers of safety must be in place. They are the safety net that helps keep air travelers and crews from harm.

Only by investigating, discovering, and correcting the ways in which our design, certification, training and other systems have failed us and led to these tragedies can we begin to regain the trust of our passengers, flight attendants, pilots and the American people. And, of course, in order for passengers to trust that the 737 MAX is safe to fly, pilots will have to trust that it is.

We have a moral obligation to do this.

If we don't – if we just file the findings away on a shelf to gather dust, we will compound these tragedies. What would make the loss of lives in these accidents ever more tragic is if we say these were black swan events, unlikely to happen again, and decide not to act on what we learn from them. To protect the status quo.

The best way to honor the lives tragically lost is to make sure that nothing like this ever happens again.



The Boeing Company
P.O. Box 3707
Seattle, WA 98124-3707

MAR 01 2019

RA-19-00256

[REDACTED]
Manager, AIR-860
BASOO Branch
Department of Transportation
Federal Aviation Administration
2200 S. 216 Street
Des Moines, WA 98198-6547

[REDACTED]

Subject:	Submittal of MCAS Development and Certification Overview
Model:	737MAX
FAA Project No.:	N/A
RA Project No.:	N/A
EASA Project No.:	N/A
EASA Level:	N/A
Response Requested:	None – Informational Only
Expedited Flow:	No
Reference:	FAA/Boeing meeting on December 17, 2018, MCAS Development and Certification Overview
Special Instructions:	Please forward to [REDACTED]

This letter is to submit:

Updated presentation material from the Reference meeting

This letter is being sent for:

Information only



RA-19-00256
Page 2

Please contact this office or the following individuals if you have further questions:

Certification Engineer: [Redacted]
Program Manager: [Redacted]

The information being forwarded to the FAA by or with this correspondence, which is being submitted voluntarily and in confidence to the FAA, is for reference only and is considered proprietary to The Boeing Company and/or its suppliers, is not customarily released to the public, and has ongoing commercial value to Boeing.

The data provided should be returned to Boeing immediately following use by the FAA, including any copies thereof which the FAA may be required to make in the course of its review. Boeing does not authorize the FAA to retain any portion of the materials being supplied.

Sincerely,

[Redacted Signature]

Director, BCA Engineering

[Redacted Name]

GWO

Enclosure: MCAS Development and Certification Overview

cc

Name	SP	Encl	MC	Title
[Redacted]			X	FAA Program Mgr., 0600-1222
[Redacted]			X	FAA
[Redacted]			X	FAA
[Redacted]			X	FAA
[Redacted]			X	FAA



MCAS Development and Certification Overview



No license is required for the dissemination of the commercial information contained herein to foreign persons other than those from or in the terrorist supporting countries identified in the United States Export Administration Regulations (EAR) (15 CFR 730-774). It is the responsibility of the individual in control of this data to abide by U.S. export laws. ECCN 9E991.

Copyright © 2018 Boeing. All rights reserved.

BOEING PROPRIETARY | 1

Compliance Review Summary

737 MAX MCAS Control Law

- All certification deliverables (Cert Plans, ICA Documents, etc...) in support of MCAS control law certification are compliant.
- Review of all Boeing internal analysis in support of MAX development and certification deliverables were completed per process and are compliant.
- Assessment of Compliance Identified Several Areas for Improvement
 - Opportunities to Enhance Records of Decisions
 - Inconsistencies in Documentation
- Aerodynamics Stability & Control completed further evaluation of the Functional Hazard Assessment for loss of MCAS control law function in a corner condition of the normal flight envelope.
 - Confirmation via Flight Test that loss of MCAS rated as minor

Agenda

- Development and Certification Timeline
- MCAS Control Law Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- Maintenance Training and Documents
- MCAS Compliance Assessment Summary
- AoA Disagree Flight Deck Indication

Agenda

- Development and Certification Timeline
 - System Design Overview
 - System Level Hazard and Safety Assessments
 - Flight Controls Certification Deliverables
 - Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
 - Instructions for Continued Airworthiness (ICA)
 - Flight Crew Training and Documents
 - Maintenance Training and Documents
 - Assessment Summary
 - AoA Disagree Flight Deck Indication



Agenda

- Development and Certification Timeline
- **System Design Overview**
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- Maintenance Training and Documents
- Assessment Summary
- AoA Disagree Flight Deck Indication

System Design Overview

Summary

Maneuvering Characteristics Augmentation System (MCAS) Description:

- MCAS is a pitch augmentation flight control law implemented on the 737 MAX that commands nose down stabilizer to enhance pitch characteristics with flaps up during elevated angles of attack.
- MCAS is activated without pilot input and only operates when the autopilot is disengaged.
- MCAS control law becomes active and applies automatic nose down stabilizer in increments based on a table schedule as a function of AOA and Mach
 - The maximum command amount at any point in the table schedule is limited to 2.5 degrees
 - Stabilizer is commanded at a rate of 0.27 degrees per second (same rate as flaps down speed trim)
 - Maximum magnitude of stabilizer command is lower at high Mach number and greater at low Mach number (for the same AOA above the activation threshold)
- After AOA falls below the hysteresis threshold (0.5 degrees below the activation angle), MCAS commands nose up stabilizer to return the airplane to the trim state that existed before it entered the MCAS activation region
- MCAS stabilizer operation can be stopped and reversed by a pilot using the electric thumb switches and commanding stabilizer trim in the nose up direction
- If elevated AOA conditions persist and increase, MCAS commands additional incremental stabilizer in accordance with the table schedule referenced above

System Design Overview

MCAS vs. Speed Trim: Pilot Inputs and Effect on MCAS and Speed Trim

Effect of Column Cutout

- Does not inhibit MCAS commands
- Inhibits Speed Trim commands

Effect of Electric Stabilizer Trim (i.e. thumb switch input)

- Overrides both MCAS and Speed Trim commands

Effect of Stabilizer Cutout switches

- Inhibit both MCAS and Speed Trim commands

Effect of Manual Trim (i.e. trim wheel)

- Overrides both MCAS and Speed Trim commands

Effect of Trim Override switches

- Overrides column cutout switches only

Agenda

- Development and Certification Timeline
- System Design Overview
- **System Level Hazard and Safety Assessments**
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- Maintenance Training and Documents
- Assessment Summary
- AoA Disagree Flight Deck Indication

MCAS System Level FHA

Summary

- Development of FHAs for MCAS control law was consistent with process and assumptions used on all Boeing models.
- Loss of MCAS control law function assessed as Minor in the Normal Flight Envelope and Major in the Operational Flight Envelope.
- All FHAs involving unintended MCAS activation were assessed as Major in the Normal Flight Envelope and Hazardous in the Operational Flight Envelope.
- Consistent with FAA regulations and Boeing process MCAS FHA events were not evaluated in the SSA as they were assessed as Major.

Fundamental Assumptions Utilized in Functional Hazard Assessments

- Fundamental assumptions used in flight control FHAs across all Boeing models. Consistent with 25.671, 25.672 and AC 25-7C for compliance evaluation for 25.143.
 - Uncommanded system inputs that 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 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 increase 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
- FHA evaluation for MCAS and Stab Trim was consistent with the above fundamental assumptions and resulted in the following.
 - 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) 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.

System Level Functional Hazard Assessment (FHA)

MCAS Certification Approach

- Determination of functional hazard categories (e.g., Major, Hazardous, Catastrophic) was by Boeing pilot assessment performed in the simulator and aligned with Advisory Circular AC 25-7C.
- Single MCAS unintended activations were inserted via the Stabilizer Trim System in the Simulator to assess impact to handle qualities and associated flight crew actions.
- Accumulation or combination of failures leading to unintended MCAS activation were not simulated nor their combined flight deck effects.
- Upon each design iteration of MCAS, the functional hazard categories were re-assessed. The assessments were validated following each iteration.
- When assessing unintended MCAS activation, 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 available to offload column forces.
 - Stabilizer cutouts were available but not required to counter failures.
- Based on this evaluation, unintended MCAS activation was assessed as Major in the Normal flight envelope.

System Level Functional Hazard Assessment (FHA)

MCAS FHAs

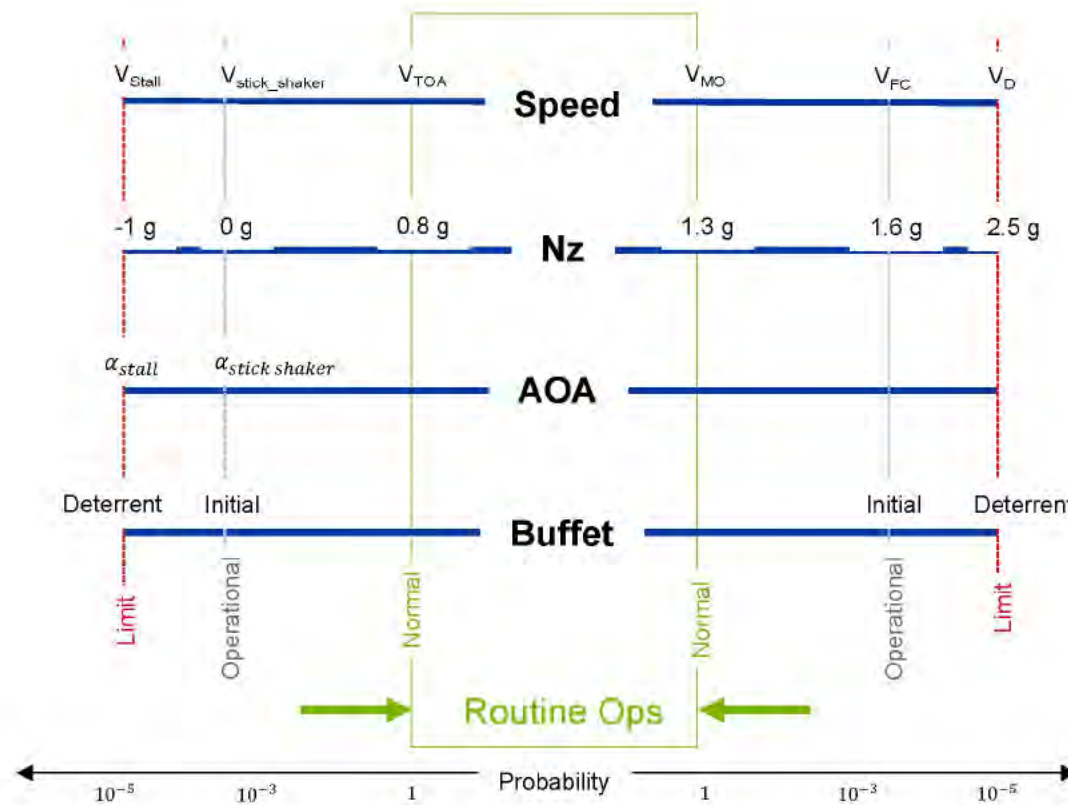
- Four failure conditions were evaluated per our FHA process in the Normal flight envelope and in Operational flight envelope and then assessed the effect for each failure condition in both of those envelopes.
 - Conditions assessed:
 - Loss of MCAS function
 - Unintended MCAS activation to the control law table limit (accounted for erroneous AoA)
- [REDACTED]
- [REDACTED]
- All four conditions determined to meet hazard assessment / probability requirements.
 - Erroneous Angle of Attack (AoA) was accounted for within unintended MCAS activation to control law table limit.

System Level Functional Hazard Assessment (FHA)

Erroneous Inputs to MCAS Control Law

- Erroneous inputs to MCAS control law could result in loss of MCAS function or unintended MCAS activation.
- Unintended MCAS activation due to erroneous input would still be subject to the control law table limits encoded in the MCAS software (2.5 deg maximum incremental stabilizer movement)
- Unintended MCAS activation has previously been shown to be:
 - Major in normal flight envelope.
 - Failure can be countered by using elevator alone.
 - Stabilizer trim available to offload column forces.
 - Stabilizer cutouts available but not required to counter failure.
 - Hazardous in the operational flight envelope.
 - The probability of being outside the normal flight envelope is 10^{-3} (ref AC 25-7C). 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.

Flight Envelope Definitions



Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- **Flight Controls Certification Deliverables**
 - Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
 - Instructions for Continued Airworthiness (ICA)
 - Flight Crew Training and Documents
 - Maintenance Training and Documents
 - Assessment Summary
 - AoA Disagree Flight Deck Indication

MCAS Flight Controls Certification

Summary

- “737 NG/MAX Enhanced Digital Flight Control System, Autothrottle, and Yaw Damper Safety Analysis” showed compliance for [REDACTED]
- “737 Stabilizer Trim Control System Safety Analysis” showed compliance for [REDACTED]
- Flight test conducted concurrent with Aero S&C flight testing to demonstrate MCAS control law function and effects of loss of function during Control System Malfunctions Testing.
- During MAX development FCC and MCAS Control Law identified as Development Assurance compliant system following ARP 4754.

MCAS Certification

CP 13474 “737-8 Amended Type Certificate – Flight Controls – Autoflight (EDFCS/FCC)”

- Deliverable 8: D241A018-12, “737 NG/MAX Enhanced Digital Flight Control System, Autothrottle, and Yaw Damper Safety Analysis” for [REDACTED]
[REDACTED]
 - Existing catastrophic fault trees modified to account for the MCAS failure contributions to the top event
 - No warning required as a failure of the function did not pose an unsafe condition. In addition, counteraction of failures of the function did not require exceptional pilot skill or strength and is accomplished by movement of the flight controls in the normal sense.
 - Detected failures in MCAS are annunciated by the illumination of the existing SPEED TRIM (caution) light – repurposes existing speed trim structure

MCAS Certification

CP 13471 “737-8 Amended Type Certificate – Flight Controls – Primary, Elevator and Stabilizer Control”

- Deliverable 9: D251A018-6, “737 Stabilizer Trim Control System Safety Analysis” for [REDACTED] AR Recommend Approval
 - Existing catastrophic fault trees modified to account for the MCAS engage discrete failures contributing to loss of the control column cutout function
 - Identification of the established functional hazards in normal and operational flight envelope

G-4.2 FHA Results

Functional Hazard Assessment findings for the 737 MAX Stabilizer Trim Control System are presented in Table G4-1 below. Probabilities are given for both a 1.9 hour standard flight length case as well as for a 9.0 hour maximum duration ETOPS mission. Note the two different flight phases designated for MCAS related hazards – “Normal Flight Envelope” and “Operating Flight Envelope”. Operating flight envelope for the MCAS function refers to a wind-up turn.

Effect Category Event Source	Hazard Event	Flight Phase	Contributing Interfacing Systems	Calculated Probability		FTA Reference
				Standard Flight (1.9 FH)	ETOPS Flight (9.0 FH)	
Hazardous	Loss of main electric nose down trim prior to piloted go around, but after stabilizer flare spring on dual channel autoland	Go around	None	[REDACTED]	[REDACTED]	G6-4, p. 1, STABGA
Hazardous	Stabilizer trim system uncommanded motion with override, but requires very high flight crew workload for safe landing	Landing	None	[REDACTED]	[REDACTED]	G6-2, p. 3, G015
Hazardous	Uncommanded MCAS function operation	All (Operating Flight Envelope)	None	[REDACTED]	[REDACTED]	G6-2, p. 8, G047

Flight Test

CP 13471 “737-8 Amended Type Certificate – Flight Controls – Primary, Elevator and Stabilizer Control”

- Deliverable 15: CFTP C1.39.AAC “737-8 Primary Flight Control System” – AR Recommend Approval for 1st Rev
 - [REDACTED]
 - Test Report Deliverable 17 – AR Approval
 - Test report points to conditions flown concurrently with C1.21.AAL “737-8 Maneuvering Characteristics” (reference CP 13669)

Flight Test

CP 13669 “737-8 Amended Type Certificate –Aerodynamics – Performance, Stability and Control”

- Deliverable 40: CFTP C1.14.ADD “737-8 Stall Characteristics” – AR Recommend Approval
 - [REDACTED] Demonstrate compliant stall characteristics.
 - Test Report Deliverable 42 – AR Approval
- Deliverable 34: CFTP C1.21.AAL “737-8 Maneuvering Characteristics” – AR Recommend Approval for 1st Rev
 - [REDACTED] Demonstrate compliant maneuvering characteristics and associated column force characteristics during wind up turns.
 - Test Report Deliverable 36 – AR Approval
- Deliverable 7: CFTP C1.33.AAD “737-8 Control System Malfunctions” - AR Recommend Approval for 1st Rev
 - [REDACTED] Demonstration of loss of MCAS function
 - Test Report Deliverable 9 – AR Approval

Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- **Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments**
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- Maintenance Training and Documents
- Assessment Summary
- AoA Disagree Flight Deck Indication

Airplane Level Hazard, Safety, and Single & Multiple Failure Assessments

Summary

- For the MAX development Single and Multiple Failure analysis was completed and followed BPI- [REDACTED]
- Per BPI- [REDACTED], MCAS was not evaluated individually as a new/novel on the MAX as the control law had been previously implemented on 767 GTTA.
- “Erroneous AOA, one source” was identified and not analyzed as part of S&MF assessment per Engineering judgment.
- During case selection per Engineering judgment the worst case multiple failure of “Erroneous L & R Air Data” and “Erroneous L or R Air Data” replaced “Erroneous AOA, one source” failure scenario.
- S&MF analysis completed prior to the design change to MCAS control law during flight test. Reevaluation of design change not required per BPI- [REDACTED].
- While the version of MCAS included in the S&MF analysis was not reflective of the certified configuration; current assessment is that the S&MF final report would have included the same crew action that is already considered in the S&MF analysis.

Airplane Level Safety Assessments (ASA)

Single and Multiple Failure Accomplishment Summary – D910A010

- Completed by Systems Engineering with input from Safety and Functional Areas
- Developed per BPI-██████, “Conducting Single and Multiple Failure Analyses”
 - Step 1 – Team identifies cases based on prior models, changes in airplane/architecture. Cases accepted/rejected in this step. Rationale for rejection reviewed.
 - Step 2 – Analysis performed. Data includes failure effects and cascading effects.
 - Step 3 – Teams determine if failure hazard classification is appropriate for case.
 - Step 4 – Resolve actions in AI database.
 - Step 5 – E-CAB testing.
 - Step 6 – Document results.

Airplane Level Safety Assessments (ASA)

Single and Multiple Failure Accomplishment Summary – D910A010

- AVN-16: Loss of one AOA followed by an erroneous AOA
- Deemed potentially catastrophic before crew recognition of issue
- Catastrophic rating consistent with Displays and Air Data system safety assessments and AC 25-11A
- Acceptability Rationale based on crew training, appropriate flight crew action and the probability of failure being extremely remote.

4.19.2 Analysis Summary

Baseline Configuration: 737-7, -8, and -9 MAX

Significant Flight Phase and Conditions:

- Flight phase of failure occurrence: All flight phases
- Environmental conditions: IMC, Night, wet runway
- Operational conditions: IFR
- Significant flight phase and conditions for follow-on effects: No

Airplane-Level Effects:

- MMEL: No
- Diversion by Procedure: No
- Diversion Expected by Pilot: Not called out by procedure, but flight crew likely would divert

Failure Case Probability	Failure Case Cumulative Hazard Category	Required Probability On the Order Of (Based on Hazard Categorization)
[REDACTED]	Catastrophic	1E-9 or less

Acceptability Rationale:

- Results in a misleading single source air data situation for primary displays. Potentially catastrophic before flight crew recognition of issue. Crew training supports recognition and appropriate flight crew action.
- Failure event probability is beyond extremely improbable

Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- **Instructions for Continued Airworthiness (ICA)**
- Flight Crew Training and Documents
- Maintenance Training and Documents
- Assessment Summary
- AoA Disagree Flight Deck Indication

Instructions for Continued Airworthiness (ICA)

ICA Documents

- For the MAX development program all ICA documents required for certification were produced to comply with [REDACTED] and followed Boeing release process BPI-[REDACTED] "Showing Compliance for Instructions for Continued Airworthiness (ICA)"
- Aircraft Maintenance Manual & Integrated Fault Isolation Manual did not require inclusion of information specific to MCAS as they include all pertinent information required to diagnose MCAS control law input failures in the material that addresses Stab Trim control law input failures.
- MCAS not included in Systems Description Section of AMM.
- Wiring Diagram Manual properly captures the airplane wiring changes for the Stabilizer Column Cutout due to incorporation of the MCAS control law.
- Relay implemented in Stabilizer Column Cutout system to incorporate MCAS is monitored by the FCC and no periodic maintenance is required.

Instructions for Continued Airworthiness (ICA)

ICA Documents

- Airworthiness Limitations Certification Maintenance Requirements (ALCMR)
- Enhanced Zonal Analysis Procedure (EZAP)
- Aircraft Maintenance Manual (AMM) ★
- Configuration, Maintenance and Procedures (CMP)
- Fault Isolation Manual (FIM) ★
- Damage Tolerance Rating (DTR)
- Maintenance Review Board (MRB)
- Non Destructive Testing (NDTG)
- Structural Repair Manual (SRM)
- Standard Wiring Practices Manual (SWPM)
- Task Cards (TC) – data not in AMM
- Weight and Balance Manual (WBM)
- Wiring Diagram Manual (WDM) ★

★ Denotes item reviewed for inclusion of MCAS

Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- **Flight Crew Training and Documents**
- Maintenance Training and Documents
- Assessment Summary
- AoA Disagree Flight Deck Indication

Flight Crew Training & Manuals

Summary

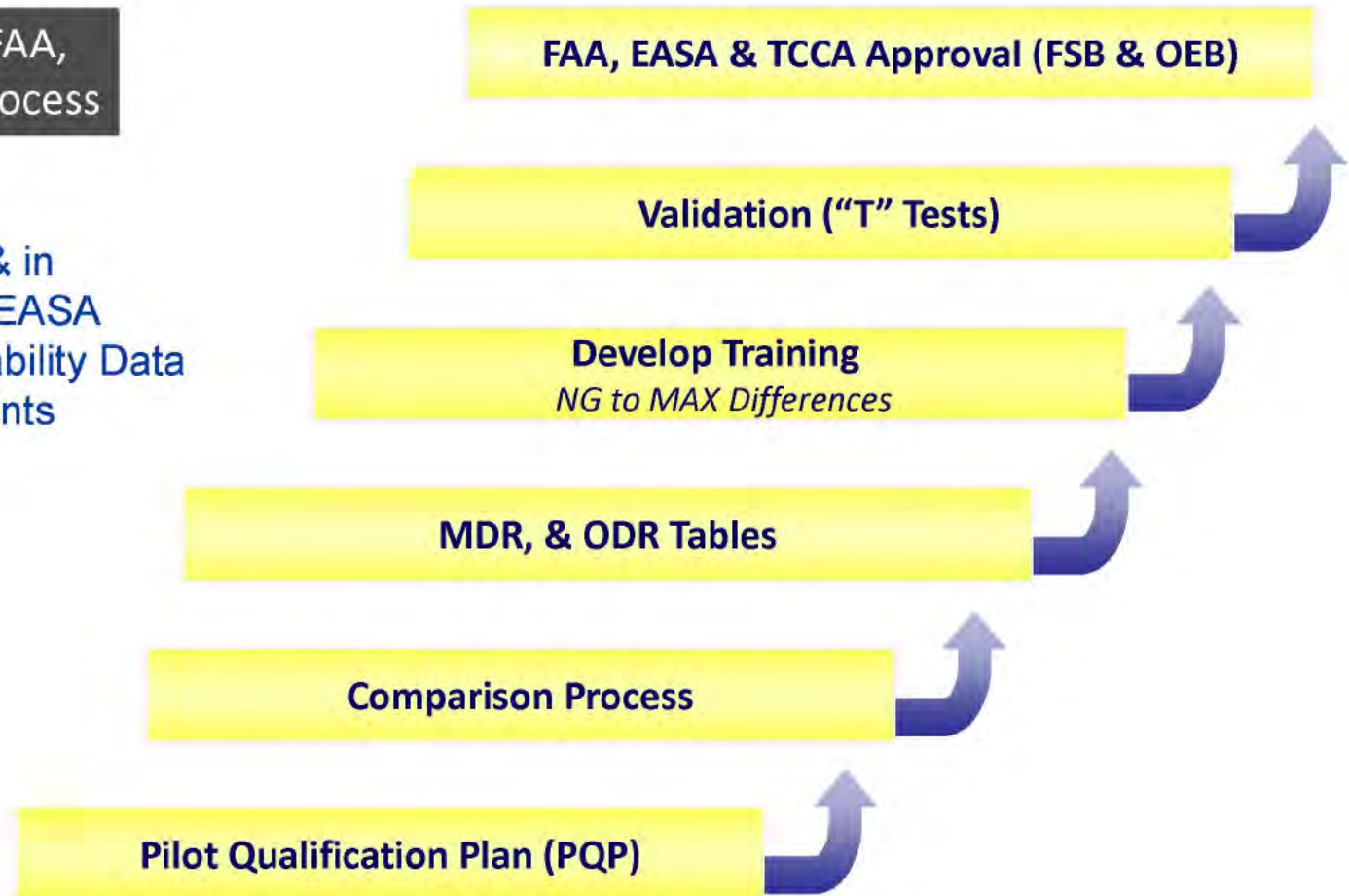
- Pilot Qualification process for the MAX followed AC 120-53B and Issue Paper O-1.
- Final approved FSB Report and Other Differences Requirements (ODR) Tables for the MAX did not include MCAS control law.
- Flight Crew Operations Manual (FCOM) does not include a specific systems description of MCAS control law.
- Boeing and FAA AEG specifically discussed inclusion of MCAS in ODR table and system description in FCOM. FAA concurred with Boeing recommendation that inclusion of MCAS in the ODR table and FCOM was not necessary.

Training and FCOM

Pilot Qualification Plan Process

A Joint Boeing, FAA, EASA and TCCA process

- Gated process
- Per AC120-53B & in compliance with EASA Operational Suitability Data (OSD) requirements



Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- **Maintenance Training and Documents**
- Assessment Summary
- AoA Disagree Flight Deck Indication

Maintenance Training and Documents

Summary

- As part of ATA Chapter system description the MCAS control law is referenced including the control law schematic.

HORIZONTAL STABILIZER TRIM CONTROL SYSTEM -- FUNCTIONAL DESCRIPTION - ELECTRIC TRIM

During autopilot operation the stabilizer trim speed changes. When the flaps are up, the low speed trim is 0.09 units per second. When the flaps are not up, the high speed trim is 0.27 units per second.

Only the F/O's column cutout switch module is affected because it is the only module that interfaces with the FCCs.

Stabilizer Trim Cut Out Switch

If there is a stabilizer runaway condition, the pilots move the STAB TRIM PRI (primary) switch to the CUT OUT position. This removes power to the STAB TRIM B/U (backup) switch and these:



Column Cutout Switches and Column Input

The column cutout switches are in the column cutout switch module. There are two modules, captain and F/O. When the pilot moves the elevator column out of the neutral range, the column cutout switches open for trim in a direction opposite to the column movement. One other set of switches let the actuator operate the stabilizer in the same direction as the column movement.

The pilot uses the STAB TRIM override switch to do a bypass of the column cutout switches if the two switches have internal failures.

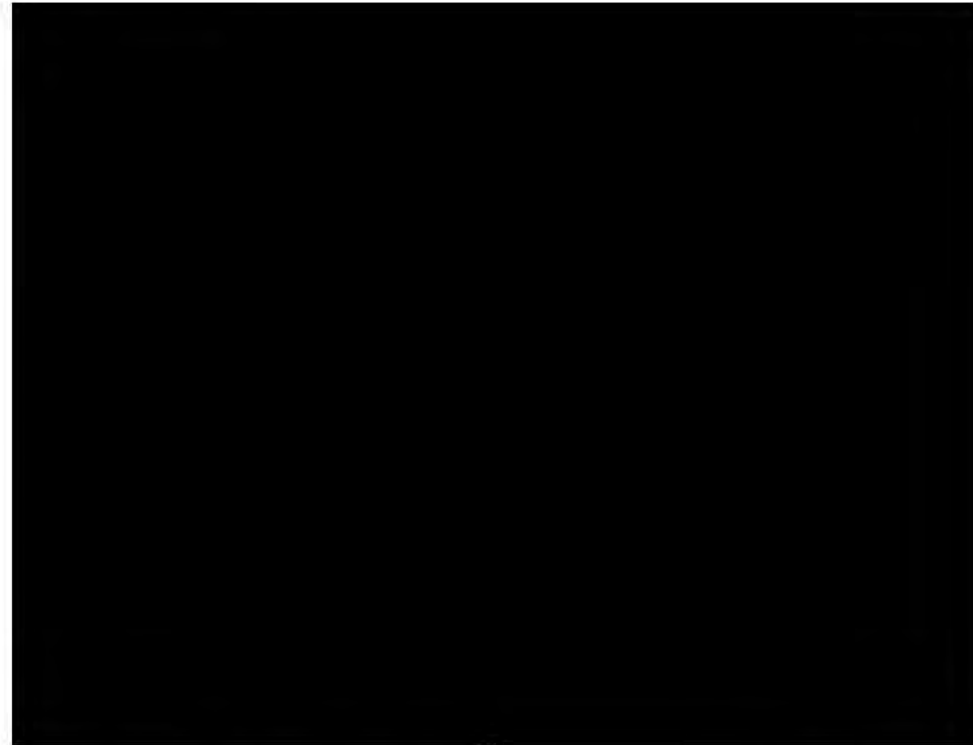
Maneuvering Characteristic Augmentation System

The maneuvering characteristic augmentation system (MCAS) allows the stabilizer to move in the nose down direction when approaching high angles of attack at high speeds. This requires the stabilizer to move in the opposite direction in which the pilot is pulling the column for nose up pitch. The MCAS only operates at extreme high speed pitch up conditions that are outside the normal operating envelope.

20-Sep-2016

- 252 -

BOEING PROPRIETARY



Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- Maintenance Training and Documents
- **Assessment Summary**
- AoA Disagree Flight Deck Indication

Assessment Summary

• Opportunities to Enhance Records of Decisions

- MCAS Control Law Removal from Differences Training Table (ODR) and FCOM
 - Boeing and FAA AEG discussed and agreed on removal of MCAS control law during MAX development and certification.
 - Supporting rationale discussed between Boeing and FAA and accepted by FAA, but not formally documented in meeting minutes.
 - Reviewed FCOM and released MAX FSB Report do not reference MCAS.
 - No process violation or non-compliance
- Engineering & Pilot Assessment of Repeated Unintended MCAS Control Law Activation
 - Engineering and Test pilots discussed scenario of repeated unintended MCAS activation during MAX development and deemed no worse than single unintended MCAS activation.
 - Discussion and supporting rationale documented in pilot meeting summary email on June 22, 2016 and not documented in formal certification artifacts
 - No process violation or non-compliance

Assessment Summary

• Inconsistencies

- MCAS Systems Descriptions in Maintenance Training Material and Not Included in ICA Documents
 - Maintenance Training material developed and released prior to ICA documents provide description of pre-flight test MCAS control law.
 - No process violation or non-compliance
- FCOM Acronyms Section Referencing MCAS
 - Artifact left behind from earlier drafts of the FCOM prior to removal of MCAS from FCOM and FAA acceptance.
 - No process violation or non-compliance
- EDFCS SSA Data Document D241A018-13
 - Data Document is a repository for SSA supporting data and is not a certification deliverable nor referenced in SSA Compliance Documents D241A018-12 for the MAX or NG.
 - Supplemental non-certification data documentation updates not yet formally published to include the MAX.
 - EDFCS SSA D241A018-12 document used appropriate data in support of compliance for the MAX.
 - No process violation or non-compliance

Assessment Summary

- Inconsistencies
-
- D251A018-6, "737 Stabilizer Trim Control System Safety Analysis" Compliance Document
 - Description of functional failure in the Fault Hazard Assessment table referenced preliminary MCAS control law authority limits and was not updated to reflect certified design.
 - Identification of the probability for the Hazardous condition of unintended MCAS activation referenced the incorrect gate within the Fault Tree Analysis for Stabilizer Runway.
 - Compliant probabilistic assessment in Fault Tree Analysis maintained with revision.
 - D910A010, "Single and Multiple Failure Accomplishment Summary"
 - "Erroneous AOA, one source" was identified and not analyzed as part of S&MF assessment. Similar to previous derivative development programs like 747-8
 - Supporting rationale provided was, "Covered by Erroneous L&R Air Data, Erroneous L or R Air Data covers single probe loss case".
 - Rationale should have pointed to "Loss of one AOA followed by Erroneous AOA" which was a part of the S&MF assessment during MAX development. Condition was not evaluated in the simulator but deemed acceptable as failure was found to be extremely improbable.
 - S&MF analysis completed prior to the design change to MCAS control law during flight test and not reevaluated. Current reassessment is consistent with previous S&MF analysis which is supported by crew action in acceptability rationale.
 - No process violation or non-compliance

Compliance Review Summary

737 MAX MCAS Control Law

- Review of all certification deliverables (Cert Plans, ICA Documents, etc...) in support of MCAS control law certification are compliant.
- Review of all Boeing internal analysis in support of MAX development and certification deliverables were completed per process and are compliant.
- Assessment of Compliance Identified Several Areas for Improvement
 - Opportunities to Enhance Records of Decisions
 - Inconsistencies in Documentation
- Aerodynamics Stability & Control completed further evaluation of the Functional Hazard Assessment for loss of MCAS control law function in a corner condition of the normal flight envelope.
 - Confirmation via Flight Test that loss of MCAS rated as minor

Agenda

- Development and Certification Timeline
- System Design Overview
- System Level Hazard and Safety Assessments
- Flight Controls Certification Deliverables
- Airplane Level Hazard, Safety, and Single & Multiple Fault Assessments
- Instructions for Continued Airworthiness (ICA)
- Flight Crew Training and Documents
- Maintenance Training and Documents
- Assessment Summary
- **AoA Disagree Flight Deck Indication**

'AOA DISAGREE' and Optional Angle of Attack Flight Deck Indication

Design Overview

- **Optional Angle of Attack Indication**
 - Implemented in BP99 for 737NG - first delivered December 1999.
 - Requirements carried over for 737 MAX.
- **'AOA DISAGREE' disagree**
 - Implemented in BP06 for 737NG - first delivered July 2006.
 - Annunciation was a customer request to assist maintenance troubleshooting.
 - Displayed on PFDs when the left and right AOA disagree 10+ degrees for 10 continuous seconds.
 - [REDACTED]
 - AOA data received from the ADIRUs via A429.
 - If the data from the ADIRUs are unavailable or invalid, the annunciation will not be displayed.
 - Requirements carried over for 737 MAX.



- AOA DISAGREE alert does not require any pilot action.
- There are other flight deck effects that pilots should understand that may indicate the presence of erroneous AOA data, including the ALT DISAGREE and IAS DISAGREE alerts.

737 MAX 'AOA DISAGREE' Flight Deck Indication

COSP 2018-2116

- MDS PR693 "AOA DISAGREE Annunciation" discovered in October 2017
- AOA DISAGREE is not displayed unless the optional AOA indicator is displayed.
- Determined to be requirements not implemented correctly by supplier in display system software.
- Testing of previous black label software on versions did not discover this issue.
- PR Review Process concluded to resolve the PR with MDS BP2 which is part of MAX-10 ATC (EIS 3Q 2020).

737 MAX 'AOA DISAGREE' Flight Deck Indication

COSP 2018-2116 Summary Rationale

Determined to be Not a Safety Issue (Dec 6, 2018)

- IAS DISAGREE and ALT DISAGREE may be displayed with an AOA DISAGREE. AOA DISAGREE is supplementary information with no additional crew action.
- All appropriate crew action is contained in the IAS DISAGREE and ALT DISAGREE QRH procedures.
- The IAS DISAGREE and ALT DISAGREE annunciations are displayed independent of the AOA DISAGREE annunciation.
- AOA DISAGREE, IAS DISAGREE, and ALT DISAGREE are observed faults and have corresponding IFIM Tasks.
 - Task 34-10-00-810-801 SPEED DISAGREE Shows on PFD – (Captains's) – Fault Isolation
 - Task 34-10-00-810-802 SPEED DISAGREE Shows on PFD – (First Officer's) – Fault Isolation
 - Task 34-20-00-810-801 ALT DISAGREE Shows on PFD – (Captains's) – Fault Isolation
 - Task 34-20-00-810-802 ALT DISAGREE Shows on PFD – (First Officer's) – Fault Isolation
 - Task 34-20-00-810-803 AOA DISAGREE Shows on PFD (Captains's) – Fault Isolation
 - Task 34-20-00-810-804 AOA DISAGREE Shows on PFD (First Officer's) – Fault Isolation
 - The first step in all tasks is to look in OMF Existing Faults, 34 Air Data Inertial Reference System for related maintenance messages.



Matthieu WILLM
7, avenue Marcel Proust
75016 PARIS
FRANCE

Committee on Commerce, Science and Transportation
US Senate
Washington DC, 20510

e-mail : mwillm@laposte.net

Subject: Aviation Safety Bill & 17th June hearing of FAA Administrator

Dear Senator,

I am the brother of Clémence-Isaure Boutant-Willm, who lost her life in the crash of the Boeing 737 Max of flight ET302 on March 10th, 2019. She was 44, and left behind her widowed husband and two children, aged 9 and 11 when the accident occurred. Clémence-Isaure devoted her life to others and made it her job. She worked for several NGOs for 20 years. On March 10th, 2019, she was flying from home to Nairobi for her work to provide humanitarian training.

I am writing this letter on behalf of Clémence-Isaure's family about the upcoming hearing of FAA Administrator Steve Dickson, and about the Aviation Safety Bill that is currently discussed at the US Senate.

Much has been written on the Boeing 737 Max. It has an unsafe, single chain design. Safety assessments were fragmented, based on wrong assumptions, were non-comprehensive, and actually wrong, as the two crashes demonstrated it. 346 people paid these errors with their life. There have been huge failures in the design process, as well as in the certification process. These accidents caused a tremendous loss of confidence, not only towards Boeing and the FAA, but also towards the entire aeronautical industry.

My purpose is not to comment all the failures and how to avoid them again thanks to the safety bill, this wouldn't fit in a 3 pages letter. But, as a mourning brother and as an engineer for the aeronautical industry, I rather chose to highlight two important points: the actually international scope of the safety bill you are considering, and the fact that the second crash should have never occurred.

I am aware that, as a French citizen, I do not have the legitimacy to express an opinion on an American bill. However, I would like to draw your attention to the fact that the changes in the American aeronautical regulations that you are studying have a global impact due to the agreements between certification authorities. For example, an FAA certified aircraft in the United States is not fully recertified in Europe thanks to the bilateral agreement between the FAA and EASA. EASA trusts the FAA for its certification work, and recertifies only certain specific points, for example where there are regulatory differences. If these agreements were

a force for the aeronautical industry, to avoid multiplying the costs of certification, the two accidents of the Boeing 737 Max showed that it was also a huge weakness. Indeed, due to bilateral agreements, the certification authorities of many countries have trusted the work of the FAA, and have not looked into the safety of the new MCAS system.

I think that the regulatory enforcement project that you are currently studying must be thought of globally, and not only at the American level, because the civil aviation regulation is a global, interconnected, regulatory system. For example, it should consider the consequences of bilateral agreements and better frame them, to prevent a chain reaction like the tragedy of the Boeing 737 Max from happening again.

Worldwide aviation regulations are largely based on trust between national certification authorities. With the tragedies of the Boeing 737 Max, Boeing and the FAA have broken that trust. This was expressed publicly by Patrick Ky, Executive Director of EASA, during a hearing in September 2019 at the EU parliament¹. As a consequence, following the accident of flight ET302, EASA decided to no longer rely on the bilateral agreement with the FAA for the certification of modifications to the Boeing Max, but to recertify itself all the flight control systems.

Hence, I think it would be very useful for the American Senate to consider hearing Patrick Ky, executive Director of EASA, and why not, other leaders of certification authorities from other countries. This would allow the Senate to better understand the international consequences of the bill on the overall safety of flight, due to bilateral agreements.

Secondly, the bill should consider not only the design and certification process, but also the whole airworthiness regulatory framework. The two Boeing 737 Max accidents highlighted terrible shortcomings in the airworthiness process, and in the response to an accident.

In particular, the second accident should never have occurred. After the Lion Air JT610 accident, it is absolutely impossible that Boeing could ignore the weaknesses of the 737 Max design. It is also unbelievable that they issued an Airworthiness Directive with a runaway trim procedure that was inefficient in some parts of the flight envelope. It is as much unbelievable that the FAA “blindly” approved this procedure. Given all the failures and shortcomings known by Boeing, the 737 Max should have been grounded promptly after the first crash. Here again, due to bilateral agreements, other certification authorities like EASA in Europe completely relied on FAA and Boeing reactions to the first crash. If appropriate reactions and decisions had been made by Boeing and the FAA after the first crash, Clémence-Isaure would be still alive, as well as all 157 passengers and crew who lost their lives on March 10th 2019. Boeing and the FAA had all the information to issue appropriate reaction after the first crash.

¹ https://multimedia.europarl.europa.eu/en/committee-transport-tourism-ordinary-meeting-ordinary-meeting_20190903-1000-COMMITTEE-TRAN_vd

Interesting sequences are (approx.) :

- from 10:35:00 to 10:46:20 : point by Patrick Ky on Boeing 737 Max
- from 11:28:30 to 11:39:25 : answers from Patrick Ky on questions related to FAA
- from 11:54:45 to 11:56:07 : answers from Patrick Ky on questions return into service schedule

As a conclusion, I sincerely hope that the bill will bring regulatory improvements to meet the challenge to restore confidence in overall aviation safety, and will be designed to handle not only national US issues, but also to take into account its worldwide impacts, so that my sister and the 346 passenger and crew did not die for nothing, and to avoid such disaster occurring again.

Best Regards,

Matthieu Willm, June 15th, 2020.

Brother of late Clémence-Isaure Boutant-Willm, on behalf of Denis Boutant, her husband, Lilas and Zélie her 2 two daughters, Elisabeth Willm her mother, Vincent and Violaine Willm, her brother and sister and on behalf of all Clémence-Isaure's family and friends.

A handwritten signature in blue ink, consisting of several fluid, overlapping strokes that form a stylized name.