DRAFT
NOT FOR DISTRIBUTION
1/19/2020

FAULT TREE ANALYSIS AND ALTERNATIVE CONFIGURATIONS OF ANGLE OF ATTACK (AOA) SENSORS AS PART OF MANEUVERING CHARACTERISTICS AUGMENTATION SYSTEM (MCAS)

Magdi Ragheb
Department of Nuclear, Plasma and Radiological Engineering
University of Illinois at Urbana-Champaign,
216 Talbot Laboratory, 104 South Wright Street,
Urbana, Illinois 61801, USA.
mragheb@illinois.edu, https://www.mragheb.com

ABSTRACT

A Fault Tree Analysis of different hardware and software serial and parallel configurations of the Angle of Attack (AoA) sensors as input to the Maneuvering Characteristics Augmentation System (MCAS) is undertaken in view of identifying optimal configurations with minimal failure probabilities for future as well as current platforms in service. Boolean expressions are deduced and example cases are presented. Two-out-three logic within the context of a three-level redundancy and three-out-of-four logic within a four-level redundancy configurations are identified as leading to minimal failure probabilities and subsequent enhanced safety and minimized risk. As an extension of the discussed configurations, "Performance Level" for anticipatory or predictive monitoring and control, as well as "Surety" as necessary in high risk systems, can be envisioned.

INTRODUCTION

Mission critical systems are supplemented with reliable array sensors. They can check each other, and if a deviation in their readings is too large, an alarm is issued and any automatic equipment that relies upon the suspected faulty sensor input is either shut down or deactivated. The systems should disable themselves if multiple conflicting inputs are detected from the operators' controls over a period of time.

Both Ethiopian Airlines Flight ET302 flying a Boeing 737 MAX 8 accident on March 10, 2019 with 157 people aboard, following a five-month earlier on October 29, 2018 Indonesian Lion Air JT610 with 189 passengers crash carrier had the MCAS software activated when the accidents occurred. The MCAS system is designed to help pilots avoid the plane's nose pitching up and entering a stall, leading to a loss of control of the plane.

Boeing had two optional safety features that could have helped the pilots detect erroneous AoA readings. One of the optional upgrades, the angle of attack indicator, displays the readings of the two sensors. The other, called a disagree light, is activated if those sensors are at odds with one another. This disagree light and the angle of attack indicator will be made standard, not just optional on all new aircraft. Neither feature was mandated by the Federal Aviation Administration.

MCAS took readings from only one sensor out of two on any given flight, leaving the system vulnerable to a single point of failure: "During the late stages of the Max's development, Boeing engineers decided to increase the plane's reliance on MCAS to fly smoothly. Unfortunately, a new version of the system relied on a single sensor which could malfunction and push the plane into a nosedive [1]." In the Lion Air crash, MCAS was receiving faulty data from one of the sensors, prompting an unrecoverable nose dive. In a software update, MCAS is modified to take readings from both sensors. If there is a meaningful

disagreement between the readings, MCAS will be disabled. In the future, the system will rely on information from two angle-of-attack sensors, rather than just one. If the two sensors give different readings, the pilots will be alerted to the fact and if they vary too much MCAS will simply be switched off. There will be other safeguards ensuring that the system can always be counteracted by the flight crew, and preventing it from deploying multiple times “in non-normal conditions”.

Investigators have reached a conclusion that the software automatically activated, according to what they told Federal Aviation Administration (FAA) officials during a high-level briefing with the FAA on March 28, 2018. It is the "strongest indication yet" that the software was involved in both the Lion Air and Ethiopian Airlines crashes. The aircraft took off and it could not climb out without nearly stalling almost immediately, a possible sign of an aircraft that has been overloaded taking-off at a higher elevation’s thin air.

The pilots of ET302 successfully switched off the MCAS system as they struggled to right the plane after the software had automatically tipped its nose down. As they struggled to right the plane, the pilots ended up reactivating the software, while trying a few other steps from their training, before the plane began its final plunge. The MCAS system was reengaged four times as the pilots scrambled to right the plane**,** and investigators were looking into the possibility that the software might have reengaged without prompting from the pilots. The data show the pilots maneuvered the plane back upward twice before deactivating the software. If the system sensor input was not disabled, then as soon as the pilot picked the nose back up, the faulty sensor re-reported an erroneous AoA, which might have re-engaged the MCAS. That would mean either MCAS could not be completely disengaged, or, the pilot did not know how to fully disengage the system. The jet could have been losing parts off its control surfaces under full trim condition without a reset just before it crashed.

There was only one sensor feeding the AoA data to an automated system. Faulty data that could not be verified started a chain of events that caused the two 737max planes to nosedive into the ground. That there was an option for an additional sensor, but was not mandatory. The 737 is the last of the commercial airliners in which actual flight control cables and hydraulic lines are routed through the cockpit. In every other airliner, the computer controls everything, and the pilots can only access the flight controls through the computer.

The Boeing Company announced software changes to the MCAS system, including allowing input from two sensors instead of one. Investigators suspect faulty data from the sensors helped trigger the system. Boeing is also adding certain cockpit lights and voice alerts:

> “In future, the system will rely on information from two angle-of-attack sensors, rather than just one. If the two sensors give different readings, the pilots will be alerted to the fact and if they vary too much MCAS will simply be switched off.
>
> There will be other safeguards, too - ensuring that the system can always be counteracted by the flight crew, and preventing it from deploying multiple times “in non-normal conditions”.

According to Boeing, the additional layers of protection include:

"Flight control system will now compare inputs from both AOA sensors. If the sensors disagree by 5.5 degrees or more with the flaps retracted, MCAS will not activate. An indicator on the flight deck display will alert the pilots.

If MCAS is activated in non-normal conditions, it will only provide one input for each elevated AoA event. There are no known or envisioned failure conditions where MCAS will provide multiple inputs.

MCAS can never command more stabilizer input than can be counteracted by the flight crew pulling back on the column. The pilots will continue to always have the ability to override MCAS and manually control the airplane.

These updates reduce the crew's workload in non-normal flight situations and prevent erroneous data from causing MCAS activation."

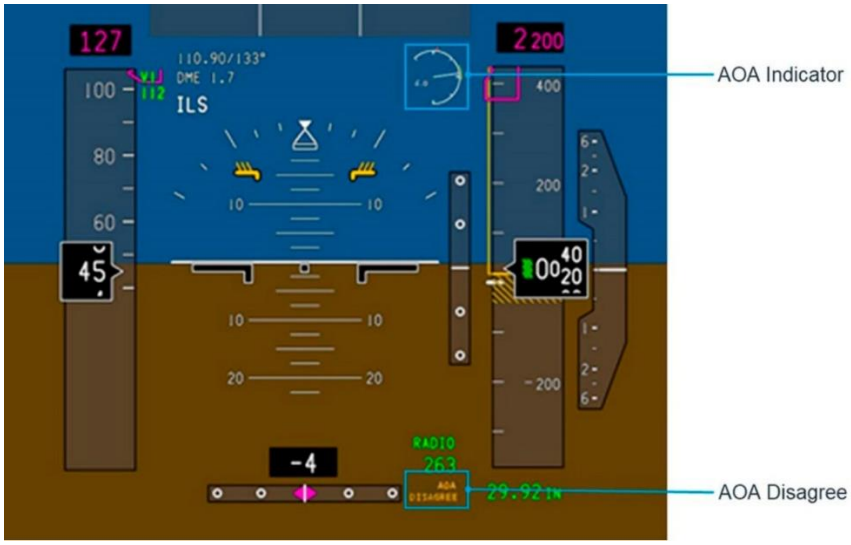


Figure 1. Boeing new enhanced flight deck display showing AoA sensor settings. "The AoA (Angle of Attack) indicator provides supplementary information to the flight crew. The AoA disagree alert provides additional context for understanding the possible cause of air speed and altitude differences between the pilot's and first officer's displays."

The Lion Air flight did a high banked turn and it is believed that Ethiopian Airline aircraft did the same. On the Lion Air flight accident, the MCAS was fed erroneous information from a sensor, causing the system to repeatedly push the angle of the nose down after detecting a risk of stalling. Pilots did not disengage the mechanism as it failed in performing its intended function.

European-manufactured fly-by-wire Airbus aircraft as well as USA Boeing hydraulic control aircraft possess similar functionality. The MCAS is not very different from other types of systems like the Alpha Protection used on fly-by-wire Airbus aircraft. Quantas Flight 72 flying an Airbus A330 met similar circumstances. The outcome was different because this occurred at a 37,000 feet elevation and not during takeoff at about a 5,000-9,000 feet elevation, giving the pilot time to take corrective action based on advice from ground support.

Figure 2. Angle of Attack, AoA sensor is heated to prevent icing.

Figure 3. Angle of Attack AoA sensor and Pitot tubes on side of the cockpit. The AoA sensor reading triggers the MCAS system, as well as the stick shaker and the stall warning.

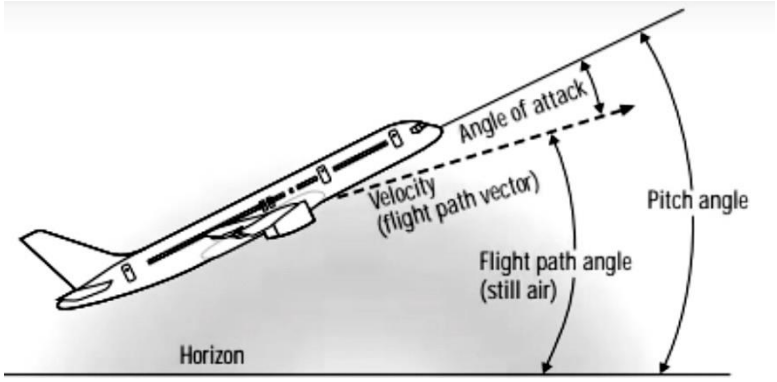


Figure 4. Angle of attack definition as the angle between the virtual wind direction and a line along the fuselage and wing.

Figure 5. Steep angle of attack of an airfoil causes flow separation and loss of lift.

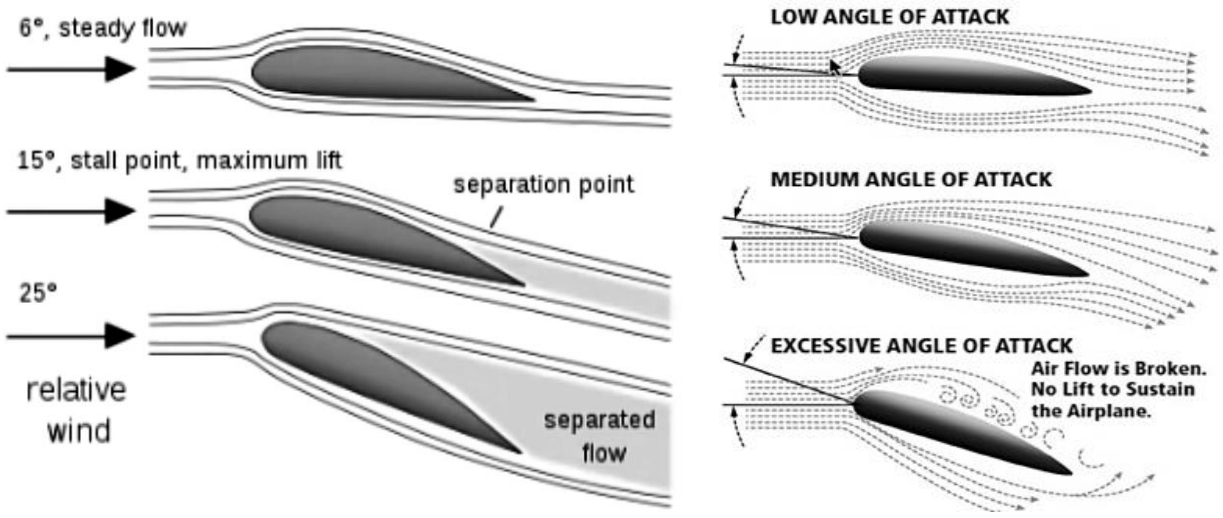


Figure 6. Angle of attack effect.

Figure 7. Buffeting (abbreviated as buffet) alert on simulator main display screen.

Figure 8. Angle of attack cockpit display.

Two safety features, an “angle of attack indicator” and an “angle of attack disagree light”, were not considered as standard safety features, and were offered as options to the airliners. The Boeing Company made at least one of the safety features, the “disagree light,” standard on future 737 Max 8 aircraft.

MCAS MANEUVER CHARACTERISTICS AUGMENTATION SYSTEM DESCRIPTION

Pitch Stability is a complex aspect of aeronautical engineering and is implemented on all airliners: "An airliner designer has to protect the aircraft from over control by the pilot at high speed while giving him adequate pitch authority at low speed. This requires a variable gearing of the elevator movement versus stick/yoke force. At low speed, the elevator shall have a large movement from a control column input, at high speed a small movement."

The moving of the engines up and forward because of lack of available height with the existing landing gears clearance did not result in an inherently unstable plane. This is due to the engines needing to be further forward than previous models, as they are physically bigger. The problem is not center of gravity balance. It may be extra lift generation at high angles of attack, even flapless. The forward mounted engines

may generate vortices which could flow over the top of the wing generating extra lift that needs wind tunnel experimental testing. The instability assessment was widely propagated immediately after the second 737 MAX crash and remains in the public's mind. What moving the engines up and forward did was change the handling characteristics to the point they were different from the previous 737 under certain flight parameters. Boeing was trying to make an old design merge with a modern fuel efficient engines to match its European competitor. The approach worked but caused complications in trying to get the new plane to feel and handle like the old one.

In order for Boeing to avoid the red tape, expense, extra time and extra pilot training of getting a new plane type certificate from the FAA, something they would be required to do if the plane is not considered just a derivative of the previous 737, Boeing developed the MCAS software to force the plane mimic the old 737 under certain flight dynamics. From the pilot's perspective, the 737 MAX had to "feel" and handle like the old 737. And in some cases, the MAX did not.

The MCAS software allowed a derivative 737 certificate from the FAA. The MCAS software was the problem. Major mistakes were made in the MCAS software system. Major mistakes. But the plane is naturally stable.

The MCAS system was originally programmed to bring the plane’s nose down if one single AoA sensor, out of two, signaled that the aircraft is in danger of encountering a stall condition with a +10 degrees AoA. “A persistent blind system that takes no notice of anything beyond one sensor with enough control to crash the plane.” It then attempts to push the nose down by forcing the angle of the plane’s horizontal stabilizer up, even if the plane has not climbed enough and was still at low altitude. If the single sensor reading is incorrect, the MCAS would activate and push the nose down anyway, even at low take-off altitude (e. g. 1,000-5,000 ft), eliminating the possibility of recovery if the aircraft was at higher altitude (e. g. 40,000 feet). Fault Tree Analysis as attempted in this work demonstrates that this amounts to an OR failure gate that doubles the overall probability of failure of the system since it would equal the sum of the probabilities of failure of each of the two sensors (e. g. 0.001 + 0.001 = 0.002). Adoption of an AND logical gate instead, would have significantly reduced the overall failure probability since the probability of failure in that case would be equal to the product of each sensor’s failure probability (e. g. 0.001 x 0.001 = 0.000,001).

The pilots could temporarily switch off the MCAS and manually control the aircraft climb, however the system reactivates itself with a time delay if a false stall condition is still detected, creating a faulty condition that could be irreversible and non-recoverable at low takeoff altitude.

Specifically, the MCAS automatically is activated when:

The Angle of Attack AoA is too high (e. g. + 10^{o}),

The automatic pilot is off,

The flaps are in the up position,

When the plane is in a sharp banking situation.

It then pushes the plane’s nose down by acting on the trim of the horizontal stabilizer at the back of the fuselage. The stabilizer trim is proportional to the Mach number. The trim is adjusted upward at a rate of 0.27 degrees per second up to a limit of 2.5 degrees / second for a duration of 9.26 seconds for each activation. The activation repeats the cycle after 5 seconds and terminates if:

The angle of Attack AoA is corrected, or

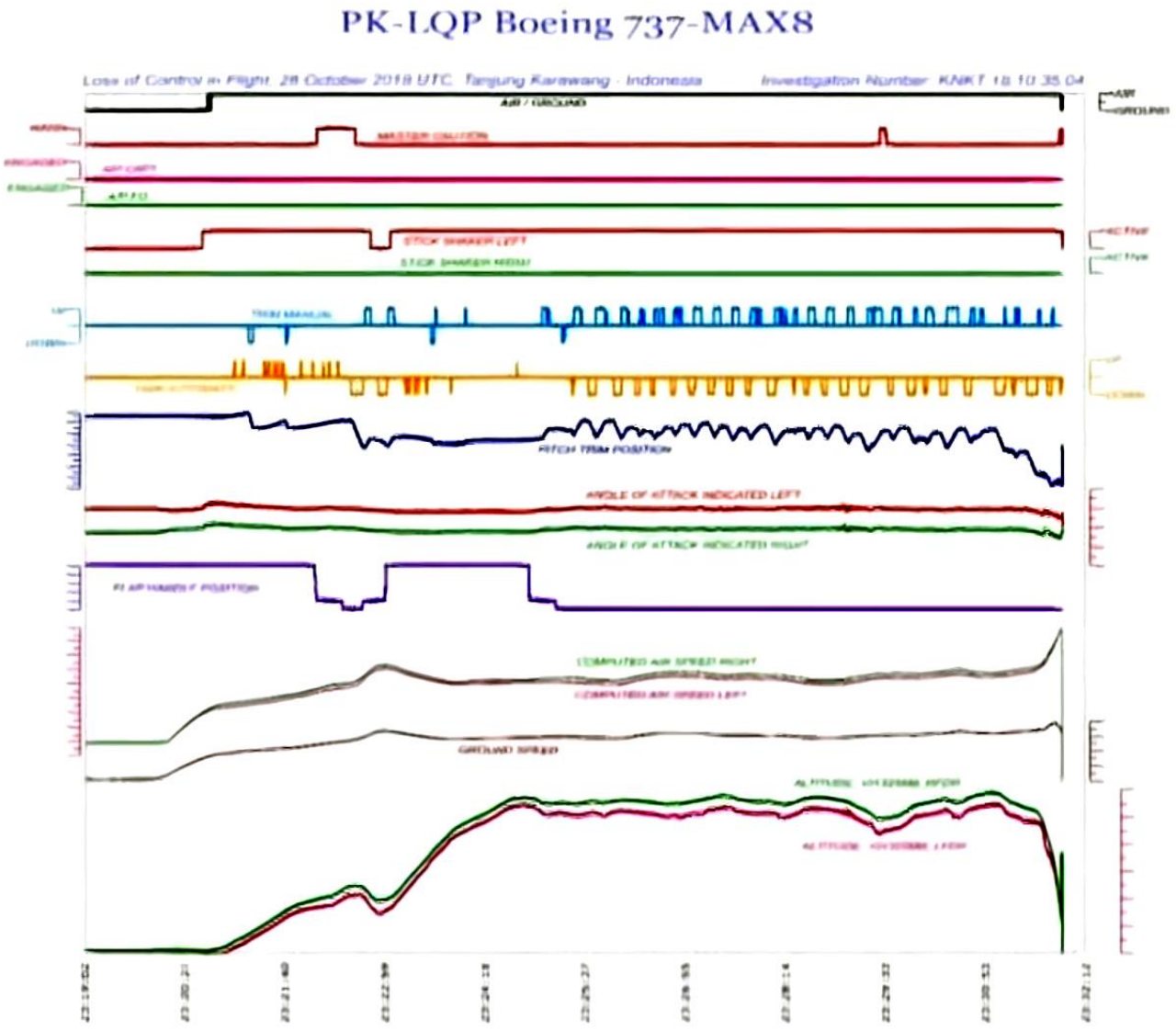
The pilots override it by manual trim.

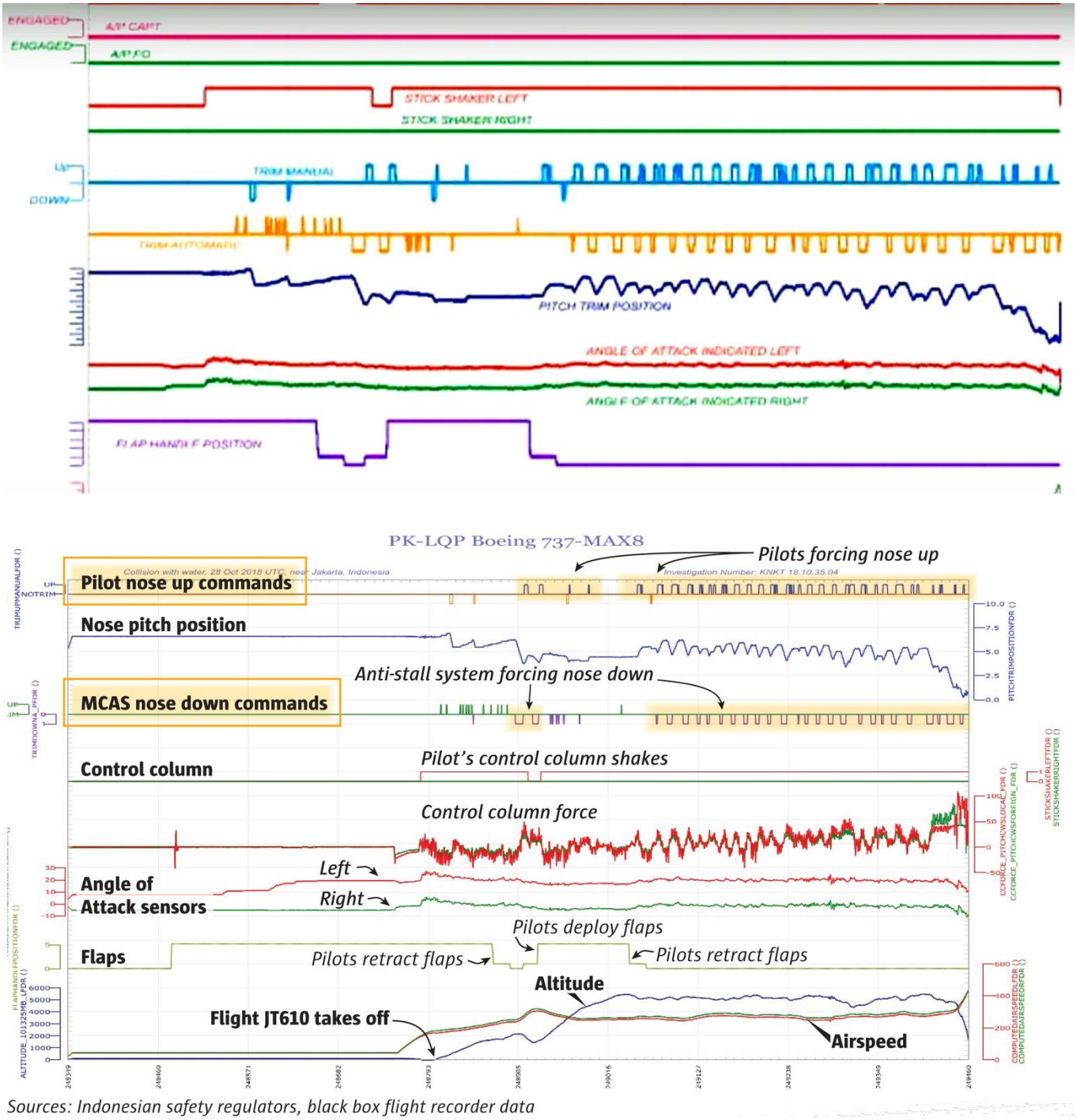
The trim system under MACS does not get deactivated by just movement of the control yoke.

The stabilizer does not reset and is not returning to where it originally was prior to each 9.26 seconds operation.

The AoAs sensors on the two sides of the cockpit are independence of each other.

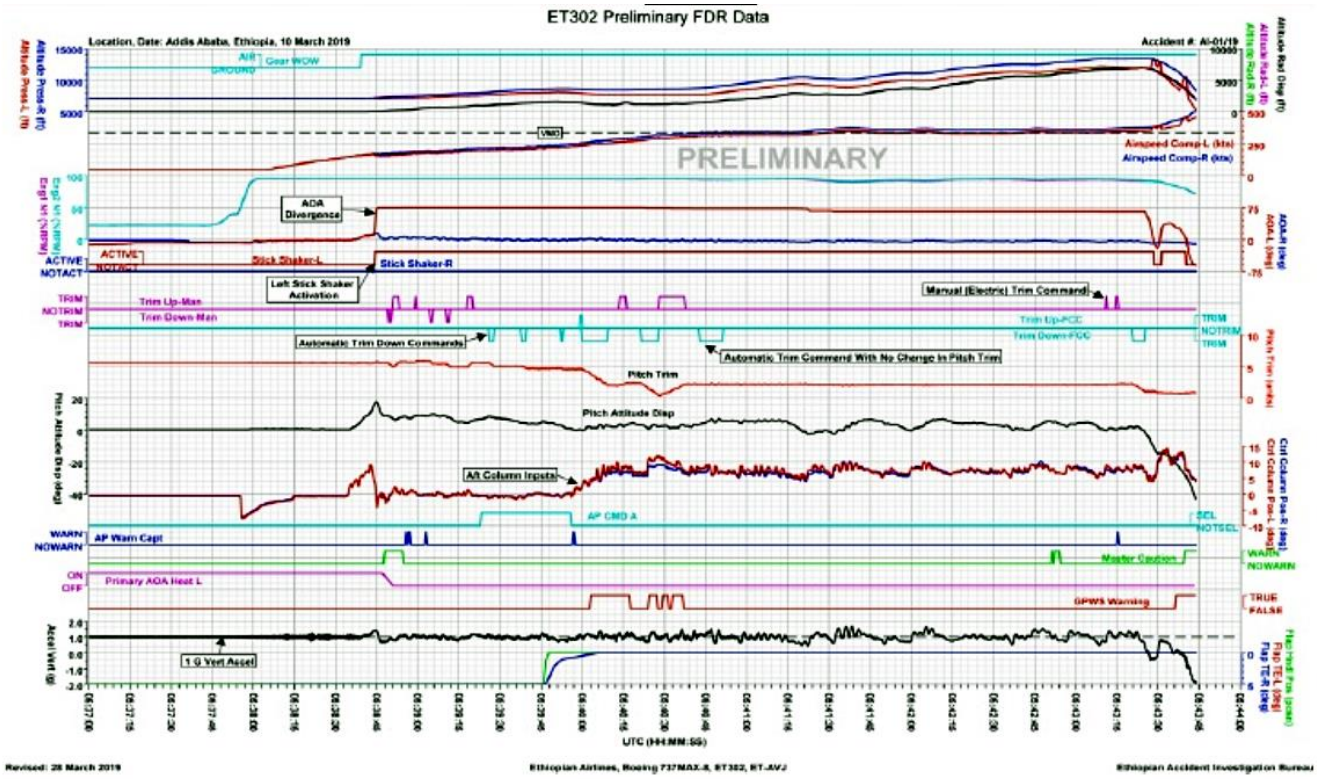
The AoA on the side that is flying the aircraft (either side) dictates the stall event.





Sources: Indonesian safety regulators, black box flight recorder data

Figure 9. The MCAS system on the Lion Air accident forced the nose of Lion Air JT610 down 26 times in 10 minutes before loss of control by the crew causing a sea crash.



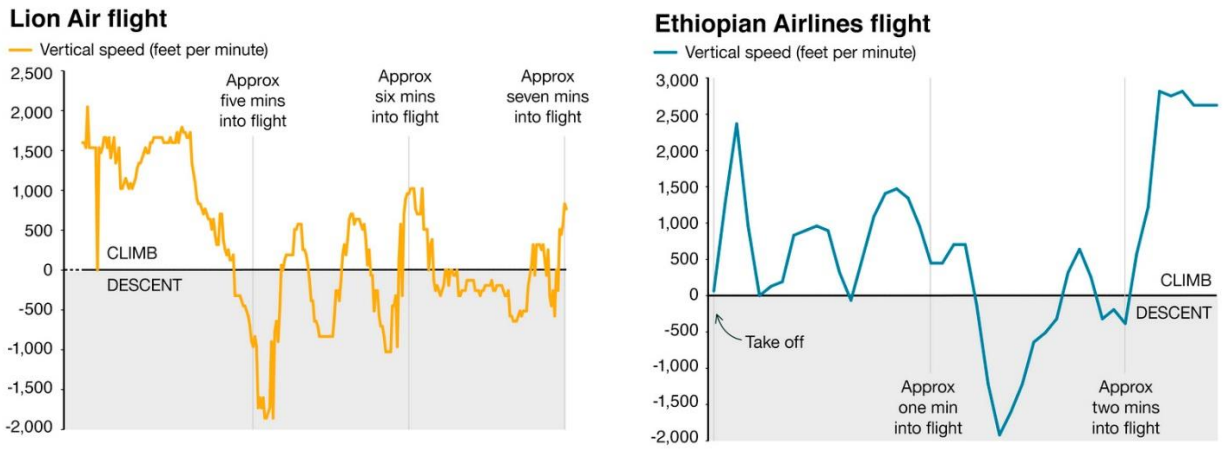


Figure 10. ET302 FDR data [7]. In most aircraft pulling on the yoke will totally disengage the auto trim and the pilots obtain control. MCAS engages in 10 sec bursts and will only disengage for 5 sec on pulling back the yoke then engages again. Vertical speed of aircraft from radar data suggest similar behavior.

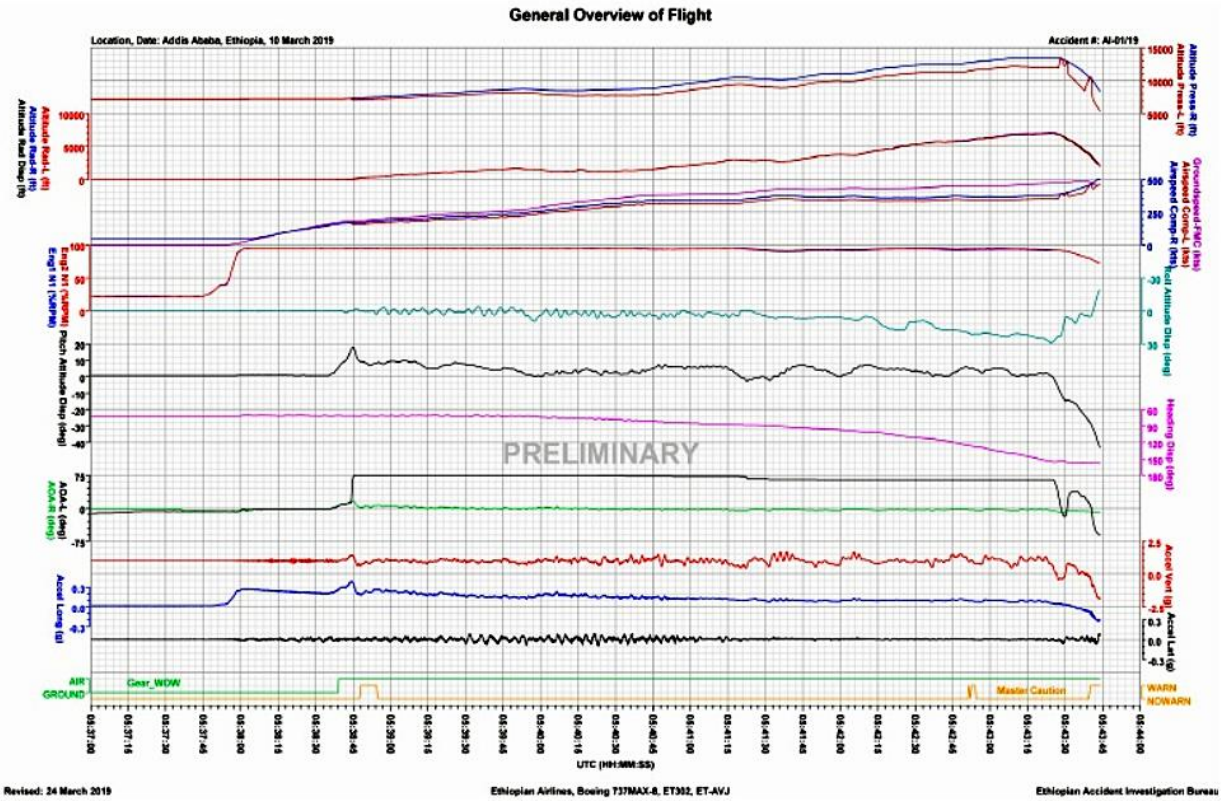


Figure 11. ET302 General Overview of flight. "On March 10, 2019, at 05:38 UTC, Ethiopian Airlines flight 302, Boeing 737-8(MAX), ET-AVJ, took off from Addis Ababa Bole Int. Airport bound to Nairobi, Kenya Jomo Kenyatta Int. Airport. Shortly after takeoff, the Angle of Attack sensor recorded value became erroneous and the left stick shaker activated and remained active until near the end of the flight. In addition, the airspeed and altitude values from the left air data system began deviating from the corresponding right side values. Due to flight control problems, the Captain was unable to maintain the flight path and requested to return back to the departure airport. The crew lost control of the aircraft which crashed at 5: 44 UTC 28 NM South East of Addis Ababa near Ejere village. [67]"

9.2.5.5 Maneuver Characteristics Augmentation System

Revised: 02/01/2019

A pitch augmentation system function called Maneuver Characteristics Augmentation System (MCAS) is implemented on the B737MAX to enhance pitch characteristics with flaps UP and at elevated angles of attack. The MCAS function commands nose down stabilizer to enhance pitch characteristics during steep turns with elevated load factors and during flaps UP flight at airspeeds approaching stall.

MCAS is activated without Pilot input and only operates in manual, flaps UP flight. The system is designed to allow the Flight Deck Crew to use the COLUMN TRIM switch or stabilizer aisle stand CUTOUT switches to override MCAS input. The function is commanded by the Flight Control computer using input data from sensors and other aircraft systems. The MCAS function becomes active when the aircraft angle of attack exceeds a threshold based on airspeed and altitude. Stabilizer incremental commands are limited to 2.5° and are provided at a rate of 0.27° per second. The magnitude of the stabilizer input is lower at high Mach numbers and greater at low Mach numbers.

The function is reset once the angle of attack falls below the angle of attack threshold or if manual stabilizer commands are provided by the Flight Deck Crew. If the original elevated AOA condition persists, the MCAS function commands another incremental stabilizer nose down command according to the current aircraft Mach number at actuation.

Figure 12. Description of Maneuver Characteristics Augmentation System MCAS.

Figure 13. Stick shaker stall warning device.

Figure 14. Horizontal Stabilizer Jackscrew.

The MCAS system normally kicks in during high banked maneuvering. Its malfunction remedy is the same as for a "runaway trim" by turning off the trim motor switches.

Trim motors are driven in one direction or the other by electrical relays by the Flight Control Computer (FCC) or from Thumb switches on the control yoke. The Trim Runaway Fault event can happen if the relay that finally control the power to the trim motor gets welded for any reason. The same can happen if the thumb switch contacts remain closed due to a malfunction. These are very rare occurrences even on a ten year old aircraft. On a new aircraft, these are extremely low probability fault events.

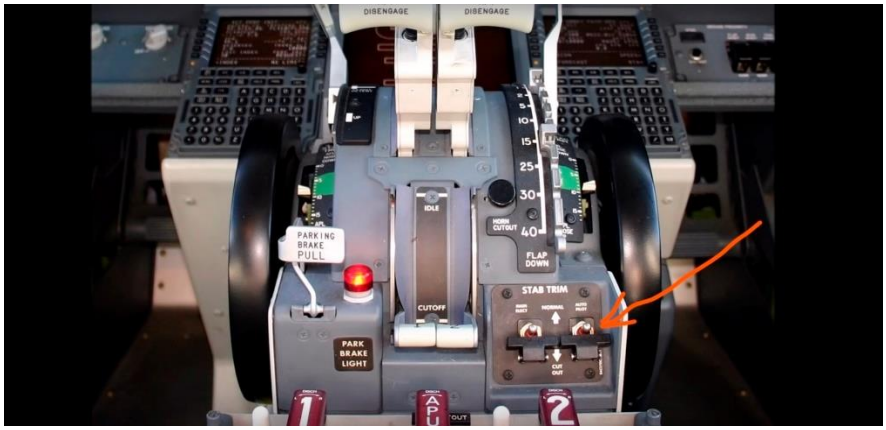


Figure 15. Trim motor switches location in cockpit.

Figure 16. Location of Trim Wheels in cockpit.

Figure 17. Steps in overriding MACS system.

Figure 18. Manual control switches on yoke. The trim system under MCAS is not stopped by simply moving the control yoke, it must be disengaged.

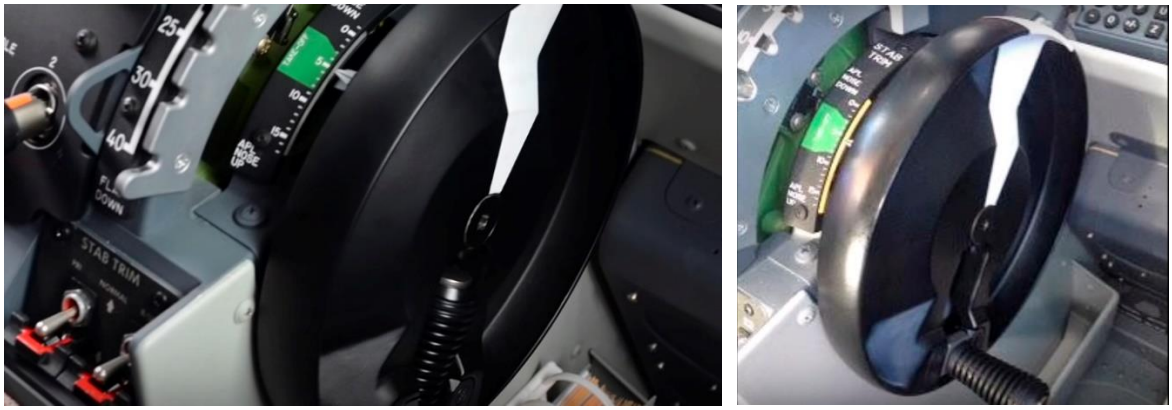


Figure 19. Manual Trim Control using hand-cranked trim wheels.

DRAFT
NOT FOR DISTRIBUTION
1/19/2020

Key highlights from the investigation report of Ethiopian Airlines Flight 302 by the Ethiopian Accident Investigation Bureau (AIB) are:

> "Altitude, airspeed readings from738 were erroneous on one side,
> Ethiopian angle of attack sensors differed by 59.2 degrees,
> Automatic nose-down commands show anti-stall system activated,
> Nose-down pitch eventually reached 40 degrees,
> Captain requested copilot 'pitch up with him'"

In hindsight the MCAS is perceived to have been hindered in its intended function by possible design flaws as it operated in the background:

1. It relied on the input data from a single angle of attack sensor, even though the aircraft had two of them. But relying on only one of them meant that if it failed, the system could deploy at the wrong time, and push the nose of the aircraft down when it was supposed to be climbing.
2. Although the pilot could use a thumb control to correct the pitch of the aircraft, MCAS would deploy repeatedly in cycles, forcing the nose down again and again.

Boeing emphasizes that there are set procedures for pilots to follow, which are meant to help them deal with uncontrolled stabilizer movements, whatever their cause. These were contained in the manual, and should have been memorized by the pilots as well. The manual did tell crews to expect automatic stabilizer movements as the plane approached stalling speed, the "same type of aircraft behavior" caused by MCAS. It has also pointed out that the day before the Lion Air crash, the same aircraft experienced similar problems, but was able to continue safely to its destination. On that flight, within seconds of take-off, the airspeed and altitude indicators gave sharply different readings. Then the nose of the aircraft began moving down of its own accord. But this time, the pilots worked out what to do about it. They cut off power to the electronics operating the stabilizers and began controlling them manually. They were assisted in what to do by a third pilot who happened to be in the cockpit, having hitched a ride aboard the plane.

FAULT TREE ANALYSIS OF ANGLE OF ATTACK AoA SENSORS CONFIGURATIONS

Configuration of two parallel AoA sensors.

Such a configuration allows successful continuous operation even if one sensor fails since the measurement's signal can propagate successfully through even if one sensor fails. Failure of such a configuration logically occurs if the first sensor AoA1 fails AND the second sensor AoA2 also fails, hence a logical AND gate is used in the Fault Tree even though a parallel physical configuration exists.

The actual physical configuration is expressed in the actual hydraulic connections and wiring as well as the computer algorithms. The logical faulty condition is described by the Boolean expression describing the Fault Tree.

The Boolean Expression logically describing the fault condition is:

$$\begin{aligned} T &= AoA1 \cap AoA2 \\ &= AoA1 AND AoA2 \\ &= AoA1.AoA2 \end{aligned}$$

where: $. \cap, AND, .$ represent the logical intersection of events .

The corresponding Failure Probability is deduced as:

$$P(T) = P(AoA1)P(AoA2)$$

where: $P(T)$ is the overall failure probability
$P(AoA1)$ is the failure probability of sensor $AoA1$
$P(AoA2)$ is the failure probability of sensor $AoA2$

EXAMPLE 1

Consider the numerical values:

$$P(AoA1) = P(AoA2) = 10^{-2}$$
$$Then:$$
$$P(T) = P(AoA1) \times P(AoA2)$$
$$= 10^{-2} \times 10^{-2}$$
$$= 10^{-4}$$

This is a substantial decrease in the failure probability, an increase in reliability and expresses the expected reward of using redundancy.

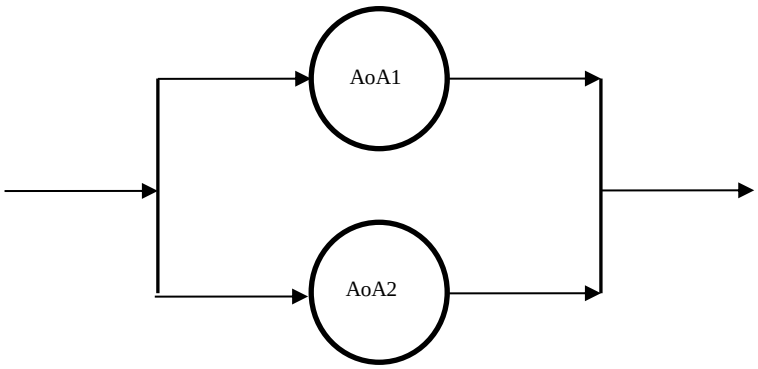


Figure 20. Physical configuration of two parallel AoA sensors.

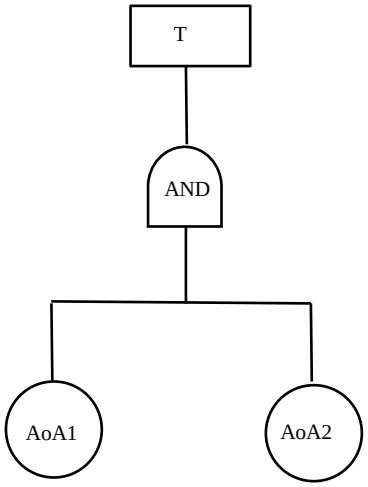


Figure 21. Fault Tree of two parallel AoA sensors configuration.

Since existing platforms in service already possess two sensors; one on each side of the cockpit, a reconfiguration along this line would substantially reduce the failure probability and allow continued safe operation in association with enhanced maintenance and training protocols.

For other secure systems two-out-of-three and three-out-of-four control logics can be implemented as discussed below.

Configuration of three parallel AoA sensors.

Such a configuration allows successful continuous operation even if two sensors fail since the signal can propagate successfully through from the remaining sensor that did not fail. Failure of such a configuration logically occurs if the first sensor AoA1 fails AND the two other sensors AoA2 and AoA3 also fail, hence a logical AND gate is used in the Fault Tree even though a parallel physical configuration exists.

The actual physical configuration is expressed in the actual hydraulic connections and wiring as well as the computer algorithms. The logical faulty condition is described by the Boolean expression describing the Fault Tree.

The Boolean Expression logically describing the fault condition is:

$$\begin{aligned} T &= AoA1 \cap AoA2 \cap AoA3 \\ &= AoA1 AND AoA2 AND AoA3 \\ &= AoA1.AoA2.AoA3 \end{aligned}$$

The overall Failure Probability is:

$$P(T) = P(AoA1)P(AoA2)P(AoA3)$$

EXAMPLE 2

Consider the numerical values:

$$P(AoA1) = P(AoA2) = P(AoA3) = 10^{-2}$$
$$Then:$$
$$P(T) = P(AoA1) \times P(AoA2) \times P(AoA3)$$
$$= 10^{-2} \times 10^{-2} \times 10^{-2}$$
$$= 10^{-6}$$

This is an even more dramatic decrease in the failure probability, an increase in reliability and a high reward for using redundancy.

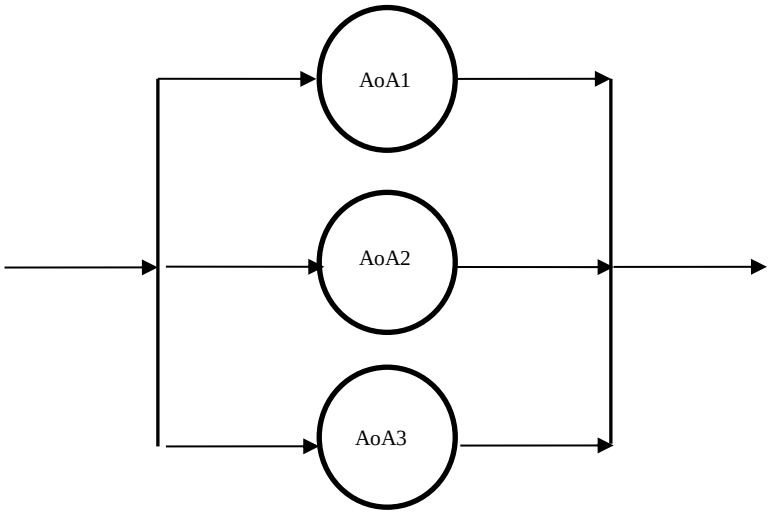


Figure 22. Physical configuration of three parallel AoA sensors.

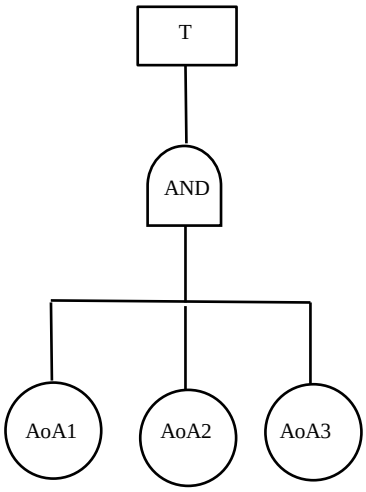


Figure 23. Fault Tree of three parallel AoA sensors configuration.

Configuration of series AoA sensors.

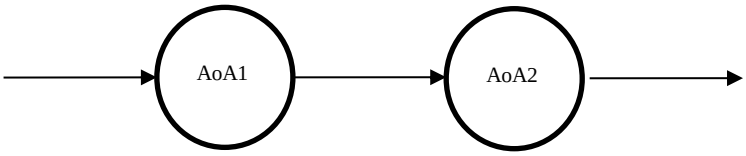


Figure 24. Physical configuration of two serial AoA sensors.

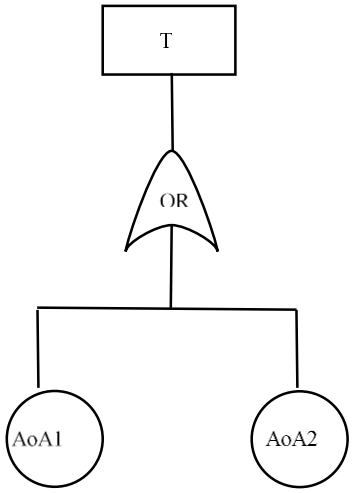


Figure 25. Fault Tree of two serial AoA sensors configuration.

Figure 26. Front view of plane equipped with AoA sensor on the left side of cockpit.

What if one single sensor is used or two sensors are used interchangeably from one trip to another. A maintenance error where one sensor is tested only once, and not twice. would not only possibly test the non-defective sensor if the setting has been switched after a trip, but also restore the defective sensor for use on the next trip. In that case, one sensor or the other is used implying an OR gate in the Fault Tree diagram, and the Boolean Expression is:

$$T = AoA1 \cup AoA2$$
$$= AoA1 OR AoA2$$
$$= AoA1 + AoA2$$

The Failure Probability is:

$$P(T) = P(AoA1) + P(AoA2) - P(AoA1)P(AoA2)$$

EXAMPLE 3

Consider the numerical values:

$$P(AoA1) = P(AoA2) = 10^{-2}$$
$$Then:$$
$$P(T) = P(T) = P(AoA1) + P(AoA2) - P(AoA1)P(AoA2)$$
$$= 10^{-2} + 10^{-2} - (10^{-2} \times 10^{-2})$$
$$= 2 \times 10^{-2} - 10^{-4}$$
$$= 0.0200 - 0.0001$$
$$= 0.0199$$
$$\simeq 0.02$$

Such a configuration is not recommended since it even doubles the probability of failure and totally defeats the concept of using two sensors for the purpose of redundancy and gives a false sense of security even though its failure probability is double that of using a single sensor.

Configuration of two-out-of-three logic AoA sensors.

The Indicated Airspeed System on the 737 is triplex redundant, one for P1, one for P2 and a standby system for the backup instrumentation. All 3 measurements can be accessed, provided to the control system and displayed on both pilots' screens if two out of the three agree.

Such a logic allows the choice in the displays and control actions to polling and choosing the most plausible two readings out of three sensors, possibly eliminating any conflicting or suspect pair of readings by the sensors that have a large discrepancy implying a possible defective sensor.

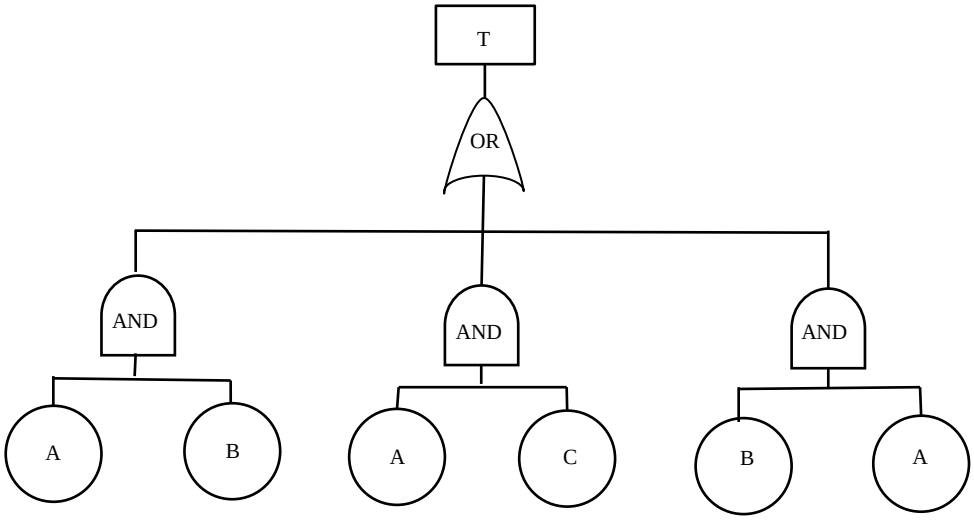


Figure 27. Fault Tree of Two-out-of-three logic sensors configuration.

For three AoA sensors designated as A, B, C, the Boolean expression for a two-out-of-three logic would be:

$$\begin{aligned} T &= (A \cap B) \cup (A \cap C) \cup (\mathrm{B} \cap C) \\ &= (A \mathrm{AND} B) \mathrm{OR} (A \mathrm{AND} C) \mathrm{OR} (\mathrm{B}\,\mathrm{AND} C) \\ &= (A.B) + (A.C) + (\mathrm{B}.C) \end{aligned}$$

The Failure Probability is:

$$P(T) = [P(A)P(\mathrm{B})] + [P(A)P(\mathrm{C})] + [P(\mathrm{B})P(\mathrm{C})]$$

EXAMPLE 4

Using the small probabilities approximation:

$$P(a+b+c) \simeq P(\mathrm{a}) + P(\mathrm{b}) + P(\mathrm{c}),$$

consider the numerical values:

$$\begin{aligned} & P(A) = P(\mathrm{B}) = P(\mathrm{C}) = 10^{-2} \\ & Then: \\ & P(T) = [P(A)P(\mathrm{B})] + [P(A)P(\mathrm{C})] + [P(\mathrm{B})P(\mathrm{C})] \\ & \quad \simeq (10^{-2} \times 10^{-2}) + (10^{-2} \times 10^{-2}) + (10^{-2} \times 10^{-2}) \\ & \quad = 3 \times 10^{-4} \end{aligned}$$

Configuration of three-out-of-four logic AoA sensors.

For four AoA sensors designated as A, B, C, D, the Boolean expression for a three-out-of-four logic would be:

$$\begin{aligned} T &= (A \cap B \cap C) \cup (A \cap B \cap D) \cup (\mathrm{A} \cap C \cap D) \cup (\mathrm{B} \cap C \cap D) \\ &= (A \mathrm{AND} B \mathrm{AND} C) \mathrm{OR} (A \mathrm{AND} B \mathrm{AND} D) \mathrm{OR} (\mathrm{A}\ \mathrm{AND} C \mathrm{AND} D) \mathrm{OR} (\mathrm{B}\ \mathrm{AND} C \mathrm{AND} D) \\ &= (A.B.C) + (A.B.D) + (\mathrm{A}.C.D) + (\mathrm{B}.C.D) \end{aligned}$$

The Failure Probability is:

$$P(T) = [P(A)P(\mathrm{B})P(\mathrm{C})] + [P(A)P(B)P(D)] + [P(A)P(\mathrm{C})P(D)] + [P(\mathrm{B})P(\mathrm{C})P(D)]$$

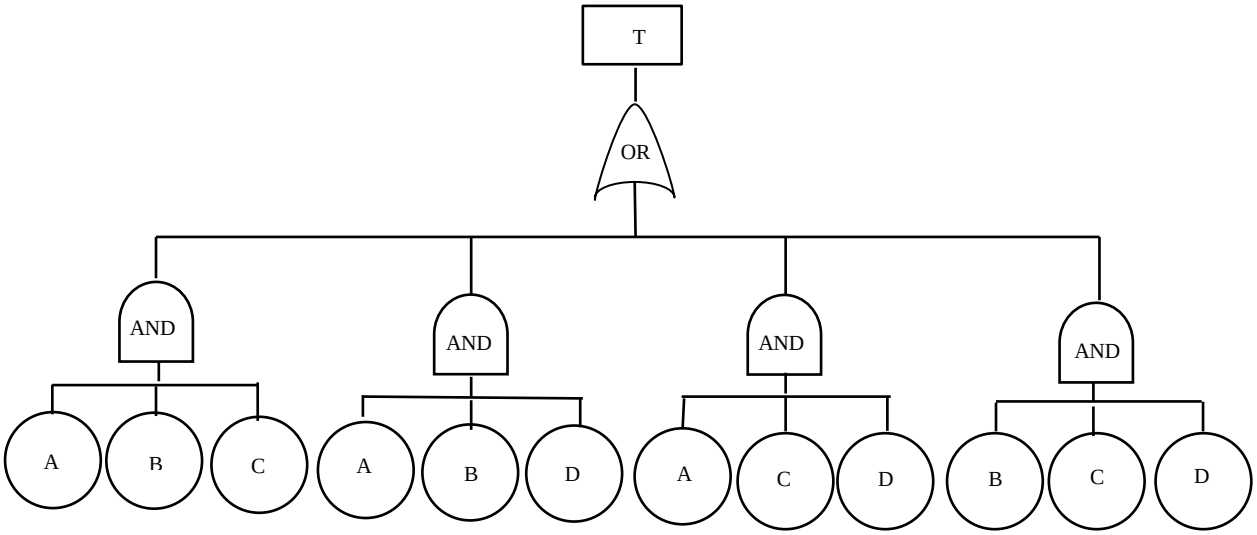


Figure 28. Fault Tree of Three-out-of-four logic sensors configuration.

EXAMPLE 5

Using the small probabilities approximation:

$$P(a+b+c+d) \simeq P(\mathrm{a}) + P(\mathrm{b}) + P(\mathrm{c}) + P(\mathrm{d}),$$

consider the numerical values:

$$P(A) = P(\mathrm{B}) = P(\mathrm{C}) = P(D) = 10^{-2}$$

Then:

$$\begin{aligned} P(T) &= [P(A)P(\mathrm{B})P(\mathrm{C})] + [P(A)P(B)P(D)] + [P(A)P(\mathrm{C})P(D)] + [P(\mathrm{B})P(\mathrm{C})P(D)] \\ &= (10^{-2} \times 10^{-2} \times 10^{-2}) + (10^{-2} \times 10^{-2} \times 10^{-2}) + (10^{-2} \times 10^{-2} \times 10^{-2}) + (10^{-2} \times 10^{-2} \times 10^{-2}) \\ &= 4 \times 10^{-6} \end{aligned}$$

This would be indeed lead to a substantial decrease in the failure probability and a spectacular increase in the level of safety.

ELEVATOR BLOW BACK PHENOMENON

The Elevator Blow back phenomenon occurs when the elevator is gradually blown back to lower and lower elevation angles by the pressure of the air as the aircraft speed increases. The hydraulic actuators cannot overcome the force of the air and gradually back down if the force of the air flow grows too strong.

Pilots are restricted in all airliner flying to stay below 250 kts below 10,000 ft, so they should not go there unless they have declared an emergency.

The blow back system is designed to prevent the structural destruction of a control surface when design speeds are exceeded, with the surface in the fully deflected position. Some actuators have a relief valve to prevent its force exceeding limits, if for any reason the Power Control Unit (PCU) gets stuck in its full travel.

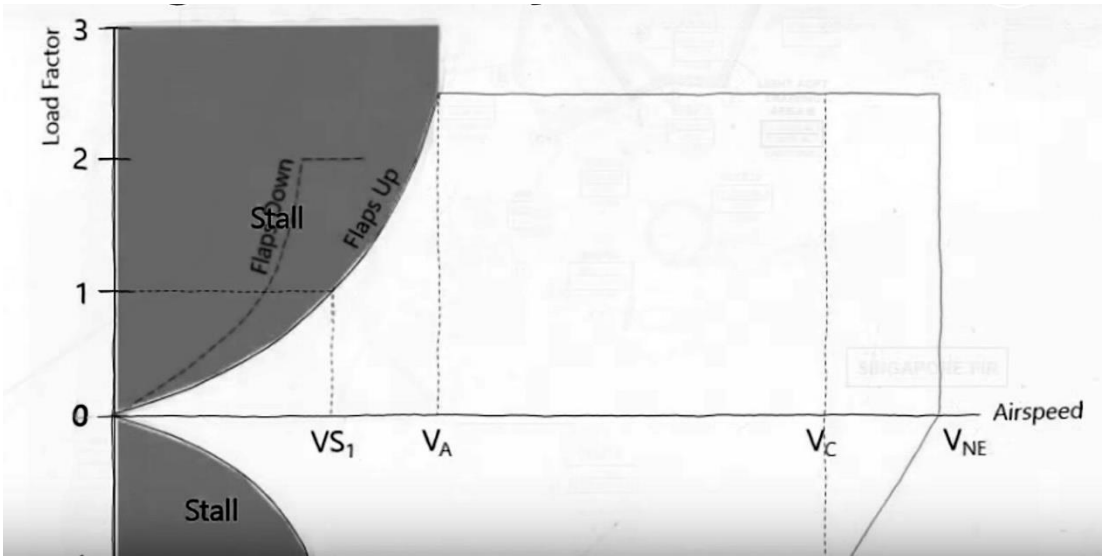


Figure 29. Aircraft Flight Envelope shows the regions of the Load factor and airspeed where stall would be expected.

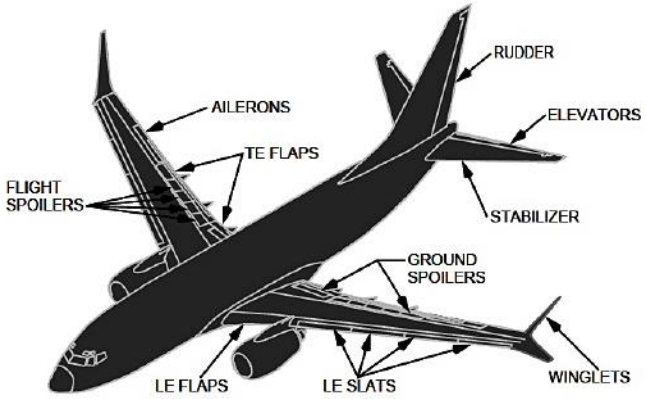


Figure 30. Plane flight control surfaces.

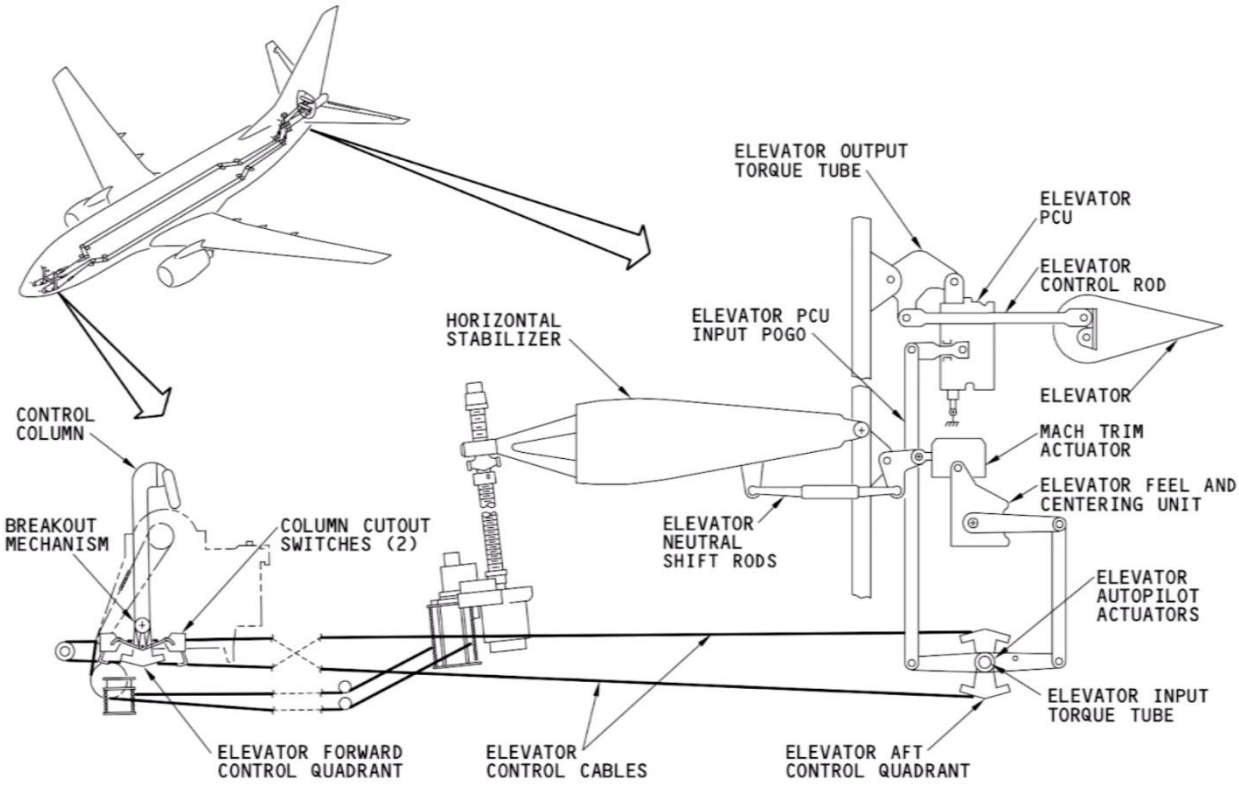


Figure 31. Elevator and Horizontal Stabilizer control functions.

Figure 32. Elevator and horizontal stabilizer back view.

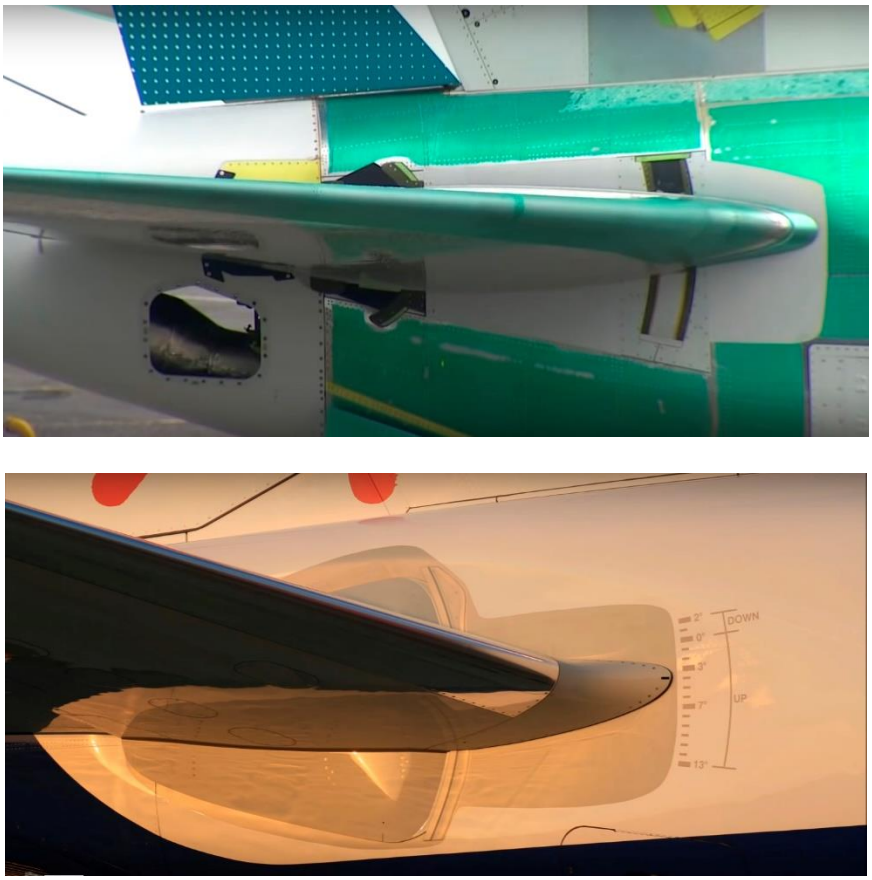


Figure 33. Horizontal stabilizer trim front view.

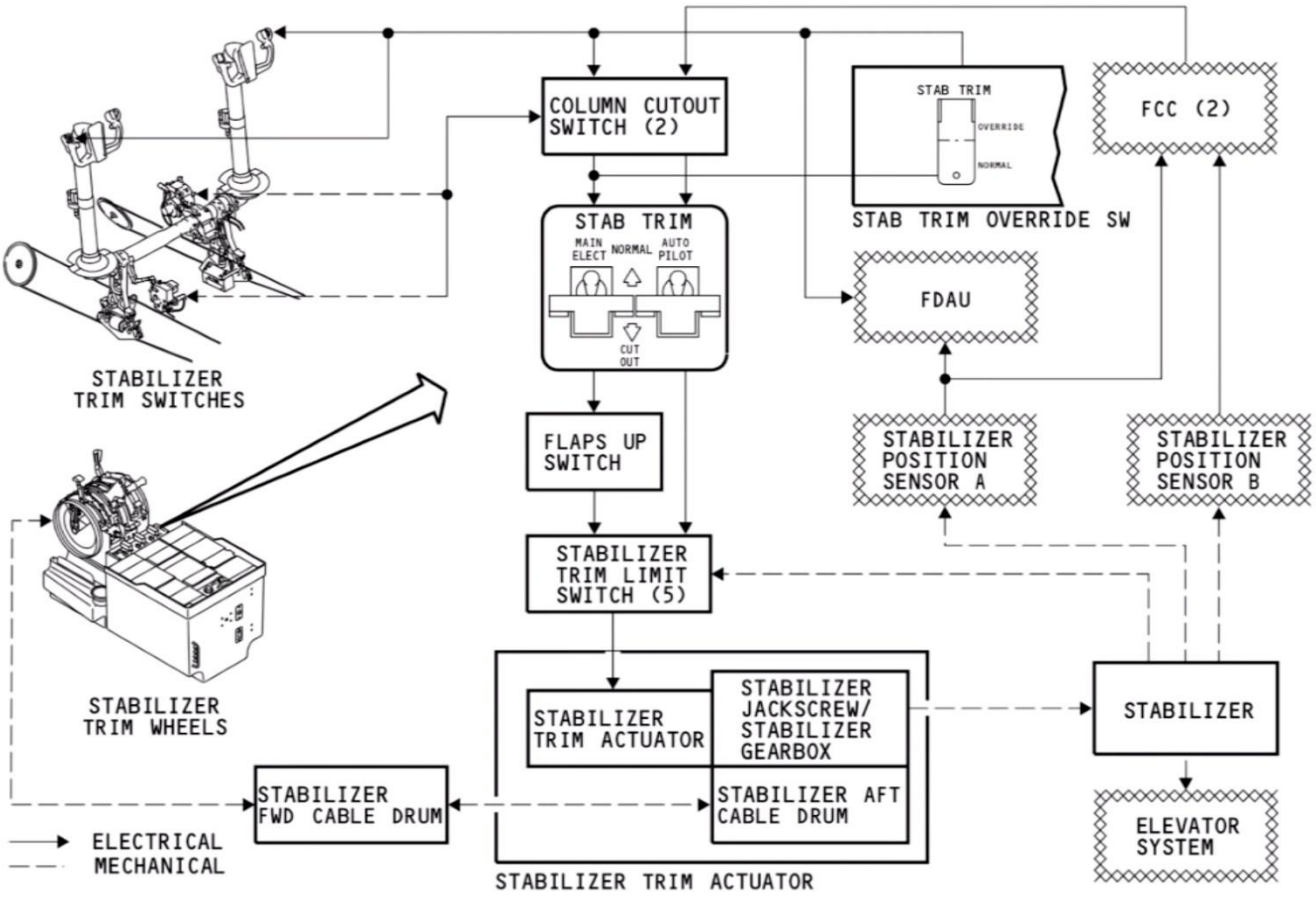
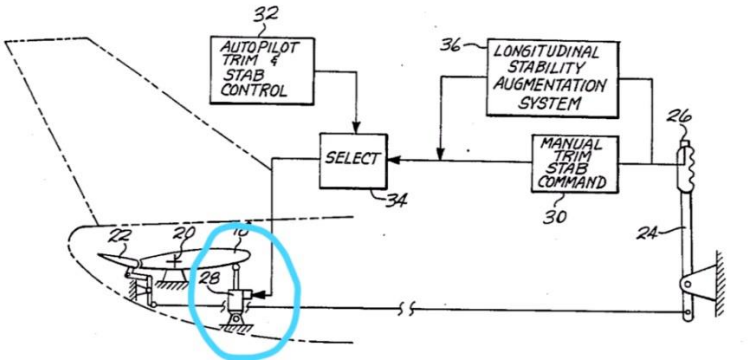


Figure 34. Horizontal trim control diagram.



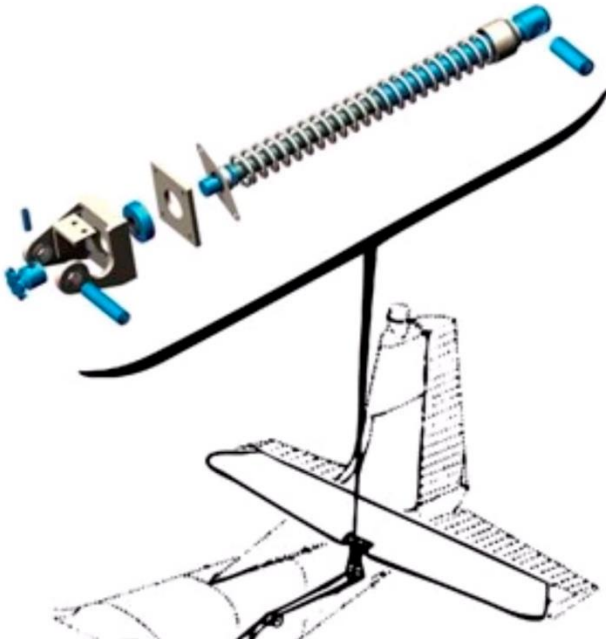


Figure 35. Mechanical configuration of a jackscrew trim control.

Blow back applies to most aircraft, if they operated out of their published flight envelope for structural damage from over-speed to be avoided; and it is a normal, expected response. It may have been a factor in the FlyDubay 981 accident. According to Wikipedia:

> "At a height of 900 m, there was a simultaneous control column nose down input and a trimming of the horizontal stabilizer to a nose down position, from -2.5 deg (6.5 units) to +2.5 deg (1.5 units).
>
> The result was that after the aircraft climbed to about 1,000 m, it then began a rapid descent with negative vertical acceleration of -1g. The subsequent crew attempts to recover were not sufficient to avoid an impact with the ground.
>
> At 00:41:49, the aircraft hit the runway approximately 120 m from the threshold with a speed of over 600 km/h and a nose down pitch exceeding 50 degrees."

Some pilot circles suggested that if a blow back phenomenon occurrence is confirmed for the 737 at the speeds and the altitudes flown, this may have happened at the end of the JT610 flight and probably the ET302 flight. In both cases the pilots were flying faster than normal at low altitudes: 5,000 ft pressure altitude for JT610, and 9,000 ft for ET302. This was to build a safety margin while sorting out stall warning and flight control problems.

When a pilot experiences a stall warning signal like a stick shaker, his reaction is to lower the nose and increase the speed. His goal is to build a margin to an eventual stall. If he simultaneously has an "Unreliable airspeed" warning, the built margin will be larger.

The recognized operational remedy to a blow back induced dive is a full nose up trim application, for a long time. The throttles brought to idle condition and the air brake would also be helpful. The reaction to trim is slow and the aircraft would be heading down. The reflex is not to trim but to pull for all there is, by both pilots as they have seconds to stop the dive.

A design remedy negating the effects of Blow back negated is by resizing the stabilizer / elevator. An alternate approach is to re-profile the tail by extending its size resulting in a less severe pressure wave.

AoT SENSORS FAILURE MODES

The problem with the AoR sensors does not appear to be in the software, since it would occur on the different versions of the aircraft, inferring a possible physical failure mode. The “non-return to-zero” failure mode is prominently listed.

Two flight control computers are programed by two different teams as a method of ensuring that no code is written duplicating to the computer what is not a dual failure under the same circumstances. Swapping to the other side for control should avoid the fault. It must be noted that the computers are getting analog signals as inputs.

A Federal Aviation Administration incident database that lets pilots anonymously self-report, one USA incident in November 2018 occurred when a commercial airline pilot reported that during takeoff trouble started when he engaged the autopilot after leveling off from takeoff. As the autopilot was engaged and "within two to three seconds the aircraft pitched nose down," in a manner steep enough to trigger the plane's warning system “Descending,” followed by an almost immediate: “Don’t sink, Don’t sink!” warning. The plane resumed climbing after the crew disengaged the autopilot.

Peter Lemme [5], a former flight engineer at the Boeing Co., identifies the failure modes of the AoA sensors, as discussed in the context of a paper pertaining to Airbus systems as shown in the tables displayed in Fig. 34.

Table 1. Different sensor faults to be detected

Failure type	Parameter
small bias	between 0.5 and 5deg
slow sensor drift	with slope magnitude between 0.2 and 10deg/s
large bias	between 5 and 180deg
freezing	at current value
oscillatory failure	with an amplitude of 0.5-25deg at 0.5-1Hz
fast sensor drift	with slope magnitude between 10 and 25deg/s
excessive sensor noise	with a standard deviation between 0.4 and 4deg
non-return-to-zero	random sequence of step signals with a minimum amplitude of 2deg

The actual cause of these sensor faults are not the main topic of this paper. They may result from malfunctions of the sensors itself (as short-circuits), of the sensor’s heating, of the signal conversion from analog to digital or simply from aging or external influences as temperature or dust, just to name a few examples.

Table 4. Different sensor faults to be detected

Failure type	Parameter setting	min/max detection time	mean
bias - small	4deg	0.67s / 14.6s	1.71s
bias - large	8deg	0.04s / 0.08s	0.06s
drift - slow	1deg/s	2.11s / 6.64s	4.05s
drift - slow	8deg/s	0.69s / 1.33s	1.07s
drift - fast	25deg/s	0.06s / 0.10s	0.07s
excessive sensor noise	with a standard deviation of 0.6deg	0.04s / 0.31s	0.11s
frozen sensor signal	at current value	10.48s / 10.92s	10.84s
non-return-to-zero	with an amplitude of 2deg	0.12s / 0.24s	0.18s
oscillatory failure - small	2deg at 0.5Hz	3.08s / 8.68s	7.46s
oscillatory failure - large	5deg at 0.5Hz	0.04s / 0.08s	0.06s

Figure 36. Identified failure modes of AoA sensors [5]. Note the suspected "non-return-to-zero" failure mode.

Peter Lemme [5] offers the following recommendations as a summary of his analysis:

> "The source of the AoA vane error must be found and fixed or explained. The flight deck effects of stick shaker, Elevator Feel Shift Module (EFSM) activation, Airspeed and Altitude disagree may overwhelm some flight crews (feared for ET302 in particular). The fact that these features have existed on 737 for decades without any reported incident is in marked contrast.
> MCAS authority and ability to reset must be rectified.
> MCAS use of a single input and without the ability to reject misleading data must be rectified. It is better for MCAS to be fail-safe on AoA disagree unless the flight scenario where MCAS is needed overlaps sufficiently to AoA disagree.
> The aft-column cutout switch must either be restored with MCAS, or there must be evidence that recovery from an MCAS failure would not benefit from it.
> Does Speed Trim bear a redesign to address its single sensor aspects and to make it fail-safe?
> Does a special alert need to be applied with MCAS application to allow the flight crew to recognize MCAS separate from Speed Trim?
> Should the ability to use electric stab trim be retained if the autopilot trim command malfunctions?"

DISCUSSION

The 1952 innovative high-flying, pressurized-cabin, jet-powered De Havilland /BOAC Comet-1 jet in 1953-1954 had three crashes within a year, and this led to its abandonment. The pressurization/depressurization cycles on the fuselage over a given time span, were faster than the

equivalent cycles in the slower, propeller-driven airplanes, and this lead to metal fatigue that caused the catastrophic failure of the fuselage. In one case, a fracture started in the corner atop the aircraft where radio aerials were housed and continued for eight feet, passing directly through a window frame in its path. Fatigue failure cracks caused by stress concentration at the corners of square, rather than circular windows, developed in the fuselages around doors and window apertures as the aircraft were subject to repeated pressurization cycles. The particular form of used riveted construction could not contain the stretching forces at work on the aircraft's stressed hull. Discoloration and crystallization of the metal occurred as a telltale evidence of metal fatigue. At high altitude, after many pressurization cycles, the Comet-1's fuselage simply lost their ability to contain high air pressure, and three planes literally exploded while taking off killing all on board: two over the Mediterranean as they climbed in January and April from Rome's Ciampino airport, and a third was caught in a thunder squall on the Calcutta to Delhi leg of a BOAC flight from Singapore to London. The Comet-1 flights were grounded, and its production was halted.

The Boeing 707, entered service in 1958, at the same time as the much smaller Comet-4. Eight hundred and fifty-five 707s were produced leading the USA into dominance in the jet age. The fate of the Comet-1 hopefully will not be the same for the Boeing 737 Max with the introduction of new alarms and recovery strategies; as it is only one crash away from meeting the same fate.

Automation has undeniably contributed to the excellent safety record of modern aviation, both civilian and military. The Airbus A series aircraft have anywhere between 80 to 120 million lines of code depending on the type and configuration. The operational record always provides clues to future improvements as lessons are learned and remedies are envisioned and implemented. Improved failure detection configurations must be implemented in future manufactured platforms. The training simulators must be programmed to replicate the failure modes of the MCAS system and reflect the learned experience. The airflow over a wing is what the AoA sensor is supposed to measure so a better alarm could be placed on the wing as it loses lift.

The "Mistakenly" determination by the crash investigators means that the pilots make an error in flying, whilst "automatically activated" MCAS system without the pilots' knowledge or signaling its activation means the designers of the aircraft made an error in the design. Using "only one sensor" on a critical attribute of the airplane that can cause it to take control of and crash the plane would make it appear that a design error occurred. Not training all pilots on the existence of a new system and how it functioned, and making it clear how to turn it off upon malfunction is another regrettable management tragic error.

Based on economic considerations, airlines tended to eliminate the Flight Engineer function. A reported instance where recovery from a faulty situation was successful was when a jump seat pilot identified it and assisted the pilots in the recovery process. Flight engineers have the big picture on the air-frame and train to know that air frame operates. The pilots fly the aircraft while the flight engineer monitors and operates the systems.

As the MCAS system has such authority to cause the plane to crash, it should be multiply redundant to prevent a single source of corrupt data from causing a catastrophic loss of life. The level of automation of the aircraft, the behind the scenes systems, the risk analysis processes, the oversight by the regulator, the conversion training, the level of training generally, and the manual flying skills of the crews are under review.

The recent events are identifying an unforeseen risk of flying airliners too fast at low altitudes and performing banking procedures that initiate the MCAS system which would be forcing the horizontal stabilizer to full nose down. The Lion Air JT610 flight crew apparently were not cognizant about the functioning of the MCAS system and about a potential blow back problem. After a period of time, the elevator is going to lose, and the stabilizer is going to win if the airspeed exceeds 300 knots at low altitude. The Ethiopian Airline ET302 flight crew probably knew about the MCAS system but not about the danger of flying too fast being prone to the blow back phenomenon while sorting out the MCAS.

The Boeing Company announced that it would reduce production of the 737 MAX by 20 percent, before announcing that its aircraft orders in in the first quarter of 2019 fell to 95 from 180 a year earlier. There was total of 5,012 orders by airlines and other buyers for the Boeing 737 MAX ($80 million) family of aircraft, with 376 delivered by April 2019. In the narrow-body single-aisle airline market it is in competition in narrow-body Airbus A-320 neo ($100 million), Russia with the United Aircraft Corporation's Irkut MC21-300, and China with the Commercial Aircraft Corporation of China Comac light-weight carbon-composites C919 ($43 million).

Boeing is considering a Middle of the Market (MOM) new model 797 airplane for the middle of the next decade that could fly on medium range routes as a replacement for the 757. Airlines around the world, including the USA need to retire their old 757s and find the 737 to be too small to accommodate the airlines' needs, and the 777 and 787 too large and costly to fly. As the world's second-largest economy, China alone is expected to need some 7,690 airplanes.

In 2018 there was one fatal accident for every 2,520,000 flights, according to the Aviation Safety Network. In the previous generation, the adage: "If it is not Boeing, I am not going," prevailed and would hopefully return. Price is not the sole factor for airlines in buying their planes. Overall quality, reliability, maintenance, and readily available replacement parts, as well as the pilot and mechanic training that manufacturers provide, are also important.

Safety in engineering systems is assured by excellence in design, reliability, performance, durability, and resilience. It is dependent on overlapping redundancies that correct and eliminate failures in operating systems. These redundancies add to the cost of the manufactured goods and some are necessary despite the added cost. Detailed complex system engineering evaluates the redundancies and proves that each is required to ensure with high reliability adequate performance levels. The risk of reduced profit compared with the risk of lost capital should be an economic consideration. In the world of aviation, as in other critical engineering fields, everything comes down to safety; not just cost and profit, as a design priority.

REFERENCES

1. Natalie Kitroeff, David Gelles and Jack Nicas "The Roots of Boeing's 737 Max Crisis: A Regulator Relaxes Its Oversight," The New York Times, Business, July 27, 2019. https://www.nytimes.com/2019/07/27/business/boeing-737-max-faa.html
2. M. Ragheb, "Safety Analysis of Nuclear Reactor Systems," https://mragheb.com/NPRE%20457%20CSE%20462%20Safety%20Analysis%20of%20Nuclear%20Reactor%20Systems/index.htm , 2019.
3. M. Ragheb, "Probabilistic and Possibilistic Fault Tree Analysis,"https://mragheb.com/NPRE%20457%20CSE%20462%20Safety%20Analysis%20of%20Nuclear%20Reactor%20Systems/Probabilistic%20and%20Possibilistic%20Fault%20Tree%20Analysis.pdf, 2019.

4. L. Tsoukalas, G. W. Lee, and M. Ragheb, "Anticipatory Monitoring and Control in a Process Environment," IEA/AIE '89 Proceedings of the 2nd International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, Volume 1, pp.278-287, 1989, Digital Library, Association of Computing Machinery, ACM.
5. Peter Lemme, "Ethiopian ET302 Similarities to Lion Air JT610," https://www.satcom.guru/2019/03/ethiopian-et302-similarities-to-lion.html , March 19.2019.
6. Chris Brady, "The Boeing 737 Technical site," http://www.b737.org.uk/mcas.htm , September 1999.
7. "Aircraft Accident Investigation Bureau Preliminary Report," Report No. AI-01/19, Federal Democratic Republic of Ethiopia Ministry of Transport, Aircraft Accident Investigation Bureau, Aircraft Accident Investigation Preliminary Report Ethiopian Airlines Group B737-8 (MAX), Registered ET-AVJ 28 NM South East of Addis Ababa, Bole International Airport March 10.

APPENDIX I

LEAP-1B ENGINE CHARACTERISTICS

The 737 originally was equipped with the Pratt & Whitney JT-8 series jets, which had an inner fan diameter of 49.2 inches. They looked like cigars, long and skinny. In comparison, the LEAP-1b engines on the Max 8 have a diameter of 69 to 79 inches, nearly 20 inches more than the original. The back of the engine has a serrated edge on the max.

The CFM LEAP-1B28B engine is a high bypass, dual rotor, axial flow turbofans. The engine consists of 3 major assemblies: Low Pressure Compressor (LPC), core engine, and Low Pressure Turbine (LPT). The core engine consists of a two-stage high pressure turbine (HPT) which drives the ten-stage high pressure compressor (HPC). The four-stage integrated fan and low-pressure compressor (booster) is driven by a five-stage LPT. The annular designed combustion chamber increases the HPC discharge air velocity to drive the high- and low-pressure turbines. An accessory drive system provides drive requirements for engine mounted aircraft accessories and is driven by the high-pressure module. The accessory drive system includes two sub-modules which can be removed or installed at engine level, the accessory gearbox (AGB) and the transfer gearbox (TGB).

According to the engine's FAA Type Certificate Data Sheet (TCDS) E00088EN, Revision 4, dated November 30, 2018, the engine has a maximum takeoff thrust rating of 29,317 pounds flat-rated to 86°F (30°C) and a maximum continuous thrust rating of 28,690 pounds flat-rated to 77°F (25°C).

The large size of the LEAP-1B engine with its higher bypass ratio necessitated their emplacement on the 737 MAX wings further to the front and higher compared with the original 737NG design. This remedy was adopted in lieu of adopting a higher ground-clearance landing gear. Such a design choice, without lengthening the length of the fuselage affected the location of the aircraft's center of mass. The nose has the tendency to go up when power is applied.

Moving the entire wing attachment assembly forward to accommodate the larger engines, and the larger power of the engine created a nose-up situation in banking situations with a supplemental lift created by the engines nacelles. This necessitated the use of the MCAS system to correct any unstable situation created around the change of the center of mass and the bending moment encountered causing lift asymmetry in banking situations.

The moving of the engines up and forward did not result in an inherently unstable plane. This assessment was widely propagated immediately after the second 737max crash and remained in the public's mind. What moving the engines up and forward did was change the handling characteristics to the point they were different from the previous 737 under certain flight parameters. Boeing was trying to make an

old design merge with modern engines. And it worked. But it caused complications in trying to get the plane to feel and handle like the old plane.

In order for Boeing to avoid the red tape, expense, extra time and extra pilot training of getting a new plane type certificate from the FAA, something they would be required to do if the plane is not considered just a derivative of the previous 737, Boeing developed the MCAS software to force the plane mimic the old 737 under certain flight dynamics. From the pilot's perspective, the 737max had to feel and handle like the old 737. And in some cases, the MAX did not.

The MCAS software allowed a derivative 737 certificate from the FAA. The MCAS software was the problem. Major mistakes were made in the MCAS software system. But the plane is naturally stable.

There was reliance on complex software solutions to what appear to be aerodynamic issues created by modifying an established and previously safe design. The addition of larger more fuel efficient engines to the established 737 design significantly changed the aerodynamic flight characteristics of the design. Redesigning the product physically in addition to software modifications was needed to accommodate the new situation. When software was used to overcome a physical design problem, complexity was added resulting in new unforeseen failure modes.

Figure Ia. LEAP-1B engine front and rear views with a large fan allowing a high bypass ratio (BPR).

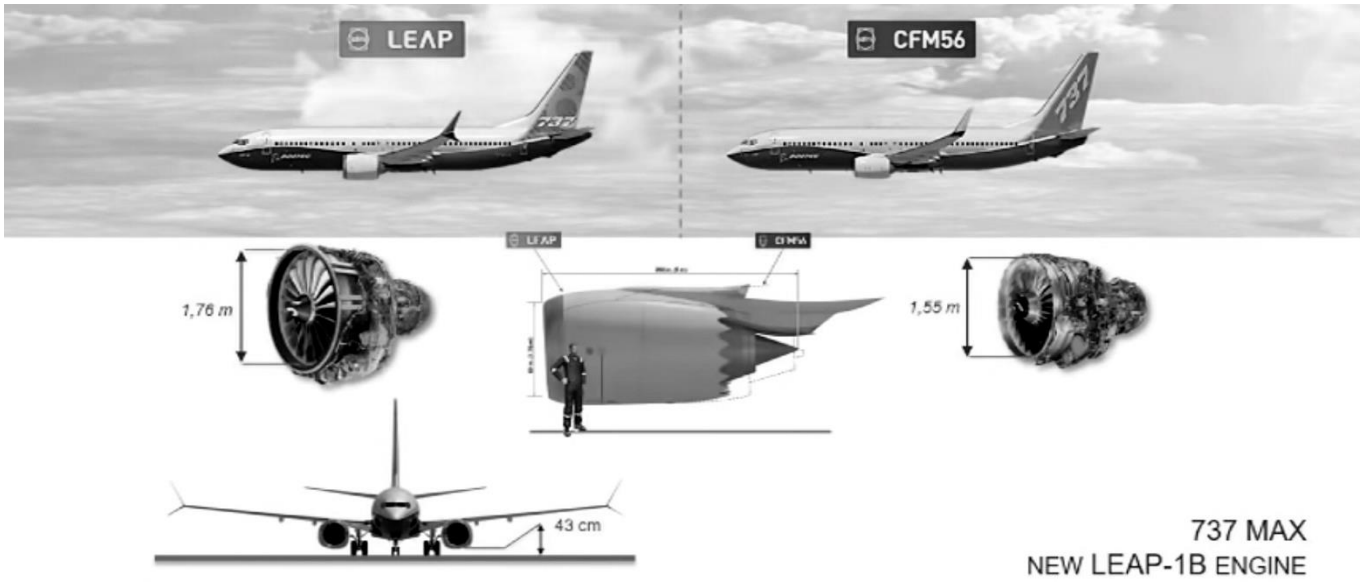


Figure Ib. LEAP-1B engine powering 737 MAX fleet compared with CFM56 engine powering 737 NG (New Generation) fleet. Source: CFM.

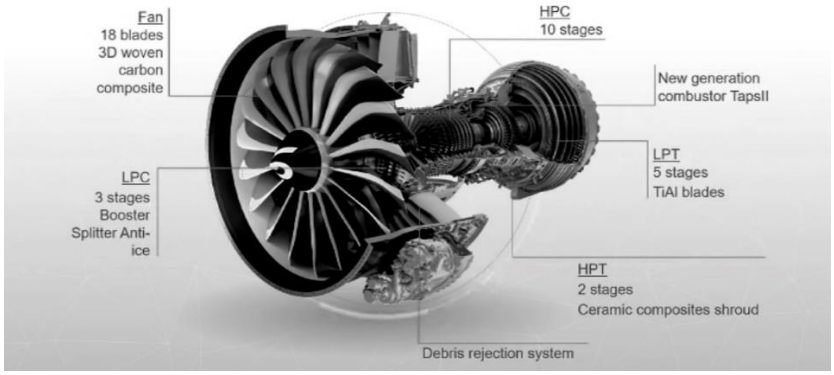


Figure Ic. LEAP-1B engine powering 737 MAX fleet compared with CFM56 engine powering 737 NG (New Generation) fleet. Source: CFM.

Table Ia. Comparison of Technical Specifications of LEAP-1B engine powering 737 MAX fleet compared with CFM56 engine powering 737 NG (New Generation) fleet. BPR: By-Pass Ratio. HPC: High Pressure Compressor. Source: CFM.

Parameter	LEAP Engine	LCFM56 Engine	Comment
Fan Diameter	176 cm 69 in	155 cm 61 in	Larger fan increases BPR
Bypass Ratio, BPR	9:1	5:1	BPR provides 50 percent efficiency improvement
HPC Pressure Ratio	22:1	11:1	Core efficiency provides the other 50 percent

N1 Red Line	4,586 rpm 104.3 percent max	5,382 rpm 104 percent max	
N2 Red Line	20,171 117.5 percent max	15,183 rpm 105 percent max	
EGT Red Line Takeoff	1,038 ºC	950 ºC	15 percent fuel saving

Table Ib. Basic thrust ratings of LEAP-1B engine powering whole 737 MAX fleet. Source: CFM.

Aircraft	LEAP-1B21 23.0 klbf	LEAP-1B23 24.0 klbf	LEAP-1B25 25.0 klbf	LEAP-1B27 26.4 klbf	LEAP-1B28 27.9 klbf
737 MAX 7	*	*			
737 MAX 8			*	*	*
737 MAX 9				*	*
737 MAX 200			*	*	*

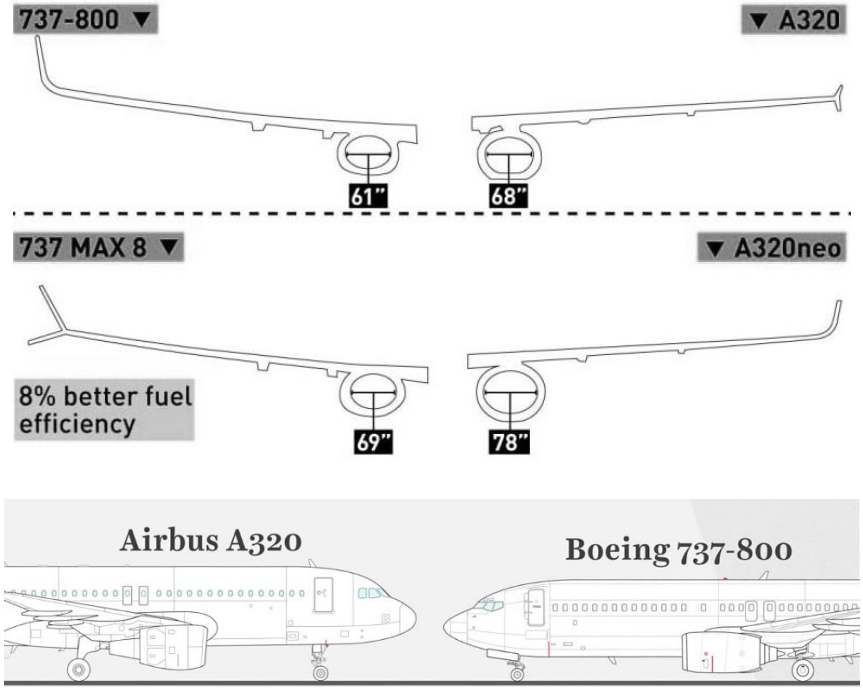


Figure Ic. Comparison of LEAP-1B engine powering 737 MAX fleet with A320neo.

APPENDIX II

ET302 HISTORY OF FLIGHT

1 FACTUAL INFORMATION

1.1 HISTORY OF FLIGHT

DRAFT
NOT FOR DISTRIBUTION
1/19/2020

On March 10, 2019, at about 05:44 UTC (Universal Time Coordinated), Ethiopian Airlines flight 302, a Boeing 737-8 (MAX), Ethiopian registration ET-AVJ, crashed near Ejere, Ethiopia, shortly after takeoff from Addis Ababa Bole International Airport (HAAB), Ethiopia. The flight was a regularly scheduled international passenger flight from Addis Ababa to Jomo Kenyatta International Airport (HKJK), Nairobi, Kenya. There were 157 passengers and crew on board. All were fatally injured, and the Aircraft was destroyed.

The following is based on the preliminary analysis of the DFDR (Digital Flight Data Recorder), CVR (Cockpit Voice Recorder) and ATC communications. As the investigation continues, revisions and changes may occur before the final report is published.

At 05:37:34, ATC issued take off clearance to ET-302 and to contact radar on 119.7 MHz.

Takeoff roll began from runway 07R at a field elevation of 2333.5 m at approximately 05:38, with a flap setting of 5 degrees and a stabilizer setting of 5.6 units. The takeoff roll appeared normal, including normal values of left and right angle-of-attack (AOA). During takeoff roll, the engines stabilized at about 94% N1, which matched the N1 Reference recorded on the DFDR. From this point for most of the flight, the N1 Reference remained about 94% and the throttles did not move. The N1 target indicated non data pattern 220 seconds before the end of recording. According to the CVR data and the control column forces recorded in DFDR, captain was the pilot flying.

At 05:38:44, shortly after liftoff, the left and right recorded AOA values deviated. Left AOA decreased to 11.1° then increased to 35.7° while value of right AOA indicated 14.94°. Then after, the left AOA value reached 74.5° in ¾ seconds while the right AOA reached a maximum value of 15.3°. At this time, the left stick shaker activated and remained active until near the end of the recording. Also, the airspeed, altitude and flight director pitch bar values from the left side noted deviating from the corresponding right side values. The left side values were lower than the right side values until near the end of the recording.

At 05:38:43 and about 50 ft radio altitude, the flight director roll mode changed to LNAV.

At 05:38:46 and about 200 ft radio altitude, the Master Caution parameter changed state. The First Officer called out Master Caution Anti-Ice on CVR. Four seconds later, the recorded Left AOA Heat parameter changed state.

At 05:38:58 and about 400 ft radio altitude, the flight director pitch mode changed to VNAV SPEED and Captain called out “Command” (standard call out for autopilot engagement) and an autopilot warning is recorded.

At 05:39:00, Captain called out “Command”.

At 05:39:01 and about 630 ft radio altitude, a second autopilot warning is recorded.

At 05:39:06, the Captain advised the First-Officer to contact radar and First Officer reported SHALA 2A departure crossing 8400 ft and climbing FL 320.

Between liftoff and 1000 ft above ground level (AGL), the pitch trim position moved between 4.9 and 5.9 units in response to manual electric trim inputs. At 1000 ft AGL, the pitch trim position was at 5.6 units.

At 05:39:22 and about 1,000 feet the left autopilot (AP) was engaged (it disengaged about 33 seconds later), the flaps were retracted and the pitch trim position decreased to 4.6 units.

Six seconds after the autopilot engagement, there were small amplitude roll oscillations accompanied by lateral acceleration, rudder oscillations and slight heading changes. These oscillations continued also after the autopilot was disengaged.

At 05:39:29, radar controller identified ET-302 and instructed to climb FL 340 and when able right turns direct to RUDOL and the First-Officer acknowledged.

At 05:39:42, Level Change mode was engaged. The selected altitude was 32000 ft. Shortly after the mode change, the selected airspeed was set to 238 kt.

At 05:39:45, Captain requested flaps up and First-Officer acknowledged. One second later, flap handle moved from 5 to 0 degrees and flaps retraction began.

At 05:39:50, the selected heading started to change from 072 to 197 degrees and at the same time the Captain asked the First-Officer to request to maintain runway heading.

At 05:39:55, Autopilot disengaged,

At 05:39:57, the Captain advised again the First-Officer to request to maintain runway heading and that they are having flight control problems.

At 05:40:00 shortly after the autopilot disengaged, the FDR recorded an automatic Aircraft Nose Down (AND) activated for 9.0 seconds and pitch trim moved from 4.60 to 2.1 units. The climb was arrested and the aircraft descended slightly.

At 05:40:03 Ground Proximity Warning System (GPWS) “DON’T SINK” alerts occurred.

At 05:40:05, the First-Officer reported to ATC that they were unable to maintain SHALA 1A and requested runway heading which was approved by ATC.

At 05:40:06, left and right flap position reached a recorded value of 0.019 degrees which remained until the end of the recording.

The column moved aft and a positive climb was re-established during the automatic AND motion.

At 05:40:12, approximately three seconds after AND stabilizer motion ends, electric trim (from pilot activated switches on the yoke) in the Aircraft Nose Up (ANU) direction is recorded on the DFDR and the stabilizer moved in the ANU direction to 2.4 units. The Aircraft pitch attitude remained about the same as the back pressure on the column increased.

At 05:40:20, approximately five seconds after the end of the ANU stabilizer motion, a second instance of automatic AND stabilizer trim occurred and the stabilizer moved down and reached 0.4 units.

From 05:40:23 to 05:40:31, three Ground Proximity Warning System (GPWS) "DON'T SINK" alerts occurred.

At 05:40:27, the Captain advised the First-Officer to trim up with him.

At 05:40:28 Manual electric trim in the ANU direction was recorded and the stabilizer reversed moving in the ANU direction and then the trim reached 2.3 units.

At 05:40:35, the First-Officer called out "stab trim cut-out" two times. Captain agreed and First-Officer confirmed stab trim cut-out.

At 05:40:41, approximately five seconds after the end of the ANU stabilizer motion, a third instance of AND automatic trim command occurred without any corresponding motion of the stabilizer, which is consistent with the stabilizer trim cutout switches were in the ''cutout'' position

At 05:40:44, the Captain called out three times "Pull-up" and the First-Officer acknowledged.

At 05:40:50, the Captain instructed the First Officer to advise ATC that they would like to maintain 14,000 ft and they have flight control problem.

At 05:40:56, the First-Officer requested ATC to maintain 14,000 ft and reported that they are having flight control problem. ATC approved.

From 05:40:42 to 05:43:11 (about two and a half minutes), the stabilizer position gradually moved in the AND direction from 2.3 units to 2.1 units. During this time, aft force was applied to the control columns which remained aft of neutral position. The left indicated airspeed increased from approximately 305 kt to approximately 340 kt (VMO). The right indicated airspeed was approximately 20-25 kt higher than the left.

Note 1: At such a 340 kts (later-on 458-500 kts) airspeed from high engine power, movement of the horizontal stabilizer by the jack-screw trim control using hand-cranking of the trim wheels may become impossible to achieve as it requires overcoming high aerodynamic forces. Speed should have been reduced to rotate the jackscrew for trim control by hand to be achievable.

The data indicates that aft force was applied to both columns simultaneously several times throughout the remainder of the recording. At 05:41:20, the right overspeed clacker was recorded on CVR. It remained active until the end of the recording.

At 05:41:21, the selected altitude was changed from 32000 ft to 14000 ft.

At 05:41:30, the Captain requested the First-Officer to pitch up with him and the First-Officer acknowledged.

At 05:41:32, the left overspeed warning activated and was active intermittently until the end of the recording.

At 05:41:46, the Captain asked the First-Officer if the trim is functional. The First-Officer has replied that the trim was not working and asked if he could try it manually. The Captain told him to try. At 05:41:54, the First-Officer replied that it is not working.

At 05:42:10, the Captain asked and the First-Officer requested radar control a vector to return and ATC approved.

At 05:42:30, ATC instructed ET-302 to turn right heading 260 degrees and the First-Officer acknowledged.

At 05:42:43, the selected heading was changed to 262 degrees.

At 05:42:51, the First-Officer mentioned Master Caution Anti-Ice. The Master Caution is recorded on DFDR.

At 05:42:54, both pilots called out “left alpha vane”

At 05:43:04, the Captain asked the First Officer to pitch up together and said that pitch is not enough.

At 05:43:11, about 32 seconds before the end of the recording, at approximately 13,400 ft, two momentary manual electric trim inputs are recorded in the ANU direction. The stabilizer moved in the ANU direction from 2.1 units to 2.3 units.

At 05:43:20, approximately five seconds after the last manual electric trim input, an AND automatic trim command occurred and the stabilizer moved in the AND direction from 2.3 to 1.0 unit in approximately 5 seconds. The aircraft began pitching nose down. Additional simultaneous aft column force was applied, but the nose down pitch continues, eventually reaching 40° nose down. The stabilizer position varied between 1.1 and 0.8 units for the remainder of the recording.

Note 2: Once deactivated, the MACS system should not have been reactivated again as it led to full=trim of elevator without resetting it to neutral.

The left Indicated Airspeed increased, eventually reaching approximately 458 kts and the right Indicated Airspeed reached 500 kts at the end of the recording. The last recorded pressure altitude was 5,419 ft on the left and 8,399 ft on the right.

1.2 INJURIES TO PERSONS

Injuries	Flight Crew	Passengers	Total in Aircraft	Others
Fatal	8	149	157	-
Serious	-	-	-	-
Minor	-	-	-	-
None	-	-	-	-

TOTAL	8	149	157	-

1.3 DAMAGE TO AIRCRAFT

The aircraft is completely destroyed.

1.4 OTHER DAMAGE

No other damage.

2 INITIAL FINDINGS

On the basis of the initial information gathered during the course of the investigation, the following facts have been determined:

The Aircraft possessed a valid certificate of airworthiness;
The crew obtained the license and qualifications to conduct the flight;
The takeoff roll appeared normal, including normal values of left and right angle-of-attack (AOA).
Shortly after liftoff, the value of the left angle of attack sensor deviated from the right one and reached 74.5 degrees while the right angle of attack sensor value was 15.3 degrees; then after; the stick shaker activated and remained active until near the end of the flight.
After autopilot engagement, there were small amplitude roll oscillations accompanied by lateral acceleration, rudder oscillations and slight heading changes; these oscillations also continued after the autopilot disengaged.
After the autopilot disengaged, the DFDR recorded an automatic aircraft nose down (AND) trim command four times without pilot's input. As a result, three motions of the stabilizer trim were recorded. The FDR data also indicated that the crew utilized the electric manual trim to counter the automatic AND input.
The crew performed runaway stabilizer checklist and put the stab trim cutout switch to cutout position and confirmed that the manual trim operation was not working.

3 SAFETY ACTIONS TAKEN

The day of the accident, the operator decided to suspend operation of B737-8MAX. On 14 th March 2019, Ethiopian Civil Aviation Authority issued NOTAM regarding "The operation of Boeing B737-8 'MAX' and Boeing B737-9 'MAX' aircraft from, into or over the Ethiopian airspace, which is still active at the date of this report publication.

4 SAFETY RECOMMENDATIONS

Since repetitive un-commanded aircraft nose down conditions are noticed in this preliminary investigation, it is recommended that the aircraft flight control system related to flight controllability shall be reviewed by the manufacturer.

Aviation Authorities shall verify that the review of the aircraft flight control system related to flight controllability has been adequately addressed by the manufacturer before the release of the aircraft to operations.

APPENDIX II

ASIMOV LAWS OF ROBOTICS

Law 1: “A robot may not injure a human being or, through inaction, allow a human being to come to harm.”
Law 2: “A robot must obey orders given to it by human beings except where such orders would conflict with the First Law.”
Law 3“A robot must protect its own existence, as long as such protection does not conflict with the First or Second Law.”
The “Zeroth Law,” above all the others: “A robot may not harm humanity, or, by inaction, allow humanity to come to harm.”