CW1: A Reflection on a Software Based System Failure (Boeing 737 MAX)

Samara Cunningham H00429775
Year 2 Computer Science- F28SD
Edinburgh Campus

Figure 1: Image Depicting the Boeing 737 MAX

List of Contents

Samara Cunningham **H00429775**

05/04/2025

D1: Describe the content of the Boeing 737 MAX airliner.

Why was the Boeing 737 MAX initially devoloped?

"Airbus first started using the CFM Leap engine, which boasts a 15% reduction in fuel production" (Design and Inquiry, 2024)

Boeing developed the 737 MAX in response to the Airbus A320neo. This Airbus set new fuel efficiency standards in the industry.

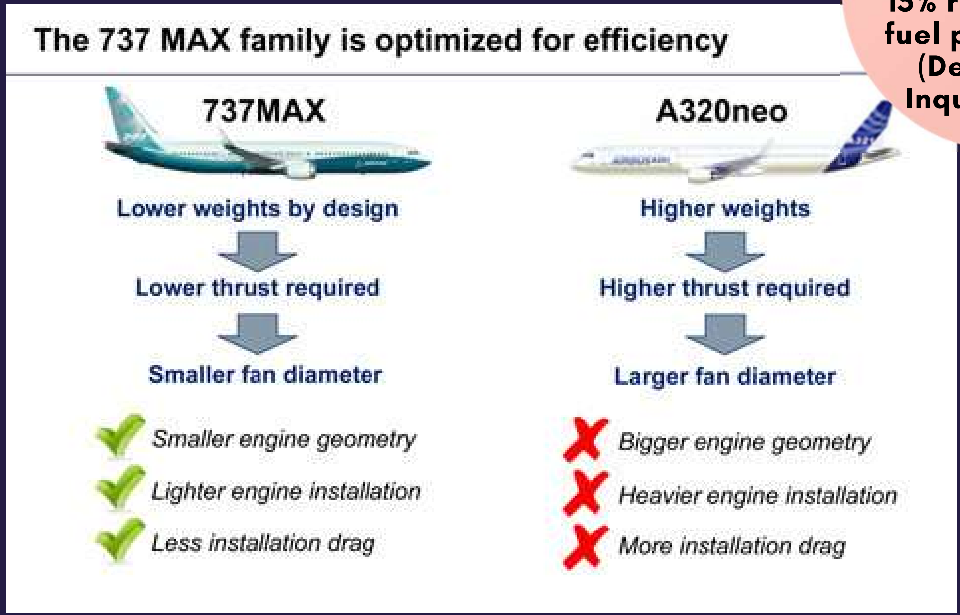

Figure 2: A comparison of the Boeing 737 MAX and the Airbus A320neo.

Samara Cunningham H00429775 05/04/2025

D1: Describe the content of the Boeing 737 MAX airliner.

Why was the additional on-board system MCAS required?

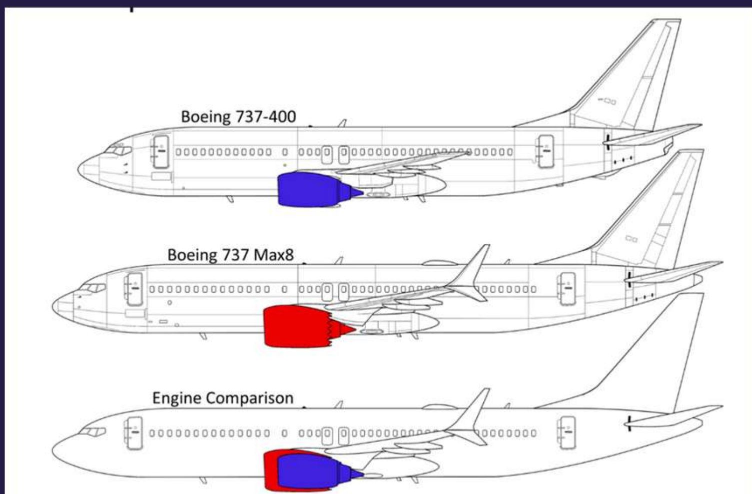

Figure 3: Comparison of Engine Placement between the Boeing 737-400 and the Boeing 737 MAX

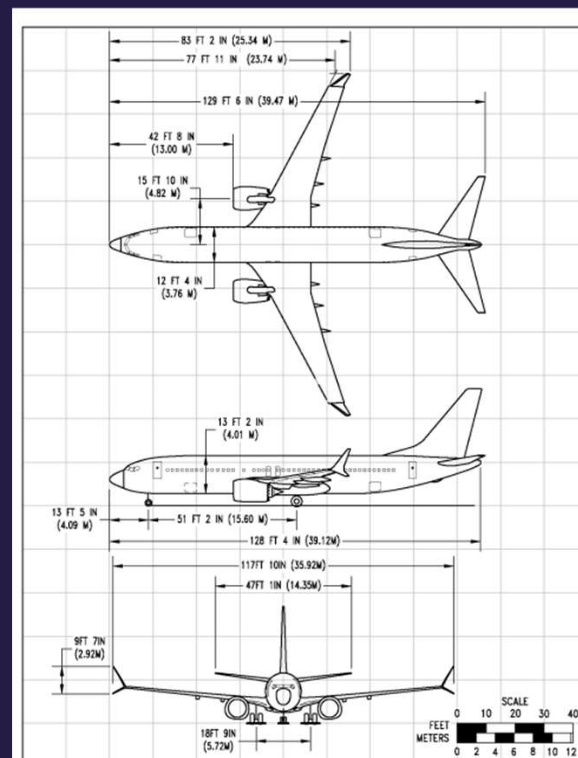

Figure 4: Illustration showing the Engine Placement on the Boeing 737 MAX

Due to larger, heavier engines placed further forward and higher on the wings, the aircraft would pitch up, increasing the stall risk.

The MCAS was required to push the nose down when the plane pitched upwards.

Samara Cunningham H00429775 05/04/2025

D1: Describe the content of the Boeing 737 MAX airliner.

How was MACS intended to operate?

STEP 1

AoA sensor detects excessive AoA.

STEP 2

MCAS activates.

STEP 3

Nose is pushed down

"MCAS IS ACTIVATED WITHOUT PILOT INPUT AND ONLY OPERATES IN MANUAL, FLAPS UP FLIGHT." (SKYBRARY, DATE UNKNOWN)

Prevents activation during takeoff and landing.

"THE MCAS FUNCTION BECOMES ACTIVE WHEN THE AOA EXCEEDS A THRESHOLD BASED ON AIRSPEED AND ALTITUDE. MCAS WILL ACTIVATE FOR UP TO 9.26 SECONDS BEFORE PAUSING FOR 5 SECONDS." (MAKO ET AL, 2019)

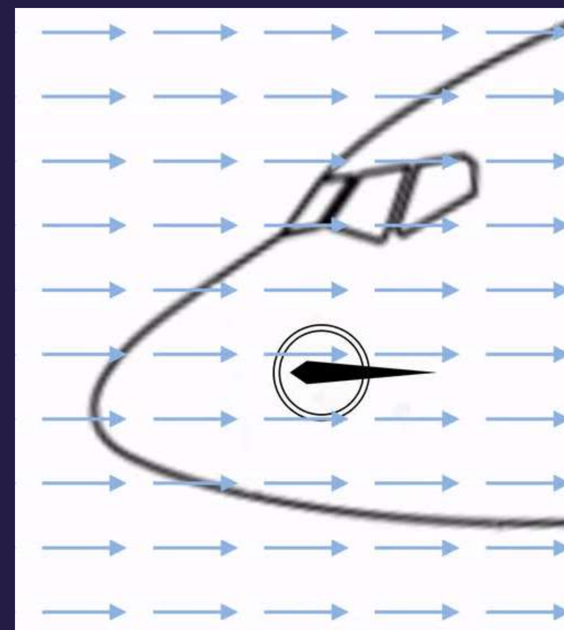

Figure 5: Animation demonstarting how the AoA Sensor works.

D1: Describe the content of the Boeing 737 MAX airliner.

What was the engineering and operational perspectives considering economic and regulatory perspectives?

ENGINEERING PERSPECTIVE

The MCAS had a single AoA (angle of attack) sensor.

This made it vulnerable to failure.

As MCAS was reliant on the sensor, if the sensor was damaged, the MCAS would not work as intended.

REGULATORY PERSPECTIVE

If Boeing called MCAS a new function the training would have been required.

So, Boeing decided to externally communicate it as an addition to Speed Trim.

The FAA gave Boeing a lot of the certification process, allowing safety concerns to go largely unnadressed.

Samara Cunningham H00429775 05/04/2025

D1: Describe the content of the Boeing 737 MAX airliner.

What was the engineering and operational perspectives considering economic and regulatory perspectives?

OPERATIONAL PERSPECTIVE

Pilots were not adequetly trained for the MCAS. They were not initially told about the system. Then they were told if the MCAS was malfunctioning to turn it off.

According to a Netflix Documentary about BOEING (Downfall: The Case Against Boeing, 2022, 1:08:58), a coordination sheet showed that pilot reaction time should be <10 seconds or the consequences would be "catastrophic".

The pilots weren't told about this either.

ECONOMIC PERSPECTIVE

The decision to not tell the pilots about MCAS or its safety examinations and the change in sensors were cost-saving decisions to create a cheap and fuel-efficient plane.

Samara Cunningham H00429775 05/04/2025

D2: The sequence of events that led to each of the Boeing 737 MAX accidents

Initial design and concealment of MCAS

EARLY 2010'S

The MCAS was initially developed. This can be shown by a meeting had about it in 2013.

INTERNAL EMAILS DETAIL "IF WE EMPHASIZE MCAS IS A NEW FUNCTION THERE MAY BE GREATER CERTIFICATION AND TRAINING IMPACT," ACCORDING TO (HUISAN LAW, 2024)

2017-2018

Beoing did not disclose the existence of MCAS in pilot manuals or training material. MCAS was framed as a minor upgrade.

Internal Emails showed Boeing downplayed MCAS risks to avoid further scrutiny.

Samara Cunningham H00429775 05/04/2025

D2: The sequence of events that led to each of the Boeing 737 MAX accidents

Lion Air Flight 610- Crashed October 29th 2018

29TH OCTOBER 2018

Lion Air Flight 610 dissapeared of the radar after leaving Jakarta, Indonesia. Killed 189 people onboard.

The MCAS falsely activated due to a faulty AoA (angle-of-attack) sensor.

This repeatededly pushed the nose down, regardless of there being no high AoA or stall.

Figure 6: Image showing Lion Air Flight 610 after crashing.

D2: The sequence of events that led to each of the Boeing 737 MAX accidents

Lion Air Flight 610- Crashed October 29th 2018

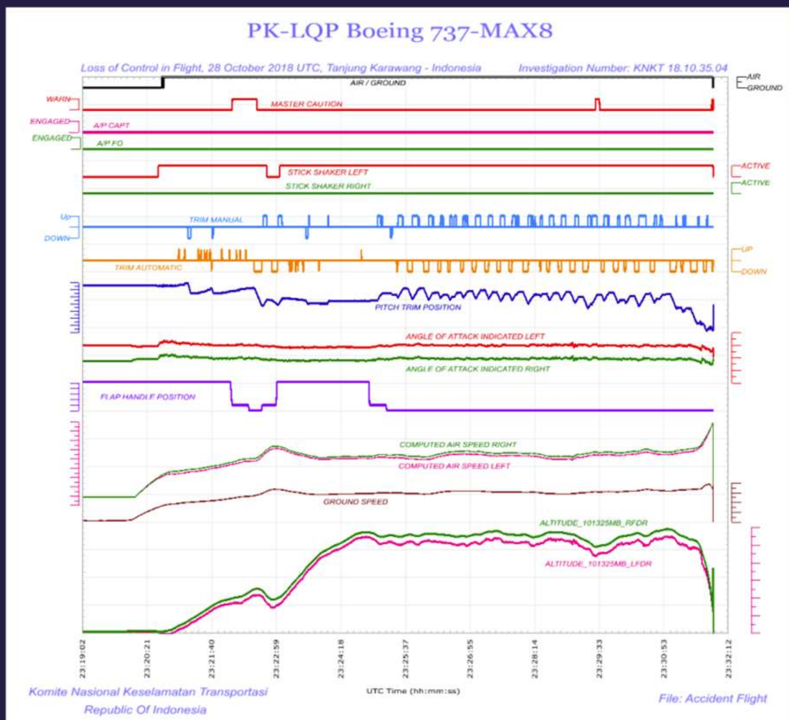

Figure 7: Data Diagram showing flight details of Lion Air Flight 610

Figure 5 shows the multitude of alarms that went off before the Lion Air Flight 610 crashed.

Furthermore, the Trim Automatic data can be seen in Figure 5. This shows a consistent down movement suggesting that the MCAS was pushing the nose down continuesly.

D2: The sequence of events that led to each of the Boeing 737 MAX accidents

Boeing actions and reports between the Lion Air 610 accident and Ethipian Airlines 302 accident.

2018-2019

Boeing blamed pilot error depite knowing internally MCAS was at fault. A software fix was promised but delayed.

“THE FAA CONDUCTED PRELIMINARY RISK ASSESSMENTS ON NOVEMBER 5, 2018, AND DETERMINED URGENT MANDATORY ACTION WAS NEEDED TO MITIGATE THE UNINTENDED MOVEMENT OF THE HORIZONTAL STABILIZER TRIM SYSTEM IN RESPONSE TO THE ERRONEOUS AOA VANE INPUT.” (FEDERAL AVIATION ADMINISTRATION, 2020)

THE NTSB (NATIONAL TRANSPORTATION SAFETY BOARD) PUBLISHED A REPORT (NTSB, 2019) “URGING THE FAA” ON THE SAFETY OF THE BOEING 737 MAX. IT DISCUSSES THE “HAZORDOUS” AND “MAJOR” SAFETY FAULTS FOUND IN BOEINGS INITIAL ASSESMENT OF THE BOEING 737 MAX AND THE LEGAL REQUIREMENTS IGNORED FOR PILOT TRAINING.

2018-2019

After no initial pilot training was given, pilots were told to turn off the MCAS system if this fault occured again.

Samara Cunningham H00429775 05/04/2025

D2: The sequence of events that led to each of the Boeing 737 MAX accidents

Ethiopian Airlines Flight 302- crashed 10th March 2019.

10TH MARCH 2019

Unlike Lion Air Pilots, Ethopion Airlines pilots knew about MCAS and recognised the failure.

As instructed, the pilots disabled the MCAS system, but were unable to regain control due to insufficient time.

The plane crashed into the ground at 500-600 mph killing 157 people.

Figure 8: Image showing Ethiopian Airlines Flight 302 after crashing.

Samara Cunningham H00429775 05/04/2025

D2: The sequence of events that led to each of the Boeing 737 MAX accidents

Ethiopian Airlines Flight 302- crashed 10th March 2019.

Figure 9: Data showing Ground Altitude and Speed of the Ethiopian Airlines flight 302 in comparison to the previous Ethiopian Airline Flights.

Figure 9 shows that the Ethipian flight struggled to gain altitude compared to the previous flights.

Figure 9 also shows that the Ethiopian flight experienced flunctuation in altitude suggesting control issues.

Figure 10 shows that both the Ethiopian and Lion Air flights experienced a loss of altitude within the first few minutes of flight.

The similarities between the date for the Lion Air and Ethiopian flight (shown in Figure 10) implies a systematic issue with the aircraft rather than isolated incidents.

Figure 10: Data showing Ground Altitude of the Ethiopian Airlines flight 302 in comparison to the Lion Air Flight 610.

Samara Cunningham H00429775 05/04/2025

D3: What aspects of the development/deployment of the MCAS system could have been undertaken differently to avoid these accidents?

Requirement Engineering should have been a main focus in the development of the MCAS.

Requirement Engineering
Establishing a precise rendition of what is required

ASSUMPTIONS

Assumptions should be reasonable and relevant.

Boeing SHOULD have assumed that the sensor could get damaged.

Boeing SHOULD have assumed that pilots may not be able to immediatly recognise the a failure in the MCAS system.

Boeing SHOULD have assumed that pilots needed full knowledge and training of the MCAS system.

NON-FUNCTIONAL REQUIREMENTS

COMPLIANCE

Compliance ensures that laws, regulations and standards are met. Being did not comply with most/any of these. Boeing outwardly explained the purpose of the MCAS as an addition to speed trim. This could have been to avoid these constraints.

DEVELOPMENT CONSTRAINTS

Boeing faced time and money constraints when developing the Boeing 737 MAX, as they were competing againts the Airbus neo320. Prioritising safety would have slowed the release of the new plane, causing them to lose money, but it could have helped prevent these accidents.

Samara Cunningham H00429775 05/04/2025

D3: What aspects of the development/deployment of the MCAS system could have been undertaken differently to avoid these accidents?

Requirements Engineering
Establishing a precise rendition of what is required

COMMUNICATION WITH STAKEHOLDERS

Communication with stakeholders helps gather and validate what a system should do. In the case of the MCAS, the stakeholders include: FAA, pilots etc. By communicating with pilots, Boeing might have seen the risk in not them not being informed about the system. Pilots being better informed could have identified and responded quicker to a fault in the MCAS.

FUNCTIONAL REQUIREMENTS

By having clear definitive functional requirements, ambigious behaviour, such as how a pilot would respond to a fault in the MCAS, would have allowed for edge-cases to be accounted for. Pilot authority should have been able to override the MCAS and this potentially could have been identified through claryfing pilot interaction.

Samara Cunningham H00429775 05/04/2025

D3: What aspects of the development/deployment of the MCAS system could have been undertaken differently to avoid these accidents?

Test Cases

TESTING AND VERIFICATION

Extensive testing, including giving MCAS errenous data, should have been done to ensure that all boundary cases were accounted for. Using diagrams and models such as a flow diagram or a traceability matrix could have shown the edge cases clearly and allow the developers to spot mistakes easily.

BOUNDARY CASES

Although test cases were use for the development of the MCAS, Boeing focused on improving the system. For example, making the initial MCAS more powerful. However, some boundary cases such as sensor failure were overlooked. By ensuring that all boundary and edge cases were accounted for, Boeing could have avoided the two accidents.

Samara Cunningham H00429775 05/04/2025

D3: What aspects of the development/deployment of the MCAS system could have been undertaken differently to avoid these accidents?

Safety is key when developing a system such as the MCAS.

Safety

Safety ensures that bad things do not accidently happen.

ACCEPTABLE RISK AND DESIGN

When developing a safety-critical design, a balance has to be made between the risk and the cost of reducing the risk. In the case of the Boeing 737 Max, the severity of an accident occuring is severe. Additionally, with only one sensor, the likelyhood of an accident could be classed as occasional. “Birds and balloons hitting the plane happen more often than you would think” (Downfall: The Case Against Boeing, 2022, 1:08:58). Potentially, the risk should have outweighed the cost in this scenario.

OVERCONFIDENCE IN SOFTWARE

Factors such as one-failure point and suggest that Boeing was overconfident in thier software. The software may not have been fully understood by key decision-makers in the Boeing company. Therefore, these safety precausions were overlooked. A more safety-precosious approach could have meant many failure points.

Samara Cunningham H00429775 05/04/2025

Sources:

Ahmed et al. (2019) Figure 8: Image showing Ethiopian Airlines Flight 302 after crashing. From: *Ethiopian Airlines Pilots Followed Boeing's Safety Procedures Before Crash, Report Shows.* Available at: https://www.nytimes.com/2019/04/04/world/asia/ethiopia-crash-boeing.html (Accessed 2 April 2025)

AllAboutLean (2022) Figure 4: Comparison of Engine Placement between the Boeing 737-400 and the Boeing 737 MAX. From: *Boeing 737-400 and Max8 Engine Comparison*. Available at: https://www.allaboutlean.com/boeing-management/boeing-737-400-and-max8-engine-comparison/ (Accessed: 2 April 2025).

AllAboutLean (Date Unknown) Figure 5: Animation demonstarting how the AoA Sensor works. From: *Angle of Attack Sensor Animated.* Available at: https://www.allaboutlean.com/boeing-management/angle-of-attack-sensor-animated (Accessed: 2 April 2025)

BBC (2019) Figure 6: Image showing Lion Air Flight 610 after crashing. From: *Lion Air crash: Boeing 737 plane crashes in sea off Jakarta.* Available at: https://www.bbc.co.uk/news/world-asia-46014463 (Accessed 2 April 2025).

Boeing (Date Unknown) Figure 1: Image Depicting the Boeing 737 MAX. From: *Boeing 737 Gallery*. Available at: https://www.boeing.com/commercial/737max#orders-deliveries (Accessed: 2 April 2025).

Boeing (2019) Figure 3: Illustration showing the engine placement on the Boeing 737 MAX. From, *737 MAX Airplane Characteristics for Airport Planning.* Available at: https://www.boeing.com/content/dam/boeing/boeingdotcom/commercial/airports/acaps/737MAX_RevD.pdf (Accessed: 31 March 2025).

Clark, Z. (2016) Figure 2: A comparison of the Boeing 737 MAX and the Airbus A320neo, From *How does the Boeing 737 MAX compare to the Airbus A320neo?* Available at: https://www.linkedin.com/pulse/how-does-boeing-737-max-compare-airbus-a320neo-zach-clark (Accessed: 02 April 2025).

Design and Inquiry (2024) *737 MAX Decision-Making: A Case Study.* Available at: https://sites.google.com/view/designandinquiry/case-studies/737-max-decision-making-a-case-study(Accessed: 02 April 2025).

Federal Aviation Administration (2020) *Summary of the FAA's Review of the Boeing 737 MAX* Available at: https://www.faa.gov/sites/faa.gov/files/2022-08/737_RTS_Summary.pdf (Accessed 2 April 2025)

Huisan Law (2024) *Jedi Mind Tricks: Boeing 737 MAX Emails Show Attempts to Manipulate Airlines & FAA.* Available at: https://hlalawfirm.com/jedi-mind-tricks-boeing-737-max-emails-show-attempts-to-manipulate-airlines-faa/ (Accessed: 31 March 2025).

Kennedy, R. (2022) Downfall: The Case Against Boeing. [Film] Netflix. Available at: https://www.netflix.com (Accessed: 23/03/2025)

Samara Cunningham H00429775 05/04/2025

Mako et al. (2019) ***EVALUATION OF MCAS SYSTEM Available at:***
https://www.researchgate.net/publication/343474935_Evaluation_of_MCAS_System (Accessed: 2 April 2025).

National Transportation Safety Board (2019) *Assumptions Used in the Safety Assessment Process and the Effects of Multiple Alerts and Indications on Pilot Performance* Available at:
https://www.ntsb.gov/investigations/AccidentReports/Reports/ASR1901.pdf (Accessed 2 April 2025)

Republic of Indonesia (2019) Figure 7: Data Diagram showing flight details of Lion Air Flight 610 From: *Pleminary Aircraft Accident Investigation Report* Available at: https://tailstrike.com/media/5abb0zcw/291018.pdf (Accessed: 2 April 2025)

Skybrary.(Date Unknown) Maneuvering Characteristics Augmentation System (MCAS) Available at:
https://skybrary.aero/articles/maneuvering-characteristics-augmentation-system-mcas (Accessed: 2 April 2025)

Simon et al. (2019) Figure 9: Data showing Ground Altitude and Speed of the Ethiopian Airlines flight 302 in comparison to the previous Ethiopian Airline Flights. From: Alarm in the aviation industry Ethiopian Airlines crash. Available at:
https://www.reuters.com/graphics/ETHIOPIA-AIRPLANE/0100911Q1DX/ (Accessed 3 April 2025)

Simon et al. (2019) Figure 10: Data showing Ground Altitude of the Ethiopian Airlines flight 302 in comparison to the Lion Air Flight 610. From: Alarm in the aviation industry Ethiopian Airlines crash. Available at:
https://www.reuters.com/graphics/ETHIOPIA-AIRPLANE/0100911Q1DX/ (Accessed 3 April 2025)