Workshop - Design of Dependable Systems – Fundamentals of Aircraft Safety
7th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY, Stockholm, October 22-23, 2019

Design of Dependable Systems
Fundamentals of Aircraft Safety
Part 1

Kristina Forsberg, Saab, Håkan Forsberg, MDH
2019-10-23

Schedule

- 08:30-09:20 Part 1
  - Introduction
  - Boeing 737 - MAX 8
  - Accident 1 – Indonesia, 29th of October 2018
  - What happened after accident 1 but before 2?
- *09:20-09:40 Break 1*
- 09:40-10:40 Part 2
  - Aircraft development from a safety perspective
    - Requirements for development of aircraft and aircraft systems
- *10:40-11:00 Break 2*
- 11:00-12:00 Part 3
  - Accident 2 – Ethiopia, 10th of March 2019
  - The aftermath from the accidents
    - JATR's final report to FAA
  - Boeings serious attempt to change the safety culture
  - Discussions

Who Are We?

- Kristina Forsberg
- Håkan Forsberg

Boeing 737 MAX

Air Canada Boeing 737 MAX 8 landing in Calgary, Alberta, Canada, 2018-06-06, Credit: Acefitt, CC-BY-SA-4.0

Boeing 737 – 4 Generations

- Boeing 737 Classics Series (1967, 737-100)
  - Small aircraft
  - Small engines – fan diameter 100 cm
  - Relatively simple systems
  - One of the first 2 cockpit crew aircraft
  - Counts as generation 1 (-100, -200) and 2 (-400)

Boeing 737-100, Credit: PhillipC, CC-BY-2.0

- Boeing 737 NG (1993, 737-600)

- Boeing 737 MAX is the 4th generation of 737
  - Type certified in 2017
  - Engine fan diameter 176 cm (MAX 8)

Boeing 737 MAX-8, Credit: Acefitt, CC-BY-SA-4.0

Boeing 737 MAX 8

Some Information

- Much larger engines,
  - turbofan CFM Leap-1B engines
  - Moved forward on the wing
  - Changes aerodynamic performance
- Split winglets
  - Saves 1.8% fuel
- Taller landing gear
- Tail nose cone
- Fly-by-wire spoilers
- …
- and a Maneuvering Control Augmentation System

MCAS

Boeing 737 MAX 8

Flight Control Surfaces Location

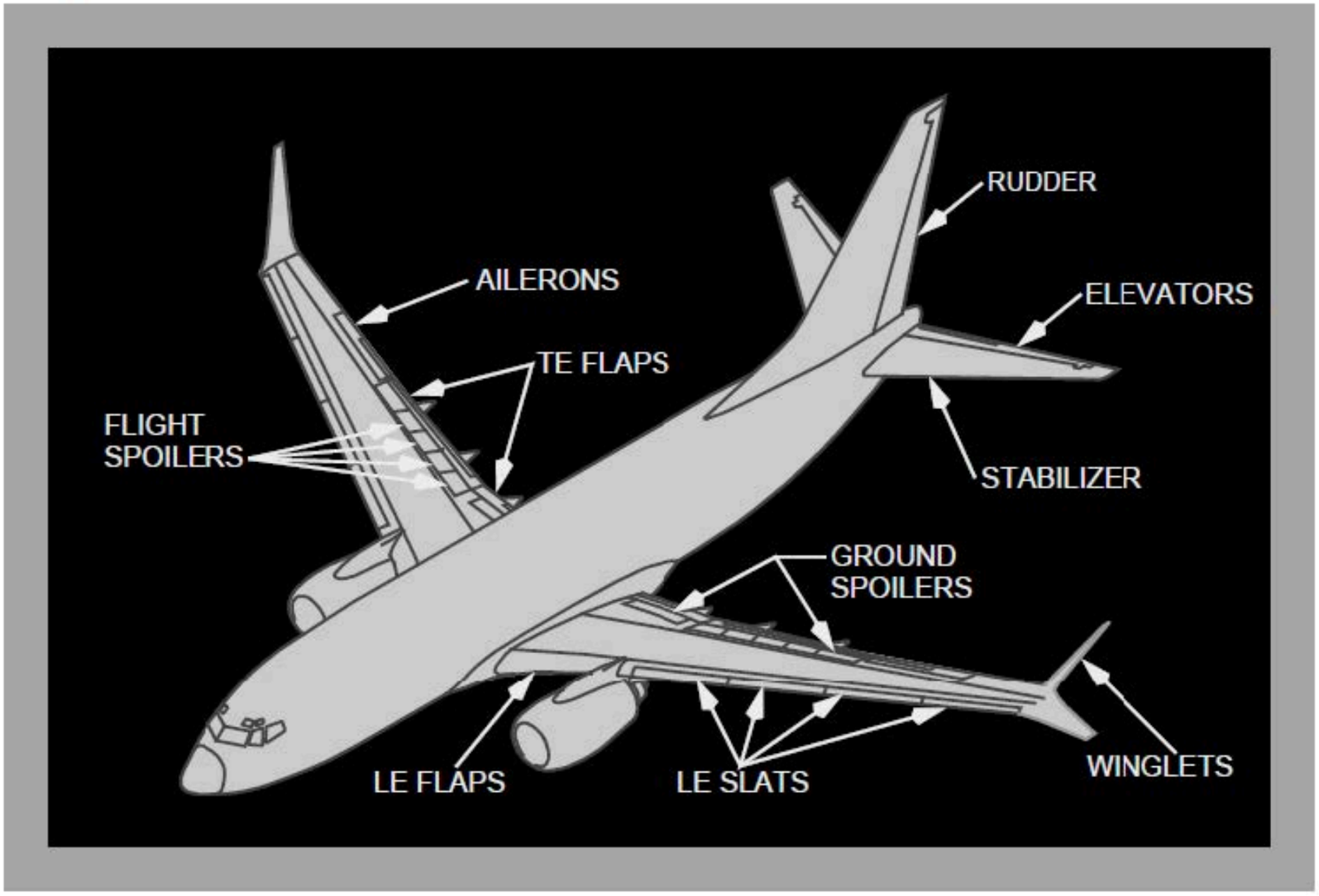


Image Source: Aircraft Accident Investigation Preliminary Report
Ethiopian Airlines Group
B737-8 (MAX) Registered ET-AVJ
28 NM South East of Addis Ababa, Bole International Airport
March 10, 2019, Report No. AI-01/19

Boeing 737 MAX 8

Flight controls

- Conventional control wheel, column and pedals –> mechanical and electrical arrangement (and computers)

--> hydraulic power control units which command the primary flight control surfaces; ailerons, elevators and rudder

The flight controls are powered by redundant hydraulic sources; system A (red) and system B (green)

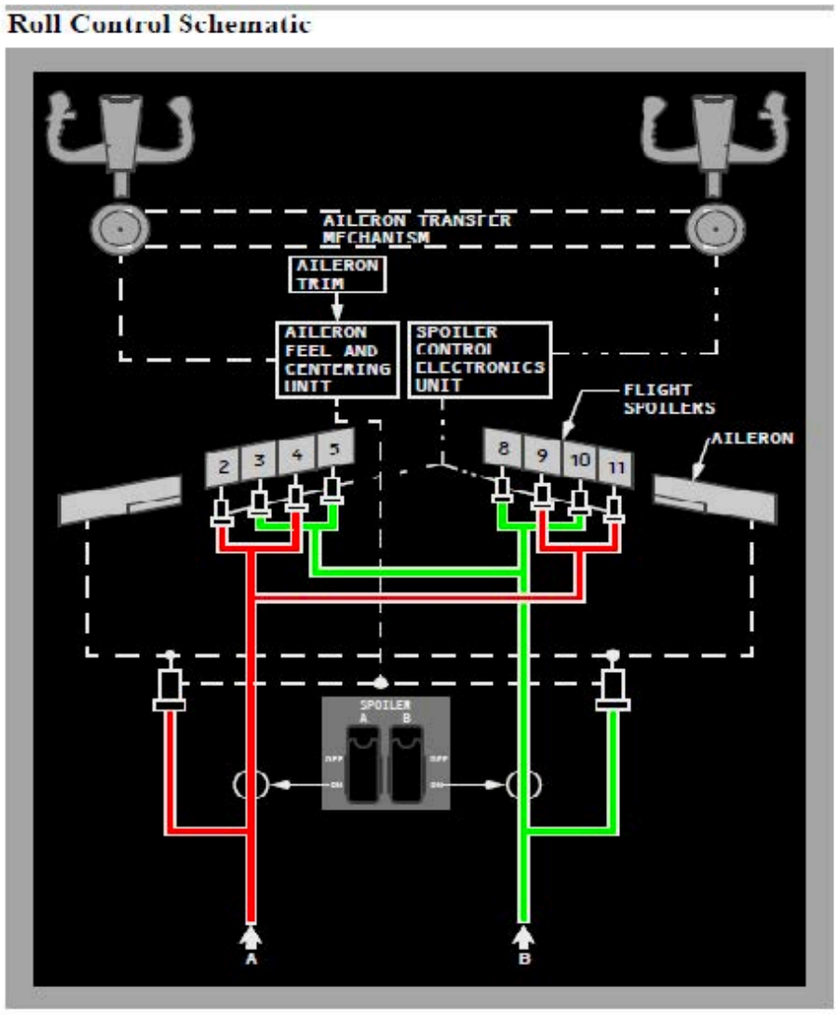


Image source: Aircraft Accident Investigation Preliminary Report
Ethiopian Airlines Group
B737-8 (MAX) Registered ET-AVJ
28 NM South East of Addis Ababa, Bole International Airport
March 10, 2019, Report No. AI-01/19

737 NG and MAX Flight Control Computers

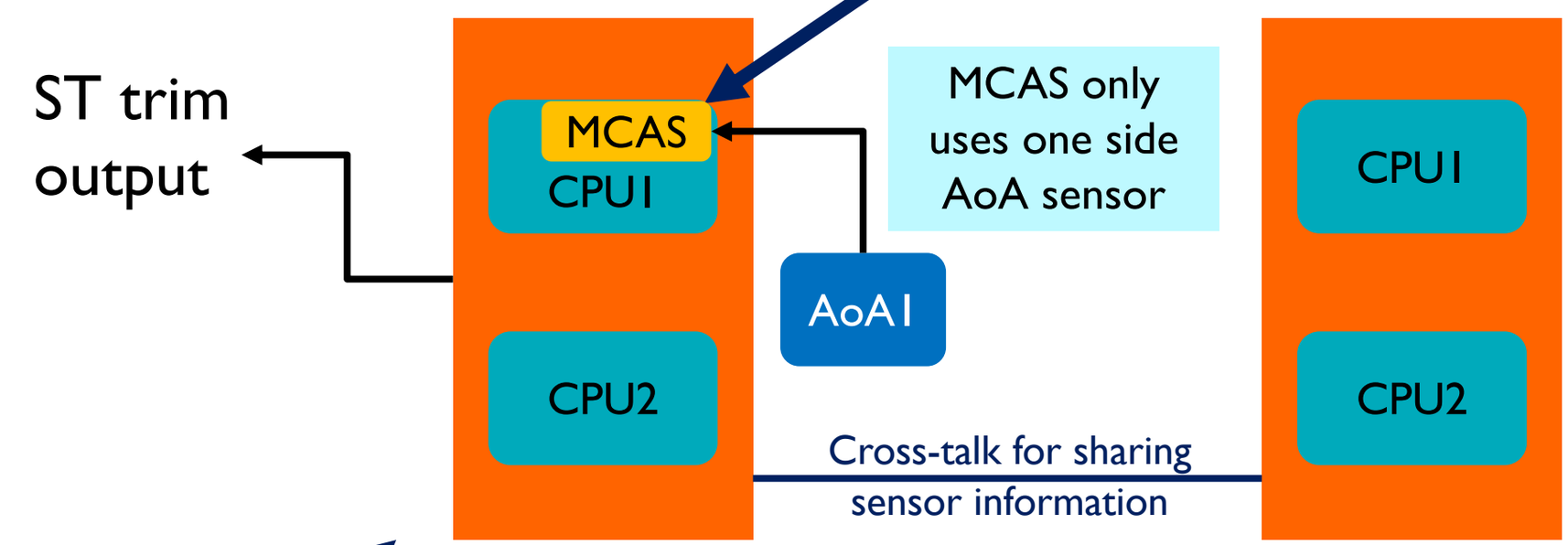
- Boeing 737 FCCs from the early days had separated very simple computers
  - Roll computers and pitch computers

- Nowadays, more complicated but not so sophisticated as other modern fly-by-wire aircraft

MAX Flight Control Computers

MCAS only implemented in one processor, with one AoA sensor as input and direct control of the stabilizer (ST)

Dual redundant FCCs (used for autoland and auto go-around)



Source: Satcom Guru: 737 FCC pitch axis augmentation – command integrity mandate for dual channel, fail-safe, Nov. 20, 2018 (which has a disclaimer of the correctness of content)

MCAS and the Stabilizer - I

- The stabilizer (ST) and the elevator both changes the pitch of the aircraft

- The ST is aerodynamically "stronger" than the elevator (compare areas)

- The ST can be changed by
  1. The autopilot
  2. The pilot
     - Electronically
     - Mechanically (manually)
  3. The MCAS

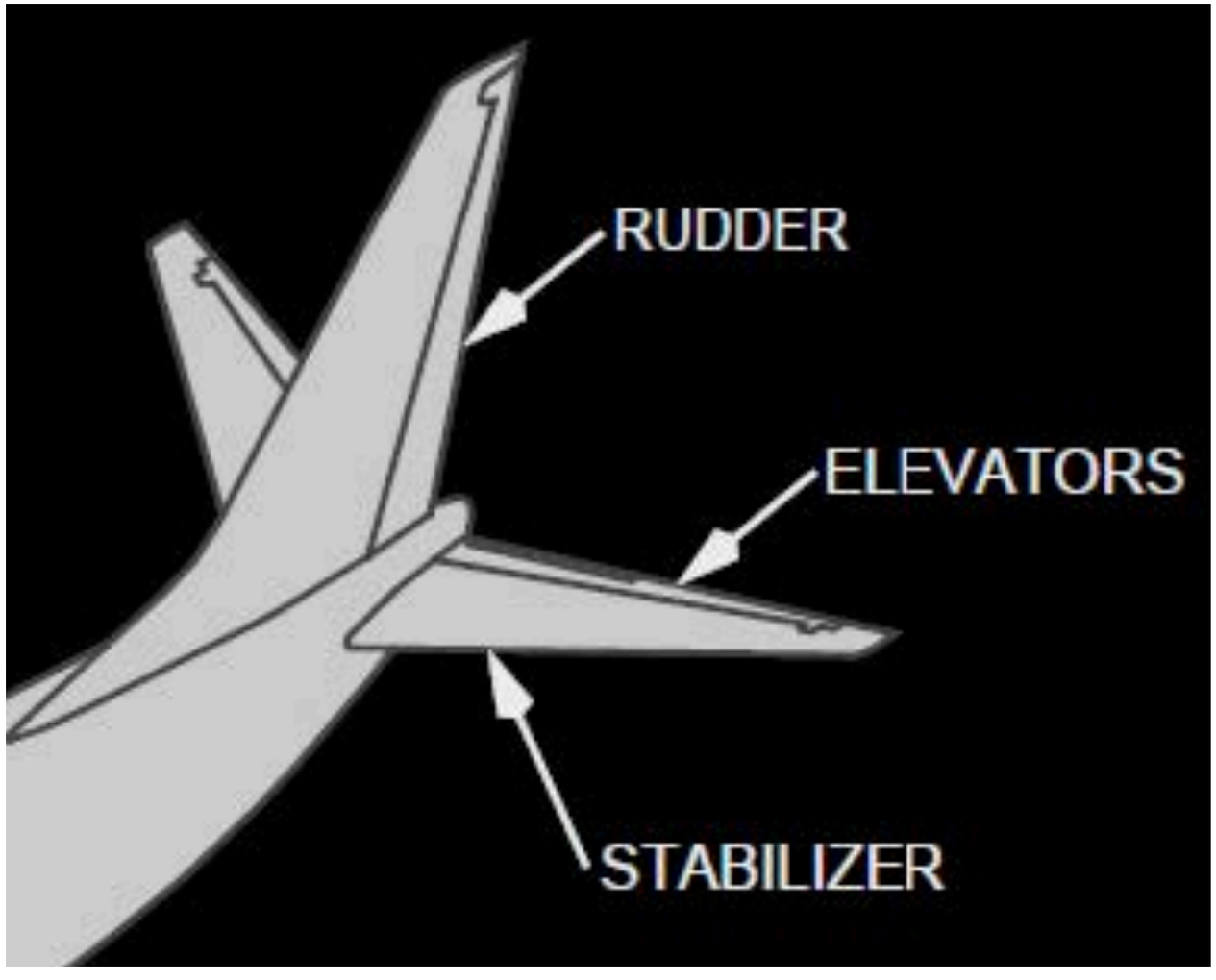


Image Source: Aircraft Accident Investigation Preliminary Report
Ethiopian Airlines Group
B737-8 (MAX) Registered ET-AVJ
28 NM South East of Addis Ababa, Bole International Airport
March 10, 2019, Report No. AI-01/19

MCAS and the Stabilizer - II

- If the stabilizer (ST) doesn't stop when needed it is called a runaway
  - To get back a stabilizer trim cut out has to be performed followed by a rollercoaster maneuver

- When MCAS is running it is impossible to manually override it via the control wheel or the manual trim, the ST trim cut out switch has to be used

- MCAS can only run if
  - The autopilot is disabled
  - The flaps are retracted
  - Value of AoA sensor exceeds certain limit

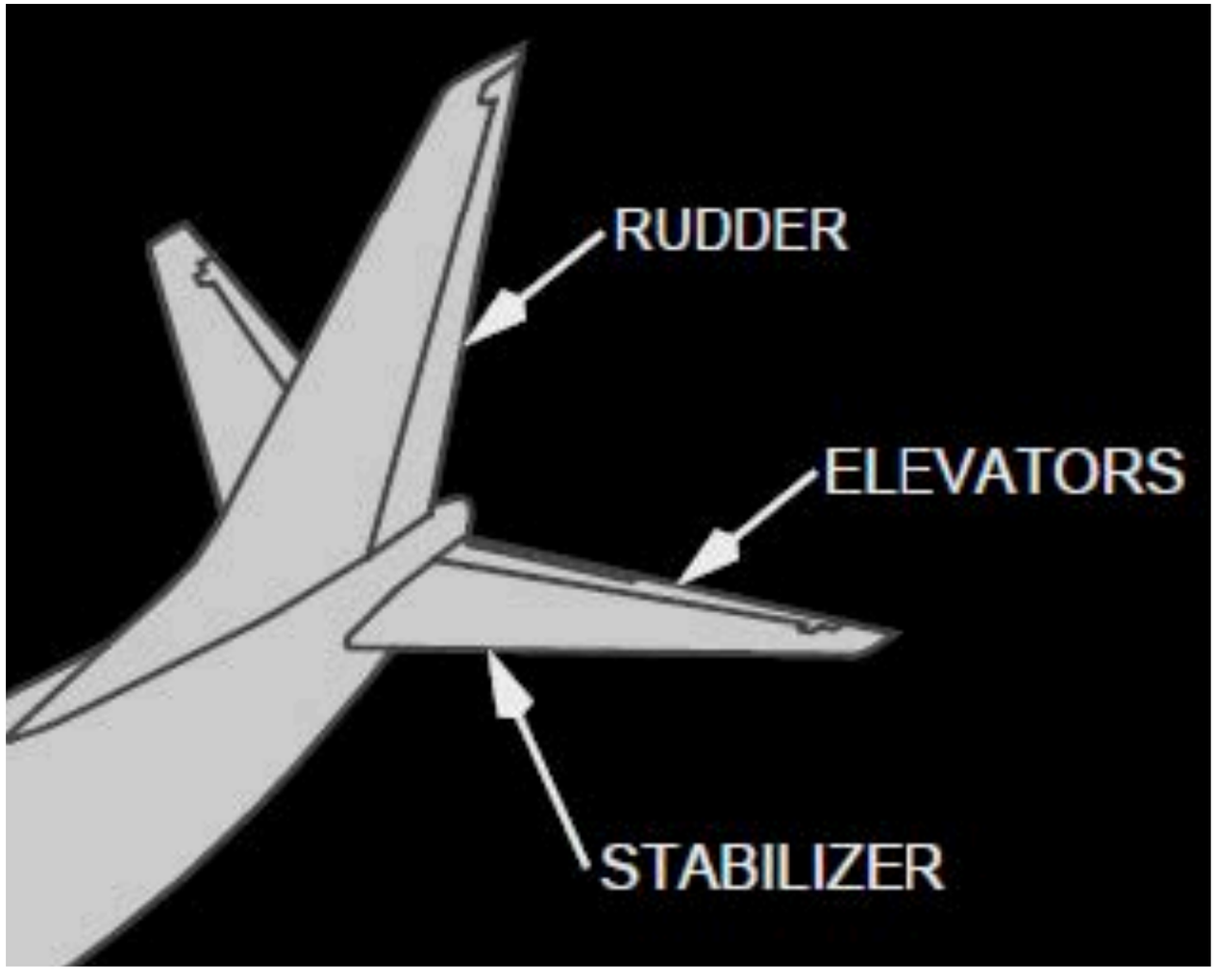


Image Source: Aircraft Accident Investigation Preliminary Report
Ethiopian Airlines Group
B737-8 (MAX) Registered ET-AVJ
28 NM South East of Addis Ababa, Bole International Airport
March 10, 2019, Report No. AI-01/19

Accident 1 – Indonesia - I

29th of October 2018

- 23:20 UTC the aircraft departed from Jakarta
  - The digital flight data recorder (DFDR), recorded a difference from start between left and right AoA sensors of 20 degrees
  - Directly after take-off, the left control column stick shaker started to shake and remained until end of flight

- 23:21:28 the pilots checked the altitude with ground and acknowledged (900 feet)

- 23:21:58 the ground controller knows the aircraft has flight control problems

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

Accident 1 – Indonesia - II

29th of October 2018

- 23:22:05 DFDR recorded that flaps were retracted (last logic true value for MCAS to operate)
  - At the same time the DFDR recorded an automatic aircraft nose down (AND) for ten seconds
  - Followed by a crew commanded trim aircraft nose up (ANU)
- 23:22:48 the flaps extends and the automatic AND stops
- 23:25:18 DFDR recorded that flaps were retracted to 0, and the automatic AND triggered, followed by crew commanded ANU
  - This kept going on until the end of the flight

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

Accident 1 – Indonesia - III

29th of October 2018

- 23:26:32 – 23:28.15 communication ongoing between pilots and the ground, to guide the aircraft to safe landing

- 23:29:37 the ground controller asks the pilots if they are descending (they should ascend), and the pilots confirmed and said they had problems and flew the aircraft manually

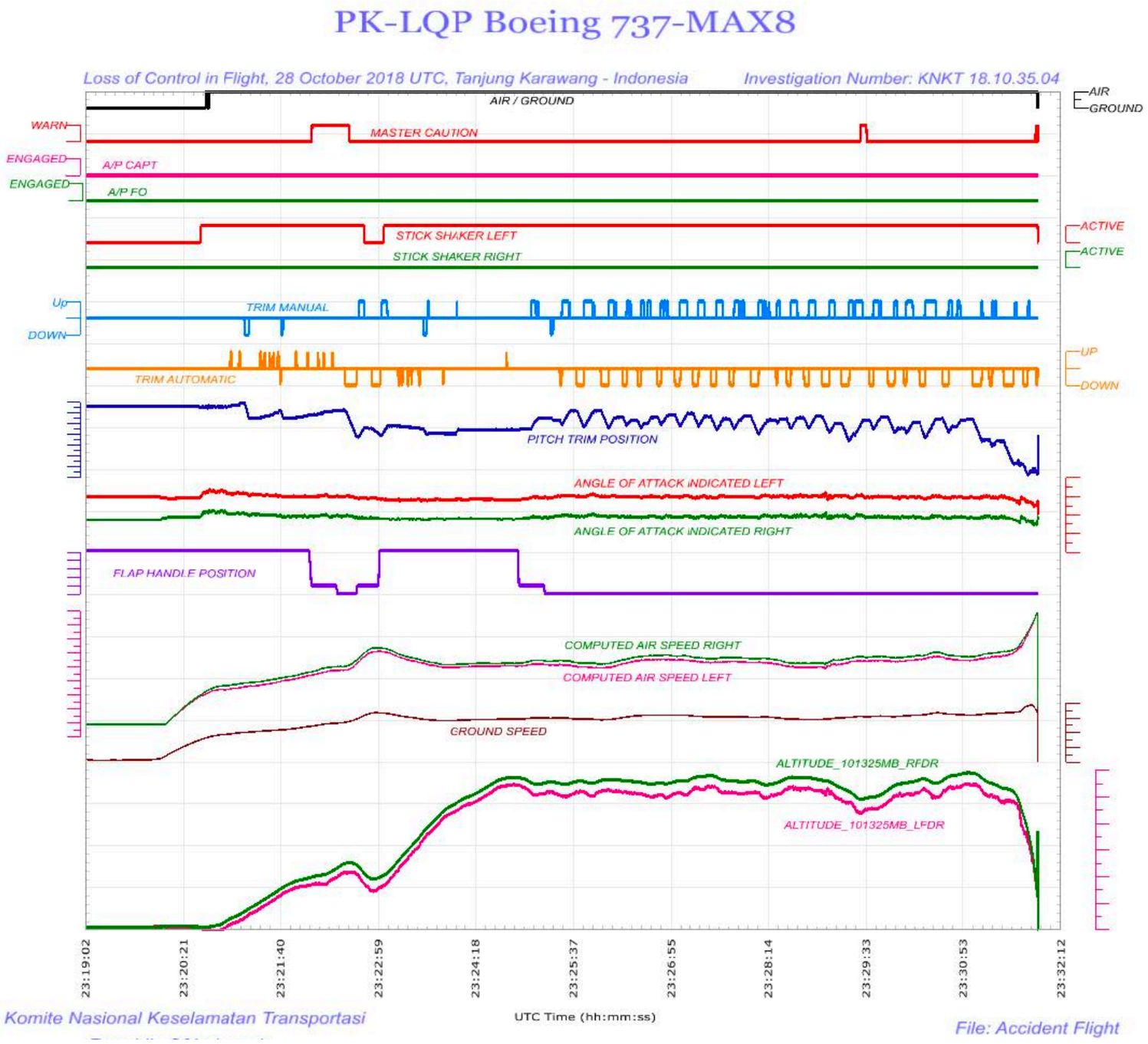
- 23:31:23 the pilots requested the ground controller to block in principle all other traffic on all altitudes in their direction

- 23:31:54 the DFDR stopped recording

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

Accident 1 – Indonesia - IV

29th of October 2018



- Significant parameters

Image Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

Aftermath Accident 1

- On Nov 6th 2018, Boeing issues a Flight Crew Operation Manual Bulletin (OMB) #TBC-19
  - This OMB addresses un-commanded nose down stabilizer trim due to erroneous AoA during manual flight and
  - To use runaway stabilizer non-normal checklist (NNC)

- On 7th of Nov 2018, the FAA issues an Emergency Airworthiness Directive (AD) #2018-23-51 for the owners and operators of the Boeing 737-8 and -9 aircraft

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

Boeing Bulletin TBC-19

Extracts - I

Background Information

The Indonesian National Transportation Safety Committee has indicated that Lion Air flight 610 experienced erroneous AOA data. Boeing would like to call attention to an AOA failure condition that can occur **during manual flight only.** This bulletin directs flight crews to existing procedures to address this condition. In the event of erroneous AOA data, the pitch trim system can trim the stabilizer nose down in increments lasting up to 10 seconds. The nose down stabilizer trim movement can be stopped and reversed with the use of the electric stabilizer trim switches but may restart 5 seconds after the electric stabilizer trim switches are released. Repetitive cycles of uncommanded nose down stabilizer continue to occur unless the stabilizer trim system is deactivated through use of both STAB TRIM CUTOUT switches in accordance with the existing procedures in the Runaway Stabilizer NNC. It is possible for the stabilizer to reach the nose down limit unless the system inputs are counteracted completely by pilot trim inputs and both STAB TRIM CUTOUT switches are moved to CUTOUT.

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

Boeing Bulletin TBC-19
Extracts - II

Flight Crew Operations Manual Bulletin No. TBC-19 , Dated November 6, 2018 (continued)

Additionally, pilots are reminded that an erroneous AOA can cause some or all of the following indications and effects:

- Continuous or intermittent stick shaker on the affected side only.
- Minimum speed bar (red and black) on the affected side only.
- Increasing nose down control forces.
- Inability to engage autopilot.
- Automatic disengagement of autopilot.
- IAS DISAGREE alert.
- ALT DISAGREE alert.
- AOA DISAGREE alert (if the AOA indicator option is installed)
- FEEL DIFF PRESS light.

Operating Instructions

In the event an uncommanded nose down stabilizer trim is experienced on the 737-8 /-9, in conjunction with one or more of the above indications or effects, do the Runaway Stabilizer NNC ensuring that the STAB TRIM CUTOUT switches are set to CUTOUT and stay in the CUTOUT position for the remainder of the flight.

Note: Initially, higher control forces may be needed to overcome any stabilizer nose down trim already applied. Electric stabilizer trim can be used to neutralize control column pitch forces before moving the STAB TRIM CUTOUT switches to CUTOUT. Manual stabilizer trim can be used after the STAB TRIM CUTOUT switches are moved to CUTOUT.

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

FAA Emergency AD
Extracts - I

AD Requirements

This AD requires revising certificate limitations and operating procedures of the airplane flight manual (AFM) to provide the flight crew with runaway horizontal stabilizer trim procedures to follow under certain conditions.

(e) Unsafe Condition

This AD was prompted by analysis performed by the manufacturer showing that if an erroneously high single angle of attack (AOA) sensor input is received by the flight control system, there is a potential for repeated nose-down trim commands of the horizontal stabilizer. We are issuing this AD to address this potential resulting nose-down trim, which could cause the flight crew to have difficulty controlling the airplane, and lead to excessive nose-down attitude, significant altitude loss, and possible impact with terrain.

Source: PRELIMINARY KNKT.18.10.35.04, Aircraft Accident Investigation Report PT. Lion Mentari Airlines Boeing 737-8 (MAX); PK-LQP Tanjung Karawang, West Java Republic of Indonesia 29 October 2018

FAA Emergency AD
Extracts - II

(g) Revision of Airplane Flight Manual (AFM): Certificate Limitations

Within 3 days after receipt of this AD, revise the Certificate Limitations chapter of the applicable AFM to include the information in figure 1 to paragraph (g) of this AD.

(h) AFM Revision: Operating Procedures

Within 3 days after receipt of this AD, revise the Operating Procedures chapter of the applicable AFM to include the information in figure 2 to paragraph (h) of this AD.

Source: PRELIMINARY KNKT.18.10.35.04,
Aircraft Accident Investigation Report
PT. Lion Mentari Airlines Boeing 737-8 (MAX);
PK-LQP Tanjung Karawang, West Java Republic of
Indonesia 29 October 2018