Perspectives on the Boeing 737MAX MCAS

Ron Carson, PhD, ESEP, INCOSE Fellow

Seattle Pacific University, University of Washington
https://www.linkedin.com/in/ron-carson-phd-esep-573549b/

2020 INCOSE Western States Regional Conference – Seattle, WA

Outline

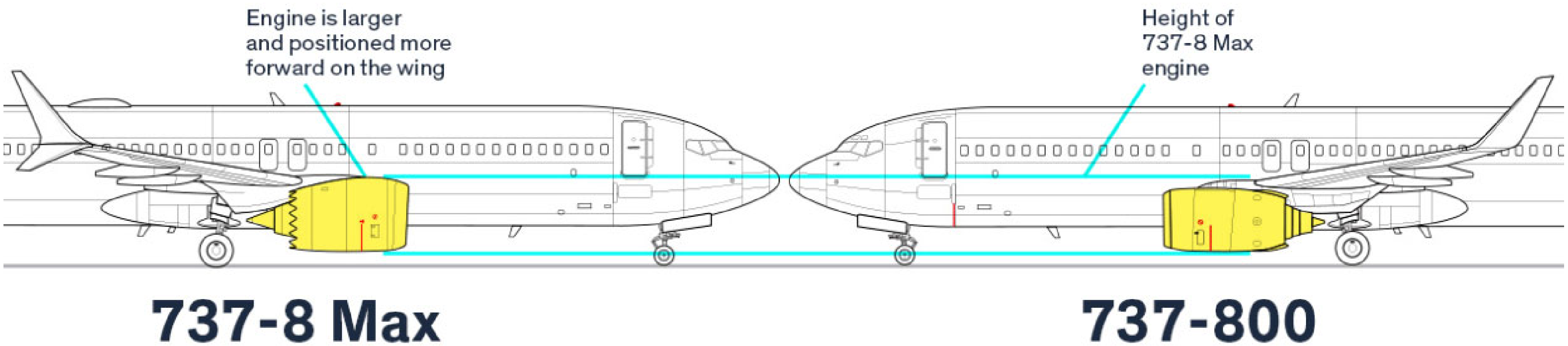
- Background of this presentation
- What / Why MCAS
- 737MAX Operation with MCAS
- MCAS system design and operation
- Failure severity classification and analysis
- Root-cause analysis
- Implications and Summary

- Reminder: no Boeing proprietary material (presentation or discussion)!
  – NOTE: Material marked “Boeing Proprietary” is from US Congressional Report from materials Boeing submitted

Background

- This presentation began as a special lecture for EGR4610, “Systems Design” (juniors and seniors) at Seattle Pacific University – see paper #4
- The objective was to demonstrate how several course topics come together…
  - Safety and reliability (failure rates, severity classification, redundancy, fault trees,)
  - Laws and standards (safety standards, especially ARP4761)
  - Human-systems integration (operator reaction to information, physical capability)
- ….And what can happen if we don’t get it right – our technical and ethical obligations
- This presentation augments the original course materials based on published reports as well as the original news and trade articles (Seattle Times, IEEE Spectrum)

What / Why MCAS –
Maneuvering Characteristics Augmentation System

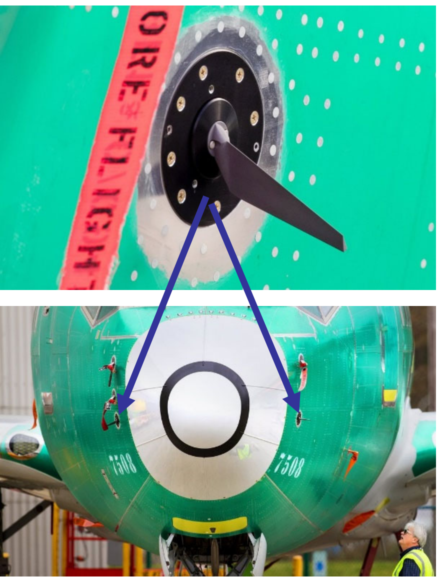


- MCAS is a software *Function* that was added to MAX family to limit tendency to "pitch up" at higher thrust levels (e.g., climbing from takeoff) because of more forward engine position
- "Pitch up" can lead to "stall" – loss of wing lift
- MCAS causes horizontal stabilizer to force nose down ("pitch down") when a stall is being detected by existing Angle of Attack sensor(s)

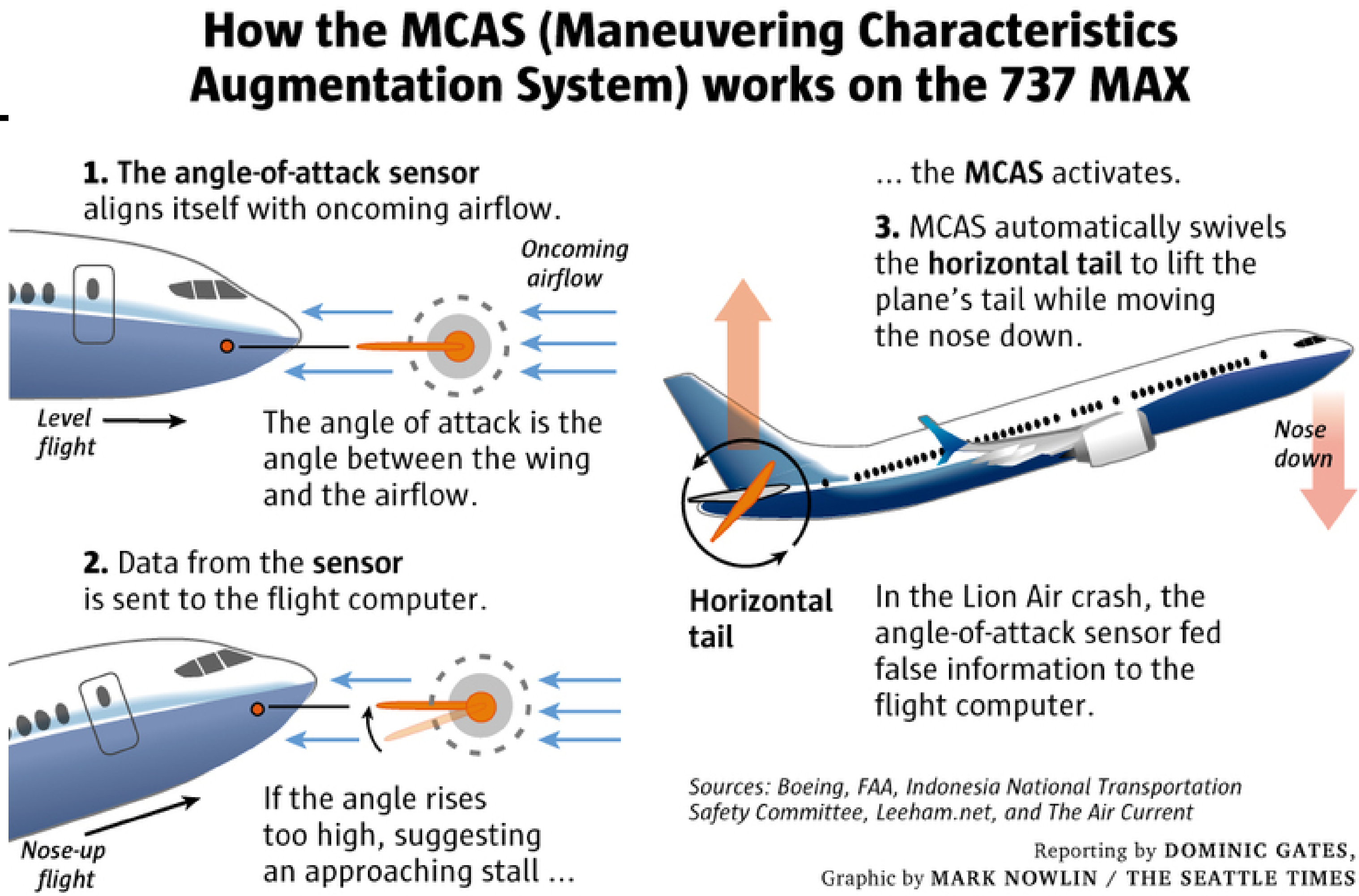
https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer

MCAS Operation

AOA Sensors

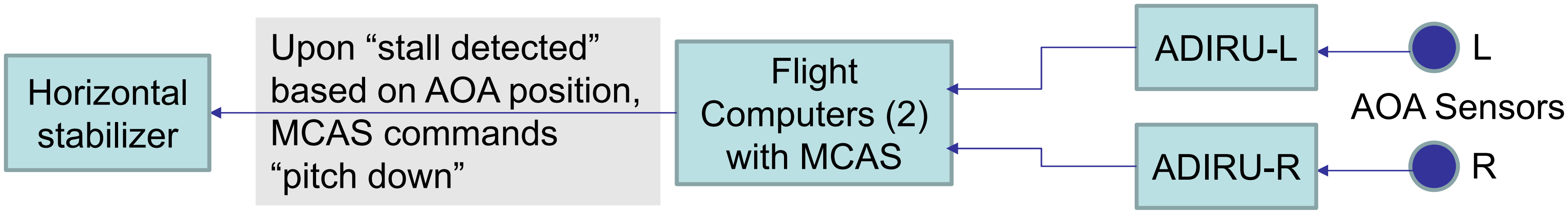


https://www.seattletimes.com/business/boeing-aerospace/a-lack-of-redundancies-on-737-max-system-has-baffled-even-those-who-worked-on-the-jet/



https://www.seattletimes.com/business/boeing-aerospace/failed-certification-faa-missed-safety-issues-in-the-737-max-system-implicated-in-the-lion-air-crash/

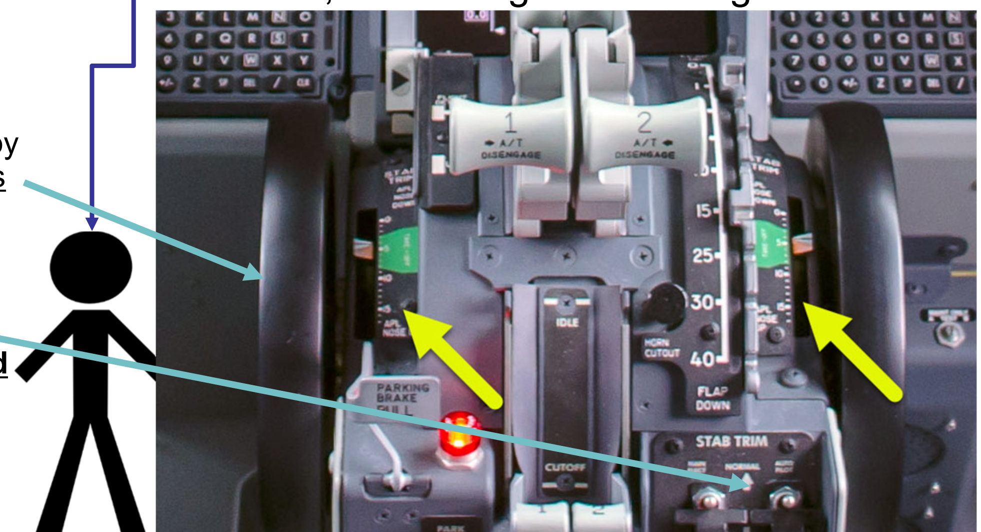
System Design and Operation



MCAS software is hosted on the two Flight Computers

MCAS uses input from **ONE** AOA sensor, alternating between flights

- Single failure of AOA is not reported to pilots
- Erroneous AOA input can cause MCAS to announce “stall” and pitch nose down
  - Assumption: pilots would quickly recognize and could override MCAS by turning it off and manually control the horizonal stabilizer via the wheels on the center console
- Pilots
  - Don’t know about MCAS (automation)
  - May react to erroneous stall warning by pushing nose down, **as trained**
  - May not be able to override horizontal stabilizer position because of forces at high speeds
- MCAS can self-reactivate (multiple pitch-down commands)



https://aviation.stackexchange.com/questions/61553/why-do-the-stabiliser-trim-wheels-not-move-exactly-in-sync

Relevant Severity Classification Basis: Can the Pilots Recover?

- "For the stabilizer runaways in the WUT [wind-up turn] maneuver (i.e. in the operational envelope) to the CLAW [structural] limit, the runaways were found Major [10^{-5}/hr*], and the 3 second runaways found Hazardous [10^{-7}/hr]. The Hazardous category was applied mainly due to the tendency to overspeed during the recovery rollout for those cases where the WUT was performed near the maximum operating speeds."….
- "With pilot training to recognize the runaway and use of teamwork, the failure was found Hazardous, which is the same as the item C finding. A typical reaction time was observed to be approximately 4 seconds. A slow reaction time scenario (> 10 seconds) found the failure to be catastrophic [10^{-9}/hr] due to the inability to arrest the airplane overspeed." [emphases added]

➢ Delay in pilot response is catastrophic
  ➢ Pilot ability to react to failure is a critical part of the system design

Item	Hazard Description	Phase	Failure Condition	Effect Class
A	Loss of Flaps Up High Alpha Stabilizer function (MCAS)	**Flaps Up flight** ~~Cruise~~	**Decrease in stability with load factor and angle of attack**	IV(Minor) Normal flight envelope III (Major) Operational flight envelope
B	Uncommanded High Alpha Stabilizer function operation (MCAS) to maximum authority ~~(0.55 deg)~~	ALL	Stabilizer runaway due to MCAS control law stabilizer deflection limit. Pitch trim functionality is retained.	III (Major) Normal flight envelope II(Hazardous) Operational flight envelope
C	Uncommanded MCAS function operation equivalent to 3 second mistrim (0.81 deg)	ALL	Stabilizer runaway equivalent to 3 seconds of mistrim (FAR25.255). Pitch trim functionality is retained.	III (Major) Normal flight envelope II (Hazardous) Operational flight envelope
D	Uncommanded MCAS function operation to pilot reaction	ALL	Stabilizer runaway until pilot recognition and reaction	II (Hazardous) Operational flight envelope

The **original** hazard assessments were obtained by pilot assessment in the motion simulator. Critical combinations of weight and CG were tested.

Export Controlled ECCN: 7E994

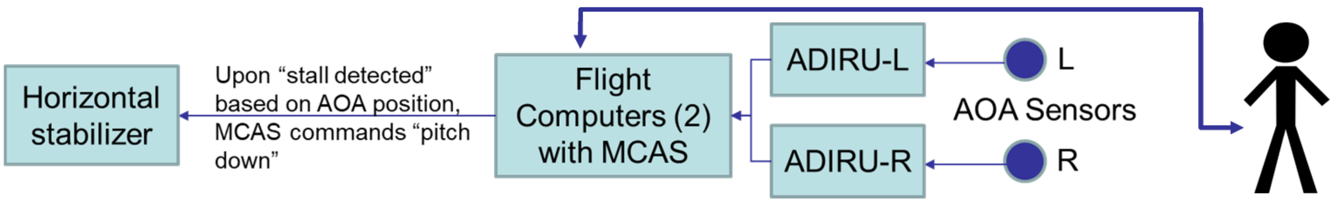
BOEING PROPRIETARY

TBC-T&I029164

From Boeing Coordination Memo Aero-B-BB1\8-C12-0159, Rev. C, compiled in https://www.govinfo.gov/content/pkg/CHRG-116hhrg38282/pdf/CHRG-116hhrg38282.pdf as artifact TBC-T&I 029164-65 (footnote 46 of GOVPUB-Y4_T68_2)

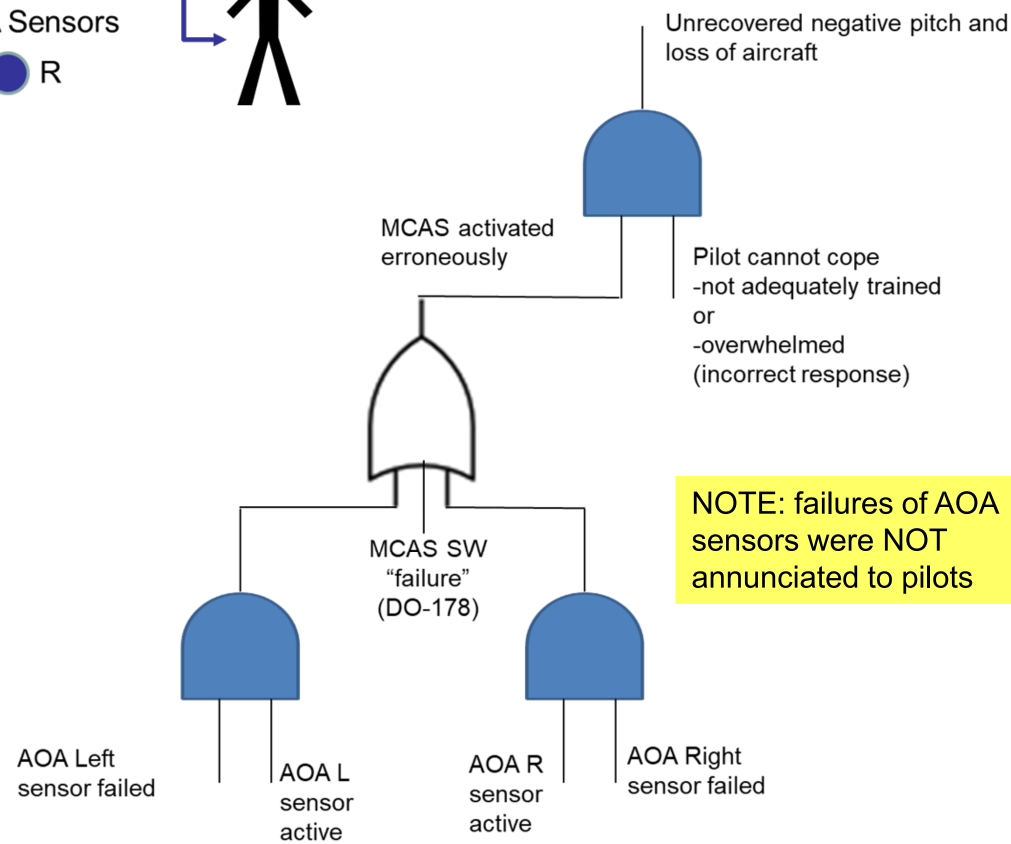
*Allowable failure rates from ARP4761, "**Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment**"

System Design: Fault Tree and Human Factors



- Certification was Amended Type Cert (ATC): limits scope of analysis and test
- In assessing allowable failure rate, the scope of “MCAS” is critical (SW-only, or include existing hardware and pilots?)
- Flight manuals did not address MCAS (hidden automation)
- Training updates did not include MCAS or criticality of “runaway” response
  - No changes to simulator training

Partial Fault Tree



NOTE: failures of AOA sensors were NOT annunciated to pilots

Why did this happen? Root-cause analysis

- Three reports:
  - KNKT.18.10.35.04, "Aircraft Accident Investigation Report, PT. Lion Mentari Airlines, Boeing 737-8 (MAX); PK-LQP" (Republic of Indonesia) 29 October 2018
  - Joint Authorities Technical Review (JATR), "Boeing 737 MAX Flight Control System: Observations, Findings, and Recommendations Submitted to the Associate Administrator for Aviation Safety, U.S. Federal Aviation Administration October 11, 2019 [review of certification process]
  - US House Committee on Transportation & Infrastructure, "The Boeing 737 MAX Aircraft: Costs, Consequences, and Lessons from its Design, Development, and Certification - Preliminary Investigative Findings", March 2020:
    1. "Production Pressures"
    2. "Faulty Assumptions"
    3. "Culture of concealment"
    4. "Conflicted Representation"
    5. "Boeing Influence over FAA Oversight"

"Production Pressures"

- Business context: 737MAX was developed in sales/delivery competition with Airbus A320neo with pressure to control costs, maintain schedule
- "Schedule" and business considerations contributed to "update" vs. new, leading to engine placement and resulting MCAS results
- "Boeing's business objective for the 737 MAX from the start was to build an airplane that required no simulator training for pilots who were already flying the 737 NG." [see footnote 21, p. 5 of US House report (Boeing internal e-mail, "Subject: 737MAX Firm Configuration Status/Help Needed," May 4, 2013, (see "Differences Pilot Training" section), TBC T&I 048706-048708, accessed here: https://www.govinfo.gov/content/pkg/CHRG-116hhrg38282/pdf/CHRG-116hhrg38282.pdf p. 129)

"Faulty Assumptions"

- Pilot capability:
  - "Boeing's own analysis showed that if pilots took more than 10 seconds to identify and respond to a "stabilizer runaway" condition caused by uncommanded MCAS activation the result could be catastrophic. The Committee has found no evidence that Boeing shared this information with the FAA, customers, or 737 MAX pilots."
    - Also acknowledged by Boeing President David Calhoun interview (February 2020), https://www.king5.com/video/tech/science/aerospace/boeing/boeings-new-ceo-reacts-to-what-went-wrong-with-the-737-max/281-e0ebd2c3-8b66-4547-bb53-13985a179c02
  - "The 10-second reaction time and the potential for it to result in catastrophic consequences was discovered early on in the development of the 737 MAX program. [see footnote 46, p. 9 of US House report: Coordination Sheet—Revision D—TBC-T&I 029160–029166, accessed here: https://www.govinfo.gov/content/pkg/CHRG-116hhrg38282/pdf/CHRG-116hhrg38282.pdf]
  - "Multiple Boeing ARs were aware of these findings and never reported them to the FAA."
- Training
  - "In July 2014, two years before the FAA made a decision regarding pilot training requirements for the 737 MAX, and at a time when the FAA was questioning Boeing on its presumption that no simulator training would be required, Boeing issued a press release asserting: "Pilots already certified on the Next-Generation 737 will not require a simulator course to transition to the 737 MAX."[see footnote 51, p. 10 of US House report: "Boeing Selects Supplier for 737 MAX Full-Flight Simulator," Boeing Press Release, July 11, 2014, accessed here: https://boeing.mediaroom.com/2014-07-11-Boeing-Selects-Supplier-for-737-MAX-Full-Flight-Simulator]
  - Updated simulator training was **not required** for pilots moving from NG to MAX configurations.

"Relax! I know this road perfectly! I've been driving it all my life!"

https://www.shelterwood.org/wp-content/uploads/2014/01/Screen-Shot-2014-12-15-at-7.12.10-PM.png

"Culture of Concealment": US House Report, page 3

- "In several critical instances, Boeing withheld crucial information from the FAA, its customers, and 737 MAX pilots. This included
- "hiding the very existence of MCAS from 737 MAX pilots [13] and
  - Note 13: Benjamin Shang, "Boeing's CEO explains why the company didn't tell 737 Max pilots about the software system that contributed to 2 fatal crashes," Business Insider, April 29, 2019, accessed here: https://www.businessinsider.com/boeings-ceo-on-why-737-max-pilots-not-told-of-mcas-2019-4 .
- "failing to disclose that the AOA disagree alert was inoperable on the majority of the 737 MAX fleet, despite having been certified as a standard cockpit feature.[14] This alert notified the crew if the aircraft's two AOA sensor readings disagreed, an event that occurs only when one is malfunctioning.
  - Note 14: Julie Johnsson, Ryan Beene and Mary Schlangenstein, "Boeing Held Off for Months on Disclosing Faulty Alert on 737 Max," Bloomberg, May 5, 2019, accessed here: https://www.bloomberg.com/news/articles/2019-05-05/boeing-left-airlines-faa-in-dark-on-737-alert-linked-to-crash .
- "Boeing also withheld knowledge that a pilot would need to diagnose and respond to a "stabilizer runaway" condition caused by an erroneous MCAS activation in 10 seconds or less, or risk catastrophic consequences.[15]"
  - Note 15: Boeing Coordination Sheet, Revision D, 3/30/16 TBC-T&I 29160 – TBC-T&I 29166 at TBC-T&I 29166, accessed at p. 164 here: https://www.govinfo.gov/content/pkg/CHRG-116hhrg38282/pdf/CHRG-116hhrg38282.pdf .

“Conflicted Representation” (US House Report, page 4)

- “Boeing ARs failed to represent the interests of the FAA in carrying out their FAA-delegated functions.
  - “For example, at least one AR [Authorized Representative] concurred on a decision **not** to emphasize MCAS as a “new function” because of Boeing’s fears that “there may be a greater certification and training impact” if the company did and the Committee has no evidence the AR shared this information with the FAA.” [18] [emphasis in original]
    - Note 18: Boeing internal email, “Subject: PRG – 37MAXFCO-PDR_AI22 – MCAS/Speed Trim,” June 7, 2013, accessed at p. 93 here: https://transportation.house.gov/imo/media/doc/Compressed%20Updated%202020.01.09%20Boeing%20Production.pdf .
  - “In addition, the Committee has found no evidence to date that any Boeing ARs who were aware of the fact that Boeing had evidence suggesting a slow pilot reaction time to address a runaway stabilizer event caused by uncommanded MCAS activation could result in catastrophic consequences informed the FAA of this critical information.”
  - “The Committee also discovered that one AR who was aware that Boeing knowingly delivered aircraft with inoperable AOA Disagree alerts to its customers took no action to inform the FAA. Not all of these instances violated FAA regulations or guidance, but they indicate that Boeing ARs are not communicating with the FAA enough about issues of concern.”
- JATR, cover letter, p. 2: “The specific recommendations include reviewing whether the ODA process can be made less cumbersome and bureaucratic to avoid stifling needed communications…[and]... revisiting the FAA's standards regarding the time needed by pilots to identify and respond to problems that arise.”

Illustration by Robert Neubecker
https://compote.slate.com/images/13036372-e8b6-42ae-b6ca-e40b9900a6a9.jpg

“Boeing Influence Over FAA Oversight”

- [Overlaps “Conflicted Representation”]
- “In at least one instance, the FAA failed in its duty to hold Boeing accountable for violations of FAA regulations in the 737 MAX program.[20]
  - Note 20: “Letter from FAA Acting Administrator Daniel Elwell to Chair Peter DeFazio, July 11, 2019, (on file with Committee (regarding the mandatory installation of functional AOA Disagree alerts on all Boeing 737 MAX aircraft)).”
- Contributing: Limited FAA capacity and capability to <u>independently</u> evaluate information [JATR “Finding F5.2-A: There may be a lack of capacity and depth of experience of BASOO engineering members to approve and make findings of compliance for retained items.”]

https://vevscientific.com/wp-content/uploads/2019/03/Compliance.jpg

SW configuration error – not per requirements and approved design – violates DO-178

Summary: 737MAX Program Constraints and Actions

- Program choice
  - Update 737, ATC
  - Retain fuselage and landing gear
  - Define MCAS as “Speed Trim” addition (US House Rpt, p. 8)
  - Don’t disclose time-criticality of pilot response
  - No new Simulator training
  - Don’t disclose “Disagree Alert” inoperability
  - “Disagree Alert” not fixed immediately

- Alternate choice
  - New, airplane TC
  - Modify aircraft for larger engines
  - MCAS as new system
  - Disclose time-criticality of pilot response
  - New simulator training
  - Disclose “Disagree Alert” condition
  - Update/release new software

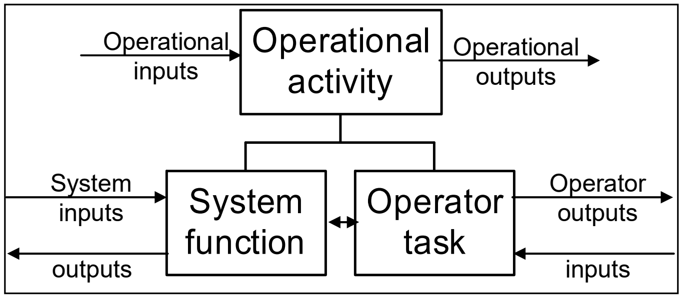
- Rationale
  - ?
  - ?
  - ?
  - ?
  - $1M/ airplane (SWA) (US House Rpt, p. 10)
  - ?
  - Planned release in MAX-10 update (US House Rpt, p. 8)

Results: Changes

- Regulatory: FAA Emergency Airworthiness Directive (AD) 2018-23-51 (7 November 2018) defined pilot procedures after Lion AIR crash
- Technical:
  - MCAS understood to be safety-critical
  - MCAS software updated to incorporate redundancy and “AOA disagree” alert – note: no hardware required to implement redundancy
  - Manuals and simulator training (mandatory) being updated
- Organizational
  - Boeing and FAA: JATR recommendations to review ODA process regarding FAA interaction with airplane manufacturers
  - Boeing internal structure: engineering to report separately from “project” https://www.nytimes.com/2019/09/15/business/boeing-safety-737-max.html

SE Implications

- **Incremental system design** (add or modify existing system) has inherent risks of overlooking an *emergent* (unplanned, unexpected, undesired) behavior (JATR, p. IV):
  - "The JATR team reviewed how the Changed Product Rule process was applied to the certification of the flight control system of the B737 MAX. The JATR team determined that the Changed Product Rule process was followed and that the process was effective for addressing discrete changes. However, the team determined that the <u>process did not adequately address cumulative effects, system integration, and human factors issues</u>. The Changed Product Rule process allows the applicant to only address in a limited way changed aspects (and areas affected by the change) and does not require analysis of all interactions at the aircraft level." [emphasis added]
- **Operators** must be considered as "part of the system" when they are relied upon for failure compensation
  - Operator requirements must be *validated* for feasibility of the functional allocation and required performance
- **Automation** can reduce workload, and can also create confusion because of incomplete information



Carson & Sheeley, "Functional Architecture as the Core of MBSE", Proceedings of INCOSE 2013.

Summary

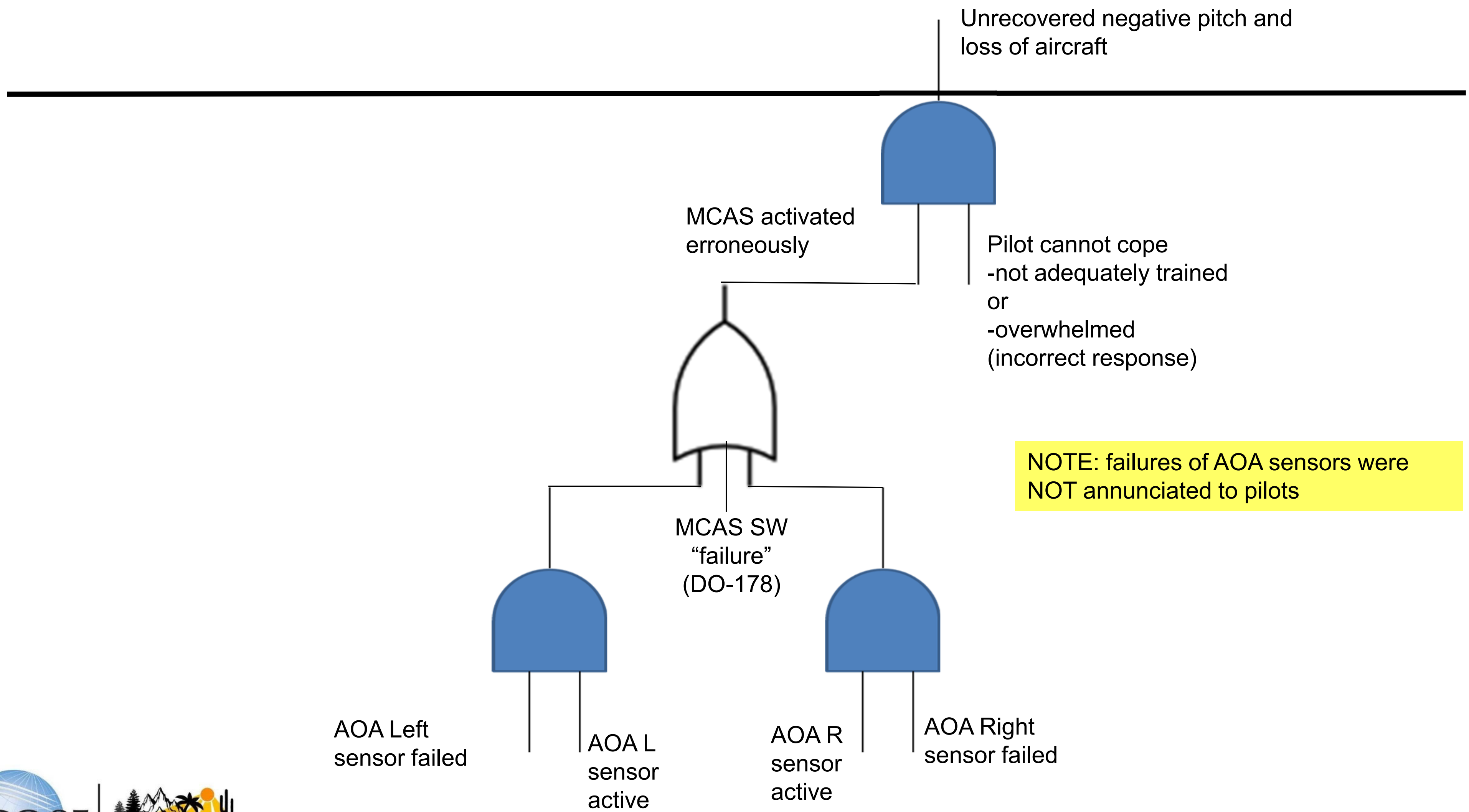
- 737MAX is a tragedy on many levels
  - Passenger and crew lives lost
  - Boeing financial impact and reputation
- Many contributing causes
  - Primary issue is the baseline design that pilots would effectively cope with MCAS failure
- Continuous vigilance in safety is paramount
  - It's not just about "complying with rules"
  - For engineers, "hope is not a plan"
- Addendum: US Department of Justice – Boeing Settlement January 7, 2021
  - Agreement resolves "a criminal charge related to conspiracy to defraud the [US FAA] Aircraft Evaluation Group in connection with the FAA AEG's evaluation of Boeing's 737 MAX airplane."
  - Identifies two Boeing "Flight Technical Pilots" as responsible for concealing information.

Questions? In order, by category

1. Corrections of presented information based on public domain information
2. Questions requesting clarification of presented information
3. “What if” and “why” questions that require additional inference and/or speculation

Hazard Consequences – Severity

Hazard Classification ("Severity") (ARP4761)	**Commercial Airplanes – Description / Criteria "Consequences"**	Maximum Probability per Flight Hour
Catastrophic	Results in multiple fatalities and/or loss of the system	10^{-9}
Hazardous	•Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be: •Large reduction in safety margin or functional capability •Crew physical distress/excessive workload such that operators cannot be relied upon to perform required tasks accurately or completely •Serious or fatal injury to small number of occupants of aircraft (except operators) •Fatal injury to ground personnel and/or general public	10^{-7}
Major	•Reduces the capability of the system or the operators to cope with adverse operating conditions to the extent that there would be: •Significant reduction in safety margin or functional capability •Significant increase in operator workload •Conditions impairing operator efficiency or creating significant discomfort •Physical distress to occupants of aircraft (except operator) including injuries •Major occupational illness and/or major environmental damage, and/or major property damage	10^{-5}
Minor	•Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Include: •Slight reduction in safety margin or functional capabilities •Slight increase in workload such as routine flight plan changes •Some physical discomfort to occupants or aircraft (except operators) •Minor occupational illness and/or minor environmental damage, and/or minor property damage	--
No Effect	Has no effect on safety	--


Unrecovered negative pitch and loss of aircraft
MCAS activated erroneously
Pilot cannot cope
-not adequately trained
or
-overwhelmed
(incorrect response)
NOTE: failures of AOA sensors were NOT annunciated to pilots
MCAS SW “failure” (DO-178)
AOA Left sensor failed
AOA L sensor active
AOA R sensor active
AOA Right sensor failed

FAR **25.255 Out-of-trim characteristics.**

- **(a)** From an initial condition with the airplane trimmed at cruise speeds up to VMO/MMO, the airplane must have satisfactory maneuvering stability and controllability with the degree of out-of-trim in both the airplane nose-up and nose-down directions, which results from the greater of -
- **(1)** A three-second movement of the longitudinal trim system at its normal rate for the particular flight condition with no aerodynamic load (or an equivalent degree of trim for airplanes that do not have a power-operated trim system), except as limited by stops in the trim system, including those required by § 25.655(b) for adjustable stabilizers; or
- **(2)** The maximum mistrim that can be sustained by the autopilot while maintaining level flight in the high speed cruising condition.
- **(b)** In the out-of-trim condition specified in paragraph (a) of this section, when the normal acceleration is varied from + 1 g to the positive and negative values specified in paragraph (c) of this section -
- **(1)** The stick force vs. g curve must have a positive slope at any speed up to and including VFC/MFC; and
- **(2)** At speeds between VFC/MFC and VDF/MDF the direction of the primary longitudinal control force may not reverse.
- **(c)** Except as provided in paragraphs (d) and (e) of this section, compliance with the provisions of paragraph (a) of this section must be demonstrated in flight over the acceleration range -
- **(1)** −1 g to + 2.5 g; or
- **(2)** 0 g to 2.0 g, and extrapolating by an acceptable method to −1 g and + 2.5 g.
- **(d)** If the procedure set forth in paragraph (c)(2) of this section is used to demonstrate compliance and marginal conditions exist during flight test with regard to reversal of primary longitudinal control force, flight tests must be accomplished from the normal acceleration at which a marginal condition is found to exist to the applicable limit specified in paragraph (b)(1) of this section.
- **(e)** During flight tests required by paragraph (a) of this section, the limit maneuvering load factors prescribed in § § 25.333(b) and 25.337, and the maneuvering load factors associated with probable inadvertent excursions beyond the boundaries of the buffet onset envelopes determined under § 25.251(e), need not be exceeded. In addition, the entry speeds for flight test demonstrations at normal acceleration values less than 1 g must be limited to the extent necessary to accomplish a recovery without exceeding VDF/MDF.
- **(f)** In the out-of-trim condition specified in paragraph (a) of this section, it must be possible from an overspeed condition at VDF/MDF to produce at least 1.5 g for recovery by applying not more than 125 pounds of longitudinal control force using either the primary longitudinal control alone or the primary longitudinal control and the longitudinal trim system. If the longitudinal trim is used to assist in producing the required load factor, it must be shown at VDF/MDF that the longitudinal trim can be actuated in the airplane nose-up direction with the primary surface loaded to correspond to the least of the following airplane nose-up control forces:
- **(1)** The maximum control forces expected in service as specified in § § 25.301 and 25.397.
- **(2)** The control force required to produce 1.5 g.
- **(3)** The control force corresponding to buffeting or other phenomena of such intensity that it is a strong deterrent to further application of primary longitudinal control force.