Australian Safety Critical Systems Association

A National Special Interest Group of the

Newsletter

AUSTRALIAN COMPUTER SOCIETY

July 2019

Learning the hard way: the Boeing 737 MAX

aSCSa Chair's Note: Definitive findings of all 737 MAX8 accident investigation boards are not yet complete. Yet many admissions, opinions, insider accounts and public hearing statements have been released apparently coalescing on some key common contributing factors. Commentary and industry response are also arising in some reputable publications looking beyond design decisions to some contributions of Operator pilot competency and experience level standards. This is a complex and deep accident cause chain. In reprising these sources in this Newsletter for our readership, the aSCSa do not pre-judge any final findings or corrective actions required by any party. However, we do find these accidents particularly noteworthy, and believe there are many cautionary messages and potentially re-learnt lessons for safety engineering practices and safety culture worth reinforced highlighting at length.

It has taken the deaths of 346 people for the aviation industry to probe business commercial and engineering practices and the role of regulators and aircraft certifiers.

The fact that it took a second crash in less than four months after the first to question the safety integrity of the 737 MAX aircraft says more about protecting self-interests, than genuinely seeking out any inherent flaws. One needs to ask, had the second crash not happened to an airline company with an excellent safety reputation like Ethiopian Airlines, would there have been the world-wide grounding of the 737 MAX?

Much is emerging as to the history of the 737 MAX development, the design decisions, the response to concerns raised by test pilots, and the process of certification. It is becoming increasingly apparent systemic process failure was a major contributing factor in both the Air Asia and Ethiopian Airline crashes.

Despite Boeing's expectation for the grounding order to be quickly lifted given that the problem has been identified and a "fix" has been thoroughly tested, regulators in many jurisdictions have yet to be convinced. Prior to the 737 MAX crashes, the US Federal Aviation Administration (FAA) was trusted by other jurisdictions; this is now not so. The recertification of the 737 MAX with the "fix" now requires Boeing to seek approval from the FAA and other jurisdictions. The FAA is also now taking a more cautions role.

The crashes

On 29 October 2018, a Boeing 737-8 (MAX) aircraft being operated by PT. Lion Mentari Airlines (Lion Air) as a scheduled passenger flight from Jakarta with intended destination of Pangkal Pinang[1], the plane crashed in the Java Sea, killing all 189 people on board in less than 15 minutes from take-off.

On March 10, 2019, at about 05:44 UTC1, Ethiopian Airlines flight 302, a Boeing 737-8 (MAX), Ethiopian registration ET-AVJ, crashed at 5: 44 UTC 28 NM South East of Addis Ababa near Ejere village Ejere, Ethiopia killing all 157 people on board.

Boeing statements after crashes

(After the first crash)

November 28, 2018 – Following the Lion Air crash, Boeing issued a response statement to a preliminary report by Indonesia's National Transportation Safety Committee (NTSC). The response focussed on the airworthiness doubts due to airspeed sensor maintenance performed following the problems encountered during the previous flight. The statement did not suggest the possibility of a flawed design.

(After the second crash)

March 12, 2019 – "*Safety is Boeing's number one priority and we have full confidence in the safety of the 737 MAX……The United States Federal Aviation Administration is not mandating any further action at this time…….. we do not have any basis to issue new guidance to operators".*

March 13, 2019 – "*Boeing continues to have full confidence in the safety of the 737 MAX. However, after consultation with the U.S. Federal Aviation Administration (FAA), the U.S. National Transportation Safety Board (NTSB), and aviation authorities and its customers around the world, Boeing has determined -- out of an abundance of caution and in order to reassure the flying public of the aircraft's safety -- to recommend to the FAA the temporary suspension of operations of the entire global fleet of 371 737 MAX aircraft*".

Continues Page 5

[1] Depati Amir Airport (WIPK), Pangkal Pinang is named as Pangkal Pinang in the Lion Air report.

Contents

aSCSa Committee

National Committee

BJ Martin	Chairman (ACT)
Luke Wildman	Secretary (QLD)
George Nikandros	Treasurer (QLD)
Clive Boughton	(ACT)
Holger Becht	(QLD)
Tariq Mahmood	(VIC)
Derek Reinhardt	(QLD)
Ed Kienast	(QLD)
Vamsi Madasu	(VIC)
Web Site	www.ascsa.org.au

The term of the current committee expires 30 June 2019 but will remain in place until the 2019 Annual General Meeting to be held later in the year. Nominations are now open. BJ Martin has advised that he won't be available for the full year. He will remain as chairman in the interim. The committee elects the chairman. The committee members and positions will be confirmed at the 2019 Annual General Meeting later in the year.

Research Award

In the December 2006 Newsletter, the aSCSa announced the establishment of student research award. The rules governing the award and associated forms are available from the aSCSa website.

The purpose of this annual award is to encourage Australian research in the science of software/system engineering or the application of that science for safety and/or mission critical software-intensive systems. At $5000, it is a substantial award.

The nominated closing date requirement has now been removed; nominations can now be made any time.

Presentation to Achim Washington, the 2018 Research Award winner at the 2019 Australian System Safety Conference, 23 to 24 May 2019, Customs House, Brisbane. Presentation was made by BJ Martin, Chairman aSCSa.

Griffith UNIVERSITY ***Course offering***

Introduction to System Safety

Course Ref: 7009LHS

A 5-day course from Griffith University – more details inside. Classroom and online options available.

Online – Nov-2019 to Jan-2020

Classroom – Nov-2019

Dates for the 2019 course will be updated prior to 3rd Trimester (September 2019). Please check the Griffith University course page for course dates.

Venue: Nathan Campus, Griffith University, QLD

To register you will need to use the Single Course of Study Application Form

From the Chair

What a satisfying experience the 2019 ASSC was! We seemed to have got the Theme right for the zeitgeist and the availability of some fantastic speakers (Keynotes and Presenters) that are right in the thick of the state of the art- articulating and solving the contemporary challenges for dependability in the domains of Rail, Aviation, Road Vehicles autonomy, medical devices and Space. We were inspired by Kelvin Ross examples of understanding and taking advantage of the opportunities that AI presents for improvements in safety in medical practice, and Drew Rae explained why we shouldn't throw our hands up in despair for safety certainty (we already live with that deficit!).

Phil Koopman and David Ward were extremely generous with their time, providing tutorials, social and conference panel engagement with respect to Autonomous Road Vehicles technology.

Not strictly on an AI theme, but certainly a new age of risks the public are exposed to – we couldn't miss an opportunity to listen to an experienced Astronaut, Shuttle Commander, cum researcher program manager, then regulator, now commercial space industry whisperer in Australia. Col (retired) Pam Melroy had the audience transfixed about the traditional considerations to space operations risk and how that must evolve for paying passengers and commercial ventures.

We also retained the mixer style of social event with a view of the Brisbane River at night which attracted a higher proportion of Conference attendees than recent years in what turned out as our smallest space. Good community bonding.

The committee was most pleased to receive several unsolicited thanks and compliments during the closing stages. However, in order to make most objective assessments of what went well and less so for future, we ask that anyone who went to complete the short survey. All conference presentation and tutorial materials are now available on the aSCSa website.

Prior to ASSC, in April we hosted another successful running of the Uni of York Safety Case Development and Review course, reported in this Newsletter. It felt like we'd maxed out that audience potential from 2 calendar years (same FY) as we crawled just over breakeven numbers on the second one. The committee will now have a rethink about what speciality courses we may invite in future to mix it up. However, Prof Tim Kelly will no longer be delivering as he has now taken a career turn to Theology as the new Assistant Curate at the Beverly Minster in Yorkshire. The aSCSa wish him very well and are grateful for the thoughtful inspiration, education and blessed GSN he has provided over many years to our community.

Just a short note about the emergence of a System Safety professional community for those in South Australia. Mr Mike Hurd has been hosting an 'Engineered Safety Group' via the Engineers Australia SA Division for the last few years. He has just handed over to Ms Lana Haigh and recently held a 2 day symposium in Adelaide that was well attended and got EA to notice System Safety as a discipline in its own right. Monthly-ish sharing sessions are held. Membership is also free and getting on their mailing list can be arranged via EA Member Services in SA. We hope to share more in future.

Finally - I will flag that we intend to hold an AGM in November in Brisbane (allowing dial-in), where all committee positions are up for renewal. An announcement will be made via email and the website. I will be making way for a new Chair, while remaining on the committee. We are always interested in new blood and enthusiasm to share the load and satisfaction bringing home the conference and other professional development initiatives for 2020.

BJ Martin
Chairman aSCSa

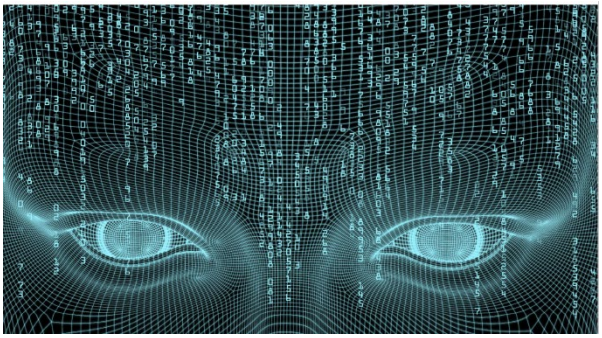
Bulletin Boards etc

ACM Risk Forum on Risks to the Public in Computers and Related Systems – http://catless.ncl.ac.uk/Risks.

System Safety List - http://www.systemsafetylist.org/

Safety-Critical Mailing List Forum formerly hosted by the University of York is now hosted by the University of Bielefeld. Need to join using the form located at System Safety Info Page for access.

2019 System Safety Conference



How can we be artificially safe?

The ninth two-day Australian System Safety Conference and the 24th conference hosted by the aSCSa, was held in May 2019 at the Customs House in Brisbane. The conference attracted an attendance of 60.

The 2019 ASSC theme was "*how can we be artificially safe"*; how can we be safe with artificial intelligence technologies, including simulations, model-based systems engineering, auto code generation and checking, agile development, machine learning, perception systems and the Internet of Things. Are we able to derive safety requirements for such systems and achieve adequate assurance of compliance initially and continuously for a dynamic safety case? Are traditional safety by design programs and system review constructs sufficient?

ASSC 2019 – Panel Session
(L to R, Philip Koopman, Ganesh Pai, David Ward, Kelvin Ross, with BJ Martin as moderator)

As in recent conferences, the conference program included invited keynote speakers, one from the UK, and was preceded by a tutorial day.

Conference Day 2 - Pam Melroy at the lectern

This year's conference was supported by four sponsor organisations with six gold sponsorships:

- RGB Assurance
- Nova Systems
- Department of Defence (*Capability Acquisition and Sustainment Group*) (3)
- Dedicated Systems

As had been the norm for conferences since 2002, this conference was supported by six invited keynote speakers, namely:

- *Pamela Melroy, Nova Systems, USA*
- *Philip Koopman, Carnegie-Mellon, USA*
- *Bijan Elahi, Medtronic, AUS*
- *David Ward, Horiba Mira, UK*
- *Ganesh Pai, SGT (KBRWylie), USA*
- *Kelvin Ross, KJR, AUS*

The conference was also supported by three pre-conference tutorials:

- *Machine learning for dependable decision-making (Dr Zhe Hou, Hadrien Bride & Prof. Jim Song Dong - Griffith University)*
- *Safety of the intended functionality (SOTIF; ISO/PAS 21448) in road vehicle automation (Dr David Ward - Mira)*
- *Introduction to Critical Systems & Automotive Software Safety Issues (Prof. Philip Koopman – Carnegie-Mellon)*

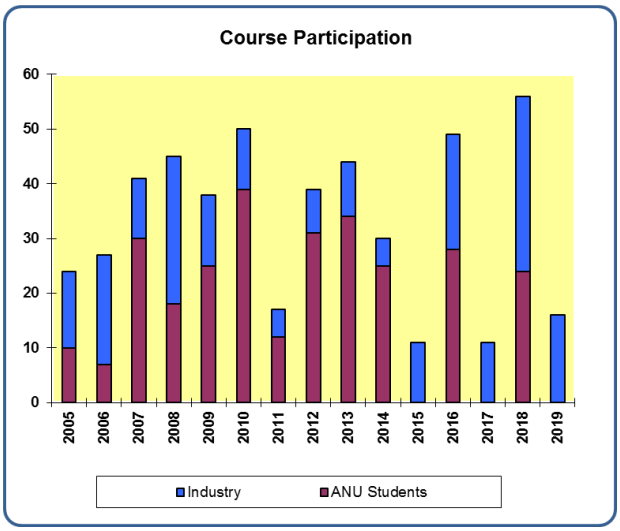
More information about the conference, the papers, presentations and the tutorials can be found at the 2019 conference papers page on the aSCSa website.

The aSCSa acknowledges the administrative support of ACS National Office (Krystal Ng) and the ACS QLD Branch (Holly Bretherton, Kylie Barringer).

Professional Development

The aSCSa hosted an Introduction to System Safety in conjunction with the Australian National University in April 2018, and Safety Case Development and Review courses in August 2018 and April 2019.

The chart below shows the participation at the aSCSa courses since 2005.



Introduction to System Safety

The next Introduction to System Safety course will be provided by Griffith University commencing around November 2019 – ***see advert on Page 3***.

To register, use the single course of study route, and use the Single course of study application form. The course title and reference number is ***Introduction to System Safety (7009LHS)***.

The course convenor is Drew Rae.

Safety Case Development and Review

Following on from the success of the August 2018 course and the industry interest, the aSCSa hosted the second Safety Case Development and Review Course in April 2019 in Canberra.

There were 16 participants, a little less than expected, but enough to cover costs.

The total number for the two courses during the 2018-19 financial year was a healthy 36.

Possible Other Course Options

The University of York have several system safety engineering short-course offerings. Excluding the foundation (introduction) course and the Safety Case Development & Review course, the other possible options are:

- Systems Engineering for Safety (SEFS)
- Hazard and Risk Assessment (HRAS)
- Software Requirements and Architectures (SWRE)
- System Safety Assessment (SSAS)
- Safety Management Systems (SMSY)
- Human Factors for Safety (HUFS)
- Through Life Safety (TLSA)
- Computers and Safety (CASA)
- Security for Safety-Critical Systems (SESA)

These short courses aim to provide participants with a thorough grounding and practical experience in the use of state-of-the-art techniques for development of safety critical systems, emphasising their software; together with an understanding of the principles behind these techniques so that they can make sound engineering judgements during the design and deployment of such a system, particularly when software is involved.

The aSCSa intends to seek feedback from the aSCSa members for their preferences for the next hosted course tentatively planned for April 2020. The decision on the course will also be subject to the University of York's availability to delivery it in Australia.

From Page 1

Boeing 737MAX continued

April 4, 2019 – "*We at Boeing are sorry for the lives lost in the recent 737 MAX accidents. These tragedies continue to weigh heavily on our hearts and minds, and we extend our sympathies to the loved ones of the passengers and crew on board Lion Air Flight 610 and Ethiopian Airlines Flight 302…..it's apparent that in both flights the Manoeuvring Characteristics Augmentation*

System, known as MCAS, activated in response to erroneous angle of attack information". (An acknowledgement that there is a defect).

Competition

A recent Forbes (28-Mar-2019) article says that Boeing rushed the 737 MAX to market -- it did not even wait for its board of directors to approve the design before offering it to American Airlines, which was on the cusp of buying [A320neo craft] from Airbus. Boeing's board didn't formally sign off on the MAX until a month later.

Boeing's problem was that Airbus was poised to make a big sale to American Airlines. Boeing needed a fuel-efficient aircraft to retain its market share -- so it launched the 737 MAX.

[The FCPA Blog] As the delivery of Airbus' A320neos, an aircraft model comparable to Boeing's 737, started hitting the market in early 2016, Boeing felt compelled to accelerate delivery of the first Max to early 2017, roughly six months ahead of schedule.

To avoid the need for a whole new aircraft type certificate, Boeing opted for an amended type certificate based on the 737 NG (new generation). Changes therefore were kept to a minimum. The intent was that from the pilot's perspective, the MAX was just a variant within the 737 NG type.

The "new features" included:

- CFM LEAP-1B fan with 18-blade, woven carbon-fibre fan blades giving a 69.4 in diameter compared to 61 in. for the 24-blade titanium fans of the CFM56-7. This gives 9:1 bypass ratio versus 5.1:1 for the older engine. Rated thrust LEAP-1B28: 29,317lbs.
- New CFM LEAP-1B custom core with 11-12% reduction in fuel burn and 7% reduction in operating cost.
- New engine nacelle and pylon will cause engines to project further forward than CFM56-7BE on 737NG.
- Updated EEC software, fuel and pneumatic systems.
- Nose gear extension of 15-20cm to give more engine ground clearance.
- Minor changes to nose wheel well to accommodate longer nose gear strut.
- Fly-by-wire spoiler system - to improve production flow, reduce weight and improve stopping distances.
- Manoeuvring Characteristics Augmentation System (MCAS) – Applies nose down stabilizer trim during high AoA (angle-of-attack) flight when the flaps are up, and the A/P (auto-pilot) is not engaged.

The MAX CFM LEAP-1B fan with a 69.4-inch fan diameter will have a 11-12% reduction in fuel burn and 7% reduction in operating cost compared to the NG. The nacelle and pylon *will cause the engines to project further forward* than the CFM56-7BE on 737NG.

About MCAS

MCAS (Manoeuvring Characteristics Augmentation System) is implemented on the 737 MAX 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 crew to use column trim switch or stabilizer aisle-stand cut-out switches to override MCAS input. The function is commanded by the Flight Control computer using input data from sensors and other airplane systems.

The MCAS function becomes active when the airplane Angle of Attack exceeds a threshold based on airspeed and altitude. Stabilizer incremental commands are limited to 2.5 degrees and are provided at a rate of 0.27 degrees per second. The magnitude of the stabilizer input is lower at high Mach number and greater at low Mach numbers. The function is reset once angle of

attack falls below the Angle of Attack threshold or if manual stabilizer commands are provided by the flight crew. If the original elevated AoA condition persists, the MCAS function commands another incremental stabilizer nose down command according to current aircraft Mach number at actuation.

The Lion Air Preliminary Accident Investigation Report[2] includes a copy of a Boeing "multi-operator message" (MOM), MOM-18-066444-018, which discloses the nose-down stabiliser limit of 2.5 degrees. This MOM was issued 10-Nov-2018, following the Lion Air Crash.

That limit was apparently new to the FAA; the FAA believed the airplane was limited to 0.6 degrees!

Why the need for MCAS?

During the early development of the 737 Max while testing high-speed situations on a flight simulator, like manoeuvres to avoid an obstacle or to escape a powerful vortex from another plane, handling issues were identified. While such moves might never be necessary for the pilot of a passenger plane, the F.A.A. requires that a jet handle well in those situations.

The relocated engines and their nacelle[3] shape caused an upward pitching movement – in essence, the nose of the MAX was being pushed up. Boeing added MCAS to compensate for the observed handling issues during the flight simulator tests. The role of MCAS was to help pilots to bring the nose down in the event the jet's angle-of-attack drifted too high when flying manually.

MCAS to operate in the background

The MAX's new MCAS automatic flight control system was designed to act in the background, without pilot input. Designed to activate automatically only in the extreme flight situation of a high-speed stall, this extra kick downward of the nose would make the plane feel the same to a pilot as the older-model 737s.

First test flight

The maiden test flight in late January 2016, was a success. Several weeks later, testing identified handling issues when nearing stalls at low speeds.

Boeing's response was to expand the role of MCAS to avoid stalls in all types of situations, thus enabling MCAS throughout much more of the flight, and made it more aggressive in pushing down the nose of the plane.

As MCAS now needs to operate through much more of the flight and because there are no excessive G-forces at low speed, the G-force factor was removed as a trigger. This meant MCAS was now activated by a single angle-of-attack sensor.

MCAS safety requirements

Internet articles such as from the Seattle Times question Boeing's MCAS safety analysis and in particular the failure classification for MCAS.

A follow-up Seattle Times article provides more on Boeing's safety analysis for MCAS:

> "*In a separate presentation made for foreign safety regulators that was reviewed by The Times, Boeing described MCAS as providing "a nose down command to oppose the pitch up. Command is limited to 0.6 degrees from trimmed position."*
>
> *"Two people involved in the initial design plans for MCAS said the goal was to limit the system's effect, giving it as little authority as possible. That 0.6-degree limit was embedded in the company's system safety review for the FAA.*
>
> *"The Boeing submission also included an analysis that calculated the effect of possible MCAS failures, with each scenario characterized as either a minor, a major or a hazardous failure — increasingly severe categories that determine how much redundancy must be built in to prevent the event.*
>
> ---
>
> *"Boeing analysed what would happen if, in normal flight mode, MCAS triggered inadvertently up to its maximum authority and moved the horizontal stabilizer the maximum 0.6 degrees.*
>
> *"It also calculated what would happen on a normal flight if somehow the system kept running for three seconds at its standard rate of 0.27 degrees per second, producing 0.81 degrees of movement, thus exceeding the supposed maximum authority.*
>
> *"Boeing assessed both of these failure modes as "major." Finally, the analysis looked at the inadvertent operation of MCAS during a wind-up turn, which was assessed as "hazardous…"*
>
> ---
>
> *According to a document reviewed by The Seattle Times, Boeing's safety analysis calculated this hazardous MCAS failure to be almost inconceivable*

Failure classification through system safety analysis influences the level of redundancy required. For a "major failure", the probability must be less than one in 100,000, for "hazardous" less than one in 10,000,000 per flight hour.

The original version of MCAS required two factors — angle of attack and G-force — to activate, Boeing's analysis indicated that just one sensor would be acceptable in all circumstances.

Pilot awareness of MCAS

Following the Lion Air crash, Boeing issued a Flight Crew Operations Manual Bulletin, TBC-19.

> "*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.*
>
> *Additionally, pilots are reminded that an erroneous AoA can cause some or all of the following indications and effects:*

[2] Komite Nosional Keselamatan Transportasi (KNKT), Preliminary Aircraft Accident Investigation Report: PT. Lion Mentari Airlines Boeing 737-8(MAX) – KNKT.18.10.35.04

[3] A streamlined casing on the outside of an aircraft, especially one housing an aircraft engine

- *Continuous or intermittent vibrate the control yoke (the "stick") of an aircraft to warn the pilot of an imminent stall (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.*

There is no specific mention of MCAS in the bulletin.

Following the Lion Air crash, it emerged that the MAX automatic stall prevention system, the manoeuvring characteristics augmentation system (MCAS), was not in the FCOM (Flight Crew Operations Manual).

The FAA issued an airworthiness directive AD #: 2018-23-51 on November 7, 2018 and revised it on December 21, 2018:

> *"We are adopting a new airworthiness directive (AD) for all The Boeing Company Model 737-8 and -9 airplanes. This emergency AD was sent previously to all known U.S. owners and operators of these airplanes. 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. 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 the unsafe condition on these products."*

The issue of this directive supports the claim that the MCAS was not prominent in the AFM. According to a CBC article, the *flight manual of Boeing's 737 Max 8 planes mentions MCAS computer system only once by name – in the glossary of abbreviated terms*.

The lack of prominence in the AFM may have been the reason for omission in the FCOM and the lack of pilot training as suggested in the Lion Air preliminary investigation report.

However, according to the Accident Investigation Preliminary Report by the Aircraft Accident Investigation Bureau of Ethiopia, "*the AFM provided by Ethiopian Airlines showed that the airline had incorporated the revisions A180625 on November 11, 2018 required by Airworthiness Directive 2018-23-51*".

The report's initial findings included the finding that "*the crew performed runaway stabilizer checklist and put the stab trim cut-out switch to cut-out position and confirmed that the manual trim operation was not working"*. This essentially confirms that the flight crew followed the procedure as specified but were not able to prevent the crash.

Boeing could no longer focus on maintenance or pilot error as a likely cause – there had to be something wrong with the aircraft's design, and specifically MCAS.

Aircraft certification

The following are progressive updates from the FAA, the aircraft's USA certifier:

Immediately after the Ethiopian Airlines crash (12-Mar-19):

> *"The FAA continues to review extensively all available data and aggregate safety performance from operators and pilots of the Boeing 737 MAX. Thus far, our review shows no systemic performance issues and provides no basis to order grounding the aircraft. Nor have other civil aviation authorities provided data to us that would warrant action. In the course of our urgent review of data on the Ethiopian Airlines Flight 302 crash, if any issues affecting the continued airworthiness of the aircraft are identified, the FAA will take immediate and appropriate action."*

The next day (13-Mar-19), the FAA changed their view:

> *"The FAA is ordering the temporary grounding of Boeing 737 MAX aircraft operated by U.S. airlines or in U.S. territory. The agency made this decision as a result of the data gathering process and new evidence collected at the site and analysed today. This evidence, together with newly refined satellite data available to FAA this morning, led to this decision.*
>
> *"The grounding will remain in effect pending further investigation, including examination of information from the aircraft's flight data recorders and cockpit voice recorders."*

The aircraft remains grounded world-wide. Despite initial expectations for a quick return-to-service, there is currently no proposed date. It is not likely to be soon (FAA update 26-Jun-19):

> *"The FAA is following a thorough process, not a prescribed timeline, for returning the Boeing 737 Max to passenger service. The FAA will lift the aircraft's prohibition order when we deem it is safe to do so. We continue to evaluate Boeing's software modification to the MCAS and we are still developing necessary training requirements. We also are responding to recommendations received from the Technical Advisory Board (TAB). The TAB is an independent review panel we have asked to review our work regarding 737 Max return to service.*
>
> *"On the most recent issue, the FAA's process is designed to discover and highlight potential risks.*

The FAA recently found a potential risk that Boeing must mitigate."

FAA's certification

According to Boeing's media room (9-Mar-17), the certification of the Boeing 737 MAX 8, after "*a rigorous process, the FAA granted Boeing an Amended Type Certificate for the 737 MAX 8, verifying the design complies with required aviation regulations and is safe and reliable*".

Following both crashes, on March 27, 2019, the US Secretary of Transportation; the Chairman of the House Committee on Transportation and Infrastructure and its Subcommittee on Aviation et al, initiated an audit of the FAA's oversight of the Boeing 737 MAX certification. No time line has been set for this audit and to date no official findings seemed to have been released.

It is widely speculated that the FAA delegated much of the Boeing 737 MAX 8 certification tasks to Boeing. This delegation mechanism is long standing, with some variation, and used by both FAA and EASA and other regulators. It seems that early in the certification, the FAA safety engineering team allocated some, the less critical supposedly, of the technical assessments to Boeing. However due to the development significantly lagging the rival Airbus A320 neo, FAA management requested a re-evaluation of what would be delegated to Boeing. There is also an opinion, that when there was no time to complete a document review, FAA management either signed-off the documents or delegated the review back to Boeing.

The FAA has a world-wide leader reputation for the certification of aircraft through its tough and stringent rules. This is probably now tarnished somewhat. The speculated outsourcing of much of the certification to Boeing, created a cosy relationship with respect to the certification of the Boeing 737 MAX. Changes made to MCAS arising from flight testing; changes which significantly altered the original intended MCAS operation, did not prompt the FAA to delve deeper. It may be that Boeing did not convey their impact to the FAA.

Alert Systems and Crew Experience

As mentioned above, a certification design requirement (FAR25.1309c) includes that:

> *"(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards."*

Much has been commented about the optional AoA disagree alert system. Whether a poor engineering assumption or a lack of effective criticality management for system functions – the assumption under-pinning implies a level of competence of crews to handle emergencies. The uneven standards and focus on hours v competence across the globe, notably from USA to other ICAO minimum compliant nations, has been a subject of recent hearings of House Committee on Transportation and Infrastructure and its Aviation Subcommittee.

However, expert witnesses included Chesley Sullenberger who suggested that although checklists weren't followed perfectly, other crews might well have performed exactly the same in the scenario presented.

Aviation Week (paywalled) presented a lengthy article in late May titled "MCAS Accident Factors: Training, Airmanship, Experience Deficiencies" That is a worthy non-sensationalised lengthy read from an industry publication of record.

aSCSa Insight

1. The introduction of the MCAS system was a significant contributing factor in both the Lion Air and Ethiopian Airlines crashes.
2. The Boeing 737 MAX 8 was classified as a variation of 737 NG type by opting for an amended type certificate rather than a new aircraft type certificate, despite what appears to be significant changes. It can only be presumed that this certification route was for expediency.
3. The discovery of handling problems during flight testing, presumably late in the development cycle and when the development was late, encouraged the expanded application of the MCAS solution to other phases of flight and should have warranted a reassessment of fundamental safety assumptions, system criticalities and conditions.
4. The failure classification of MCAS functions were "Hazardous" yet were seemingly subject to a single point of failure and included an implied assumption of a hard-working crew being able to arrest any unwanted aircraft behaviour before it became a "Catastrophic" condition. The sole purpose of MCAS was to help pilots to bring the nose down to avoid a Catastrophic condition. A case of the fix being as hazardous as the original problem.
5. The discovery of further handling problems when nearing stalls at low speeds during the first test flight led to further modifications to MCAS, leaving just one angle-of-attack sensor as input. From a Seattle Times article there appears to be have been no reassessment of the failure classification given the expanded role of MCAS:

   > *"One of the people familiar with MCAS's evolution said the system designers didn't see any need to add an additional sensor or redundancy because the (original) hazard assessment had determined that an MCAS failure in normal flight would only qualify in the "major" category for which the single sensor is the norm."*

   Whether this was an oversight by both Boeing and the FAA or whether this was influenced by lateness of the 737 MAX development will hopefully be revealed by the Department of Transportation audit commissioned on March 27, 2019.

6. The independence between the developer, Boeing and the certifier (regulator), FAA, appears to have been seriously compromised. Whether by the technical assessments by Boeing designated authorities or by breakdowns in the design / analyse / test / certify and configuration management processes. The FAA would have to

rely somewhat on the technical specialist expertise and process compliance at Boeing for the more complex elements of the development as it would be impracticable for the FAA to have such capacity to review detailed analyses in-house. However, it is also expected that FAA would raise probing questions to test the developer's claims and critical assumptions. This must be the principle on which delegation is based.

7. Boeing's denial of any systematic (design) fault with the 737 MAX 8 following the Lion Air crash and persisting with this view immediately following the Ethiopian Airlines crash is somewhat contradictory to Boeing's claim that "*safety is our number one priority*" (March 12, 2019). The FAA and NTSB encouraged Boeing to recommend the temporary global grounding of the Boeing 737 MAX aircraft (March 13, 2019). It was not until April 4, 2019 that Boeing admitted that in both crashes MCAS had activated.
8. The FAA and other concerned jurisdictional regulators are adopting much more rigor in the certification of the MCAS and other changes prior to removing the grounding of the Boeing 737 MAX aircraft. Boeing (May 16, 2019) announced that they have completed development of the updated software for the 737 MAX, along with associated simulator testing and the company's engineering test flight and that Boeing has flown the 737 MAX with updated MCAS software for more than 360 hours on 207 flights. The FAA and other regulators, at the publication of this newsletter, continue their evaluation.
9. What level of safety-based equipment choices can Airlines be expected to make as an informed customer? Such as to account for basic minimum experience levels and competency standards maintained at the airline's choice, for emergency procedures and upset recovery training approaches? Is the industry compromised by expansionary demands?

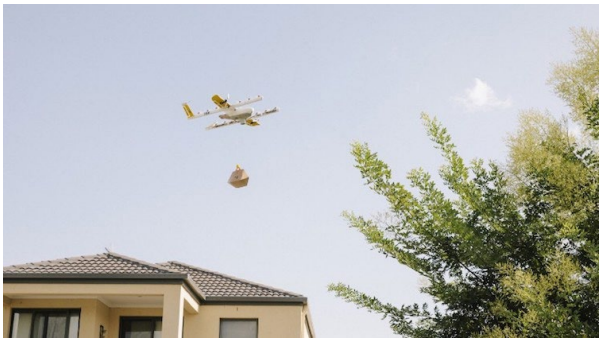
Boeing Statement on 737 MAX software

(June 26, 2019) – *The safety of our airplanes is Boeing's highest priority. During the FAA's review of the 737 MAX software update and recent simulator sessions, the Federal Aviation Administration (FAA) identified an additional requirement that it has asked the company to address through the software changes that the company has been developing for the past eight months. The FAA review and process for returning the 737 MAX to passenger service are designed to result in a thorough and comprehensive assessment. Boeing agrees with the FAA's decision and request and is working on the required software. Addressing this condition will reduce pilot workload by accounting for a potential source of uncommanded stabilizer motion. Boeing will not offer the 737 MAX for certification by the FAA until we have satisfied all requirements for certification of the MAX and its safe return to service.*

Will the Boeing 737 MAX fly again? Probably, given that 371 were in service prior to the grounding order. Also, there seems to be demand for the aircraft MAX models despite being currently grounded.

Drone Delivery systems in Operation in Canberra

CASA have approved delivery drone operations, for small supplies (food, medical supplies etc) within 10km of an operating base in northern Canberra suburbs. Wing Aviation Pty Ltd (subsidiary of Google's parent – Alphabet) have been trialling in the region over remote areas since 2014 and are now permitted to deliver in some suburban zones.



A Wing remotely piloted aircraft with a delivery - picture from Australian Aviation

CASA state that Wing were required by Part 101 regulations to submit a Safety Case, including reliability information, and were satisfied an acceptable level of safety was achieved. Part of the permit is to allow operations closer to people than the regulations normally allow.

Licenced drone pilots are required as well as flashing strobe lights for other air traffic. CASA is also keen to point out that Noise and Privacy concerns are not part of their remit for permit!

Other News: Safety Regulation of New Technology

In recent months:

National Transport Commission has released another Regulatory Impact Statement for comment on In-Service Safety. Comments close 26Aug19

CSIRO Data 61 circulated a Discussion Paper on an Artificial Intelligence Ethics Framework and Standards Australia one for Developing Standards for AI.

Australian Space Agency, has its feet under the table and are imminently to issue a new Act for Space Launch and Returns from our territories, including a refresh of 30 year old Rules that were in regulations, but will now need to evolve more dynamically with new launch technologies such a re-usable launch vehicles, Virgin Galactic style air-launched space entry and the likes of Spin Launch (centrifugal).

Amtrak Accident – NTSB Final Report

The US National Transportation Safety Board (NTSB) issued its final report into the fatal December 18, 2017 Amtrak accident near Dupont, Washington state. The NTSB cited a failure to provide an effective mitigation method for a hazardous curve and inadequate training of the train driver (crew) as causes that lead to the overspeed derailment of the Amtrak Cascades train 501 passenger train that hurtled off a railroad – highway overbridge and onto the busy highway.

This was the inaugural train service. The derailment occurred as the train entered a 30mph speed restricted curve at approximately 78mph.

The report lists 53 findings. Finding #13 cites the collective failure of the organisations involved to better identify and address safety hazards:

"*Had the Washington State Department of Transportation, Central Puget Sound Regional Transit Authority, Amtrak, and the Federal Railroad Administration been more engaged and assertive, and had clearly defined roles and responsibilities during the preparation of the inaugural service, it would have been more likely that safety hazards, such as the speed reduction for the curve would have been better identified and addressed.*"

Finding #14 specifically cites the rail regulator, the Federal Railroad administration for not using "*its authority provided under the Fixing America's Surface Transportation Act to approve speed limit action plans with conditions to require inclusion of planned and under-construction alignments owned or operated by railroads and require periodic updates to railroads' speed limit action plans, which led to no speed limit action plan being developed*".