MCAS new MVS algorithm simulation with AOA sensor upset - supporting explicative

NOTE: This was initially put together quickly as an aid on how to employ the simulation tool Excel file, along with the overall explanation of why I think this is a massive problem, for the purposes of the relative emergency to discuss this with TCCA ASAP. Gilles Primeau, December 3rd 2020. Adapted for transmission to EASA December 14th 2020.

I confirm my hypothesis was correct of what I now consider as an UNSAFE latent (unannunciated) failure condition, first suggested as a possibility under question #35 in my comments filed with the FAA under https://beta.regulations.gov/comment/FAA-2020-0686-0172 (see Ref 01 pp 5-6 therein), remaining in the new MCAS software that the FAA has re-certified on 11/18/2020.The simulation, built with adjustable parameter provisions, allowed on one hand increased confidence that an elevated AOA signal failure would be contained to avoid premature MCAS command triggering (thus putting to rest the scenario initially presented under question #35), however on the other hand, it was found that a decreased AOA signal failure would cause the more hazardous, pre-cited UNSAFE latent condition. The a priori inconsequential effect of a reduced AOA signal when considering possible premature MCAS triggering, could explain the possible oversight of this failure condition (at the time of this writing TCCA has not confirmed whether Boeing or the FAA considered this failure scenario). The implementation flaw resides specifically in the newly-introduced MVS (mid-value select) algorithm which merges the now dual AOA sensor usage, intended for feeding higher integrity AOA data to the MCAS. Under the identified failure condition, the goal of increased integrity AOA input to the MCAS is defeated, because the MVS output will disregard a subsequent increased AOA maneuver (such as for clearing an obstacle or avoiding a collision), and will even "latch" temporarily on the signal of the affected AOA signal. As a result, the MCAS might be prevented from performing its function, UNANNUNCIATED. The whole concept centers around exactly the same type of disruption that the ET302 L AOA sensor was subjected to, but with a reduced (instead of increased) signal readout, and requiring a much smaller deviation amplitude, but still able to cause an UNSAFE condition, of less than 5.5 degrees per the disclosed parameters of the split-vane monitor, thus escaping detection. The simulation is based on the FAA disclosure of how the MVS algorithm works (see "Notes" tab in Excel simulation file for references). This strongly indicates a potential hazardous, unacceptable latent failure scenario (based on my experience and expertise).

I completed building this simulation tool late on Nov. 30th 2020, and my numerous subsequent inspections of the implementation have consolidated my confidence in the correctness of the simulation. I have prepared this as soon as I could, given the urgency of notifying TCCA of this identified latent failure condition before re-certifying the 737 MAX, and revised it for disclosure to the EASA, because this situation closely relates to their position that a 3rd independent AOA source should be implemented. The potential severity of this latent failure condition may end up justifying rescinding FAA's recertification and require Boeing to fix this inadequate implementation of intended increased integrity AOA input to the MCAS - I will demand credible and reliable rebuttal before altering my opinion currently based on this work, and especially demonstration that Boeing & FAA had considered this (which may not have been the case).

User guide for this Excel-based MCAS MVS simulation tool:

1. No provisions were made to protect cells, so in using the simulation to assess various conditions, please only modify the values in green-colored cells in the leftmost tab entitled "Simulation setup"

2. Provisions were made to dial in a L to R offset "**AOAoffset**" (from aircraft installation, calibration etc), and sensor signal noise "**Noise**" (from physics of flight realities like vibrations, small scale short-lived airflow fluctuations, etc.), so that this simulation can be as realistic as possible (random number generator function of Excel was employed, see "**Pre-Upset**" tab in Excel file illustrating output based on parameter values choices).
3. The L AOA upset "**Upset**" simulates the ET302-equivalent sudden divergence typically presumed from a bird strike (again, must be of amplitude below 5.5 deg. (after above noise & offset considerations, i.e. still escaping detection).
4. Any sinewave amplitude "**ManAmp**"& frequency "**ManPer**" (where "Per" stands for *period* i.e. inverse of frequency) maneuver can be simulated post-upset (i.e. after the L AOA sensor is affected by a postulated "bird strike" or equivalent event), to simulate parts of maneuvers, as long as fitting within 15-6 = 9 seconds. **NOTE**: The negative ManAmp requirement to simulate an increased AOA maneuver is simply an effect of the COSINE function usage in the simulation, initially chosen for tangential continuity with the preceding post-upset AOA “plateau”; in hindsight, use of the SINE function could have been simpler, but the simulation implementation remains valid. This was also the initial step for a possible future re-use of the approach at harmonic frequencies for implementing a Fourier series expansion, in order to generate any desired maneuver waveform, but upon identification of the latent failure condition this was no longer deemed necessary and was superseded with the urgency of advising TCCA of the finding.
5. Three second plateaus of pre- & post-upset are simply intended to illustrate the initial conditions, and of course in real life the duration of each plateau could be vastly longer, along with slightly-varying AOA signals instead of plateaus.
6. **The blue trace is the affected L AOA sensor, while the red trace is the unaffected R AOA sensor. The green trace is the MVS algorithm output, which is the new signal now feeding the MCAS (*). *The surface delimited under the red trace and above the green trace thus defines the domain of reduced MCAS AOA input integrity.***

(*) Again that's how Boeing chose to merge the new usage of two AOA vanes in their revised MCAS software. The identified failure condition demonstrates its inadequacy, and my current opinion is that **only a true 3-sensor approach, even if the 3rd source is synthesized (as long as independent of the 2 existing AOAs), per EASA demand, would resolve this UNSFAE condition, and should thus be imposed *prior* to re-certifying the MCAS.**

Background considerations and author’s general opinion on the current 737 MAX situation

Many talk about potential instability arising from the engines repositioning. I can't confirm or deny this, because I don't have access to relevant data (everybody's problem outside the circle of the Boeing & FAA entities, likely persistent in part with other certification authorities). However, the following tends to confirm the possibility:

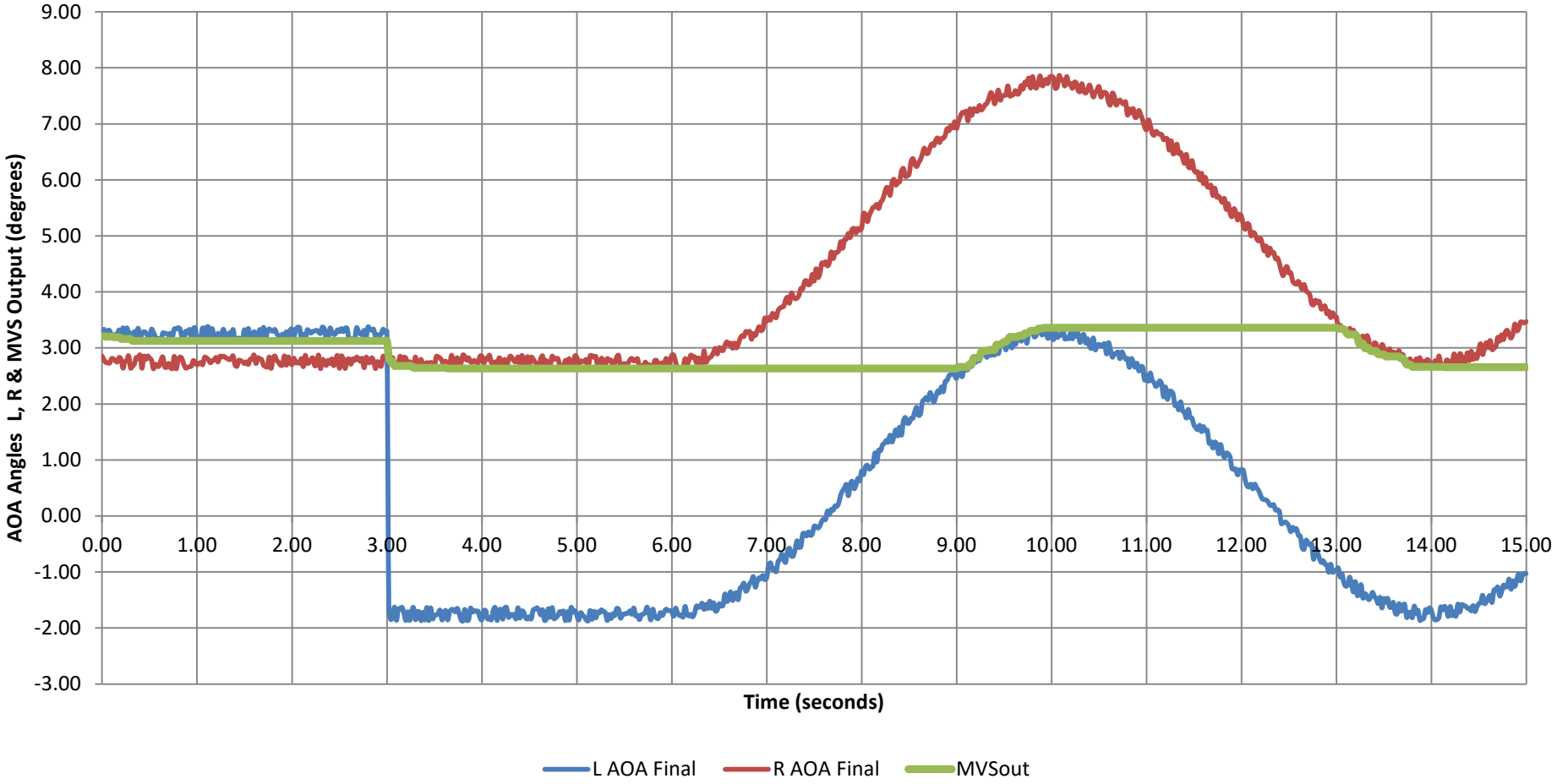
Likely, the forward displacement of the engines has a much greater effect on the potential problem than their increased height for ground clearance. The reason for this is that if one accepts the notion that the large engine nacelles can start acting as an airfoil especially at increased AOAs, the nacelles’ resulting CP (center of pressure) for their lift contribution could indeed interact with the aircraft’s CG (center of gravity) in a manner contributing a significant nose up pitching moment. If this is correct, there might indeed be a longitudinal stability problem (at least static, and possibly also dynamic, but again only access to data can positively answer that question), confirming the need for an MCAS implementation. For over a year I have presumed the root of the problem could be illustrated through a class of flight testing a maneuvers, part of certification requirements generally referring to *windup turns* in the flight

dynamics domain. *This, at the base, in my engineer as well as pilot opinion, relates to an aircraft's required ability to clear, among other things, the proverbial 50-foot obstacle, and the ability to maneuver fast to avoid a collision, notably*.

Please review the image on the next page, illustrating one of many possible embodiments of the identified failure condition; postulate a need for a sudden maneuver, nose up, to avoid an obstacle. Look at the red trace showing the good AOA (unaffected R sensor) that comes with this maneuver. I don't know the real AOA numbers that apply to the 737 MAX, but that's besides the point; this shows what WILL happen, following an *undetected* upset, to here the L AOA (in real life this is fully symmetrical L-R), that biases DOWNWARD its readout by less than 5.5 degrees (which is the threshold Boeing has encoded in their logic for the split-vane monitor). As you can probably see from this graph, the correct red trace moves the aircraft toward stall detection territory (with accompanying stick shaker and increased control column pull-back forces if it reaches the trigger threshold), while the green trace shows that with this MVS logic, the MCAS input will be biased downward by 5 degrees in this example, causing the MCAS *NOT* to trigger when it SHOULD, due to the upset L AOA in the blue trace, thus **breaking down proper functioning of the nominal MVS algorithm intended to provide a higher integrity AOA input to the MCAS. *Under this latent failure scenario therefore, instead of forcing the aircraft nose down through an erroneous MCAS activation as occurred on JT610 & ET302, the MCAS might not intervene when required to, risking a stall*.**

We call such cases UNANNUNCIATED or latent failures (because of the lack of detection, since the algorithm allows up to 5.5. degrees before declaring the split-vane magnitude too high); some also call them latent failures, or dormant failures. They are massively dangerous, because lack of detection will cause NO cockpit warning telling the crew the MCAS is compromised, thus misleading the crew into thinking the MCAS is still there so prevent the stall, which will NOT happen. Note this carefully: Authorities, TCCA in particular, have pushed for more training; the training covers cases with MCAS, and without MCAS, however with reliance on proper crew messaging to know whether MCAS is active or not; here, the crew would mistakenly think the MCAS still functions normally while it in reality does not, and could get caught off-guard because MCAS did not activate, if an obstacle avoidance maneuver is required, for instance. In the example figure, all the area below the red trace and above the green trace, defines the zone under which the MCAS is unable to perform its required function due to the upset that affected the L AOA. This upset is of exactly the same type as what occurred on ET302, but with a different sign and a much lower amplitude. Don't be misled by the lower value compared to the 20 deg AOA delta on JT610 or 60 deg AOA delta on ET302; this improper MVS intended to merge the two AOA signals to feed the MCAS primary input, is HUGE for any aerodynamicist comparing this value with the AOA for maximum lift coefficient (I usually employ 12 degrees for CLmax as a first order estimate before putting my hand on actual aircraft-specific data); in this example, one can see the MCAS protection is biased down by around 4.5 degrees (distance between red and green traces at the peak of the maneuver); this is *massive,* in my view.

Upset Sensor with Maneuver MVS Algorithm Behavior



Simulation Parameter	Name	Value	Expected Parameter Value Range
AOAs (L& R) Initial Baseline Value (deg)	AOAinit	3.00	Should use typical post-rotation ascent AOA (737-specific data unavailable; using presumed typical values); this parameter is mainly useful to gauge how close to actual CLmax current algorithm can get the aircraft after an upset
AOAs (L vs R) Initial Offset Value (deg)	AOAoffset	0.50	Using presumed typical value, subject to revision with 737-specific data if/when available; this is where sensor mounting on aircraft imprecision is injected, to assess it's effect on MVS algorithm robustness
AOA Signal Noise Amplitude (deg)	Noise	0.25	Peak-to-peak maximum variation due to noise sources, in computation will be multiplied by a randon number (value 0 to 1) to affect with different random number for each raw AOA signal, and shifted down by noise/2 to recenter
L AOA Upset Magnitude (deg) (< 5.5)	Upset	-5.00	Must be <5.5 deg (in magnitude) per disclosed algorithm details; above this, AOA values are rejected under new logic **[NEGATIVE VALUES ALLOWED]**
Post-Upset Maneuver Amplitude (deg)	ManAmp	-5.00	To assess effects of maneuver magnitude, compared to L AOA upset amplitude, for MVS output to intersect with affected L AOA and latching on this bad signal OR plateaus while good AOA varies **[NEGATIVE VALUES ALLOWED]**
Post-Upset Maneuver Period (s)	ManPer	8.00	Maneuver simply consisting in a sinewave (to illustrate capture/switch of MVS algorithm output following any significant pust-upset maneuver
MVS Output Initialization Value (deg)	MVSinit	L	Value will be "L" or "R" to select the 1st computed value for L AOA or R AOA, as initial MVS ouptut (to check if it impacts algorithm behavior, for instance if affected AOA being or not also the side chosen for MVS initialization has an
Iteration Time Step Duration (s) (FIXED)	Ts	0.02	Should be matched to actual 737 MAX MCAS MVS algorithm iteration period (i.e. presumed as inverse of AOA sensors sampling frequency; value unknown)
Pre-Upset Idle Time (s) (FIXED)	StartDLY	3.00	Intent is simply to provide plateau for graphic outputs, to distinguish beginning of AOA upset
L AOA Upset Onset Rate (deg/s) (FIXED)	UpsetRT	50.00	Using rate similar to seen on ET302 L AOA i.e. 60 deg divergence in 1 s but this may simply be 1Hz FDR sampling; used value for simplicity so upset would appear fully in one iteration i.e. matched to presumed AOAs sampling rate

Whereas up to now my discourse on the 737 MAX file centered principally on the need to modernize the HSTS (horizontal stabilizer trim system) because it only meets minimum requirements and is thus LESS SAFE than contemporary pitch trim systems, *this situation here, by virtue of the inability of MCAS to function when required, furthermore in a unannunciated condition, i.e. of the worst kind, is completely unacceptable, and I can guarantee based on my prior experience that TCCA would NOT have accepted a situation like this; the FAA needs to rescind its authorization and insist to get Boeing to correct it.* All my prior arguments have been about modernizing a critical system (the HSTS) to make the aircraft SAFER, while this case here, definitely makes the aircraft UNSAFE, in my experience-based and in my expertise-based view. Furthermore and finally, even if this UNSAFE failure condition is resolved (1st layer of concern), and even if the HSTS is made SAFER through it's modernization to contemporary standards (2nd layer of concern), for which I will use the analogy, for the general public and until such modernization is implemented, of a new car with a known propensity of power steering function failure in a tight turn (re: insufficient redundancies & monitoring and especially reliance on crew muscles as a backup on the 737 MAX), I will STILL be reluctant to fly on a 737 MAX, until being shown sufficient data to also put to rest what I now refer to as my 3rd layer of concern, as follows: The use of the pitch trim function, i.e. the only control surface electrically-commandable on the 737 MAX, inherently in a ON-OFF constant rate of motion, is much LESS SAFE than the gradual, smooth fashion employed in contemporary fly-by-wire (FBW) flight controls making primary use of the elevators for stall protection; in reference to this 3rd concern, I will refer for the public to the powerful analogy of trying to use a five-pound sledgehammer as a precision alignment tool.

****

Final statement:

UNANNUNCIATED failures are of the worst kind, and I worked feverishly with TCCA to avoid many cases in my prior work, particularly in the 2001-2008 timeframe. I will therefore permit myself to be critical toward any attempt to rationalize as acceptable this latent failure condition, given the massive damage that prior oversight led to, i.e. 346 deaths. For the additional guidance of anyone reviewing this document and the associated simulation tool, I make a parallel between this work and the TARAM internally-generated FAA analysis dated December 3rd 2018, i.e. between the JT610 & ET302 crashes, which still did not cause the 737 MAX fleet to be grounded prior to March 10th 2019 (date of the ET302 crash). This stand, I take for the following inescapable reason: bird strikes happen relatively frequently, and nobody can predict the magnitude and direction of each case's individual effect on AOA readout; if in doubt, please ask US Airways Flight 1549's pilot, Captain Chesley "Sully" Sullenberger.

Supplemental explanation regarding the "Simulation results" tab in the Excel simulation file, for anyone assessing the implementation:

In the "Simulation results" tab, the two points at which the simulation switches mode are highlighted in yellow, detailed as follows:
1) At row 153 (iteration # 151), i.e. the first time step after a 3 second period during which both AOAs were constant (except for noise if you inject some), the upset to the L AOA is injected.
2) At row 303 (iteration # 301), i.e. the first time step after another 3 second period during which a constant separation between the L & R AOAs can be seen, the adjustable sinusoidal maneuver is initiated.